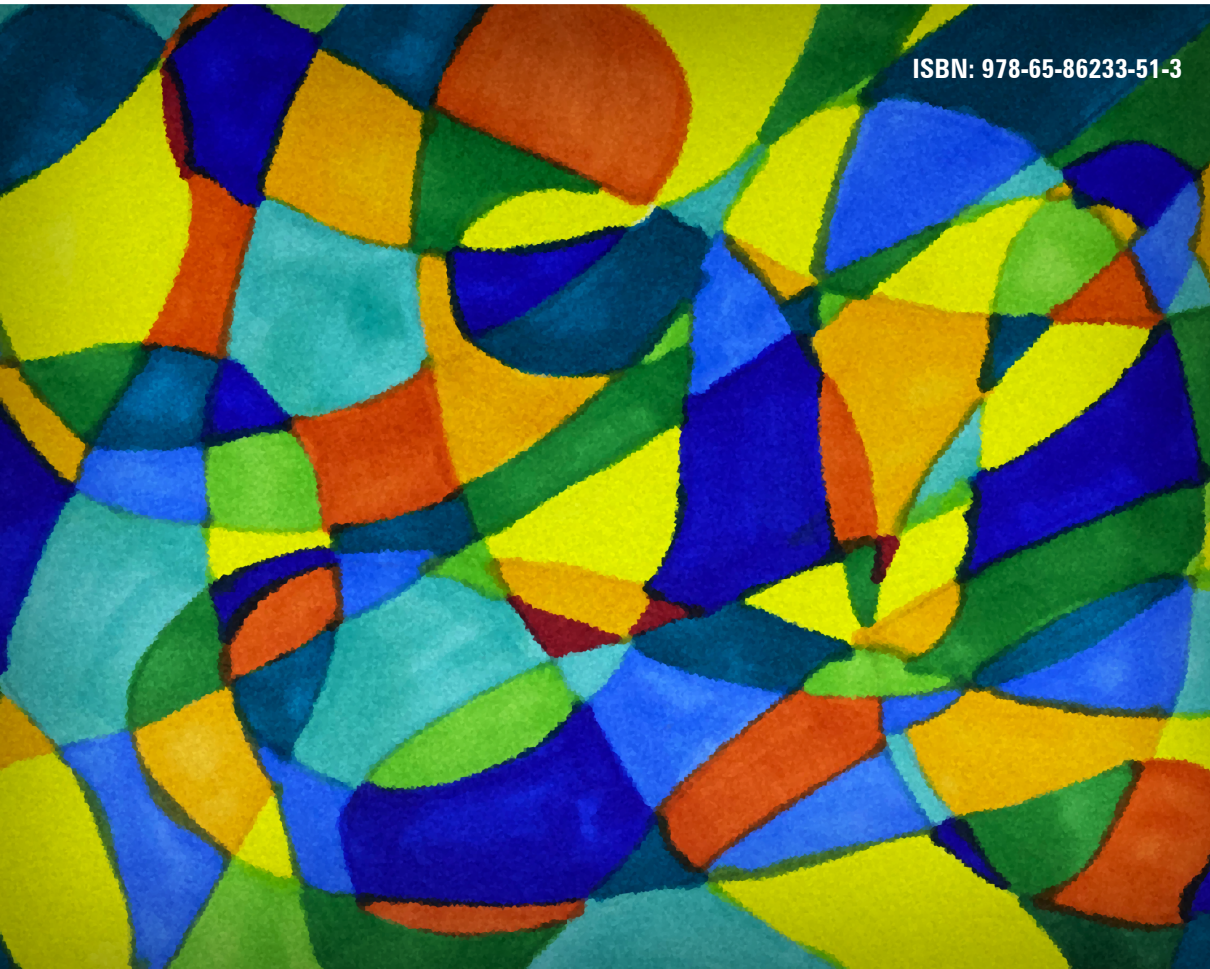
# PROTEÇÃO DE DADOS PESSOAIS EM PERSPECTIVA

## *LGPD E RGPD NA ÓTICA DO DIREITO COMPARADO*

**MARCOS WACHOWICZ**
ORGANIZADOR



ISBN: 978-65-86233-51-3

As publicações do **GEDAI/UFPR** são espaços de criação e compartilhamento coletivo. Fácil acesso às obras. Possibilidade de publicação de pesquisas acadêmicas. Formação de uma rede de cooperação acadêmica na área de Propriedade Intelectual.


GEDAI
PUBLICAÇÕES

UFPR – SCJ – GEDAI
Praça Santos Andrade, n. 50
CEP: 80020-300 - Curitiba – PR
E-mail: gedai.ufpr@gmail.com
Site: www.gedai.com.br
Prefixo Editorial: 67141
**GEDAI/UFPR**





**Capa**: Marcelle Cortiano
**Projeto gráfico e finalização**: Sônia Maria Borba
**Diagramação:** Bruno Santiago Di Mônaco Rabelo
**Revisão**: Luciana Reusing, Pedro de Perdigão Lana, Bibiana Biscaia Virtuoso, Alice de Perdigão Lana, Heloísa G. Medeiros e Magna Knopik

Dados Internacionais de Catalogação na Publicação (CIP)
Bibliotecária: Maria Isabel Schiavon Kinasz, CRB9 / 626

P967 Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado / organização de Marcos Wachowicz – Curitiba: Gedai, UFPR 2020.
618p.: 23cm

ISBN: 978-65-86233-51-3 [Recurso eletrônico]
ISBN: 978-65-86233-52-0 [Impresso]

1. Proteção de dados. 2. Sistemas de recuperação da informação – Segurança. I. Wachowicz, Marcos (org.)

CDD 342.0858 (22.ed)
CDU 342.721

**Marcos Wachowicz**
Organizador

# PROTEÇÃO DE DADOS
## PESSOAIS EM PERSPECTIVA:
## *LGPD e RGPD NA ÓTICA DO DIREITO COMPARADO*

Curitiba

GEDAI
Grupo de Estudos de Direito Autoral e Industrial
Universidade Federal do Paraná

2020

# PREFÁCIO

*Dário Moura Vicente*[1]

*Diversos instrumentos normativos, de fonte nacional e supranacional, procuraram nos últimos anos regular o tratamento de dados pessoais.*

*Entre eles sobressai, na Europa, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD), aplicável desde 25 de maio de 2018, o qual foi complementado em Portugal pela Lei n.º 58/2019, de 8 de agosto, que assegura a sua execução na ordem jurídica portuguesa.*

*No Brasil, avulta a este respeito a Lei Geral de Proteção de Dados (LGPD), n.º 13.709, de 14 de agosto de 2018, alterada pela Lei n.º 13.853, de 8 de julho de 2019, a qual deverá entrar em vigor na sua plenitude, em razão do disposto na Lei n.º 14.010, de 10 de junho de 2020, a 1 de agosto de 2021, data a partir da qual passarão a aplicar-se as respetivas normas sancionatórias.*

*É manifesta a convergência de orientações entre as legislações adotadas a este respeito nos dois lados do Atlântico. Sobressai, em particular, preocupação em instituir através delas, nos Estados-Membros da União Europeia e no Brasil, uma regulamentação de índole fortemente abrangente, pormenorizada e protetora, a qual contrasta com aqueloutra, muito mais fragmentária e liberal, que prevalece nos Estados norte-americanos.*

[1] Professor Catedrático da Faculdade de Direito da Universidade de Lisboa

*Comum à União Europeia e ao Brasil é igualmente a tendência para a constitucionalização das regras sobre o direito à proteção de dados, ou à autodeterminação informacional, reconhecido na Carta dos Direitos Fundamentais da União Europeia, cujo art. 8.º, n.º 1 dispõe: "Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito".*

*Direito esse que se encontra igualmente consagrado no art. 35.º, n.º 2, da Constituição da República Portuguesa, segundo o qual: "A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente".*

*Implicitamente, encontramos também esse direito consignado no art. 5.º, inciso LXXII, da Constituição Federal brasileira, em que se pode ler: "conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo". E a Proposta de Emenda Constitucional n.º 17, de 2019, prevê o aditamento de um novo inciso XII-A ao referido preceito da Constituição brasileira, por força do qual "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais".*

*Outro tanto não sucede, porém, nos Estados Unidos da América, onde a proteção de dados pessoais é, quando muito, tida como uma emanação do direito à privacidade, ou, mais precisamente, do "direito a ser deixado só" (*"the right to be let alone"*).*

*Coincide igualmente nesta matéria, no Brasil e na União Europeia, a noção muito ampla de dados pessoais sujeitos a proteção, entendidos como "toda a informação relativa a uma*

*pessoa singular identificada ou identificável", a qual contrasta com a noção norte-americana, muito mais restritiva, que confere particular ênfase à proteção da privacidade dos indivíduos perante as agências públicas.*

*Reflete-se aqui a circunstância de que, enquanto que no Brasil e em Portugal, assim como noutros países europeus, a privacidade é essencialmente uma exigência da dignidade da pessoa humana – por seu turno uma emanação da conceção personalista do Direito que encontrou consagração constitucional em ambos os países –, a salvaguardar em particular perante entidades privadas, os norte-americanos veem antes nela uma expressão da liberdade individual, primariamente ameaçada pelo Estado.*

*Compreende-se, a esta luz, que tanto na Europa como no Brasil o tratamento de dados deva, em princípio, fundar-se no consentimento do seu titular. Esta exigência figura expressamente na Carta dos Direitos Fundamentais da União Europeia, cujo art. 8.º, n.º 2, dispõe a este respeito: "Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação".*

*No RGPD, esta regra acha-se refletida no art. 6.º, n.º 1, alínea a), segundo o qual: "O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas […]".*

*No Brasil, é esse também o sentido do art. 7, inciso I, da LGPD, nos termos do qual: "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular […]".*

*Ora, o princípio do consentimento – elemento fulcral, como é bom de ver, dos Direitos europeu e brasileiro em matéria de proteção de dados pessoais – não tem consagração equivalente no Direito norte-americano: mesmo na Califórnia, o recente Consumer Privacy Act limita-se a acolher nesta matéria um direito de opting-out, nos termos do qual o consumidor pode recusar a possibilidade de venda a terceiros da sua informação pessoal.*

*Corolário do referido princípio é o denominado direito ao esquecimento, por força do qual o titular de dados pessoais tem, na União Europeia, desde o acórdão* Costeja *do Tribunal de Justiça da União Europeia, de 2014, o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, designadamente quando os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento, o titular retira o consentimento em que se baseia o tratamento dos dados se não existir outro fundamento jurídico para o referido tratamento, o titular se opõe ao tratamento e não existem interesses legítimos prevalecentes que justifiquem o tratamento ou os dados pessoais foram tratados ilicitamente.*

*Também no Brasil o titular dos dados tem, de acordo com o art. 18, inciso VI, da LGPD, o direito à eliminação destes, ainda que tratados com o seu consentimento.*

*O direito ao esquecimento* não tem*, contudo, qualquer correspondência no Direito norte-americano, onde, pelo contrário, algumas formas de tratamento de dados alheios – incluindo as que são levadas a cabo por operadores de motores de busca na Internet – são tidas como manifestações da liberdade de expressão, protegida pela I Emenda à Constituição, consoante foi reiteradamente afirmado por tribunais federais estadunidenses.*

*O que se disse até aqui basta, por si só, a fim de demonstrar que a proteção de dados pessoais é hoje um domínio em que,*

*a par da circulação de modelos jurídicos através das fronteiras – de que o RGPD e a LGPD constituem um exemplo paradigmático –, deparamos também com conceções muito diversas nos sistemas jurídicos nacionais; e em que a comparação jurídica, permitindo descortinar as semelhanças e as diferenças entre esses sistemas jurídicos e explicá-las por apelo aos seus fundamentos e origens, constitui um instrumento essencial para a sua compreensão.*

*A obra que agora se publica, em boa hora promovida por Marcos Wachowicz, faz jus à relevância do Direito Comparado neste domínio e faculta aos leitores brasileiros e portugueses um precioso elemento de estudo e análise dos instrumentos jurídicos vigentes nos respetivos países em matéria de proteção de dados pessoais. É por isso com o maior gosto que me associo à publicação desta obra e felicito o seu Coordenador, bem como todos os autores que nela quiseram colaborar.*

*Lisboa, outubro de 2020.*

***Dário Moura Vicente***

# PREFÁCIO

*Danilo Doneda*[1]

*O convite que, honrado, recebi do Professor Marcos Wachowicz para prefaciar a obra "Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado" ocorreu após ter a oportunidade de participar, ainda que pontualmente, das atividades desenvolvidas no âmbito do Programa de Pós-Graduação em Direito da Universidade Federal do Paraná (aliás, casa na qual me graduei em Direito). A disposição e interesse dos participantes dos Seminários organizados pelo Professor Wachowicz em um debate concreto sobre proteção de dados era evidente e, certamente, é reflexo direto da trajetória acadêmica de Wachowicz, um dos maiores incentivadores dos debates e reflexões entre as interseções de diversos fenômenos relacionados ao desenvolvimento tecnológico e o direito no cenário jurídico nacional e com obra de referência a respeito.*

*Os frutos desta trajetória, de relevantes, ultrapassam os limites pessoais e se revelam na solidez, por exemplo, do GEDAI/UFPR, o Grupo de Estudos de Direito Autoral e Industrial que, em sua atuação, é um dos foros mais autorizados para os debates em torno da sua temática.*

*Este contexto é determinante para a viabilidade e relevância desta obra. A experiência do jurista com temas ligados à tecnologia, de fato, proporciona que ele desenvolva uma sensibilidade aguçada em relação a novas tendências, bem como que trate com familiaridade a própria temporalidade de boa parte*

[1] Advogado. Doutor em direito civil (UERJ). Professor no IDP. Indicado pela Câmara dos Deputados ao Conselho Nacional de Proteção de Dados

*dos debates e soluções que foram engendrados a partir da consideração de cenários tecnológicos que, rapidamente, se tornam obsoletos. Neste sentido, a escolha do tema da proteção de dados pessoais para os trabalhos que confluíram neste volume configura-se não somente em um reflexo do intenso debate que hoje tem lugar no país, motivado pela recente entrada em vigor da LGPD, a Lei Geral de Proteção de Dados, mas também - principalmente - se legitima pela possibilidade de que diversas aspectos desta consolidada tradição de reflexões em torno de temas que conjugam direito e tecnologia se encontrem com um novo marco regulatório que, ainda que sobre o tema específico da proteção de dados, apresenta elementos conjunturais comuns com outras áreas - como o direito autoral - nas quais o fenômeno tecnológico é o eixo que marca o seu desenvolvimento mais recente.*

*O tema da proteção de dados é um dos exemplos mais concretos de uma disciplina jurídica cujos contornos, conceitos e principais institutos foram moldados majoritariamente em torno de um determinado contexto determinado pelo potencial e pelos efeitos da tecnologia. A bem da verdade, mesmo institutos que, hoje, podem ser considerados quase como "ancestrais" da proteção de dados, como o direito à privacidade, tiveram sua gênese fortemente condicionada ao panorama tecnológico. Antes, mesmo o próprio direito à privacidade, que de certa forma pode se considerar uma espécie de antecedente direto do direito à proteção de dados, teve sua relevância jurídica determinada justamente por um novo contexto derivado da introdução de novas tecnologias no mercado de consumo, desde a máquina fotográfica à própria imprensa, do que nos deixaram notas muito contundentes, entre outros, Samuel Warren e Lous Brandeis em seu artigo* The right to privacy, *até hoje referência para o moderno tratamento da matéria:*

> Recent inventions and business methods call attention to the next step which must be taken for the protection

> of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[2]

*A privacidade e a própria proteção de dados são elementos já postos em nosso ordenamento. A presente obra, portanto abre o espaço para a consideração da interpretação e implementação da LGPD - trabalho ainda por realizar - considerando diversos cenários tecnológicos que se podem considerar de vanguarda e nos quais, certamente, aspectos doutrinários e práticos desta implementação irão ser fundamentais para definirmos o futuro da proteção de dados. Ao tratar de temas de fronteira como a regulamentação das decisões automatizadas e o uso e efeitos dos algoritmos, o espaço para o debate sobre a ética como parâmetro para este debate, os impactos dos mecanismos de vigilâncias, os intrincados efeitos do uso intensivo de dados no setor de saúde ou mesmo as novas dimensões que o princípio da publicidade processual assume com o advento de ferramentas capazes de capturar e submeter o conteúdo dos atos processuais a intrincados mecanismos de inteligência artificial, a obra reune tanto a preocupação em expandir as barreiras da disciplina quanto de fornecer uma análise densa e pertinente a algumas das questões mais estratégicas do nosso tempo.*

*Há outro elemento da presente obra que denota sua pertinência e relevância, e que é a sua característica mais ampla: trata-se da sua perspectiva, que procura observar a experiência brasileira com a recente normativa de proteção de dados, em viés comparativo com a europeia, justamente a experiência regula-*

[2] WARREN, Samuel. BRANDEIS, Louis. "The right to privacy", in **Harvard Law Review**, v. 4, n. 5. (1890), pp. 193-220.

*tória que inaugurou a matéria há cerca de cinco décadas, desde a lei de proteção de dados do* Land *alemão de Hesse, em 1970.*

*-Aqui, o estudo comparativo demonstra-se particularmente adequado por diversos motivos. A tradição europeia de proteção de dados pessoais hoje afigura-se como algo mais do que uma realidade regional, afigurando-se como um verdadeiro parâmetro global em relação ao qual outras normas e iniciativas vão forçosamente ser comparadas. Não se trata, assim, meramente de um recurso retórico, talvez induzido pelo fato da própria LGPD, em termos estruturais, manter forte identidade com a normativa europeia - basta ver que uma série de outra normativas, insuspeitas tanto de terem sofrido uma influência cultural incisiva e até mesmo atinentes sistemas jurídicos que não se confundem absolutamente com o europeu continental, apresentam evidências concretas de influência direta e diálogo com estas normativas, como por exemplo o CCPA (*California Consumer Privacy Act*), a legislação sobre proteção de dados de consumidores que recentemente entrou em vigor na Califórnia e que inclusive foi abordada neste volume, como até mesmo as recentes iniciativas na China com a sua legislação de cibersegurança ou com a divulgação de uma versão preliminar de sua primeira legislação geral sobre proteção de dados.*

*Ainda, a proteção de dados é uma disciplina cuja análise não pode prescindir de uma abordagem global justamente pelo fato do volume e da importância dos fluxos internacionais de dados pessoais, que induzem a conformação de parâmetros internacionais comuns, assim como também acabam influenciando as diversas normativas nacionais, no sentido de restringir a especificação de regras do direito interno que possam obstaculizar o fluxo internacional de dados - o que fundamenta justamente a tendência à convergência entre legislações mesmo de países de culturas jurídicas diversas.*

*Esta abordagem está presente de forma transversal neste volume, ressaltando a importância de que diversas temáticas*

*específicas dentro da proteção de dados tenham sido abordadas à luz desta análise comparativa. Ela engloba desde pontos nevrálgicos e fundamentais da evolução jurisprudencial e doutrinária da disciplina no Brasil bem como na Europa, como a elaboração do direito à autodeterminação informativa, passando por institutos estruturantes da disciplina da proteção de dados cujo desenvolvimento na Europa já é uma* ***praxis*** *já estabelecida que vai desde o rol dos princípios de proteção de dados, passando pelas especificidades das bases legais para o tratamento de dados como o consentimento e o legítimo interesse, ate as ainda incertas particularidades da aplicação da responsabilidade civil à esta disciplina. O quadro conceitual da disciplina da proteção de dados, introduzido pela LGPD, é também abordado sob a mesma luz, desde as disposições sobre dados pessoais, dados sensíveis e os agentes de tratamento de dados e o próprio princípio da segurança. Um elemento que, no Brasil, está inclusive mais fortemente atrelado ao desenvolvimento da proteção de dados do que na Europa merece tratamento destacado, que são os elementos de natureza consumerista presentes na legislação pátria e europeia. Finalmente, aspectos diretamente relacionais da matéria, como o compartilhamento de dados no setor público e da própria transferência internacional de dados pessoais estão destacados.*

*A obra insere-se com brilho e destaque indiscutíveis em meio à produção literária que procura tecer as primeiras reflexões sobre o marco regulatório que recém entrou em vigor, sobre proteção de dados pessoais. Desejo (aliás, estou certo!) boa leitura a todos, certo de que dentre os co-autores estarão alguns dos autores de maior relevo sobre a matéria no Brasil nos próximos anos.*

*Curitiba, outubro de 2020.*

***Danilo Doneda***

# APRESENTAÇÃO

O livro **"PROTEÇÃO DE DADOS PESSOAIS EM PERSPECTIVA: LGPD e RGPD na ótica do direito comparado"** é fruto de trabalho de pesquisa desenvolvido pelo Grupo de Estudos de Direito Autoral e Industrial – GEDAI, dentro das atividades acadêmicas realizadas no Programa de Pós-Graduação em Direito da Universidade Federal do Paraná – PPGD/UFPR.

Em maio de 2018 entrou em vigor o Regulamento Geral de Proteção de Dados – RGPD 2016/679. O RGPD é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Econômico Europeu. Regulamenta também a exportação de dados pessoais para fora da UE e EEE. Em agosto de 2018 no Brasil, foi editada a Lei 13.709, denominada a Lei Geral de Proteção de Dados – LGPD, o texto é inspirado na legislação europeia (RGPD) e estabelece também que empresas que tenham como atividade centrada no tratamento sistemático de dados pessoais sejam obrigadas a ter um Encarregado pelo Tratamento de Dados Pessoais – *Data Protection Officer* (DPO).

As atividades e os estudos do GEDAI com base nestes marcos regulatórios, no âmbito das suas linhas de pesquisa sobre Sociedade da Informação: Democracia e Inclusão Tecnológica se iniciaram em 2018 e finalizaram recentemente, em outubro de 2020.

Foram meses de intensa atividade de pesquisa, debates e reflexões envolvendo temas atualizados acerca da Proteção de Dados Pessoais.

Num primeiro momento, na análise da aplicação do RGPD europeu e suas implicações no território para diversas áreas de interesse para a sociedade brasileira.

Num segundo momento, aprofundou-se o estudo dos primados da Proteção de Dados estabelecidos pela LGPD brasileira, partindo de uma concepção ampla da Sociedade Informacional para compreensão do ambiente digital de difusão de dados na qual se materializará a norma legal.

Desta forma, a metodologia de estudos que está subjacente aos artigos pautou por uma compreensão das novas Tecnologias da Informação e Comunicação – TICs, buscando numa análise de Direito Comparado entre o RGPD e a LGPD, construir um marco teórico sobre os primados estruturantes da proteção de dados pessoais no continente europeu e no território brasileiro.

A estrutura do livro dividido em duas partes, foi decorrência da escolha metodológica da pesquisa realizada, longe de ser antagônicas são complementares.

A primeira parte é dedicada a perspectiva europeia sobre a proteção de dados, contando com a contribuição de juristas europeus para analisar a proteção de dados pessoais, numa visão Crítica do RGPD e da LGPD.

O pensamento jurídico europeu presente na obra, representa duas escolas com grande tradição no direito brasileiro, o Direito Alemão e o Direito Português.

O pensamento alemão está exteriorizado na verve dos professores **Thomas Hoeren** e **Stefan Pineli** que analisam a nova Lei de Proteção brasileira.

O posicionamento da doutrina portuguesa está nos estudos dos professores **Alexandre Libório Dias Pereira, Manuel David Masseno e Sofia Vasconcelos Casimiro** que apresentam trabalhos sobre as novas tecnologias e os desafios para a proteção de dados pessoais.

A segunda parte do livro, aglutina os estudos de direito comparado, sobre o RGPD e a LGP, estruturado em cinco seções.

A primeira seção dedicada aos princípios jurídicos de tratamento de dados pessoais, conta com a contribuição dos pesquisadores **Matheus Falck, Rodrigo Otávio Cruz** e **Silva e Laísa Fernanda Alves Vieira.**

A segunda seção analisa os dados pessoais e seu tratamento sob a perspectiva técnica e multissetorial, cláusula abertas, autoridades nacionais, proteção de dados sensíveis fruto dos estudos dos pesquisadores **Marcelo Bürger, Bruna Berco, Rangel Trindade** e **Leonardo Cordouro.**

A terceira seção aglutina estudos da autodeterminação à discriminação e o exercício democrático, analisando a ética nas decisões automatizadas relativamente a proteção subjetiva de dados pessoais, inclusive quanto a responsabilidade civil no tratamento de dados pessoais pelas aplicações de Inteligência Artificial – IA, conta com a pesquisa de **Alice de Perdigão Lana, Marcelle Cortiano, Gisele Mendes, Antônio C. Gonçalves Filho, Leticia Canut, Heloisa Medeiros, Bruna W. Paim, Lukas Ruthes Gonçalves, Ana Cristina A. Viana** e **Carolina F. de Miranda.**

A quarta seção se dedica ao estudo do tratamento de dados pessoais pelo poder público, no tocante a dicotomia da transparência e da privacidade, empreendendo um consistente comparativo entre o direito europeu e o brasileiro, reflete o trabalho desenvolvido por **Luis Marretti, Thiago Monroe, Aline Macohin** e **João Victor Carneiro.**

A quinta seção aborda a transferência internacional de dados, no que tange a extraterritorialidade e elementos de conexão de Direito Internacional Privado, resultado das pesquisas de **Bruna Osman, Jessica Soares, Luciana Reusing** e **Marcos Wachowicz.**

O leitor perceberá que tem diante de seus olhos uma obra coesa, com interconexões internas entre seus capítulos, que dialogam entre si, erigindo um pensamento jurídico uniforme e sistêmico, cujas partes se complementam e harmonizam.

Os estudos e pesquisas que agora se condensa em forma desta obra coletiva, foi objeto de extensos debates em seminários e palestras, realizadas pelos autores cujas ideias foram forjadas e refundidas sobre a Proteção de Dados Pessoais na ótica do direito comparado.

A presente obra é publicada e disponibilizada pela internet, pretende difundir a compreensão dos conceitos fundamentais da LGPD e do RGPD no contexto da Sociedade Informacional, almejando sua aplicação pelos

operadores do direito, bem como, base teórica na formulação de estratégias para a proteção de dados pessoais.

A todos os pesquisadores nacionais e estrangeiros que participaram deste projeto, queremos registrar nosso agradecimento, pela seriedade com que se dedicaram aos estudos, pelo comprometimento com o projeto e principalmente pela excelente pesquisa realizada.

O pensamento jurídico que emerge da presente obra ganhará livre fluxo semeando ideias, provocando novas reflexões e inquietações, que certamente os leitores poderão potencializar com vistas a uma sociedade democrática e inclusiva, cuja tecnologia respeite e proteja os dados pessoais em todos os setores da Sociedade Informacional.

Desejamos a todos uma boa leitura!

**Marcos Wachowicz**

# SUMÁRIO

### Seção II

**As novas fronteiras tecnológicas e os desafios para a proteção dos dados pessoais**

#### Capítulo 1



#### Capítulo II



## PARTE II

*UMA PERSPECTIVA DE DIREITO COMPARADO SOBRE A PROTEÇÃO DE DADOS*

### Seção I

**Princípios jurídicos de tratamento de dados pessoais**

#### Capítulo I



#### Capítulo II

## Seção II

### Dados pessoais e seu tratamento sob perspectiva técnica e multissetorial

## Seção III

### Da autodeterminação à discriminação: a proteção subjetiva de dados pessoais

### Capítulo I



### Capítulo II



### Capítulo III



### Capítulo IV



### Capítulo V

## Seção IV

### Tratamento de dados pessoais pelo poder público: transparência versus privacidade

### Capítulo I



### Capítulo II



## Seção V

### Transferência internacional de dados: extraterritorialidade e elementos de conexão

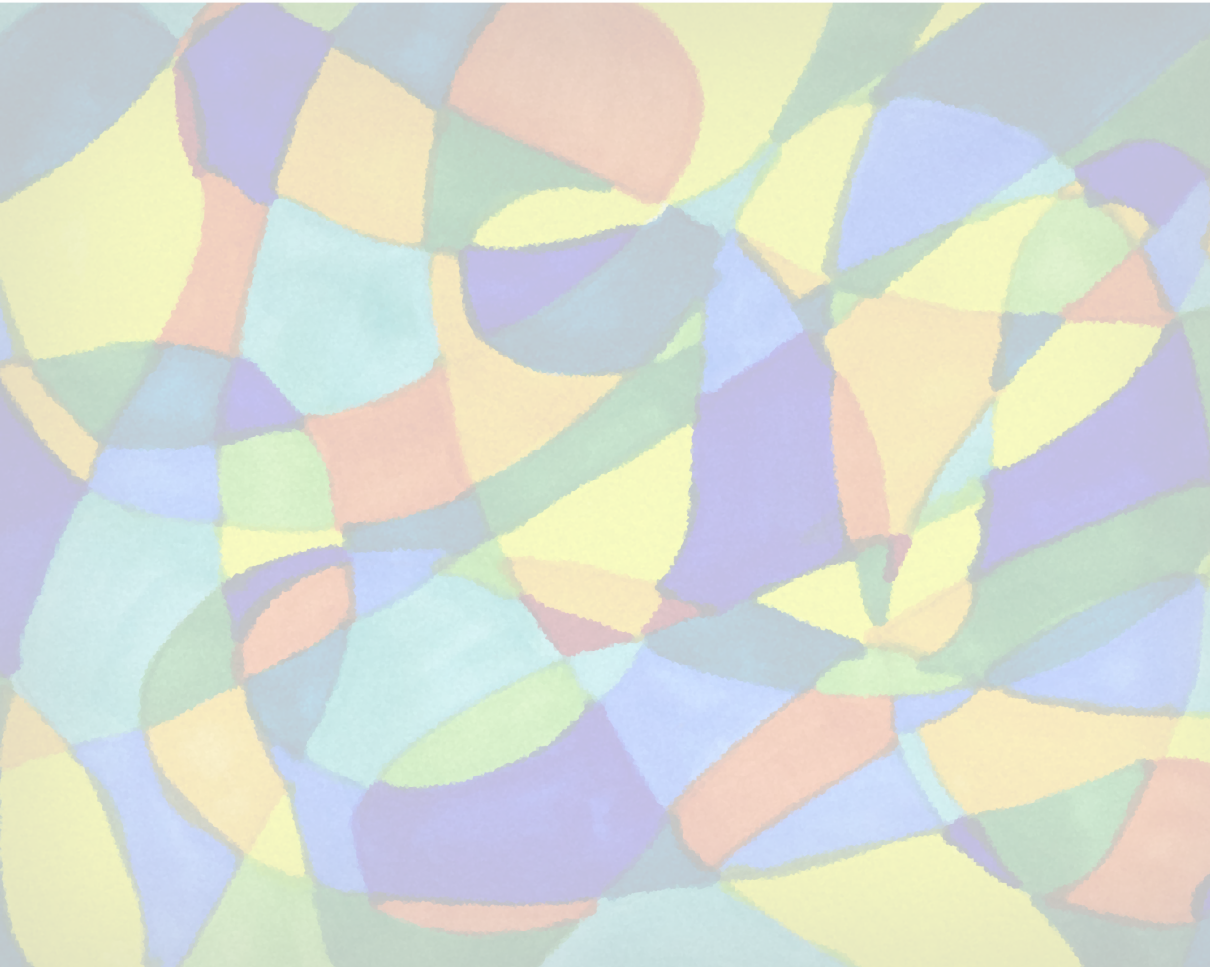
### Capítulo I



### Capítulo II

# PARTE I

## *UMA PERSPECTIVA EUROPEIA SOBRE A PROTEÇÃO DE DADOS*



# Seção I

## A proteção de dados pessoais: uma visão crítica do RGPD e da LGPD

# Capítulo I

# A NOVA LEI BRASILEIRA DE PROTEÇÃO DE DADOS - UMA VISÃO CRÍTICA

*Thomas Hoeren*[1]

*Stefan Pinelli*[2]

## SUMÁRIO



## RESUMO

O Brasil tem uma nova lei de proteção de dados, que entrará em vigor em de 2020, mas ela está em vigência parcial. Neste estudo se descrevem as principais características do novo sistema e o comparam com o Regulamento Básico de Proteção de Dados (DSGVO). Aponta-se o quanto é importante uma análise da "realidade da proteção de dados" para avaliar o critério de qualidade legal "nível adequado de proteção de dados". O artigo apresenta as vantagens e desvantagens do LGPD e faz uma comparação com o DSGVO. No contexto desta comparação, é dada especial atenção às mudanças relevantes para as empresas.

**Palavra-chave**: Proteção de Dados Pessoais – Direito Comparado – Segurança dos Dados

---

1 Doutor em Direito pela Universidade de Münster/Alemanha. Professor de Direito da Informação, Mídia e Negócios na Universidade de Münster e chefe do Instituto de Direito da Informação, Telecomunicações e Mídia (ITM). Professor adjunto do Instituto Fraunhofer de Tecnologia da Informação Aplicada (FIT). Árbitro de nomes de domínio para a Organização Mundial de Propriedade Intelectual (WIPO) e a Comissão Europeia. Professor de Direito da Informação e TI nas Universidades de Zurique e Viena. Membro do Comitê de Especialistas em Direito Autoral e Publicação da União Alemã para a Proteção da Propriedade Intelectual. Desde abril de 2015 é porta-voz do grande projeto de pesquisa do Ministério Federal da Educação e Pesquisa, ABIDA (Assessing Big Data).

2 Advogado. Chefe da Legal Digital Volkswagen AG, Wolfsburg/Alemanha. Membro do Conselho Consultivo do Instituto de Direito da Informação, Telecomunicações e Mídia (ITM).

# I INTRODUÇÃO[3]

O Brasil é o maior país da América do Sul e o quinto maior país em termos de área e população (mais de 200 milhões).[4] Ela deriva seu poder econômico de sua enorme agricultura, de seus recursos minerais e de suas grandes instalações de produção, também em nome de inúmeros investidores estrangeiros. O Brasil é uma federação de 26 estados membros. De acordo com a Constituição, a federação tem competência exclusiva em matéria civil e criminal (Art. 22(1)), mas os Estados-Membros têm competência concorrente em matéria de direito do consumidor (Art. 24). Nas últimas décadas, o uso das modernas tecnologias de informação e comunicação tem aumentado enormemente. Entretanto, não há estudos detalhados sobre os hábitos sociais dos brasileiros no que diz respeito à privacidade; estes são particularmente debatidos em conexão com a publicação ilegal de fotografias de destaque e a proteção de crianças na Internet.

A privacidade é abordada sobretudo na Constituição Brasileira de 1998 no Art. 5 como a proteção inalienável da esfera íntima, vida privada, honra e imagem das pessoas (X). Além disso, a proteção da privacidade é garantida no Código Civil 2002, na nova Lei de Proteção ao Consumidor[5] e em uma Lei de Internet separada (BCFI)[6]. Surpreendentemente, o Brasil ainda não conseguiu obter uma decisão da Comissão Européia sobre a adequação de sua lei de proteção de dados em relação ao regulamento básico de proteção de dados - ao contrário do Uruguai ou da Argentina.[7] Houve, portanto, uma enorme pressão dentro do Go-

---

3 Nossos agradecimentos ao Prof. Dr. José de Ascensao (Lisboa) e ao Prof. Dr. Marcos Wachowicz (Paraná/Brasil) por suas sugestões e amizade ao longo de muitos anos.

4 Veja https://www.cia.gov/library/publications/the-world-factbook/geos/br.html (último. Acesso em: 7 abr. 2020)

5 Lei nº 0.078/90.

6 Brazilian Civil Framework of the Internet - BCFI (Law No. 12.965/2014); siehe dazu Cíntia Rosa Pereira de Lima, **Comentários à Lei Geral de Proteção de Dados**, Almedina 2019, 7 ff.

7 No momento da aplicabilidade do regulamento básico de proteção de dados, os países terceiros seguros incluem Andorra, Argentina, Canadá (somente organizações comer-

verno Federal para elevar a lei interna de proteção de dados a um nível europeu.

## II A NOVA LEI BRASILEIRA DE PROTEÇÃO DE DADOS EM COMPARAÇÃO COM O DSGVO

A Lei Geral de Proteção de Dados Pessoais (LGPD) atualizou a legislação brasileira de proteção de dados pessoais.[8] Foi adotado em 14.8.2018 e entra em vigor em 14.8.2020.

Inicialmente, o LGPD deve ser incorporado a uma alteração geral estruturada da lei de proteção de marcas, internet e proteção de dados[9]. Devido a problemas políticos durante o processo legislativo, a reforma estruturada da lei de Internet resultou apenas em uma lei de proteção de dados independente (LGPD), uma lei de Internet separada (BCFI[10]) e uma lei de proteção de marcas ainda não reformada (BCL) de 1998[11].

O artigo apresenta as vantagens e desvantagens do LGPD e faz uma comparação com o DSGVO. No contexto desta comparação, é dada especial atenção às mudanças relevantes para as empresas.

---

ciais), Ilhas Faroe, Guernsey, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça, Uruguai, Japão e EUA (se o destinatário pertencer ao Privacy Shield). A transferência de dados para esses países é, portanto, expressamente permitida.

8 Tradução em inglês disponível em https://iapp.org/resources/article/brazils-general-data-protection-law-english-translation/ (último acesso em: 31 mar. 2020).

9 PARENTONI/SOUZA LIMA, "**Protection of Personal Data in Brazil:** Internal Antinomies and International Aspects", p. 2, disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362897 (último acesso: 31 mar. 2020)

10 BCFI significa "Marco Civil da Internet" (Marco Civil da Internet - Lei nº 12.965/2014) e é um acordo-quadro civil da Internet, que regula e garante o uso da Internet no Brasil. O BCFI teve um procedimento legislativo complicado e esteve sujeito a muitas mudanças, algumas delas provavelmente críticas, até ser aprovado pelo Congresso brasileiro em 25 de março de 2014; cf. FEIRA, "**The Brazilian Civil Rights Framework for the Internet**", disponível em https://direitorio.fgv.br/noticia/the-brazilian-civil-rights-framework-for-the-internet (último acesso: 31 mar. 2020).

11 PARENTONI/SOUZA LIMA, "**Protection of Personal Data in Brazil:** Internal Antinomies and International Aspects", p. 2, disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362897 (último acesso: 31 mar. 2020)

## 1 Área de aplicação LGPD

A LGPD aplica-se ao tratamento de dados pessoais por pessoas singulares ou colectivas de direito privado ou autoridades públicas (artigo 1º). O objetivo desta lei é proteger o direito fundamental à privacidade, por um lado, e o livre desenvolvimento da personalidade de uma pessoa interessada (art. 1º), por outro. A lei aplica-se, portanto, tanto ao setor privado quanto à administração pública.[12]

O artigo 3º define o âmbito territorial da LGPD, segundo o qual a LGPD se aplica a (i) dados do território nacional brasileiro, (ii) dados de indivíduos residentes no Brasil, e (iii) dados coletados no Brasil. Como resultado, o LGPD protege todos os indivíduos no Brasil, não apenas os cidadãos brasileiros. Este sistema extraterritorial não é o mesmo que o DSGVO.[13] O princípio do país de domicílio no Art. 3 § 1 DSGVO também é encontrado no Art. 3 LGPD. Entretanto, não há um foco restrito na intervenção final no mercado a partir do Art. 3 §2 DSGVO. Ao invés disso, é enfatizado uma espécie de princípio de direito mundial, segundo o qual qualquer contato com o Estado do Brasil desencadeia a aplicação da lei brasileira de proteção de dados. Isto também é esclarecido pelo nº 1 do art. 3º, segundo o qual uma coleta de dados deve ser considerada como tal no Brasil se o envolvido estiver atualmente no Brasil no momento da coleta. De forma correspondente, a lei contém uma disposição especial no Art. 4 (4) segundo a qual a lei não se aplica ao processamento de dados de um país não brasileiro de origem sem o envolvimento de processadores brasileiros.

Exclui-se da lei, de acordo com o art. 4º, parágrafo 1º, o tratamento de dados pessoais exclusivamente para fins privados e não econômicos. Esta disposição parece corresponder ao art. 2º, nº 2, lit. c DSGVO, com a diferença, entretanto, de que esta exceção é formulada e diz respeito a todos os fins não econômicos, privados. O processamento para fins jor-

---

12 Veja Art. 3 LGPD.

13 aA: MONTEIRO, "**The new Brazilian General Data Protection Law - a detailed analysis**", abrufbar unter: https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/ (zuletzt abgerufen: 31.03.2020).

nalísticos e artísticos também é formulado de forma mais ampla do que no DSGVO e está isento da mesma forma que, em princípio, todo o setor científico (Art. 4 (2)).

## 2 Dados pessoais e informações pessoais sensíveis no LGPD

O artigo 5º contém um catálogo de definições que são obrigatórias para lidar com a LGPD. Contém também as definições de dados pessoais e dados pessoais sensíveis. No LGPD, dados pessoais são definidos como informações que podem ser atribuídas a uma pessoa física identificada ou identificável.[14] Exemplos não estão incluídos nesta definição, mas você pode pensar em tudo, desde nomes, números de identificação, dados de navegação, nomes de usuários até fatos físicos, mentais, genéticos, econômicos, culturais ou sociais.[15] A definição está vinculada ao Art. 7, no qual se repete a proibição de processamento sujeito a autorização da DSGVO.

Dados pessoais sensíveis são definidos como dados pessoais que revelam a origem racial ou étnica, religião, opiniões políticas, filiação sindical, partido político ou crenças filosóficas ou religiosas, ou dados relativos à saúde ou sexualidade do sujeito dos dados.[16] Esta subcategoria de dados pessoais está sujeita a regras de tratamento específicas. De acordo com o Art. 11, o tratamento de dados pessoais sensíveis só é possível se

- o responsável pelo tratamento tenha dado o seu consentimento expresso para o tratamento dos dados, ou
- o tratamento de dados é utilizado no âmbito de um órgão público para a implementação de políticas públicas, ou

no contexto de estudos realizados por instituições de pesquisa.[17]

---

14 Ver Art. 5 (1) LGPD.

15 Veja FEIRA, "**O que é o LGPD? Brazil's version of the GDPR**", disponível em: https://gdpr.eu/gdpr-vs-lgpd/ (último acesso: 31 mar. 2020).

16 Cf. Art. 5 (2) LGPD.

17 Cf. Art. 11 par. 1-3 LGPD.

No contexto do LGPD, dados anonimizados referem-se a dados que podem ser atribuídos a um indivíduo que não pode ser identificado. Isto[18] não inclui mais dados que são reversíveis, ou seja, que podem ser usados para identificar os sujeitos dos dados ou para determinar seu comportamento. A definição é baseada no critério objetivo da disponibilidade de ferramentas de desanonimização (ver artigo 5(11)). Entretanto, essas operações de processamento reversíveis são baseadas nos recursos específicos dos órgãos de processamento individuais. A conseqüência deste sistema - semelhante à discussão sobre o DSGVO - é que a distinção entre dados anonimizados e pessoais depende da respectiva infra-estrutura técnica.[19]

As questões relativas à definição da data pessoal são, portanto, muito semelhantes às relativas ao DSGVO.[20] Entretanto, o LGPD difere do DSGVO por não distinguir entre dados anônimos e pseudônimos.[21]

## 3 Processamento de dados e seus requisitos

Art. 6 contém os princípios gerais do tratamento de dados pessoais similares ao art. 5 DSGVO. Entretanto, poupou o laborioso processo de estabelecer princípios gerais com complicadas exceções e simplificou os princípios e os ampliou para dez princípios. Como resultado, idéias como o princípio da não-discriminação (art. 6 (9)) também têm vindo à tona. A disposição adicional sobre o ônus da prova (Artigo 5(2)), que foi controversa após sua introdução na DPA, foi simplesmente substituída pela introdução de um simples princípio de prestação de contas (Artigo 6(10)).

---

18 Cf. Art. 5 (3) LGPD.

19 BIONI/GOMES/MONTEIRO, "**GDPR matchup**: Brazil's General Data Protection Law", disponível em: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/ (último acesso: 31 mar. 2020).

20 ERICKSON, "**Comparative Analysis of the EU's GDPR and Brazil's LGPD**: Enforcement Challenges with the LGPD", 44 Brook. J. Int'l L. 859 (2019), p. 883.

21 BIONI/GOMES/MONTEIRO, "**GDPR matchup**: Brazil's General Data Protection Law", disponível em: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/ (último acesso: 31 mar. 2020).

Segue-se a proibição geral, sujeita a autorização, no art. 7º, retomada do DSGVO. No entanto, o LGPD contém dez bases legais nas quais o processamento de dados pode ser baseado:

(1) Consentimento do titular dos dados,

(2) Cumprimento das exigências legais ou regulamentares do órgão de processamento,

(3) Implementação de atos administrativos,

(4) Realização de estudos por instituições de pesquisa,

(5) Execução do contrato ou medidas pré-contratuais, ambas a pedido da pessoa interessada,

(6) Declaração de direitos próprios em processos judiciais,

(7) Proteção do corpo e da saúde da pessoa interessada ou de terceiros,

(8) Proteção da saúde pelas autoridades sanitárias,

(9) a existência de um interesse legítimo, exceto quando prevalecerem os direitos fundamentais do titular dos dados

(10) Para proteger os empréstimos.[22]

§ 5º do art. 7º da LGPD requer um consentimento específico no caso do controlador dos dados compartilhar os dados com outra pessoa. A própria LGPD não especifica os requisitos que devem ser cumpridos para tal consentimento específico. Pode ser assumido, no entanto, que requer uma disposição explícita sobre consentimento e que este consentimento também deve especificar a identidade do segundo processador de dados que deve conter os dados.[23] No entanto, a DPA não tem uma disposição específica para tal caso de divulgação dos dados, de modo que os requisitos gerais para a licitude do processamento de dados se aplicam. O caráter exemplar do DSGVO já

[22] Veja Art. 11 LGPD.

[23] LUNDGREN, GRUR Int. 2009, 752 (755).

pode ser visto aqui[24]. No entanto, também existem diferenças fundamentais. Por exemplo, a regulamentação sobre a realização de estudos de pesquisa ou a isenção para instituições de crédito é generosa.[25] A isenção total para as autoridades públicas também é surpreendente em termos de acesso aos dados pessoais. O bloco muito pequeno e corretamente esculpido no Art. 6 § 3 DSGVO não foi adotado. Isto significa que qualquer tarefa legal pode ser usada para acessar dados. O consentimento também é tratado de forma generosa. Por exemplo, o Art. 7 ***§*** 4 LGPD afirma que o consentimento não é necessário para os dados que a pessoa em questão obviamente tornou públicos. Uma regulamentação correspondente havia sido exigida no DSGVO, mas não foi alcançada.

## 4 Visão geral dos direitos do LGPD

O LGPD não só estipula como os dados devem ser tratados, mas também dá à pessoa interessada uma riqueza de direitos no tratamento dos seus dados. Estes direitos estão listados no Capítulo 3 da LGPD (cf. Art. 17-22 da LGPD). Neste contexto, o Art. 17, em primeiro lugar, confere ao titular dos dados o direito de propriedade dos seus dados. A expressão propriedade ***é*** ambígua e soa como propriedade; isto provavelmente deve ser entendido mais como propriedade. No art. 18 há um catálogo de direitos contra a parte processadora, incluindo

- o direito à "confirmação" do processamento, mais para ser entendido como um direito de acesso aos dados,
- o direito de acesso aos dados,
- o direito de ter dados incorretos corrigidos,
- o direito à portabilidade dos dados, tendo em conta a protecção do sigilo, e

[24] ERICKSON, "**Comparative Analysis of the EU's GDPR and Brazil's LGPD**: Enforcement Challenges with the LGPD", 44 Brook. J. Int'l L. 859 (2019), p. 883.

[25] Vgl. PERRONE/STRASSBURGER, "**Privacidade e Proteção de Dados - Da Europa para o Brasil**", Panor. Braz. lei. Vol. 6, No 9-10 (2018), p. 89-90.

- o direito de ter os dados apagados.[26]

Além disso, o art. 19 regulamenta as circunstâncias de acesso aos dados pessoais. Este acesso pode ser concedido de forma simples e imediata ou de forma mais detalhada no prazo de 15 dias.[27] O art. 20 também prevê o direito de revisão de uma decisão automatizada.

Isto também soa em parte como o DSGVO. Mas também aqui existem inúmeras diferenças significativas. Por exemplo, o direito de ser esquecido está faltando no Art. 17 DSGVO. Não há especificações de direitos comparáveis ao DSGVO. A proibição das decisões automatizadas nos termos do art. 22 não se reflete na Lei, apenas um direito à revisão posterior por uma pessoa física.

Art. 46 LGPD estipula que os responsáveis devem tomar medidas técnicas, administrativas e de segurança para evitar tanto o acesso não autorizado aos dados como formas ilegais de tratamento de dados. De acordo com o Art. 46 (2) LGPD, estas medidas devem ser cumpridas desde a concepção do produto até o processamento dos dados. Isto faz lembrar a *regra de privacidade por projeto* sob o Art. 25 §1 DPA.[28] Entretanto, o DSGVO também estipula a obrigação de usar configurações padrão de proteção de dados amigáveis (*privacidade por padrão*). O LGPD não tem tal obrigação.

## 5 Autoridade de Proteção de Dados e o DPO

No *âmbito* da LGPD, o Brasil deve estabelecer uma nova autoridade, a chamada Autoridade Nacional de Proteção de Dados[29], que assumirá o papel da mais alta autoridade de proteção de dados. Será uma autoridade estatal independente cuja tarefa será monitorar a implementação da LGPD, criar novos regulamentos de implementação, aplicar as normas

[26] Cf. Art. 18 par. 1, 2, 3, 5, 6 LGPD.

[27] Cf. Art. 19 §§ 1 e 2 da LGPD.

[28] LAUBACH/DRÄGER, ZD-aktuell 2018, 06254.

[29] Abreviado como ANPD.

existentes, proteger dados pessoais e impor sanções no caso de violações[30]. A ANPD será composta pelo Conselho de Administração e pelo Conselho Nacional, que atuará como órgão consultivo.[31]

De acordo com o Art. 33 § 1 DSGVO, em caso de violação da proteção de dados, o responsável deve comunicar a violação à autoridade fiscalizadora competente sem demora e, se possível, no prazo de 72 horas. Nos termos do Art. 34 DSGVO, a pessoa interessada deve ser informada se a violação representar um risco particular para os direitos e liberdades da pessoa.

O artigo 48 da LGPD prevê um regulamento comparável, mas não especifica nenhum requisito de tempo específico.[32] De acordo com o Art. 48 § 1º, a autoridade nacional competente define o que constitui um período de tempo razoável. Ao contrário do DSGVO, a pessoa interessada também deve ser sempre informada.[33]

Além disso, as empresas brasileiras serão obrigadas a contratar um Responsável pela Proteção de Dados (DPO). O RPD deve ser uma pessoa singular ou colectiva que deve actuar como canal de comunicação entre a unidade de tratamento, a pessoa em causa e a autoridade de protecção de dados[34]. O cargo também pode ser transferido externamente para uma pessoa que não faça parte da estrutura da empresa.[35]

---

30 MONTEIRO, "**The new Brazilian General Data Protection Law - a detailed analysis**", abrufbar unter: https://iapp.org/news/a/the-new-brazilian-general-data-protection-law--a-detailed-analysis/ (zuletzt abgerufen: 31.03.2020).

31 MONTEIRO, "**The new Brazilian General Data Protection Law - a detailed analysis**", abrufbar unter: https://iapp.org/news/a/the-new-brazilian-general-data-protection-law--a-detailed-analysis/ (zuletzt abgerufen: 31.03.2020).

32 BRANCHER/THOMAZ, CRi 2018, 130 (132).

33 COOS, "**LGPD vs. GDPR**: The Biggest Differences", disponível em: https://www.endpointprotector.com/blog/lgpd-vs-gdpr-the-biggest-differences/ (último. Acesso em: 31 mar. 2020)

34 BIONI/GOMES/MONTEIRO, "**matchup PIBR**: Brazil's General Data Protection Law", abrufbar unter: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/ (zuletzt abgerufen: 31.03.2020); ERICKSON, "**Comparative Analysis of the EU's GDPR and Brazil's LGPD**: Enforcement Challenges with the LGPD", 44 Brook. J. Int'l L. 859 (2019), p. 884.

35 BIONI/GOMES/MONTEIRO, "**GDPR matchup**: Brazil's General Data Protection Law", disponível em: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/ (último acesso: 31 mar. 2020).

No início da discussão sobre o LGPD, ainda havia discrepâncias com o DSGVO no contexto das OPDs, pois, de acordo com as primeiras versões do LGPD, estas só podiam ser pessoas físicas nacionais. No entanto, os rascunhos foram alterados para o status atual no âmbito da ratificação formal pelo então Presidente Temer[36]. Art. 37 DSGVO especifica requisitos específicos, onde tanto um controlador de dados quanto um processador devem nomear um responsável pela proteção de dados. Ao contrário do DSGVO, o LGPD prevê tal obrigação no art. 41 somente para os controladores e não para os processadores. De acordo com a redação do art. 41, entretanto, todos os controladores devem ser afetados por esta obrigação, independentemente do seu tamanho e se o processamento de dados é uma de suas atividades principais. Entretanto, a ANPD ainda pode alterar esta disposição e espera-se que ela restrinja o escopo de aplicação.[37]

## 6 Segurança de dados

O sétimo capítulo da Lei de Proteção de Dados contém disposições sobre segurança de dados. De acordo com o Art. 46, o responsável pelo processamento deve tomar medidas técnicas e administrativas para garantir a segurança dos dados. De acordo com o Art. 48, as violações de segurança devem ser comunicadas à autoridade supervisora de proteção de dados e à pessoa interessada. O que exatamente é considerado como padrões adequados de segurança de dados não é mencionado na lei, semelhante ao Regulamento Básico de Proteção de Dados.

## 7 Sanções em comparação

O LGPD prevê três formas de sanções. Em particular, são advertências, bem como multas e sanções de até 2% do faturamento anual nacio-

36 Erickson, "**Comparative Analysis of the EU's GDPR and Brazil's LGPD**: Enforcement Challenges with the LGPD", 44 Brook. J. Int'l L. 859 (2019), p. 884.

37 COOS, "**LGPD vs. GDPR**: The Biggest Differences", disponível em: https://www.endpointprotector.com/blog/lgpd-vs-gdpr-the-biggest-differences/ (último. Acesso em: 31 mar. 2020)

nal ou até R$ 50.000.000.[38] Além disso, o processamento deve ser interrompido e, em caso de dúvida, os dados disputados devem ser apagados.

O DSGVO prevê medidas sancionatórias semelhantes, embora estas sejam significativamente mais elevadas do que para o LGPD. Por exemplo, o art. 83 DSGVO prevê sanções de até 4% do faturamento anual total de uma empresa.

## III AVALIAÇÃO FINAL

Em resumo, a semelhança entre o LGPD e o DSGVO, particularmente em termos de estrutura e objetivos, é sempre enfatizada.[39] Isto seria particularmente vantajoso para todas as empresas internacionais sujeitas ao DSGVO. Como resultado, pode-se pensar que "estas empresas não precisam se adaptar novamente às diretrizes de proteção de dados, mas podem simplesmente estender os modelos do DSGVO para a esfera de ação brasileira".[40] "Entretanto, surge a questão de como o Brasil vai viver os novos conceitos de proteção de dados. É impressionante que há uma diferença considerável nos detalhes entre o DSGVO e a nova lei brasileira, que é também uma expressão de diferentes raízes na lei de proteção de dados e uma cultura social e jurídica divergente.

Isso também leva a uma das questões centrais do direito internacional de proteção de dados, a saber, a questão do nível adequado de proteção de dados. Durante décadas, este conceito tem sido o elo central entre diferentes regimes de proteção de dados e determina o

---

38 Art. 52 LGPD.

39 Assim também ARTESE, "Sim! Uma lei de privacidade brasileira! Mas ainda não...", abrufbar unter: https://iapp.org/news/a/yes-a-brazilian-privacy-law-but-not-quite-yet/ (zuletzt abgerufen: 31.03.2020); BIONI/GOMES/MONTEIRO, "**matchup GDPR**: Brazil's General Data Protection Law", abrufbar unter: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/ (zuletzt abgerufen: 31.03.2020); ERICKSON, "**Comparative Analysis of the EU's GDPR and Brazil's LGPD**: Enforcement Challenges with the LGPD", 44 Brook. J. Int'l L. 859 (2019), p. 888.

40 Vgl. ERICKSON, "**Comparative Analysis of the EU's GDPR and Brazil's LGPD**: Enforcement Challenges with the LGPD", 44 Brook. J. Int'l L. 859 (2019), p. 888.

exame de casos de proteção de dados transfronteiriços. No entanto, um olhar sobre o Brasil em particular deixa claro que este termo não pode ser uma consideração formal de dois conjuntos de regras abstratas. A lei brasileira de proteção de dados difere em muitos detalhes da norma européia, apesar dos elogios dados, especialmente na literatura brasileira. Além disso, a visão puramente formal é muito curta e superficial. Ao contrário, é preciso examinar como a lei de proteção de dados é aplicada, vivida e sentida no chão. A questão da futura "realidade da proteção de dados" brasileira é, portanto, fundamental, especialmente de uma perspectiva européia.

## REFERÊNCIAS

aA:MONTEIRO, "**ThenewBrazilianGeneralDataProtectionLaw-adetailedanalysis**", abrufbar unter: https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/ (zuletzt abgerufen: 31.03.2020).

ARTESE, "Sim! Uma lei de privacidade brasileira! Mas ainda não...", abrufbar unter: https://iapp.org/news/a/yes-a-brazilian-privacy-law-but-not-quite-yet/ (zuletzt abgerufen: 31.03.2020);

BIONI/GOMES/MONTEIRO, "**GDPR matchup**: Brazil's General Data Protection Law", disponível em: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/ (último acesso: 31 mar. 2020).

BIONI/GOMES/MONTEIRO, "**matchup PIBR**: Brazil's General Data Protection Law", abrufbar unter: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/ (zuletzt abgerufen: 31.03.2020);

BRANCHER/THOMAZ, CRi 2018, 130 (132)

COOS, "**LGPD vs. GDPR**: The Biggest Differences", disponível em: https://www.endpointprotector.com/blog/lgpd-vs-gdpr-the-biggest-differences/ (último. Acesso em: 31 mar. 2020)

ERICKSON, "**Comparative Analysis of the EU's GDPR and Brazil's LGPD**: Enforcement Challenges with the LGPD", 44 Brook. J. Int'l L. 859 (2019).

FEIRA, "**The Brazilian Civil Rights Framework for the Internet**", disponível em https://direitorio.fgv.br/noticia/the-brazilian-civil-rights-framework-for-the-internet (último acesso: 31 mar. 2020).

FEIRA, "**O que é o LGPD? Brazil's version of the GDPR**", disponível em: https://gdpr.eu/gdpr-vs-lgpd/ (último acesso: 31 mar. 2020).

https://www.cia.gov/library/publications/the-world-factbook/geos/br.html (último. Acesso em: 7 abr. 2020)

LAUBACH/DRÄGER, ZD-aktuell 2018, 06254.

LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**, Almedina 2019, 7 ff.

LGPD Art. 5 (2) .

LUNDGREN, GRUR Int. 2009, 752 (755).

MONTEIRO, "**The new Brazilian General Data Protection Law - a detailed analysis**", abrufbar unter: https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/ (zuletzt abgerufen: 31.03.2020).

PARENTONI/SOUZA LIMA, "**Protection of Personal Data in Brazil:** Internal Antinomies and International Aspects", p. 2, disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362897 (último acesso: 31 mar. 2020)

PERRONE/STRASSBURGER, "**Privacidade e Proteção de Dados - Da Europa para o Brasil**", Panor. Braz. lei. Vol. 6, No 9-10 (2018), p. 89-90.

# Capítulo II

# A SEGURANÇA DOS DADOS NA LGPD, BRASILEIRA: uma perspetiva europeia, desde Portugal

*Manuel David Masseno*[1]

## SUMÁRIO



## RESUMO

Este artigo expõe, criticamente, cada uma das principais questões relativas à segurança intrínseca no tratamento de dados resultantes da Lei Geral de Proteção de Dados Pessoais, do Brasil, mas desde uma perspetiva externa, a do Regulamento Geral sobre a Proteção de Dados, da União Europeia, o qual tem sido considerado como sua matriz. Atendendo à proximidade juscultural, as referências assentam na Doutrina portuguesa especializada.

**Palavras-chave**: Brasil, Dados Pessoais, Regulação, Segurança, União Europeia

[1] Professor Adjunto do IPBeja - Instituto Politécnico de Beja, onde também integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança Informática, sendo ainda o seu Encarregado da Proteção de Dados. Pertence à EDEN – Rede de Especialistas em Proteção de Dados da Europol – Agência Europeia de Polícia e ao Grupo de Missão "Privacidade e Segurança" da APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação, em Portugal, ao Grupo de Estudos de Direito Digital e *Compliance* da FIESP – Federação das Indústrias do Estado de São Paulo, à Comissão Estadual de Direito Digital da Ordem dos Advogados do Brasil, Seção de Santa Catarina e à Comissão de Direito Digital da Subseção de Campinas da OAB.

## 1 *A LGPD* E O *RGPD* – A MODO DE *PRÉ-ENTENDIMENTO*... CONCLUSIVO[2/3]

Como ponto de partida, não podemos deixar de constatar como a Lei n.º 13.709, de 14 de agosto de 2018, a Lei Geral sobre Proteção de Dados – *LGPD*, tem sido reiteradamente exposta como sendo uma espécie de projeção *tropicalizada* do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares [físicas] no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados), o *RGPD*.[4]

Aliás, até a própria *occasio legis* seria suscetível de o demonstrar, pela coincidência da entrada em vigor do *RGPD*, no final de maio de 2018, com a aceleração do processo legislativo no Congresso brasileiro, sobretudo devida a uma muito forte pressão midiática. Assim, depois de anos de hesitações na opção entre o *modelo norte-americano*, de fragmentação legislativa vertical e aplicação judiciária *a posteriori*, e o *modelo europeu*, com uma disciplina geral e uma implementação também feita através de autoridades administrativas independentes, o Brasil escolheu seguir o segundo.

---

2 Este texto foi construído a partir da minha aula no Programa de Pós-Graduação em Direito - Mestrado da UNISC - Universidade de Santa Cruz do Sul, RS, no dia 30 de agosto de 2019, assim como da matéria lecionada no MESI - Mestrado em Engenharia de Segurança Informática do IPBeja - Instituto Politécnico de Beja e no I Curso de Pós-Graduação Avançada em Direito da Proteção de Dados da Faculdade de Direito da Universidade de Lisboa. Aliás, é patente o estilo didático do mesmo, até porque não se trata de um estudo jurídico de natureza dogmática.

3 Artigo tem publicação na **Revista do Programa de Pós-Graduação em Direito - Mestrado e Doutorado da Universidade de Santa Cruz do Sul,** n.º 2 de 2020.

4 Mesmo apenas em Portugal, os trabalhos dedicados ao *Regulamento* começam a somar-se. Assim e no que se refere a abordagens gerais, são de apontar desde os trabalhos iniciais de Catarina Sarmento e CASTRO (2016), de Angelina TEIXEIRA (2016), de Jorge Barros MENDES (2017) e de Mafalda Miranda BARBOSA (2017), até às sínteses de Sónia MOREIRA (2018) e de Alexandre Sousa PINHEIRO (2018 a), podendo também ter algum interesse o meu estudo com Cristiana Teixeira SANTOS (2018), assim como, e sobretudo, o *Comentário* coordenado por Alexandre Sousa PINHEIRO (2018) e ainda o recentíssimo *Manual* de A. Barreto Menezes Cordeiro (2020).

Porém, se assim será em termos gerais, ao descermos ao nível do estudo de cada um dos institutos que enformam a *LGPD*, metaforicamente falando "do bosque para cada árvore", verificamos como a proximidade é mais aparente do que real. Inclusive é viável identificar um padrão comum, o da menor consideração dos interesses, e dos correspondentes direitos, das pessoas físicas, relativamente aos das organizações, mormente se tratando de Instituições Públicas.

A meu ver, um dos exemplos mais claros de uma tal escolha de Política Legislativa está na legitimação dada às organizações para criarem "perfis comportamentais", através de ferramentas técnicas próprias da Inteligência Artificial, aceitando a viabilidade de ocorrerem processos decisionais sem revisão humana (Art.s 12 § 2º e 20, por força da Medida Provisória n.º 869, de 27 de dezembro de 2018, não revertida pela Lei n.º 13.853, de 8 de julho de 2019), bem como a previsão de um "uso compartilhado" por "órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados" (Art.s 5 XVI, 7 III, 9 V, 18 VII e 26), este já regulamentado pelo Decreto n.º 10.046, de 9 de outubro de 2019, no que se refere à administração pública federal, o que autoriza o monitoramento permanente dos cidadãos, inclusive antecipando seus comportamentos futuros, e permite o seu condicionamento por tais organizações.

A isto acresce a previsão de uma "Autoridade Nacional de Proteção de Dados - ANPD, enquanto órgão da administração pública federal, na esfera da Presidência da República" (Art. 55-A, mesmo após a referida Lei n.º 13.853), consequentemente, sem garantias de independência, apesar de ter ficado "assegurada [sua] autonomia técnica e decisória" (Art. 55-B, ainda segundo a mesma Lei).

Em ambos os institutos, verificamos que a *LGPD* se afasta tanto do regime aplicável às "decisões individuais automatizadas, incluindo [a] definição de perfis" (Art.ºs 4.º 4) e 22.º)[5] quanto do estatuto garantido às

[5] Quanto a esta questão, uma das mais delicadas e controvertidas no que se refere ao emprego da Inteligência Artificial no domínio do tratamento de dados pessoais, são de aten-

"autoridades de controlo" (Art.ºs 51.º e 52.º)[6], ao ponto de só a segunda discrepância ser suscetível de impedir a consideração do Brasil enquanto destino de dados pessoais tratados na União Europeia sem autorizações específicas (Art.ºs 44.º e 45.º, 1 e 2 alínea b)[7].

Quanto à disciplina da Segurança dos Dados e desde já, podemos antecipar que este padrão se confirma, com uma maior consideração dos interesses das organizações, públicas ou privadas, em detrimento dos direitos dos cidadãos, enquanto titulares dos dados.

Mas, para podermos entender as diferenças entre o *RGPD* e a *LGPD*, é preciso ter presente que os mesmos resultam de tradições diversas no que se refere à proteção de dados pessoais, apenas agora convergentes.

No que se refere às Fontes gerais europeias, o percurso já é de décadas, desde a Convenção do Conselho da Europa n.º 108, de 28 de janeiro de 1981, sobre a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, passando pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995,

---

der as referências de Catarina Sarmento e CASTRO (2016), assim como os estudos de José Afonso FERREIRA (2018), de Gabriela CALDAS (2019) e de Madalena Perestrelo de OLIVEIRA (2019), bem como o comentário de Alexandre Sousa PINHEIRO e Carlos Jorge GONÇALVES (2018 a), e as referências de A. Barreto Menezes CORDEIRO (2020, pp. 148-149); e, especificamente, além da abordagem de Ana Alves LEAL (2017), esta centrada no Setor Financeiro, aponto a minha abordagem no que se refere às viagens (2016) e o meu trabalho com Cristiana Teixeira SANTOS (2019), a propósito da proteção dos turistas enquanto cidadãos e consumidores. Sobre estas questões, são ainda fundamentais as *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*, do Grupo de Trabalho do Artigo 29.º [GT 29, o qual antecedeu o atual CEPD – Comité Europeu para a Proteção de Dados], adotadas em 3 de outubro de 2017 (Com a última redação revista e adotada em 6 de fevereiro de 2018.

6 A este propósito, mormente, relevam as considerações de Filipa Urbano CALVÃO (2015), ainda que proferidas antes da adoção do RGPD, assim como os comentários breves de Alexandre Sousa PINHEIRO (2018 c) e (2018 d), o apontamento contextualizado de João Ferreira PINTO (2018) e, ainda, a abordagem de A. Barreto Menezes CORDEIRO (2020, pp. 397-402).

7 Para estas matéria e em termos gerais, temos os estudos de Inês O. Andrade de JESUS (2018) e, sobretudo, de Ricardo Rodrigues de Oliveira (2018), assim como o comentário de Alexandre Sousa PINHEIRO e Carlos Jorge GONÇALVES (2018 b).

relativa à proteção das pessoas singulares [físicas] no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, até à respetiva *constitucionalização* pelo *Tratado sobre o Funcionamento da União Europeia* (Art.º 16.º) e a *Carta dos Direitos Fundamentais da União Europeia* (Art.º 8.º), desde o *Tratado de Lisboa* (2007 – 2009), ambos os instrumentos com o mesmo valor formal que o *Tratado da União Europeia* (*ex vi* Art.º 6.º)[8], sem esquecer a Jurisprudência do Tribunal de Justiça da União Europeia, nomeadamente o Acórdão *Google Spain* (Processo C-131/12, de 13 de maio de 2014), proferido durante o processo legislativo que conduziu ao *RGPD* e teve uma grande importância para o prosseguimento do mesmo e seu conteúdo final[9].

Enquanto a *LGPD* é uma novidade, ainda que relativa, se formos rigorosos. Com efeito, já vigorava o, dito, "Marco Civil da Internet", aprovado pela Lei n.º 12.965, 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil[10], incluindo diversas questões relativas à proteção de dados pessoais (Art.s 3, II e II,

---

8 Para uma melhor compreensão quanto à origem e à relevância destas Fontes, são sobretudo de atender os trabalhos de Maria Eduarda GONÇALVES (2003, pp. 88-97), e de Catarina Sarmento e CASTRO (2005, pp. 39-45) e, bem assim, de Alexandre Sousa PINHEIRO (2015, pp. 528-546 e 573-661) e Alessandra SILVEIRA e João MARQUES (2016); além dos comentários aos referidos preceitos do *Tratado sobre o Funcionamento da União Europeia*, de Luís Neto GALVÃO (2012), e da *Carta dos Direitos Fundamentais da União Europeia*, por Catarina Sarmento e CASTRO (2013).

9 Sobre este Acórdão, cuja importância não poderá nunca ser desvalorizada, contamos com as reflexões, ainda "a quente", de Sofia Vasconcelos CASIMIRO (2014), a que se juntaram os estudos de Filipa Urbano CALVÃO (2015), de João MARQUES (2016) e de Catarina Sarmento e CASTRO (2016), assim como as considerações mais recentes de Catarina Santos BOTELHO (2017), de Maria de Fátima GALANTE (2018) e ainda de Rui P. Coutinho de Mascarenhas ATAÍDE (2019).

10 Daí, no que se refere à proteção de dados, a correspondência será com a Diretiva relativa à privacidade e às comunicações eletrónicas (Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, tal como alterada pela Diretiva 2009/136/CE, do Parlamento Europeu e do Conselho, de 25 de novembro de 2009), a qual está em vias de ser substituída pelo Regulamento relativo à privacidade e às comunicações eletrónicas (Proposta de Regulamento relativo ao respeito pela vida privada e à proteção dos dados pessoais, COM(2017) 10 final, de 10 de janeiro de 2017), sobre o qual aponto as referência presentes no meu estudo com Cristiana Teixeira SANTOS (2019).

7, VII, VIII e X, 11, 14 e 14), regulamentado pela Decreto n.º 8.771, de 11 de maio de 2016. Pelo que tecnicamente, o "Marco Civil" até será uma Lei Geral perante a *LGPD*, no que se refere aos tratamentos de dados realizados na Internet, enquanto nos demais casos será aplicável por analogia, *legis* ou *iuris*.

Adicionalmente, também o *Código de Defesa do Consumidor*, aprovado pela Lei n.º 8.078, de 11 de setembro de 1990, e a *Lei de Acesso a Informações Públicas*, resultante da Lei n.º 12.527, de 18 de novembro de 2011, contêm regras sobre dados pessoais, a serem articuladas sistematicamente com a *LGPD* e o "Marco Civil".

No entanto, a *Constituição Federal*, de 1988, apenas trata da matéria de um modo fragmentário e indireto, além do *habeas data* (Art. 5 LXXII), só consta o direito ao respeito pela vida privada (Art. 5 X)[11].

Enquanto no que se refere à Jurisprudência, para ficarmos pelo assunto correspondente ao Acórdão *Google Spain*, há a apontar as decisões do Superior Tribunal de Justiça no *Caso Xuxa* (REsp n.º 1.316.921/RJ, de 26 de junho de 2012), que se consolidou também nos Tribunais de Justiça, salvo nos do Rio de Janeiro e de São Paulo, a qual foi superada quando a "alternativa europeia" se tornou prevalecente (REsp n.º 1.660.168/RJ, de 8 de maio), ao prevalecer o voto do Ministro Marco Aurélio Bellize sobre o da Ministra Fátima Nancy Andrighi.

## 2 UM OBJETIVO COMUM: A SEGURANÇA NO TRATAMENTO DOS DADOS PESSOAIS

Com efeito, no *RGPD* começa por ser enunciado um dever geral de "segurança no tratamento", o qual se projeta logo como um dos "princí-

[11] Entretanto, a 2 de julho de 2019, foi aprovada, em segunda votação, pelo Senado Federal a Proposta de Emenda à Constituição 17/2019, a qual acrescenta ao Art. 5º o inciso XII-A, estabelecendo que "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais", cujo primeiro subscritor é o Senador Eduardo Gomes (MDB-TO).

pios relativos ao tratamento de dados pessoais", o da «integridade e confidencialidade», pois os dados devem ser:

> "Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas." (Art.º 5.º n.º 1 alínea f).

Consequentemente, desde a conceção e por defeito [omissão], com ênfase na pseudonimização (Art.º 25.º n.º 1)[12]:

> "Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares [físicas], o responsável pelo tratamento [controlador] e o subcontratante [operador] aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco […]", (Art.º 32.º n.º 1)

O qual se articula explicitamente com o princípio da «responsabilidade», dado que "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo" (Art.º 5.º n.º 2), e, por isso mesmo,

---

[12] Daí resulta que "A fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento [controlador], ou o subcontratante [operador], deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem. Essas medidas deverão assegurar um nível de segurança adequado, nomeadamente a confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função dos riscos e da natureza dos dados pessoais a proteger. Ao avaliar os riscos para a segurança dos dados, deverão ser tidos em conta os riscos apresentados pelo tratamento dos dados pessoais, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais." (*Considerando* 83); em termos gerais, são de referir as considerações breves de Alexandre L. Dias PEREIRA (2018), de Teresa Vale LOPES (2018), de Joana MOTA (2019) e, sobretudo, de A. Barreto Menezes CORDEIRO (2020, pp. 326-335 e 346-347).

> "Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares [físicas], cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades." (Art.º 24.º n.º 1)[13].

Designadamente e em relação ao nosso objeto de estudo, este princípio tem como corolários os regimes da responsabilidade (civil[14], Art.º 82.º, contraordenacional [administrativa][15], Art.º 83.º, e, se os Estados-membros assim o decidirem, também penal, (Art.º 84.º), assim como a aplicação das regras e medidas de segurança que abordaremos em seguida.

Em termos análogos, da *LGPD* consta o princípio "da segurança", o qual exige a

---

[13] Consequentemente, "Deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares [físicas]." (*Considerando* 74). Este princípio de *accountability* havia sido já objeto do Parecer 3/2010 do GT 29, sobre o "princípio da responsabilidade", adotado em 13 de julho de 2010, e, no que se refere ao seu conteúdo, podemos referir os estudos de Mafalda Miranda BARBOSA (2018) e de Teresa Vale LOPES (2018), assim como as considerações de Joana MOTA (2019) e de A. Barreto Menezes CORDEIRO (2020, pp. 161-163 e 323-325), além das Alexandre Sousa PINHEIRO (2018 b).

[14] A propósito da mesma, são de referir os estudos de Mafalda Miranda BARBOSA (2017), de A. Barreto MENEZES CORDEIRO (2018), retomadas em A. Barreto Menezes CORDEIRO (2020, pp. 381-396), e de Tiago Branco da Costa (2019),além das referências de Marco Alexandre SAIAS (2017) e do comentário de Cristina Pimenta COELHO (2018 a).

[15] Quanto a estas, entretanto densificadas através das Diretrizes de aplicação e fixação de coimas para efeitos do Regulamento 2016/679, adotadas em 3 de outubro de 2017 pelo GT 29, temos as referências prospetivas de Catarina Sarmento e CASTRO (2016), assim como as iniciais de Marco Alexandre SAIAS (2017), além da análise de José Lobo MOUTINHO e David Silva RAMALHO (2017), depois retomada por José Lobo MOUTINHO (2018) e ainda as considerações de Pedro Miguel FREITAS (2018), sem esquecer o comentário breve de Cristina Pimenta COELHO (2018 b).

> "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão." (Art. 6 VII).

Pelo que,

> "Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares." (Art. 49)

e, por isso mesmo,

> "Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga[m]-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término." (Art. 47)

Este mesmo critério foi retomado e explicitado, até com alguma especificação, ao enunciar a Lei que

> "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito." (Art. 46, caput)

Tal como no *RGPD*, este princípio está articulado com o "da responsabilização e prestação de contas", consistente na

> "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas." (Art. 6º X)

Embora a *LGPD* **vá** um pouco mais longe, prevendo que "A autoridade nacional poderá […] sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público." (Art. 32).

De igual modo **e além de nas regras e medidas de segurança**, este princípio tem uma especial importância no concernente **às matéria** "Da Responsabilidade e do Ressarcimento de Danos" (Art.s 42 a 44) e das "Sanções Administrativas" (Art.s 52 a 54).

## 3 AS REGRAS DE SEGURANÇA

Enquanto ponto de partida, resulta que do *RGPD* não consta a previsão de serem estabelecidas normas de segurança *vinculativas*, a aprovar e/ou a auditar pela Comissão Europeia, pelos Estados-membros, pelas Autoridades nacionais ou mesmo pelo CEPD – Comité Europeu para a Proteção de Dados.

Assim, apenas são indicados padrões genéricos, referidos como "medidas técnicas e organizativas adequadas", as quais deverão ser determinadas em função de critérios casuísticos, resultantes de análises de risco (Art.ºs 25 n.ºs 1 e 2 e 32 n.º 1)[16], ou de avaliações de impacto (Art.º 35.º), se estiverem reunidos os correspondentes pressupostos[17].

[16] Pois, "Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica." (*Considerando* 26). Sobre estas análises, numa perspetiva técnica, tem interesse o estudo de Luísa A. Inácio Varandas dos SANTOS e Mário R. Monteiro MARQUES (2019), e, desde uma perspetiva jurídica, as considerações de Teresa Vale LOPES (2018), Joana MOTA (2019) e, ainda, de estudo de A. Barreto MENEZES CORDEIRO (2018), cujas conclusões são retomadas em A. Barreto MENEZES CORDEIRO (2020, pp. 317-322).

[17] Além de seguir as "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 (Revistas e adotadas pela última vez em 4 de outubro de 2017), do Comité Europeu para a Proteção de Dados, a este propósito e em geral, são de assinalar as referências breves de Luís PICA (2018) e as considerações de Teresa Vale LOPES (2018) e Joana MOTA (2019), bem como e sobretudo o estudo de Bruno PEREIRA e João ORVALHO (2019).

O que afasta esta disciplina da prevista pela Diretiva *ePrivacy*[18], remetendo explicitamente para esquemas autorregulatórios, consistentes em códigos de conduta (Art.ºs 40.º e 41.º) ou em instrumentos de certificação (Art.ºs 42.º e 43.º)[19].

Porém, se o respetivo acatamento "pode ser utilizado como elemento para demonstrar o cumprimento das obrigações" (Art.º 32.º n.º 3), o certo é que não exime de eventuais responsabilidades, apenas as podendo graduar (Art.º 83.º n.º 1 alínea d).

Mas, sendo o caso, também serão de observar as regras em matéria de Cibersegurança, cujos regimes jurídicos se sobrepõem. Antes de mais, relevam as presentes na Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União [Diretiva *NIS / SRI*][20], já que

---

[18] A antes mencionada Diretiva relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, em cujos termos "O prestador de um serviço de comunicações eletrónicas publicamente disponível adotará as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede pública de comunicações no que respeita à segurança da rede. Tendo em conta o estado da técnica e os custos da sua aplicação, essas medidas asseguram um nível de segurança adequado aos riscos existentes. [pelo que] As autoridades nacionais competentes devem ter competência para auditar as medidas tomadas por prestadores de serviços de comunicações eletrónicas acessíveis ao público e para emitir recomendações sobre melhores práticas relativas ao nível de segurança que estas medidas devem alcançar. [enquanto] a Comissão poderá, após consulta da Agência Europeia para a Segurança das Redes e da Informação (ENISA), do Grupo de Proteção das Pessoas no que respeita ao Tratamento de Dados Pessoais instituído nos termos do artigo 29.º da Diretiva 95/46/CE, e da Autoridade Europeia para a Proteção de Dados, aprovar medidas técnicas de execução respeitantes às circunstâncias, ao formato e aos procedimentos aplicáveis aos requisitos de informação e notificação a que se refere o presente artigo. Na aprovação dessas medidas, a Comissão deve envolver todos os interessados, de modo, designadamente, a ser informada sobre os melhores meios técnicos e económicos disponíveis para a aplicação do presente artigo." (Art.º 4.º, n.ºs 1 e 5). Nesta particular, têm interesse as reflexões de Carlos Pinto de ABREU (2018).

[19] Neste particular, temos já as das Orientações 1/2018 relativas à "certificação e à definição de critérios de certificação de acordo com os artigos 42.º e 43.º do Regulamento (Versão 3.0, de 4 de junho de 2019), adotadas pelo CEPD, e, embora em termos genéricos, são de lembrar os apontamentos de Luís PICA (2018) e de Teresa Vale LOPES (2018).

[20] A propósito desta disciplina, são de indicar as referências de Alexandre L. Dias PEREIRA (2018).

> "Os Estados-Membros asseguram que os operadores de serviços essenciais tomem as medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações. Essas medidas devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes." (Art.º 14.º n.º 1).

Resultando que,

> "Essas medidas devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes, e devem ter em conta [designadamente, a sua] conformidade com as normas internacionais" (Art.º 16.º n.º 1 alínea e)

Ainda neste âmbito e como referência, temos o Regulamento de Execução (UE) 2018/151, da Comissão, de 30 de janeiro de 2018, que estabelece normas de execução da Diretiva (UE) 2016/1148 […] no respeitante à especificação pormenorizada dos elementos a ter em conta pelos prestadores de serviços digitais[21] na gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação […]". Designadamente, quando esclarece que

> "As normas internacionais referidas no artigo 16.º, n.º 1, alínea e), da Diretiva (UE) 2016/1148 são normas aprovadas por um organismo internacional de normalização, como referido no artigo 2.º, n.º 1, alínea a), do Regulamento (UE) n.º 1025/2012, do Parlamento Europeu e do Conselho [de 25 de outubro de 2012, relativo à normalização europeia]." (Art.º 2.º n.º 5)

[21] Enquanto "serviços digitais" são considerados os "1. Mercados em linha. [os] 2. Motores de pesquisa em linha. [e os] 3. Serviços de computação em nuvem", Art.º 4.º c) e Anexo III da Diretiva *NIS* / *SRI*.

E pode ainda vir a ser viável recorrer às normas constantes de um "sistema europeu de certificação de cibersegurança" (Art.ºs 51.º e 52.º do Regulamento (UE) 2019/881, de 17 de abril de 2019, relativo […] à certificação da cibersegurança das tecnologias da informação e comunicação (*Regulamento Cibersegurança*)[22].

Em síntese, o Legislador europeu teve sempre por referência as normas internacionais relevantes no que se refere à Segurança da Informação, designadamente a Norma ISO 27001, na medida em que esta se ajusta à proteção de dados pessoais[23].

Por sua vez, na *LGPD* a abordagem é simétrica, pois se

> "Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares" (Art. 49).

Da mesma resulta que, proativamente,

> "A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei." (Art. 46 § 1º)

e, também,

---

22 Estas questões têm escapado ao interesse da nossa Doutrina jurídica, mas sempre é de apontar o estudo de Helena CARRAPIÇO e André BARRINHA (2018).

23 Sobre a Norma ISO 27001 (Por extenso, ISO/IEC 27001 - Tecnologia da informação - técnicas de segurança - sistemas de gestão da segurança da informação – requisitos) e sua implementação no contexto do *RGPD*, são de atender os *Modelos* propostos, ainda que desde a perspetiva da Segurança da Informação, por José C. Lourenço Martins *et al*. (2018) e, ainda mais recentemente, por José C. Lourenço Martins (2019), este tendo já em atenção a respetiva articulação com a Norma ISO/IEC 27701:2019, cujo Anexo D estabelece os correspondentes critérios.

> "[…] editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei" (Art. 55-J, XII).

De este modo, apenas em termos complementares,

> "Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais." (Art. 50, caput).

Sendo que "A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais" (Art. 51) e "As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional." (Art. 50, § 3º).

## 4 OS DADOS PESSOAIS E A *LIMITAÇÃO* DO SEU *TRATAMENTO*

Se, nos termos do *RGPD*, é considerado como "dado pessoal" toda

> "informação relativa a uma pessoa singular [física] identificada ou identificável («titular dos dados»)é considerada identificável uma pessoa singular [física] que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por

> via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular [física]" (Art.º 4.º 1)[24].

Em contrapartida, da *LGPD* apenas consta uma definição muito sintética de "dado pessoal", como a

> "informação relacionada a pessoa natural identificada ou identificável", sem indicação de identificadores (Art. 5, I). Mas, a mesma deve ser integrada com a de "dado pessoal sensível: [que é o] dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Art. 5, II) e "Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles [dados] utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada." (Art. 12 § 2)

[24] O que incluí os quase-identificadores e os metadados, como os registros de conexão [no Brasil, definidos pelo *Marco Civil* como "o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (Art. 5, VIII)]. Até, porque "As pessoas singulares [físicas] podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão (*cookie*) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares [físicas]." (*Considerando* 30 do *RGPD*). Nesta matéria, há ainda que atender ao conteúdo do Parecer 4/2007 sobre o "conceito de dados pessoais", de 20 de junho de 2007, do GT 29, assim como à Jurisprudência do Tribunal de Justiça da União Europeia, a qual culminou no Acórdão proferido no Processo C-582/14, Patrick Breyer, de 19 de outubro de 2016. Na Doutrina, são de atender as considerações de Filipa Urbano CALVÃO (2015), esta ainda durante as negociações do *Regulamento Geral*, e de Mafalda Miranda BARBOSA (2017), tal como o estudo de A. Barreto MENEZES CORDEIRO (2018), cujas conclusões são retomadas em A. Barreto MENEZES CORDEIRO (2020, pp. 107-131), ademais do comentário à definição por parte de Alexandre Sousa PINHEIRO (2018 b).

A delimitando, negativamente, pela de "dado anonimizado: [enquanto] dado relativo a titular que não possa ser identificado […]" (Art. 5, III).

Isto, sem esquecer o *Regulamento do Marco Civil da Internet*, o qual, complementarmente, o define como o

> "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa." (Art. 14 I).

Por sua vez, embora tenha por objetivo primeiro o da garantia dos direitos dos titulares dos dados, a limitação do respetivo tratamento desempenha também uma função relevante no que se refere à segurança, estando subjacente às correspondentes disciplinas. Isto, tanto por reduzir os riscos em casos de incidentes, quanto por dificultar, ou até mesmo impossibilitar, a utilização de ferramentas analíticas de *Big Data*, melhor dizendo de "megadados"[25_26]

---

[25] Como dá conta explicita o Parecer 3/2013 do GT 29, sobre a "limitação de finalidade", de 2 de abril de 2013, "O termo "Megadados refere-se ao aumento exponencial da disponibilidade e da utilização automatizada de informações: refere-se a conjuntos de dados digitais gigantescos detidos por empresas, governos e outras organizações de grandes dimensões, que são depois extensivamente analisados (daí o nome 'analítica') com recurso a algoritmos informáticos."

[26] Quanto às implicações do tratamento destes "megadados", a Autoridade Europeia para a Proteção de Dados tem sido bastante assertiva, desde o Parecer preliminar "Privacidade e competitividade na era dos grandes volumes de dados: a articulação entre a proteção de dados, a lei da concorrência e a proteção do consumidor na Economia Digital", de 14 de março de 2014, reforçado pelo Parecer 4/2015 "Rumo a uma nova ética digital: dados, dignidade e tecnologia", de 11 de setembro de 2015, logo seguido do Parecer 7/2015 "Corresponder aos desafios dos Grandes Volumes de Dados: Um apelo à transparência, controlo do utilizador, proteção de dados desde a conceção e responsabilidade", de 19 de novembro do mesmo ano, entretanto atualizado pelo Parecer 8/2016 "Aplicação efetiva da legislação na economia digital", de 23 de setembro de 2016. Por sua vez, o Grupo de Trabalho do Artigo 29.º, que enfrentara estes problemas, pela primeira vez, no seu Parecer 2/2010, sobre "a publicidade comportamental em-linha", voltou a abordá-los com o Parecer 5/2012, sobre a "Computação em Nuvem", de 1 de julho de 2012, e pelo Parecer 3/2013, sobre "limitação de finalidade", antes referido, bem como e sobretudo pela "Declaração do Grupo do Artigo 29.º sobre o impacto do desenvolvimento da

Assim, no *RGPD* é enunciado o princípio da «minimização dos dados», já que estes devem ser "Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados" (Art.º 5.º n.º 1 alínea c). O que tem também uma dimensão temporal, o que o articula com o princípio da «limitação da conservação», sendo aqueles apenas "Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados […]" (Art.º 5.º n.º 1 alínea d)[27].

Consequentemente,

> "[…] o responsável pelo tratamento [controlador] aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas […] destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização." (Art.º 25.º n.º 1).

O que é depois especificado, dado que

> "O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito [por omissão], só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares [físicas]." (Art.º 25 n.º 2).

---

*Big Data* na proteção das pessoas relativamente ao tratamento dos seus dados pessoais na UE", de 16 de setembro de 2016. A este propósito e em termos gerais, temos as referências de Catarina Sarmento e CASTRO (2016), assim como o meu estudo de 2016, no âmbito do Direito Privado, e o de Maria Eduarda GONÇALVES (2016), no do Público, seguidos do de Ana Alves LEAL (2017), podendo ainda indicar a abordagem jurídica interdisciplinar que publiquei em 2019.

27 Sobre o conteúdos deste(s) princípio(s) são de indicar as referências breves de Alexandre Sousa PINHEIRO (2018 b) e de A. Barreto MENEZES CORDEIRO (2020, pp. 158-131) e ainda as do meu estudo com Cristiana Teixeira SANTOS (2018).

O mesmo princípio releva, ainda, a propósito das "regras vinculativas aplicáveis às empresas" nas transferências de dados pessoais para países terceiros ou organizações internacionais (Art.º 47.º n.º 1 alínea d) ou do "tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos" (Art.º 89.º n.º 1).

Por sua vez, na *LGPD* é enunciado o "Princípio da necessidade", consistindo este na "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (Art. 6.º, III), tendo também limites temporais, nomeadamente com a "verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada" (Art. 15, I).

## 5 A *ANONIMIZAÇÃO* E A *PSEUDONIMIZAÇÃO*

Antes de tudo o mais e no que concerne ao *RGPD*, é necessário afirmar que a *anonimização*, enquanto técnica destinada a garantir a segurança dos dados pessoais, nem sequer a referindo no seu articulado. Por isso,

> "[…] Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação." (*Considerando* 26, *in fine*)

Mais explícito ainda é o Regulamento (UE) 2018/1807, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia, o qual complementa o *RGPD*. Este, além de distin-

guir "dados pessoais" de "dados não pessoais" e de restringir a sua aplicação a estes, incluindo as situações em que ambos "estejam indissociavelmente ligados", reitera a imperatividade dos regimes de proteção dos dados pessoais (Art.ºs 2.º n.º 2 e 3.º 1).

E, mais ainda, deixa em evidência que

> "A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. [Concluindo que] Se os progressos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados como dados pessoais, e o Regulamento (UE) 2016/679 deve ser aplicado em conformidade."[28-29].

Isto, porque a identificação a partir de dados anónimos, ou a re-identificação de dados anonimizados, passaram a ser tecnicamente viáveis, designadamente com base nas analíticas de *Big Data*[30].

---

28 Ao que acresce o explicitado pela Comissão Europeia na sua Comunicação, interpretativa, "Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados não pessoais na União Europeia" (COM(2019) 250 final, de 25 de maio de 2019), com referências específicas e desenvolvidas quanto a esta questão, concluindo que "[…] se determinados dados não pessoais puderem ser associados a uma pessoa de qualquer forma, tornando-os direta ou indiretamente identificáveis, devem ser considerados dados pessoais. [e, do mesmo modo] Aplicam-se as mesmas regras [as relativas ao tratamento de dados pessoais] quando a evolução da tecnologia e da análise de dados torna possível a conversão de dados anonimizados em dados pessoais."

29 Nesta matéria, é fundamental o Parecer n.º 5/2014, sobre "técnicas de anonimização", de 10 de abril, do GT 29, e, sobre a mesma, começámos por dispor das considerações de Catarina Sarmento e CASTRO (2016), sendo que, logo após a publicação do *RGPD*, esta questão foi identificada e analisada por Ana Alves LEAL (2017), a propósito das implicações da *Big Data*, entretanto, a questão foi enfrentada por A. Barreto MENEZES CORDEIRO (2018), a propósito dos limites da "identificabilidade", retomando-a A. Barreto MENEZES CORDEIRO (2020, pp. 126-131); porém, permito-me remeter para o meu estudo sobre os limites entre ambos os Regulamentos referidos, já publicado em 2020.

30 Neste mesmo sentido, com uma assertividade crescente, foi-se pronunciando o GT 29, designadamente, no Parecer n.º 7/2003, de 12 de dezembro, sobre a "reutilização de informações do setor público e a proteção dos dados pessoais", no Parecer n.º 6/2013, de 5 de junho, sobre "dados abertos e reutilização de informações do setor público (ISP)", de 5

O que nos permite concluir que, na União Europeia, vigora um limite móvel entre os "dados pessoais" e os "dados não pessoais", com uma tendência expansiva dos primeiros, à medida que a tecnologia o permita. O que exige uma atitude de prevenção e de precaução permanentes por parte de quem assume beneficiar do respetivo tratamento, com os inerentes riscos e sem exclusão das respetivas responsabilidades, retomando o antigo brocardo *cuius commoda eius et incommoda*.

Diferentemente do que sucede com a *anonimização*, a *pseudonimização* é definida pelo *RGPD*, como

> "[…] o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável" (Art.º 4.º 5).

E além de ser fortemente sugerida[31], surge qualificada como constituindo uma "medida técnica adequada para assegurar um nível de segurança adequado ao risco" (Art.º 32 n.º 1 alínea c). Mais ainda, constitui o

de junho, e, sobretudo, de um modo muito detalhado, no Parecer sobre as "técnicas de anonimização", antes referido.

31 Designadamente, no *Considerando* 26, segundo o qual, "Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica.", mas também no *Considerando* 28, "A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento [controladores] e os seus subcontratantes [operadores] a cumprir as suas obrigações de proteção de dados. A introdução explícita da «pseudonimização» no presente regulamento não se destina a excluir eventuais outras medidas de proteção de dados".

"exemplo" de "medidas técnicas adequadas […] destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento", no contexto da proteção de dados desde a conceção (Art.º 25.º n.º 1), com a sua especificação a dever constar dos "códigos de conduta" (Art.º 40.º n.º 2 alínea d) ou a ser usada para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos (Art.º 89.º n.º 1).

Porém, o problema" está em a re-identificação dos titulares dos dados pessoais ser ainda mais fácil tecnicamente que com a *anonimização*, não o só com base nas analíticas de *Big Data*, mas também por outras vias (*v.g.*, por correlações, ou por notícias de jornal, ou por dados de utilização de celulares ou de cartões de crédito ou ainda por reversão de pseudónimos através de *força bruta*), o que é assumido no próprio *RGPD*[32].

Daí a preocupação manifesta com os riscos inerentes à "inversão não autorizada da pseudonimização"[33]. O que torna necessária, ou muito

[32] Para começar, se é certo que "A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento [controladores] e os seus subcontratantes [operadores] a cumprir as suas obrigações de proteção de dados." (*Considerando* 28) e, "A fim de criar incentivos para aplicar a pseudonimização durante o tratamento de dados pessoais, deverá ser possível tomar medidas de pseudonimização, permitindo-se simultaneamente uma análise geral, no âmbito do mesmo responsável pelo tratamento [controlador] quando este tiver tomado as medidas técnicas e organizativas necessárias para assegurar, relativamente ao tratamento em questão, a aplicação do presente regulamento e a conservação em separado das informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico.", como explicita o *Considerando* 29. Aliás, estas mesmas limitações constam do Parecer do GT 29 sobre as "técnicas de anonimização", já referido.

[33] Pois "O risco para os direitos e liberdades das pessoas singulares [físicas], cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social;", *Considerando* 75, e "Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares [físicas], como a perda de controlo sobre os seus dados pessoais, a limitação

aconselhável, uma *pseudonimização forte*, incluindo os quase-identificadores, já próxima das técnicas de cifragem [*v.g.*, com uma atribuição aleatória de códigos, desligados dos dados originais, e não reversível com a mesma tecnologia.

Em contraponto, a *LGPD* toma a *anonimização* como uma referência técnica destinada a garantir a segurança do tratamento de dados pessoais e define-a como a

> "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (Art. 5, XI).

Depois, é referida a propósito da legitimidade "para a realização de estudos por órgão de pesquisa" (Art. 7, IV), mesmo no que se refere ao tratamento de dados sensíveis (Art. 11, II c), desde que indispensável, assim como "na realização de estudos em saúde pública", neste último caso a par da pseudonimização (Art. 13, caput).

Adicionalmente, também justifica a conservação dos dados anonimizados, "após o término do seu tratamento", desde que "para finalidades [de] de estudo por órgão de pesquisa" (Art. 16, II).

Além de poder ser exigida, pelo titular dos dados, ao controlador, "a qualquer momento e mediante requisição", a anonimização dos "dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei" (Art. 18 IV), ficando ainda excluída a portabilidade dos dados anonimizados (Art. 18 § 7º).

Porém e afastando-se do regime europeu, as suas limitações intrínsecas e temporais são assumidas *ab initio* pelo Legislador, por o critério indicado para a qualificação dos "dados anonimizados" ter por referência os

dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares [físicas]", *Considerando* 85.

"meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (Art. 5, III), o mesmo valendo para a *anonimização* enquanto processo, como acabámos de ver.

Mas, sendo certo que

> "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios [*i.e.*, não de ou por terceiros], ou quando, com esforços razoáveis, puder ser revertido. § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios." (Art. 12).

o que tem uma especial relevância em termos de responsabilidade civil, pois se

> "Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano." (Art. 44, Parágrafo único)

a aplicação dos "meios técnicos razoáveis e disponíveis no momento do tratamento", afastará a correspondente ilicitude (Art. 43, III), não torna sequer irregular o tratamento de esses dados, o mesmo é dizer que

> "[…] quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais [III] as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado." (Art. 44).

O mesmo vale para as sanções administrativas, sendo critério de apreciação da respetiva conduta

> "[…] a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei" (Art. 52 § 1º, VIII).

Em termos substancialmente análogos aos do *RGPD*, a *pseudonimização* é identificada como

> "[…] o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (Art. 13 § 4º).

No entanto, a mesma apenas surge a propósito da "realização de estudos em saúde pública, [para os quais] os órgãos de pesquisa poderão ter acesso a bases de dados pessoais", como uma alternativa, menos exigente, à *anonimização* (Art. 13, caput). Embora podendo empregue em geral, ao ser uma das possíveis

> "[…] medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão." (Art. 6, VII)

ou, mais especificamente, uma das

> "[…] medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito." (Art. 46)

Porém, ao não existir uma previsão análoga à *anonimização*, no que se relativa à determinação de regras técnicas de segurança pela autoridade nacional (Art. 12 §3º), apenas releva o poder genérico de

esta dispor "padrões técnicos mínimos", também a este propósito (§ 1º do Art. 46).

Consequentemente, fica mais difícil afastar a ilicitude em caso de incidente de segurança, no que se refere à responsabilidade civil e às sanções administrativas.

## 6 A *CIFRAGEM*

Esta é referida quase a medo pelo *RGPD*, o qual não a define, surgindo sempre a par da *pseudonimização*, a propósito dos tratamentos que não tenham por base o consentimento dos titulares dos dados (Art.º 7.º n.º 4 alínea e), da segurança no tratamento (Art..º 32.º n.º 1 alínea a) e, sobretudo, da isenção de responsabilidades no caso de ocorrerem incidentes de segurança (Art.º 34.º n.º 3 alínea a), sempre que

> "O responsável pelo tratamento [controlador] tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem."

Embora, devamos ter presente que a "cifragem dos dados pessoais", só por si, não baste (Art.º 32.º n.º 1 alínea a), por a mesma apenas poder garantir a confidencialidade dos dados, não as respetivas integridade e disponibilidade[34]. O que em especial a aconselha perante "grandes riscos", designadamente perante o tratamento de "categorias especiais de

[34] Daí, o caráter cumulativo das medidas de segurança (Art. 32 n.º 1), ou seja, "A capacidade de assegurar [não só] a confidencialidade, [mas também a] integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento" (b), "A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico" (c) e ainda "Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento." (d).

dados pessoais" [dados sensíveis] (Art.º 9.º), na sequência de avaliações de impacto (Art.º 35.º).

Ainda assim, a cifragem, e mesmo uma cifragem *forte*, sem acesso por quaisquer terceiros, inclusive com autorização judicial, tem vindo a ser proposta ou defendida institucionalmente na União Europeia ainda que no plano da *Soft Law*:[35].

Já na *LGPD* a cifragem não é, sequer, mencionada, embora esteja implícita quando refere que

> "No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los." (Art. 48 § 3º).

Pelo que estará só entre as

> "[…] medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito." (Art. 46)

Embora, tal como no *RGPD*, também não baste, só por si, para afastar a responsabilidade civil ou sanções administrativas, pois pode não ser viável reverter ou mitigar os efeitos do incidente de segurança (Art. 48 § 1º, VI, e § 2º, II), por sua natureza, a cifragem é a técnica mais pertinente para prevenir danos maiores, tal como se verifica no *RGPD*.

---

[35] Como ocorreu, reiteradamente, com a Declaração Conjunta da Europol e da ENISA, de 20 de maio de 2016, sobre "uma investigação criminal lícita que respeite a proteção dos dados no século XXI", a Resolução sobre "a luta contra a cibercriminalidade", do Parlamento Europeu, de 3 de outubro de 2017 (2017/2068(INI) e, mais ainda, a "Declaração sobre a cifragem e o seu impacto na proteção das pessoas singulares [físicas] relativamente ao tratamento dos seus dados pessoais na EU", de 11 de abril de 2018, do GT 29.

## REFERÊNCIAS

(Todas as hiperconexões foram verificadas no dia 20 de agosto de 2020)

ABREU, Carlos Pinto de. Breves notas sobre segurança da informação, acesso a dados e privacidade. **C&R - Revista de Regulação e Concorrência**. Lisboa, n. 35, 2018, pp. 49-78. <http://www.concorrencia.pt/vPT/Estudos_e_Publicacoes/Revista_CR/Documents/Revista_ReC_35.pdf>

ATAÍDE, Rui P. Coutinho de Mascarenhas. Direito ao esquecimento. **Cyberlaw by CIJIC**. Lisboa, n. 6, 2019. <https://www.cijic.org/wp-content/uploads/2019/05/Rui-Ata%C3%ADde_Direito-esquecimento.pdf>

BARBOSA, Mafalda Miranda. **Protecção de Dados e Direitos de Personalidade**: Uma Relação de Interioridade Constitutiva. Os Benefícios da Protecção e a Responsabilidade Civil. Estudos de Direito do Consumidor. Coimbra, n. 12, 2017, pp. 75-131. <https://www.fd.uc.pt/cdc/pdfs/rev_12_completo.pdf>

BARBOSA, Mafalda Miranda. *Data controllers e data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil. **Revista de Direito Comercial**. Lisboa, n. 2, 2018, pp. 424-494. <https://www.revistadedireitocomercial.com/data-controllers-e-data-processors>

BOTELHO, Catarina Santos. Novo Ou Velho Direito? – o direito ao esquecimento e o princípio da proporcionalidade no constitucionalismo global. **AB INSTANTIA.** Coimbra, n. 7, 2017, pp. 49-71. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3130258>

CALDAS, Gabriela. O direito à explicação no Regulamento Geral sobre a Proteção de Dados. **Anuário da Proteção de Dados. Lisboa,** 2019, pp. 37-53. <http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf>

CALVÃO, Filipa Urbano. A protecção de dados pessoais na internet: desenvolvimentos recentes. **Revista de Direito Intelectual**. Coimbra, n. 2, 2015, pp. 67-84.

CALVÃO, Filipa Urbano. O modelo de supervisão de tratamento de dados pessoais na União Europeia: da atual diretiva ao futuro regulamento. **Fórum de Proteção de Dados**, Lisboa, n. 1, 2015, pp. 36-48. <https://www.cnpd.pt/bin/revistaforum/forum2015_1/index.html#36>

CARRAPIÇO, Helena; BARRINHA, André. European Union cyber security as an emerging research and policy field. London, **European Politics and Society,** Vol. 19, n. 3, 2018, pp. 299-303. <https://www.tandfonline.com/doi/full/10.1080/23745118.2018.1430712>

CASIMIRO, Sofia Vasconcelos. O direito a ser esquecido pelos motores de busca: o Acórdão Costeja. **Revista de Direito Intelectua**l. Coimbra, n. 2, 2014, pp. 307-353.

CASTRO, Catarina Sarmento e. **Direito da Informática, Privacidade e Dados Pessoais**. Coimbra, Almedina, 2005.

CASTRO, Catarina Sarmento e. Comentário ao artigo 8.º. In SILVEIRA, Alessandra; CANOTILHO, Mariana (Eds.). **Carta dos Direitos Fundamentais da União Europeia Comentada**. Coimbra, Almedina, 2013, pp. 120-128.

CASTRO, Catarina Sarmento e. **A jurisprudência do Tribunal de Justiça da União Europeia**: o regulamento geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa. Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos, Vol. I. Coimbra, Almedina, 2016, pp. 1047-1070.

COELHO, Cristina Pimenta. Artigo 82.º - Direito de indemnização e responsabilidade. In PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra, Almedina, 2018 (a), pp. 633-37.

COELHO, Cristina Pimenta. Artigo 83.º - Condições gerais para a aplicação de coimas. In PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados.** Coimbra, Almedina, 2018 (b), pp. 637-647.

COELHO, Cristina Pimenta. Artigo 84.º - Sanções. In PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra, Almedina, 2018 (c), pp. 648-650.

CORDEIRO, A. Barreto Menezes. Dados pessoais: conceito, extensão e limites. **Revista de Direito Civil.** Coimbra, Vol. 3 n. 2, 2018 (a), pp. 297-321. <https://blook.pt/publications/publication/e38a9928dbce/>

CORDEIRO, A. Barreto Menezes. **Da responsabilidade civil pelo tratamento de dados pessoais – Working paper**. Lisboa, BLOOK, 2018 (b). <https://blook.pt/publications/publication/2ae6399f13bb/>

CORDEIRO, A. Barreto Menezes. **Direito da Proteção de Dados**. Coimbra, Almedina, 2020.

COSTA, Tiago Branco da. A responsabilidade civil decorrente da violação do Regulamento Geral sobre a Proteção de Dados. In SILVEIRA, Alessandra; ABREU, Joana R. S. Covelo; COELHO, Larissa (Eds.). **UNIO Ebook Interop 2019:** O Mercado Único Digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: Pensamento Sábio - Associação para o conhecimento e inovação / Universidade do Minho - Escola de Direito, pp. 68-77. <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf>

FERREIRA, Afonso José. *Profiling* e algoritmos autónomos: um verdadeiro direito de não sujeição. **Anuário da Proteção de Dados.** Lisboa, 2018, pp. 35-43. <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>

FREITAS, Pedro Miguel. The General Data Protection Regulation: an overview of the penalties' provisions from a Portuguese standpoint. **UNIO - EU Law Review.** Braga, Vol. 4 n. 2, 2018, pp. 99-104. <http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%204%20.%20Vol%201/Unio%204%20n.%202%20PT/Unio%204%20n.%202%20EN/Pedro%20Miguel%20Freitas%20(1).pdf>

GALANTE, Maria de Fátima. A Internet e o Direito ao Esquecimento: Análise jurisprudencial. **Data Venia - Revista Jurídica Digital**. S.l, n. 9, 2018, pp. 223-250. <http://datavenia.pt/ficheiros/edicao09/datavenia09_p223_250.pdf>

GALVÃO, Luís Neto. Comentário ao artigo 16.º do TFUE. In PORTO, Manuel Lopes; ANASTÁCIO, Gonçalo (Eds.). **Tratado de Lisboa Anotado e Comentado**. Coimbra, Almedina, 2012, pp. 252-256.

GONÇALVES, Maria Eduarda. **Direito da Informação**: novos direitos e formas de regulação na sociedade da informação. Coimbra, Almedina, 2 Ed., 2003.

GONÇALVES, Maria Eduarda. The EU Data Protection Reform and the Challenges of Big Data: tensions in the relations between technology and the law. In NETO, Luísa; RIBEIRO, Fernanda (Eds.). **IV Colóquio Luso-Brasileiro Direito e Informação - Atas**. Porto: Faculdade de Letras da Universidade do Porto, 2016, pp. 46-63. <https://view.joomag.com/direito-e-informa%c3%a7%c3%a3o-na-sociedade-em-rede-atas-direito-e-informa%c3%a7%c3%a3o-na-sociedade-em-rede-atas/0242499001470686892>

JESUS, Inês O. Andrade de. O direito à proteção de dados pessoais e o regime jurídico das transferências internacionais de dados: a proteção viaja com as informações que nos dizem respeito? Lisboa, **Anuário da Proteção de Dados - 2018**, pp. 71-90. <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>

LEAL, Ana Alves. Aspetos Jurídicos da Análise de Dados na Internet (Big Data Analytics) nos Setores Bancário e Financeiro: Proteção de Dados Pessoais e Deveres de Informação. In CORDEIRO, António Menezes, OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). **FinTech – Desafios da Tecnologia Financeira.** Coimbra, Almedina, 2017, pp. 75-202.

LOPES, Teresa Vale. Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados. Lisboa, **Anuário da Proteção de Dados - 2018**, pp. 45-69. <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>

MARQUES, João. Direito ao Esquecimento – A Aplicação do Acórdão Google pela CNPD. **Fórum de proteção de dados.** Lisboa, n. 3, 2016, pp. 44-55. <https://www.cnpd.pt/bin/revistaforum/forum2016_3/files/assets/basic-html/page-48.html>

MARTINS, José C. Lourenço. Método de Design, Implementação e Operação de um Sistema de Gestão de Segurança da Informação (V1.0). Proelium – **Revista Científica da Academia Militar**. Lisboa, A. VIII, n. 4, 2019. <https://www.academia.edu/40439061/M%C3%A9todo_de_Design_Implementa%C3%A7%C3%A3o_e_Opera%C3%A7%C3%A3o_de_um_Sistema_de_Gest%C3%A3o_de_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o_V1.0_>

MARTINS, José C. Lourenço [*et al.*]. Modelo Integrado de Atividades para a Gestão da Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais. Lisboa, **Cyberlaw by CIJIC**, n. 5, 2018. <https://www.cijic.org/wp-content/uploads/2018/03/MODELO-INTEGRADO-DE-ATIVIDADES-PARA-A-GESTÃO-DE-SEGURANCA-DA-INFORMACAO-CIBERSEGURANCA-E-PROTECCAO-DE-DADOS.pdf>

MASSENO, Manuel David. On the relevance of big data for the formation of contracts regarding package tours or linked travel arrangements, according to the new package travel directive. **Comparazione e Diritto Civile**. Salerno, n. 4, 2016, pp. 2-13. <http://www.comparazionedirittocivile.it/download/volumi/201604.pdf>

MASSENO, Manuel David. Como a União Europeia procura proteger os cidadãos--consumidores em tempos de *Big Data*. **Revista Eletrônica do Curso de Direito da UFSM**. Santa Maria, Vol. 14, n. 3. <https://periodicos.ufsm.br/revistadireito/article/view/41708/pdf>

MASSENO, Manuel David. Na borda: dados pessoais e não pessoais nos dois Regulamentos da União Europeia. In MARTINO, Antonio (Ed.). **Actas del IV Congreso Interactivo Virtual / Humanos – Máquinas - Derechos** (20 y 21 de noviembre / 2019). Buenos Aires, Astrea, 2020. <https://www.astrea.com.ar/resources/doctrina/doctrina0511.pdf>

MASSENO, Manuel David; SANTOS, Cristiana Teixeira. Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations. **MediaLaws – Rivista di diritto dei media**. Milano, n. 2, 2018, pp. 251-266. <http://www.medialaws.eu/rivista/assuring-privacy-and-data-protection-within-the-framework-of-smart-tourism-destinations/>

MASSENO, Manuel David; SANTOS, Cristiana Teixeira Santos. Personalization and Profiling of Tourists in Smart Tourism Destinations – a Data Protection perspective. **Revista Argumentum**. Marília, Vol. 20 n. 3, 2019, pp. 1215-1240. <http://ojs.unimar.br/index.php/revistaargumentum/article/view/1243/752>

MENDES, Jorge Barros. O Novo Regulamento de Proteção de Dados: as principais alterações. **Revista Luso-Brasileira de Direito do Consumo**. Curitiba, pp. 27, 2017, pp. 13-37. <https://issuu.com/editorabonijuris9/docs/revista_luso-brasileira_de_direito__d0959fdb6ee330>

MOREIRA, Sónia. A proteção das pessoas singulares no novo Regulamento Geral de Protecção de Dados Pessoais. In CALHEIROS, Clara [*et al*.] (Eds.). **Direito na Lusofonia:** Direito e Novas Tecnologias / Atas do 5º Congresso Internacional de Direito na Lusofonia. Braga, Escola de Direito Universidade do Minho / Centro de Investigação em Justiça e Governação, 2018, pp. 485-492. <http://repositorium.sdum.uminho.pt/bitstream/1822/59737/1/29-Lusofonia%20V%20RGPD%202018.pdf>

MOTA, Joana. Proteção de dados desde a conceção e por defeito. Avaliação de impacto e segurança. In CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). **FinTech II - Novos Estudos sobre Tecnologia Financeira.** Coimbra, Almedina, 2019, pp. 129-146.

MOUTINHO, José Lobo. Legislador português precisa-se. Algumas notas sobre o regime sancionatório no Regulamento Geral sobre Protecção de Dados (Regulamento (UE) 2016/679). **Fórum de proteção de dados**. Lisboa, n. 4, 2017, pp. 40-57. <https://www.cnpd.pt/bin/revistaforum/forum2017_1/files/assets/basic-html/page-40.html>

MOUTINHO, José Lobo; RAMALHO, David Silva. Notas sobre o regime sancionatório da proposta de regulamento geral sobre a protecção de dados do Parlamento Europeu e do Conselho. **Fórum de proteção de dados**. Lisboa, n. 1, 2015, pp. 18-33. <https://www.cnpd.pt/bin/revistaforum/forum2015_1/files/assets/basic-html/page-20.html>

OLIVEIRA, Madalena Perestrelo de. Definição de perfis e decisões individuais automatizadas no Regulamento Geral sobre a Proteção de Dados. In CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). **FinTech II - Novos Estudos sobre Tecnologia Financeira**. Coimbra, Almedina, 2019, pp. 61-88.

OLIVEIRA, Ricardo Rodrigues de. *What´s in a Name?* Uma Breve Análise do Nível de Protecção Adequado no Âmbito das Transferências de Dados Pessoais dos Cidadãos da União Europeia para Países Terceiros. Lisboa, **Anuário da Proteção de Dados - 2018**, pp. 119-145. <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>

PEREIRA, Alexandre L. Dias. 2018. A Proteção de Dados Pessoais e o Direito à Segurança Informática no Comércio Eletrónico. **Banca, Bolsa e Seguros.** Coimbra, n.º 3, 2013, pp. 303-329. <https://www.fd.uc.pt/bbs/wp-content/uploads/2019/01/bbs3_final_2p.pdf>

PEREIRA, Bruno; ORVALHO, João. Avaliação de Impacto sobre a Protecção de Dados. **Cyberlaw by CIJIC.** Lisboa, n. 7, 2919. <https://www.cijic.org/wp-content/uploads/2019/05/Bruno-Pereira-e-Joao-Orvalho_RGPD_Avalia%C3%A7%C3%A3o-de-Impacto-sobre-a-Prote%C3%A7%C3%A3o-de-Dados.pdf>

PICA, Luís. As Avaliações de Impacto, o Encarregado de Dados Pessoais e a Certificação no Novo Regulamento Europeu de Proteção de Dados Pessoais. Lisboa, **Cyberlaw by CIJIC**, n. 5, 2018. <https://www.cijic.org/wp-content/uploads/2018/03/3_AS-AVALIA%C3%87%C3%95ES-DE-IMPACTO-O-ENCARREGADO-DE-DADOS-PESSOAIS--E-A-CERTIFICA%C3%87%C3%83O-NO-NOVO-REGULAMENTO-EUROPEU--DE-PROTE%C3%87%C3%83O-DE-DADOS-PESSOAIS.pdf>

PINHEIRO, Alexandre Sousa. **Privacy e Protecção de Dados Pessoais**: A Construção Dogmática do Direito à Identidade Informacional. Lisboa, AAFD, 2015.

PINHEIRO, Alexandre Sousa. Apresentação do Regulamento (UE) 216/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 – Regulamento Geral de Proteção de Dados (RGPD). Lisboa, **Revista do Centro de Estudos Judiciários**, n. 1 (2018 a). pp. 303-327.

PINHEIRO, Alexandre Sousa. "Artigo 4.º - Definições". In PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra, Almedina, 2018 (b), pp. 115-204.

PINHEIRO, Alexandre Sousa. "Artigo 51.º - Autoridade de controlo". In PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra, Almedina, 2018 (c), pp. 533-535.

PINHEIRO, Alexandre Sousa. "Artigo 52.º - Independência". In PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra, Almedina, 2018 (d), pp. 535-539.

PINHEIRO, Alexandre Sousa; GONÇALVES, Carlos Jorge. Artigo 22.º - Decisões automatizadas, incluindo definição de perfis. In PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra, Almedina, 2018 (a), pp. 386-390.

PINHEIRO, Alexandre Sousa; GONÇALVES, Carlos Jorge. **A**rtigo 45.º - Transferências com base numa decisão de adequação. In PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra, Almedina, 2018 (b), pp. 504-512.

PINTO, João Ferreira. Autoridades de Controlo Independentes no (Novo) Regulamento Geral (UE) sobre a Proteção de Dados (RGPD): "The Never Never Land"? Lisboa, **Cyberlaw by CIJIC**, n. 5, 2018 <https://www.cijic.org/wp-content/uploads/2018/03/Opiniao_AUTORIDADES-DE-CONTROLO-<INDEPENDENTES--NO-NOVO-REGULAMENTO-GERAL-UE-SOBRE-A-PROTE%C3%87%C3%83O-DE--DADOS.pdf>

SAIAS, Marco Alexandre. Reforço da responsabilização dos responsáveis pelo tratamento de dados. **Revista Luso-Brasileira de Direito do Consumo**. Curitiba, n.. 27, 2017, pp. 72-90. <https://issuu.com/editorabonijuris9/docs/revista_luso-brasileira_de_direito__d0959fdb6ee330>

SILVEIRA, Alessandra; MARQUES, João. Do direito a estar só ao direito ao esquecimento. Considerações sobre a proteção de dados pessoais informatizados no Direito da União Europeia: sentido, evolução e reforma legislativa. **Revista da Faculdade de Direito da UFPR**. Curitiba, Vol. 61, n. 3, 2016, pp. 91-118. <https://revistas.ufpr.br/direito/article/view/48085/29828>

SANTOS, Luísa A. Inácio Varandas dos; MARQUES, Mário R. Monteiro. Gestão de Risco Aplicada à Segurança da Informação. **Cyberlaw by CIJIC**. Lisboa, n. 5, 2019. <https://www.cijic.org/wp-content/uploads/2019/05/Luisa-Santos-e-Mario-Marques_GEST%C3%83O-DE-RISCO-APLICADA-%C3%80-SEGURAN%C3%87A-DA-INFORMA%C3%87%C3%83O.pdf>

SANTOS, Lourenço Noronha dos. Inteligência Artificial e Privacidade. In ROCHA, Manuel Lopes; PEREIRA, Rui Soares. **Inteligência Artificial & Direito**. Coimbra, Almedina, 2020, pp. 147-159.

TEIXEIRA, Angelina. A Chave para a Regulamentação da Protecção de Dados (Das pessoas singulares). **Data Venia - Revista Jurídica Digital**. S.l., n. 1, 2016, pp. 6-32. <http://www.datavenia.pt/ficheiros/edicao06/datavenia06_p005-032.pdf>

# Capítulo III

# O RESPONSÁVEL PELO TRATAMENTO DE DADOS SEGUNDO REGULAMENTO EUROPEU

*Alexandre Libório Dias Pereira*[1]

## SUMÁRIO



## RESUMO

O responsável pelo tratamento de dados (data controller) é o destinatário principal dos deveres impostos pelo RGPD em matéria de tratamento de dados e das sanções previstas para o seu não cumprimento. É uma noção ampla que abrange pessoas singulares ou coletivas, públicas ou privadas, estabelecidas dentro ou, sendo caso disso, fora da EU. Cabe ao "responsável" respeitar os princípios relativos ao tratamento de dados pessoais e respeitar os direitos dos titulares, para além de cumprir um conjunto de obrigações previstas o RGPD, como sejam, por ex., designar representante quando não estiver estabelecido na EU, aplicar medidas técnicas e organizativas adequadas, registar os tratamentos, avaliar o impacto dos tratamentos ou, consoante os casos, designar um encarregado de proteção de dados (EPD). Este estudo passa em revistas as principais obrigações do responsável pelo tratamento de dados face ao RGPD (e bem ainda outros mecanismos ao seu dispor como a adoção de códigos de conduta ou procedimentos de certificação junto de organismos acreditados), bem como as sanções civis e administrativas a que ficam sujeitos no caso de não cumprimento desses deveres.

**Palavras-chave**: RGPD – dados pessoais – autodeterminação informacional - obrigações do responsável pelo tratamento – União Europeia

[1] Doutor em Direito e Professor Associado da Faculdade de Direito da Universidade de Coimbra, Portugal.

# 1 INTRODUÇÃO

## 1.1 O responsável pelo tratamento de dados como destinatário principal dos deveres impostos pelo Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados (RGPD)[2] regula a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, garantindo a liberdade de circulação de dados pessoais no interior da União Europeia (art. 1/1 e 3). Por dados pessoais entende-se, para efeitos do RGPD, "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)", sendo "considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" (art. 4/1).[3]

Se o titular dos dados pessoais é o sujeito principal de direitos no RGPD, o *Responsável pelo Tratamento de Dados* (RTD) é o principal sujeito de deveres e obrigações aí estabelecidos, e responsável pelas coimas e outras sanções previstas no RGDP para o não cumprimento das suas disposições e que são sensivelmente gravosas (artigos 83-84): o não cumpri-

[2] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Doravante, salvo outra indicação, os artigos e considerandos citados são do RGPD.
A Diretiva 95/46/CE foi transposta para a ordem jurídica interna pela Lei 67/98, de 26 de outubro, agora revogada pela Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RGPD.

[3] Para efeitos do RGPD, são ainda definidas certas categorias de dados, nomeadamente os dados genéticos, os dados biométricos e os dados relativos à saúde – *vide infra*. O considerando (26) esclarece que "Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica."

mento de uma ordem emitida pela autoridade de controlo a (por ex. em Portugal, a CNPD) fica sujeito a coimas até € 20 000 000 ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado (artigo 83/6).[4] Para além da responsabilidade pelo cumprimento dos princípios do tratamento de dados e do respeito pelos direitos dos seus titulares, o RGPD dedica especificamente um capítulo, o IV, ao responsável pelo tratamento e subcontratante.

## 1.2 Noção de responsável pelo tratamento de dados

O RGPD estabelece uma noção ampla de RTD, definindo-o como "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as *finalidades* e os *meios* de tratamento de dados pessoais" (art. 4/7, itálico nosso).[5] Assim, o RTD pode ser uma pessoa de direito privado, singular ou coletiva (por ex. associação, fundação, sociedade civil ou comercial, cooperativa), ou uma autoridade pública, agência ou outro organismo (por ex. uma câmara municipal, uma universidade pública, uma agência de regulação, uma entidade pública empresarial). A natureza pública ou privada da entidade é irrelevante. O que conta é saber se a entidade em causa, isolada ou conjuntamente com outras, determina as *finalidades* e os *meios* de tratamento de dados, i.e., o *para quê* e o *como*.

Ao RTD junta-se o subcontratante, entendido como qualquer pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do RTD (art. 4/8). Ambos realizam, por conseguinte, tratamento de dados, igualmente definido em termos

[4] Para consultar os números das chamadas empresas GAFA (Google, Apple, Facebook, Amazon) ver por ex. <https://www.statista.com/topics/4213/google-apple-facebook-and-amazon-gafa/>

[5] Para efeitos de determinação do RTD, acrescenta o referido preceito que, "sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro".

amplos como "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (art. 4/2).

## 1.3 Proteção de dados pessoais: do direito à vida privada ao direito à autodeterminação informativa

A proteção jurídica dos dados pessoais funda-se no direito ao respeito pela vida privada proclamado na Declaração Universal dos Direitos Humanos de 1948 (artigo 12) e consagrado com força normativa na Convenção Europeia do Direitos do Homem e das Liberdades Fundamentais de 1950 (artigo 8), e no Pacto Internacional dos Direitos Civis e Políticos de 1966 (artigo 17). Portugal aderiu à Convenção Europeia dos Direitos Humanos em 1978, na lei interna o Código Civil já consagrava, como direito de personalidade, a reserva sobre a intimidade da vida privada (artigo 80), tal como sucederia com a Constituição da República Portuguesa de 1976 (artigo 33 – posteriormente inserido no artigo sobre direitos pessoais – artigo 26), a qual dedicou um artigo à inviolabilidade do domicílio e da correspondência (artigo 34), limitando quaisquer restrições a casos e procedimentos previstos na lei e sujeitas a ordem judicial (nº 3), assim como proibindo "a ingerência das autoridades públicas na correspondência e nas telecomunicações, salvos os casos previstos na lei em matéria de processo criminal" (nº 4; vide atualmente os artigos 187 a 190 do Código de Processo Penal). Além disso, a CRP proibiu a utilização da informática para tratar dados da vida privada das pessoas (art. 35), matéria cujo principal regime se encontra atualmente no Regulamento Geral de Proteção de Dados.

Embora gerada no seio do "direito à privacidade", como é conhecido no EUA o direito à reserva da vida privada, a proteção dos dados pessoais

desenvolveu-se e adquiriu uma "vida própria", com fundamento no direito fundamental à "autodeterminação informativa", segundo a designação dada pelo tribunal constitucional federal alemão no seu acórdão de 15 dezembro de 1983, no âmbito de um processo relativo a informações pessoais coletadas durante o censo de 1983, em que o BFGH considerou que, no contexto do processamento moderno de dados, a proteção do indivíduo contra a recolha, armazenamento, uso e divulgação ilimitados de seus dados pessoais é abrangida pelo direito fundamental de cada pessoa determinar, em princípio, a divulgação e o uso dos seus dados pessoais, sujeitando esta autodeterminação informacional apenas a limitações justificadas por razões de interesse público primordial.[6]

Esse "produto da doutrina alemã tão exportado, quanto mal conhecido na sua origem"[7] seria recebido pela doutrina constitucional portuguesa, ao abrigo do artigo 35 da CRP, no sentido de o "direito à autodeterminação informativa" atribuir "a cada pessoa o direito de controlar a informação disponível a seu respeito" e se impedir a redução

---

6 Cf. Antoinette Rouvroy, Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", in **Reinventing Data Protection?,** ed. Gutwirth (et al.), Springer, Dordrecht, 2009, p. 45-76. Para desenvolvimentos, v. Paulo Mota Pinto, "O direito à reserva sobre a intimidade da vida privada", **Boletim da Faculdade de Direito de Coimbra 64** (1993) 479-586; Catarina Sarmento e Castro, **Direito da informática, privacidade e dados pessoais**, Coimbra, Almedina, 2005; Alexandre Sousa Pinheiro, **Privacy e protecção de dados pessoais:** a construção dogmática do direito à identidade informacional, Lisboa, AAFDL, 2015, *passim*. Sobre a proteção de dados antes do RGPD Garcia Marques, Lourenço Martins, **Direito da Informática,** 2.ª ed., Coimbra, Almedina, 2006, p. 129-313, 422-442, 330-391; Helena Moniz, "Notas sobre a protecção de dados pessoais perante a informática: o caso especial dos dados pessoais relativos à saúde", **Revista Portuguesa de Ciência Criminal 7/2** (1997) 231-298; Maria Eduarda Gonçalves, **Direito da Informação - Novos Direitos e Formas de Regulação na Sociedade da Informação**, 2.ª ed., Coimbra, Almedina, 2003, p. 82-111, 173-183; Juan Pablo Aparício Vaquero, Alfredo Batuecas Caletrío (coord.), **En torno a la privacidad y la protección de datos en la sociedad de la información**, Granada. Comares, 2015; Alexandre Dias Pereira, "A proteção dos dados pessoais no direito português, em especial no setor da saúde", in Algunos desafios en la proteccion de datos personales, org. Alfredo Batuecas Caletrio, Juan Pablo Aparicio Vaquero, Madrid, Comares, 2018. Para comentários ao RGPD, J. López Calvo, **Comentarios al Reglamento Europeo de Protección de Datos**, Madrid, Sepin, 2017; Alexandre Sousa Pinheiro (coord)., **Comentário ao Regulamento Geral de Proteção de Dados,** Almedina, Coimbra, 2018.

7 Alexandre Sousa Pinheiro, **Privacy e protecção de dados pessoais**, cit., p. 825 (propondo em alternativa à proteção de dados pessoais a designação direito à "identidade informacional").

da pessoa a mero "objeto de informação"[8]. Assim, a autodeterminação informativa confere à pessoa, por um lado, um *"direito ao segredo* (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes)" e, por outro, "um *direito à reserva* (proibição de revelação)".[9] Na jurisprudência, o direito à autodeterminação informativa foi consagrado em diversos acórdãos do Tribunal Constitucional[10]. O Supremo Tribunal de Justiça consagrou igualmente este direito à "autodeterminação informativa" em diversos casos[11], encontrando-se a figura também em acórdãos dos Tribunais de Relação[12].

De igual modo, o Tribunal Europeu dos Direitos do Homem acolheu o direito à autodeterminação informacional. No acórdão *Satakunnan Markkinapörssi Oy and Satamedia Oy c. Finlândia*, o TEDH considerou que o artigo 8.º da Convenção estabelece "o direito a uma forma de autodeterminação informacional" contra ingerência no exercício do seu direito à vida privada resultantes de recolha, processamento e disseminação coletiva dos seus dados pessoais.[13]

A afirmação do direito à "autodeterminação informativa" contra a redução da pessoa a mero objeto de informação não impede, todavia,

---

8 J.J. Gomes Canotilho & Vital Moreira, **Constituição da República Portuguesa Anotada**, vol. 1, 4.ª ed., Coimbra, Coimbra Editora, 2007, p. 551

9 Joaquim de Sousa Ribeiro, "A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas", in **Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho**, vol. III, Coimbra Editora, p. 853-859.

10 Cf. acórdão n° 442/2007, de 14 agosto de 2007, proc. n.º 815/2007 (considerando que o sigilo bancário não integra a esfera íntima da vida privada) e acórdão n.º 403/2015, proc. 773/15, de 17 de setembro de 2015 (considerando o direito à autodeterminação informativa como manifestação, juntamente com o direito à solidão e o direito ao anonimato, do direito ao livre desenvolvimento da personalidade previsto no artigo 26 da CRP).

11 Acórdão de uniformização de jurisprudência n.º 2/08, de 13 de fevereiro de 2008, proc. n.º 894/07-3, e acórdão de 16 de outubro de 2014, proc. no. 679/05.7TAEVR.E2.S1 (Helena Moniz)

12 Cf. também os acórdãos do Tribunal da Relação do Porto, de 31 de maio de 2006, proc. 0111584, do Tribunal da Relação de Coimbra, de 6 de abril de 2010, proc. 120-C/2000.C1, e do Tribunal da Relação de Évora, de 14 de setembro de 2017, proc. 2829/16.9T8PTM-B.E1, in www.dgsi.pt.

13 *Satakunnan Markkinapörssi Oy and Satamedia Oy c. Finlândia* [GC], § 137, 27 de junho de 2017.

o reconhecimento do valor económico dos dados pessoais e que considerados bens transacionáveis, por ex. como forma de pagamento de serviços digitais[14], defendendo-se, por isso, que deveriam ser objeto de um acordo internacional entre os EUA e a UE com vista a promover o seu fluxo transatlântico[15], e ainda que os dados pessoais, enquanto valores de exploração, não podem ser excluídos do direito da concorrência, designadamente do abuso de posição dominante, na medida em que podem constituir recursos essenciais da economia digital[16].

## 1.4 Âmbito territorial de aplicação do RGPD para efeitos de determinação do RTD

O RGPD delimita o seu âmbito de aplicação territorial (art. 3) no sentido de abranger o tratamento de dados pessoais:

1. efetuado no contexto das atividades de um estabelecimento[17] de um RTD ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União;

---

[14] Cf. B. Sloot, F.Z. Borgesius, "Google and Personal Data Protection", in **Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models**, ed. A. Lopez-Tarruela, Hague, Asser/Springer, 2012, 75-111; A. Franceschi, A. Lehmann, "Data as tradeable commodity and new measures for their protection", *The The Italian Law Journal* 1/1 (2015) 51-72.

[15] Margaret Byrne Sedgewick, "Transborder data privacy as trade", **California Law Review** 105/5 (2017) 1513-1542.

[16] Vijay Bishnoi, "Data protection law: An inhibition in enforcement and promotion of competition law", **European Competition Law Review 40/1** (2019) 34-40, alertando para o facto de que excluir o controlo sobre dados pessoais do direito da concorrência significa reforçar a posição das empresas dominantes na economia digital das "GAFA", para além do potencial de alavancagem que representam para atividades tradicionais.

[17] O RTD com estabelecimentos em vários Estados-Membros tem estabelecimento principal no local onde se encontra a sua administração central na União, a menos que as decisões sobre as finalidades e os meios de tratamento dos dados pessoais sejam tomadas noutro estabelecimento do responsável pelo tratamento na União e este último estabelecimento tenha competência para mandar executar tais decisões, sendo neste caso o estabelecimento que tiver tomado as referidas decisões considerado estabelecimento principal (art. 4/16).

2. de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a) a oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento[18]; ou b) o controlo

[18] O considerando (23) esclarece que "A fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio *web* do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União."
Em sede de competência judiciária, para saber se um vendedor pela Internet «dirige» a sua atividade ao Estado-Membro do domicílio do consumidor, na aceção do artigo 15/1-c) do Regulamento 44/2001, de 22 de dezembro de 2000, relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial (entretanto revogado e substituído pelo Regulamento 1215/2012 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2012), o Tribunal de Justiça da União Europeia decidiu, no acórdão *Pammer e Hotel Alpenhof*, de 7 de dezembro de 2010 (proc. apensos C585/08 e C144/09, ECLI:EU:C:2010:740), ser "necessário apurar se, antes da eventual celebração de um contrato com o consumidor, resulta desses sítios na Internet e da atividade global do comerciante que este pretendia estabelecer relações comerciais com consumidores domiciliados num ou vários EstadosMembros, incluindo o do domicílio do consumidor, no sentido de que estava disposto a com eles contratar./ Os elementos seguintes, cuja enumeração não é exaustiva, podem constituir indícios que permitem considerar que o comerciante dirige a sua atividade ao EstadoMembro do domicílio do consumidor: a natureza internacional da atividade, a menção de itinerários a partir de outros EstadosMembros para chegar ao local onde o comerciante está estabelecido, a utilização de uma língua ou moeda diferentes das habitualmente utilizadas no EstadoMembro em que o comerciante está estabelecido, com a possibilidade de reservar e confirmar a reserva nessa língua, a menção de números de telefone com a indicação de um indicativo internacional, a realização de despesas num serviço de referenciação na Internet para facilitar aos consumidores domiciliados noutros Estados-Membros o acesso ao sítio do comerciante ou a um sítio do seu intermediário, a utilização de um nome de domínio de primeiro nível diferente do do Estado-Membro em que o comerciante está estabelecido e a menção de uma clientela internacional constituída por clientes domiciliados em diferentes Estados-Membros. Cabe ao juiz nacional apurar se existem esses indícios. / Pelo contrário, é insuficiente a simples acessibilidade do sítio na Internet do comerciante ou do intermediário no EstadoMembro do domicílio do consumidor. O mesmo se aplica à menção de um endereço eletrónico e de outros elementos ou à utilização de uma

do seu comportamento, desde que esse comportamento tenha lugar na União[19];

3. por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público, por ex. no âmbito de uma missão diplomática ou num posto consular de um Estado-Membro, como refere o considerando (25).[20]

## 1.5 Exclusão de atividades pessoais ou domésticas

As atividades pessoais ou domésticas não são abrangidas pelo RGPD. O considerando (18) esclarece que o RGPD "não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma atividade profissional ou comercial. As atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades. Todavia, o presente regulamento é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas."

Assim, por exemplo, a atividade dos utilizadores de redes sociais como o *Facebook* ou o *Instagram*, não estão sujeitos ao RGPD, mas a em-

língua ou moeda que sejam habitualmente utilizadas no Estado-Membro em que o comerciante está estabelecido."

19 Segundo o considerando (24), "A fim de determinar se uma atividade de tratamento pode ser considerada «controlo do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes."

20 O recurso à computação em nuvem para o tratamento de dados não prejudica o âmbito de aplicação do RGPD. Sobre a questão do tratamento de dados pessoais em ambiente de computação em nuvem, *vide* P. Blume, "Data Protection in the Cloud", **Computer Law Review International 2011/3**, 76-80; W.K. Hon, J. Hörnle, C. Millard, "Data protection jurisdiction and Cloud Computing – when are cloud users and providers subject to EU Data protection law? The Cloud of Unknowing", **International Review of Law, Computers & Technology 26/2-3** (2012) 129-164.

presa "Facebook Inc." já é considerada RTD para efeitos do RGPD. Ora, como o RGPD não prejudica a aplicação da Diretiva 2000/31/CE sobre, nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviço previstas nos seus artigos 12 a 15 (art. 2/4), os operadores de redes sociais ou de plataformas de partilha de conteúdos em linha, não são considerados prestadores intermediários de serviços para efeitos do respetivo regime de responsabilidade estabelecido na diretiva sobre comércio eletrónico[21].

## 2 DEVERES DO RESPONSÁVEL PELO TRATAMENTO DE DADOS (*DATA CONTROLLER*)

### 2.1 O dever de respeitar os princípios de tratamento de dados pessoais

No leque de deveres a cargo do RTD surge à cabeça o de respeitar os princípios relativos ao tratamento de dados pessoais estabelecidos no RGPD, a saber: a licitude, lealdade e transparência, a limitação das finalidades, a minimização dos dados, a exatidão, a limitação da conservação, e a integridade e confidencialidade (art. 5/1). Aliás, a responsabilidade do RTD pelo cumprimento dos princípios do tratamento de dados pessoais é, também, um desses princípios, o da responsabilidade, fazendo recair sobre o RTD o ónus da prova do cumprimento dos referidos princípios (art. 5/2).[22]

A licitude do tratamento pode resultar de consentimento do titular de dados ou da sua necessidade em sede contratual, cumprimento de obrigação jurídica do responsável, defesa de interesses vitais do titular ou de terceiro, exercício de funções públicas ou autoridade pública

---

21 Sobre tema, Mafalda Miranda Barbosa, "Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil", **Revista Bolsa, Banca e Seguros 3** (2018) 215-6, em nota.

22 Em sede de responsabilidade por danos é o RTD quem terá que "provar que de modo algum é responsável pelo evento que deu causa aos danos" (art. 82/3), ao contrário da regra geral da responsabilidade extracontratual.

do responsável[23], ou interesses legítimos do responsável ou de terceiro (art. 6).[24]

## 2.2 O consentimento para o tratamento de dados pessoais

O consentimento deve ser demonstrável, específico, livre e livremente revogável (art. 7). Para ser livre, o consentimento não deve ser condição *sine qua non* de prestação de um serviço, se o tratamento de dados pessoais não for necessário para o efeito[25].

---

[23] O fundamento jurídico previsto no direito da EU ou interno pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento em conformidade com o capítulo IX

[24] Nos termos do considerando (46), "Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana." Além disso, o considerando (48) informa que "O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta." Sobre o tema, A. Barreto Menezes Cordeiro, "O tratamento de dados pessoais fundado em interesses legítimos", **Revista de Direito e Tecnologia 1/1** (2019) 1-31.
A Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), estabelece no artigo 13/1, relativamente a comunicações não solicitadas que a utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de correio eletrónico para fins de comercialização direta apenas poderá ser autorizada em relação a assinantes que tenham dado o seu *consentimento prévio* (no direito interno, vide o artigo 13-A da Lei 41/2004, de 18 de agosto).

[25] Nos termos do considerando (42), "Em conformidade com a Diretiva 93/13/CEE do Conselho (1), uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com

Por outro lado, na oferta direta de serviços da sociedade da informação a crianças, o tratamento de dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos, embora os EM possam reduzir até 13 anos a idade para consentir (art. 8). Cabe ao RTD implementar medidas técnicas de controlo da idade do menor, operação que envolverá, só por si, o tratamento de dados pessoais do menor.[26]

O tratamento de categorias especiais de dados – "dados sensíveis"[27] – está sujeito a uma proibição geral, pelo que apenas é admitido excecionalmente verificados determinados requisitos específicos. Por ex. a proteção de interesses vitais só justifica o tratamento de dados se o titular estiver incapaz de consentir. Por outro lado, é reservada aos Estados-Membros a possibilidade de manterem ou imporem novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde (art. 9/4).[28] A

conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado." Por seu turno, segundo o considerando (43), "Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução."

26 Segundo o considerando (51): "O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular."

27 Dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

28 Os primeiros (*genéticos*) são definidos como "os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa" (art. 4/13). Os segundos (biométricos) consistem em "dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa

importância destes dados retira alcance à unificação visada pelo RGPD, e compromete a almejada liberdade de circulação de dados no interior da União Europeia.

## 2.3 O dever de respeitar os direitos do titular dos dados

O RTD deve respeitar os direitos do titular de dados. Desde logo o direito à *transparência* das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados. Para o efeito deve prestar informações por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos, de forma concisa, transparente, inteligível e de fácil acesso, gratuita, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. O RGPD especifica as informações a facultar consoante os dados pessoais sejam ou não recolhidos junto do titular (art. 13 e 14).

Depois, no exercício do direito de acesso, o titular dos dados deve poder saber que dados, para que fins, durante quanto tempo, de que modo, é feito o tratamento e a quem se destinam os dados (art. 15). O RTD fornece uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o RTD pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente (art. 15/3).[29]

pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos" (art. 4/15). Por último, os dados relativos à saúde, são "os dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde" (art. 4/15). Sobre tema, Filipe Miguel Cruz de Albuquerque Matos, "O Regulamento de Protecção de Dados Pessoais (2016/679) no contexto dos desafios da actividade seguradora — o caso particular dos seguros de saúde", **Revista Bolsa, Banca e Seguros 3** (2018) 51-122.

29 Segundo o considerando (63), "Quando possível, o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais. (…) Quando o responsável proceder ao tratamento de grande quantidade de informação relativa ao titular dos dados, deverá poder

São ainda direitos do titular de dados o direito de retificação e de apagamento (ou direito a ser esquecido)[30] (art. 16), o direito à limitação do tratamento (art. 17 e 18), o direito de portabilidade dos dados (art. 20)[31] e o direito de oposição ao tratamento e a decisões individuais automatizadas (art. 21).

---

solicitar que, antes de a informação ser fornecida, o titular especifique a que informações ou a que atividades de tratamento se refere o seu pedido."

30 Este "direito a ser esquecido" foi afirmado pelo Tribunal de Justiça da União Europeia no acórdão de 13 de maio de 2014, proc. C131/12, *Google Spain SL e Google Inc c. Associação Espanhola de Dados Pessoais (AEPD)* c. *Mário Costeja Gonzalez* (ECLI:EU:C:2014:317). No sentido de que se trata antes de um "direito à desassociação" nos motores de pesquisa na internet, Filipa Calvão, "A protecção de dados pessoais na internet: desenvolvimentos recentes", **Revista de Direito Intelectual, 2015/2,** 67-84. Sobre o acórdão *Google Spain,* ver também por ex. Indra Spiecker, "A new framework for information markets: Google Spain", **Common Market Law Review, 52** (2015) 1033-1058; Sofia de Vasconcelos Casimiro, "O direito a ser esquecido pelos motores de busca: o Acórdão Costeja", **Revista de Direito Intelectual, 2014/2**, 307-353. No sentido de que o direito ao esquecimento, enquanto "direito geral de eliminação de dados pessoais", em especial na Internet, não tem equivalente na lei nem na jurisprudência dos Estados Unidos da América, Dário Moura Vicente, Sofia de Vasconcelos Casimiro, "A proteção de dados pessoais na Internet à luz do Direito Comparado", **Revista de Direito Intelectual, 2018/2,** 45-90, 67. A propósito do direito comparado registe-se no direito britânico a elaboração jurisprudencial de um novo ilícito, o chamado "tort of misuse of personal information", por ex. no caso *Naomi Campbell* c. *The Mirror*, e o critério da "expetativa razoável de privacidade": *v.* Ian Cram, **The right to respect for private life:** *digital challenges, a comparative-law perspective – The United Kingdom*, European Parliamentary Research Service, Bruxelas, October 2018, 14-20.
Mais recentemente, no acórdão de 24 de Setembro, proc. C507/17, *Google c. CNIL* (EU:C:2019:772), o Tribunal de Justiça da União Europeia concluiu que "o operador de um motor de busca não tem de efetuar [a] supressão de referências em todas as versões do seu motor, devendo fazêlo nas versões deste que correspondem a todos os EstadosMembros, e isto, se necessário, em conjugação com medidas que, embora satisfaçam as exigências legais, permitam efetivamente impedir ou, pelo menos, desencorajar seriamente os internautas que efetuam uma pesquisa a partir do nome da pessoa em causa dentro de um dos EstadosMembros de, através da lista de resultados exibida após essa pesquisa, aceder às hiperligações que são objeto desse pedido."

31 O direito à portabilidade está também previsto na Lei das Comunicações Eletrónicas (Lei 5/2004, de 10 de fevereiro, com alterações posteriores) e no Regulamento 58/2005, de 18 de agosto, da ANACOM (alterado várias vezes), que estabelece os princípios e regras aplicáveis à portabilidade nas redes de comunicações públicas (Regulamento da Portabilidade), e no Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho de 14 de junho de 2017 relativo à portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno. Sobre o direito à portabilidade ver por ex. Vítor Palmela Fidalgo, "O direito à portabilidade de dados pessoais", **Revista de Direito e Tecnologia 1/1** (2019) 89-135.

O exercício destes direitos pelo titular gera obrigações para o RTD, nomeadamente, no que respeita à retificação ou ao apagamento, o dever de comunicar "a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais […], salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado" (art. 19).[32]

## 2.4 DEVER DE APLICAR MEDIDAS TÉCNICAS E ORGANIZATIVAS ADEQUADAS

O RTD de aplicar *medidas técnicas e organizativas adequadas* (consoante a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares) para assegurar e comprovar a conformidade do tratamento com o RGPD, devendo rever e atualizá-las consoante as necessidades (art. 24). Para demonstrar o cumprimento das suas obrigações o RTD pode utilizar o cumprimento de códigos de conduta ou de procedimentos de certificação aprovados nos termos do RGPD (arts. 41 e 42).

Depois, o RTD deve adotar medidas técnicas e organizativas adequadas, como a *pseudonimização*, no sentido da proteção de dados *desde a conceção e por defeito*. Por exemplo, essas medidas devem assegurar que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares (art. 25/1-2). O cumprimento desta obrigação pode fazer-se através de um procedimento de certificação aprovado nos termos do RGPD (art. 42).

---

[32] Todavia, os direitos do titular são limitados, nomeadamente por *razões de interesse público*. Segundo o considerando (71), "a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de *controlo e prevenção de fraudes e da evasão fiscal*, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular."

No caso de as finalidades e os meios de tratamento serem determinados conjuntamente por dois ou mais responsáveis, dá-se uma situação de *responsáveis conjuntos* pelo tratamento, respondendo todos solidariamente sem prejuízo do acordo de divisão interna de responsabilidades (art. 26).

## 2.5 Dever de designação de representante na União

Os responsáveis pelo tratamento ou dos subcontratantes não estabelecidos na União devem *designar por escrito um representante*[33] na União, salvo se forem atividades ocasionais e que não envolvam o tratamento em larga escala de dados sensíveis, ou realizadas por autoridades ou organismos públicos (art. 27).[34] O RTD só pode recorrer a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas a cumprir o RGPD e respeite os direitos do titular dos dados (art. 28).

---

[33] Por *representante* entende-se "uma pessoa singular ou coletiva estabelecida na União que, designada por escrito pelo responsável pelo tratamento ou subcontratante, nos termos do artigo 27º, representa o responsável pelo tratamento ou o subcontratante no que se refere às suas obrigações respetivas nos termos do" RGPD (art. 4/17).

[34] Segundo o considerando (80), "Sempre que um responsável pelo tratamento ou um subcontratante não estabelecidos na União efetuarem o tratamento de dados pessoais de titulares de dados que se encontrem na União, e as suas atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares de dados na União, independentemente de a estes ser exigido um pagamento, ou com o controlo do seu comportamento na medida que o seu comportamento tenha lugar na União, o responsável pelo tratamento ou o subcontratante deverão designar um representante, a não ser que o tratamento seja ocasional, não inclua o tratamento, em larga escala, de categorias especiais de dados pessoais, nem o tratamento de dados pessoais relativos a condenações penais e infrações, e não seja suscetível de implicar riscos para os direitos e liberdades das pessoas singulares, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento ou se o responsável pelo tratamento for uma autoridade ou organismo público. (…) *O representante deverá ser explicitamente designado por um mandato do responsável pelo tratamento ou subcontratante, emitido por escrito*, que permita ao representante agir em seu nome no que diz respeito às obrigações que lhes são impostas pelo presente regulamento" (*itálico nosso*).

## 2.6 Dever de manter um registo dos tratamentos

O RTD tem o dever de manter um registo por escrito de todas as atividades de tratamentos efetuados, especificando as informações como o seu nome e contactos, e do seu representante e EPD, as finalidades do tratamento, as categorias de titulares de dados, dados pessoais, e destinatários, as transferências, prazos de apagamento dos dados, e descrição das medidas técnicas e organizativas de segurança (art. 30). Ficam isentos os RTD com menos de 250 trabalhadores, a menos que tratem "dados sensíveis" ou relativos a condenações penais (art. 30/5).

## 2.7 Dever de assegurar um nível de segurança adequado ao risco

O RTD tem o dever de aplicar medidas técnicas e organizativas para assegurar um nível de segurança adequado ao risco, incluindo a pseudonomização e a cifragem de dados, a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, e um processo para testar, apreciar e avaliar regularmente a eficácia dessas medidas (art. 32). A prova do cumprimento desta obrigação pode ser feita pelo cumprimento de um código de conduta ou de um procedimento de certificação aprovados conforme o RGPD (art. 40 e 42).[35]

## 2.8 Dever de cooperar com a autoridade de controlo, incluindo o dever de notificação

O RTD tem o dever de cooperação com a autoridade de controlo (art. 31). Desde logo, o RTD deve notificar, em princípio no máximo de 72 horas,

[35] O regime jurídico da cibersegurança foi aprovado pela Lei 46/2018, de 13 de agosto, que transpõe a Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Sobre o tema, Alexandre L. Dias Pereira, "Proteção do consumidor e segurança informática no comércio eletrónico", **Revista Bolsa, Banca e Seguros 3** (2018) 303-329.

uma violação de dados pessoais à autoridade de controlo (art. 33). Se a violação de dados pessoais implicar um elevado risco para os direitos e liberdades das pessoas singulares, o RTD deve comunicar esse facto ao titular dos dados, a menos que tenha usado técnicas como a cifragem (art. 34). Como informa o considerando (85), "Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares."

## 2.9. Dever de avaliação de impacto

O RTD deve avaliar o impacto sobre a proteção de dados por ex. em caso de tratamento sistemático de dados sensíveis em larga escala (art. 35).[36] Se concluir que o tratamento envolve um elevado risco para os direitos e liberdades das pessoas singulares, o RTD tem o dever de proceder a consulta prévia **à** autoridade de controlo (art. 36).

O RGPD ressalva ainda que a lei interna de cada Estado-Membro pode inclusivamente sujeitar a autorização prévia da autoridade de controlo o tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública (art. 36/6).[37]

---

[36] Nos termos do considerando (91), "O tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado. Nesses casos, a realização de uma avaliação de impacto sobre a proteção de dados não deverá ser obrigatória." A referência ao hospital juntamente com os profissionais de saúde isentos do dever de avaliação de impacto resulta manifestamente de um lapso de redação da versão portuguesa do RGPD, como se constata comparando-a com as versões inglesa, francesa ou castelhana.

[37] Sobre a avaliação de impacto, ver o documento do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, Orientações relativas à Avaliação de Impacto sobre a Proteção de

## 2.10 Dever de designar um Encarregado da Proteção de dados (EPD/DPO)

O RTD deve designar um *Encarregado de Proteção de Dados* (EPD) se for autoridade ou organismo público (podendo ser comum a vários organismos ou autoridades, tendo em conta a respetiva estrutura organizacional e dimensão), ou exercer atividade que exija o controlo de titulares de dados ou o tratamento de dados em grande escala (art. 37). Segundo as Orientações do Grupo de Trabalho do Artigo 29[38], consideram-se de grande escala: "o tratamento de dados de doentes no exercício normal das atividades de um hospital; tratamento de dados de viagem das pessoas que utilizam o sistema de transportes públicos de uma cidade (p. ex., através de passes de viagem); o tratamento em tempo real de dados de geolocalização de clientes de uma cadeia de restauração rápida internacional para fins estatísticos por parte de um subcontratante especializado na prestação desses serviços; o tratamento de dados de clientes no exercício normal das atividades de uma companhia de seguros ou de um banco; o tratamento de dados pessoais para fins de publicidade comportamental por um motor de busca; o tratamento de dados (conteúdo, tráfego, localização) por operadoras telefónicas ou por fornecedores de serviços de internet". Pela negativa, não são de grande escala os tratamentos de dados de doentes pacientes por um médico e os de dados pessoais relacionados com condenações penais e infrações por um advogado.

Sendo um grupo empresarial[39], o RTD pode designar um único EPD se houver um EPD facilmente acessível a partir de cada estabeleci-

---

Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Adotadas em 4 de abril de 2017, Revistas e adotadas pela última vez em 4 de outubro de 2017, WP 248 rev.01.

38 Sobre o EPD, ver o documento do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, Orientações sobre os encarregados da proteção de dados (EPD). Adotadas em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017, WP 243 rev.01, p. 10.

39 Por "empresa", entende-se "uma pessoa singular ou coletiva que, independentemente da sua forma jurídica, exerce uma atividade económica, incluindo as sociedades ou associações que exercem regularmente uma atividade económica". Segundo o consideran-

mento (art. 37/2). O RTD deve publicar os contactos do EPD e comunica-los à autoridade de controlo. O RTD deve apoiar o EPD e respeitar a sua autonomia, no desempenho das suas funções de zelar pelo cumprimento do RGPD; funções essas que pode cumular com outras funções e atribuições que não resultem num conflito de interesses, o que cabe ao RTD assegurar (art. 38/8).[40]

do (22), "A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto." Por grupo empresarial entende-se um grupo composto pela empresa que exerce o controlo e pelas empresas controladas (art. 4/18-19). O considerando (36) informa que "A existência e utilização de meios técnicos e de tecnologias para o tratamento de dados pessoais ou as atividades de tratamento não constituem, em si mesmas, um estabelecimento principal nem são, portanto, um critério definidor de estabelecimento principal. […]Sempre que o tratamento dos dados seja efetuado por um grupo empresarial, o estabelecimento principal da empresa que exerce o controlo deverá ser considerado o estabelecimento principal do grupo empresarial, exceto quando as finalidades e os meios do tratamento sejam determinados por uma outra empresa."

40 O Conselho Geral da Ordem dos Advogados emitiu Parecer no sentido de os advogados estarem "impedidos de exercer o mandato forense ou a consulta jurídica, para entidades para quem exerçam, ou tenham exercido as funções de encarregado de Proteção de dados" (proc. n.º 14/PP/2018-G). No essencial, cabendo ao EPD fiscalizar o RTD, não teria condições deontológicas para, ao mesmo tempo, lhe prestar o mandato forense ou a consulta jurídica. O Parecer mereceu a crítica acertada de A. Barreto Menezes Cordeiro, "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", **Revista da Ordem dos Advogados 78/I-II** (2018) 17-38. Tendo em conta que *Orientações do Grupo de Trabalho do Art. 29.º sobre o Encarregado de Proteção de Dados*, p. 19, dão como exemplo de possível conflito de interesses se "um EPD externo for chamado a representar o responsável pelo tratamento ou o subcontratante perante os tribunais no âmbito de processos respeitantes a questões de proteção de dados", defende o referido Autor que "Fora do universo da proteção de dados importa verificar, casuisticamente, a existência ou não de conflitos de interesses concretos" (*ibidem,* 38). Com efeito, o referido Parecer estabelece um impedimento geral que nos parece manifestamente excessivo. Tal como o Estatuto Deontológico dos Advogados pretende assegurar a autonomia e independência do advogado, o mesmo sucede com o RGPD relativamente ao EPD, estabelecendo que o RTD assegura que o EPD "não recebe instruções relativamente ao exercício das suas funções" e que "não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções" (art. 38/3). O Parecer reconhece a autonomia do EPD, mas o entendimento sobre natureza das funções de fiscalização do EPD não têm, a nosso, base no RGPD. Dá a entender que nesse papel, e no desempenho da função de cooperação com a autoridade de controlo, o EPD seria obrigado a denunciar eventuais infrações cometidas pelo RTD à autoridade de controlo, o que não é manifestamente o caso, tanto mais que está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, sem prejuízo de poder de contatar e solicitar o parecer da autoridade de controlo (cf. *Orientações do Grupo de Trabalho do Art. 29.º sobre o Encarregado de Proteção de Dados*, cit., p. 21)

## 2.11 Adoção de código de conduta e obtenção de certificação de proteção de dados (facultativo)

As associações de RTD elaboram códigos de conduta (art. 40). A supervisão destes códigos pode ser efetuada por um organismo que tenha um nível adequado de competência relativamente ao objeto do código e esteja acreditado para o efeito pela autoridade de controlo competente (art. 41).[41] O organismo de *supervisão acreditado* pode suspender ou excluir um RTD que não cumpra o código de conduta.

Os RTD podem cumprir *procedimentos de certificação* em matéria de proteção de dados, bem como adotar selos e marcas de proteção de dados, para efeitos de comprovação da conformidade dos tratamentos com o RGPD (art. 42). A certificação, válida em princípio por três anos, é efetuada por organismo de certificação acreditado pela autoridade de controlo ou diretamente por esta (art. 43).

## 2.12 Transferências de dados para fora da União Europeia

O RTD pode transferir dados pessoais para países terceiros ou organizações internacionais, se atuar em conformidade com o RGPD (art. 44). Para o efeito, o RTD pode fazer transferências com base numa decisão da Comissão de adequação do nível de proteção do país terceiro (art. 45).[42]

---

41 Segundo o considerando (77) "As orientações sobre a execução de medidas adequadas e sobre a comprovação de conformidade pelos responsáveis pelo tratamento ou subcontratantes, em especial no que diz respeito à identificação dos riscos relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos riscos, poderão ser obtidas nomeadamente recorrendo a códigos de conduta aprovados, a certificações aprovadas, às orientações fornecidas pelo Comité ou às indicações fornecidas por um encarregado da proteção de dados."

42 Ver o "US-EU Privacy Shield" e a Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

Na falta de uma tal decisão de adequação, a transferência pode ocorrer se o RTD apresentar garantias adequadas e os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes (art. 46). Essas garantias adequadas podem resultar, por exemplo, de *regras vinculativas aplicáveis às empresas* (art. 47), de cláusulas-tipo de proteção de dados adotadas ou aprovadas pela Comissão, de código de conduta ou procedimento de certificação, acompanhados de compromissos vinculativos e com força executiva – cf. considerando (108).

Além disso, mesmo na ausência de uma decisão de adequação ou de garantias adequadas (por ex. regras vinculativas aplicáveis às empresas), as transferências para países terceiros podem ser efetuadas para situações específicas, nomeadamente se houver consentimento explícito e informado do titular dos dados, se a transferência for necessária em sede contratual ou por razões de interesse público ou para proteger interesses vitais de pessoa incapaz de consentir, para além de outras derrogações para situações específicas previstas no art. 49.

## 2.13 Derrogações (liberdade de expressão e informação, acesso aos documentos da AP, em contexto laboral)

A liberdade de expressão e de informação, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária, justifica derrogações específicas ao regime geral de tratamento de dados (art. 85), tal como sucede com o tratamento e acesso do público aos documentos oficiais (art. 86), o tratamento do número de identificação nacional (art. 87) e o tratamento no contexto laboral (art. 88). Além disso, são previstas garantias e derrogações relativas ao tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos (art. 89). Por exemplo a pseudonimização só é obrigatória se os referidos fins puderem ser alcançados desse modo.

De igual modo, podem ser estabelecidas derrogações aos direitos de acesso, retificação, limitação e oposição na medida em que esses di-

reitos possam tornar impossível ou prejudicar gravemente a realização dos fins específicos de investigação científica ou histórica ou fins estatísticos e que tais derrogações sejam necessárias para a prossecução desses fins (art. 89/2).

## 2.14 Obrigação de sigilo

O RGPD não prejudica a obrigação de sigilo a que o RTD esteja sujeito, por lei interna do Estado-membro, relativamente aos dados pessoais que tenha recebido no âmbito de uma atividade abrangida por essa obrigação de sigilo ou em resultado da mesma (art. 90). Por ex., o Regulamento de Deontologia Médica[43] encarrega os responsáveis pelo tratamento da informação de saúde de tomarem as "providências adequadas à proteção da sua confidencialidade, garantindo a segurança das instalações e equipamentos, o controlo no acesso à informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais" (art. 37). O dever de confidencialidade da informação de saúde é reiterado no capítulo VII do Regulamento sobre a telemedicina (arts. 46 a 49).[44]

# 3 Aplicação privada dos direitos relativos aos dados pessoais

Os titulares de dados pessoais têm o direito de reclamar junto de uma autoridade de controlo (art. 77), bem como o direito de agir judicialmente contra uma autoridade de controlo (art. 78) e/ou contra um responsável pelo tratamento ou um subcontratante (art. 79). Para o efeito, podem ser representados por organismo sem fins lucrativos, incluindo uma associação de defesa dos consumidores.

---

43 Regulamento n.º 707/2016, de 21 de julho.

44 Cf. Alexandre L. Dias Pereira, "A proteção dos dados pessoais no direito português, em especial no setor da saúde", in **Algunos desafios en la proteccion de datos personales**, org. Alfredo Batuecas Caletrio, Juan Pablo Aparicio Vaquero, Comares, Madrid, 2018.

O RGPD garante expressamente o direito a obter uma indemnização por danos causados pela violação de dados pessoais (art. 82). Os titulares dos dados deverão ser *integral e efetivamente* indemnizados pelos danos que tenham sofrido. Sempre que os responsáveis pelo tratamento ou os subcontratantes estiverem envolvidos no mesmo tratamento, cada um deles deverá ser responsabilizado pela totalidade dos danos causados (responsabilidade solidária). Porém, se os processos forem apensos num único processo judicial, em conformidade com o direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido. Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento (art. 82/4-5).

O titular de dados pode intentar uma ação judicial contra o RTD perante os tribunais do seu Estado-Membro de residência ou os tribunais do Estado-Membro de estabelecimento do RTD, indica o considerando (145), ressalvando, todavia, a competência exclusiva destes últimos se o RTD "for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos".

Para ser exonerado de responsabilidade, o RTD ou o subcontratante terá que provar o facto que causou o dano não lhe é de modo algum imputável [considerando (146) e art. 82/3].

## 4 CONCLUSÃO

O RGPD impõe um conjunto de deveres sobre o RTD, entendido como "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com ou-

tras, determina as finalidades e os meios de tratamento de dados pessoais" (art. 4/7).[45]

O RGPD aplica a tratamentos de dados feitos por RTD estabelecido na União Europeia, tratamentos "ativos" (mediante oferta de bens ou serviços ou controlo de comportamento) de dados de pessoas residentes na EU, independentemente do lugar de estabelecimento do RTD, e tratamentos efetuados em lugar no qual se aplica o direito da EU por força do direito internacional público. São excluídas do âmbito de aplicação do RGPD as atividades exclusivamente pessoais ou domésticas (grosso modo, consumidores, incluindo usuários de redes sociais, mas não as dos provedores dessas plataformas [considerando (18)].

O RDT deve respeitar os princípios relativos ao tratamento de dados pessoais, como sejam (1) a licitude, lealdade e transparência; (2) a limitação das finalidades; (3) a minimização de dados; (4) a exatidão; (5) a limitação da conservação; (6) integridade e confidencialidade; (7) a responsabilidade do RTD pelo "data compliance". Nos requisitos de licitude, surge à cabeça a exigência de consentimento demonstrável, específico, livremente dado e revogável. Sendo que, relativamente a tratamento de dados no contexto de serviços da sociedade da informação, o RGPD esta-

[45] Por ex. o operador de um sítio de comércio eletrónico é considerado um RTD para efeitos do RGPD, como já antes apontado, ao abrigo da Diretiva 95/46/CE. Cf. Grupo de trabalho do artigo 29 sobre proteção de dados, Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante, WP 169, fevereiro de 2010. Para uma exposição sucinta sobre o impacto do RGPD nos sítios dos operadores de comércio eletrónico, v. Michaela Weigl, "The EU General Data Protection Regulation's Impact on Website Operators and eCommerce", **Computerrecht-international 4** (2016), 102-108; e em especial nas empresas que fazem tratamento intensivo de dados, Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies", **Computer Law & Security Review** 34 (2018) 134–153. Por outro lado, antes da aprovação do RGPD, o Tribunal de Justiça da União Europeia considerou o operador de motor de busca na Internet como RTD: "a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexálas automaticamente, armazenálas temporariamente e, por último, pôlas à disposição dos internautas por determinada ordem de preferência deve ser qualificada de «tratamento de dados pessoais», […] quando essas informações contenham dados pessoais", devendo o operador desse motor de busca ser considerado "responsável" pelo dito tratamento: acórdão de 13 de maio de 2014, proc. C131/12, *Google Spain SL e Google Inc c. Associação Espanhola de Dados Pessoais (AEPD)* c. *Mário Costeja Gonzalez.*

belece a idade mínima para consentir em 16 anos, embora permita que os Estados-Membros baixem até aos 13 anos. Além disso, o próprio RGOD confere autorização legal para certos tratamentos, por razões, nomeadamente, de proteção de interesses vitais do titular, interesse público, formação e execução de contratos, interesses legítimos, ou cumprimento de obrigação legal.

O RTD deve respeitar os direitos dos titulares, a saber: transparência do tratamento, acesso (e cópia), retificação e apagamento ("direito a ser esquecido"), limitação do tratamento, portabilidade, oposição à definição de perfis e de sujeição a decisões individuais automatizadas.[46] Por outro lado, o RTD deve: (1) designar representante quando não estiver estabelecido na EU, salvo para atividades ocasionais e sem tratamento em larga escala de dados sensíveis; (2) aplicar medidas técnicas e organizativas adequadas para cumprir o RGPD e proteger os dados desde a conceção e por defeito (por ex. pseudonimização); (3) abster-se de disponibilizar, sem intervenção humana, dados a um número indeterminado de pessoas singulares; (4) registar os tratamentos, especificando determinados elementos (podendo estar isentas deste dever as PME); (5) cooperar com a autoridade de controlo; (6) aplicar medidas de segurança informática adequadas ao risco; (6) notificar a autoridade de controlo e, havendo perigo elevado para direitos do titular, comunicar-lhe uma violação de dados; (7) avaliar o impacto e, em certos casos, consultar previamente a autoridade de controlo (estando isentos do dever de avaliação de impacto certos profissionais como advogados e médicos); (8) designar encarregado de proteção de dados (EPD), quando efetue tratamentos em "grande escala", designadamente quando o tratamento de dados faz parte das atividades principais do responsável, como sucede com os hospitais[47].

---

[46] Sobre a transparência ao nível da configuração dos algoritmos de definição de perfis e da automatização de decisões com base nesses algoritmos, Giovanni de Gregorio, "From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society", **European Journal of Legal Studies 11/2** (2019) 65-103.

[47] Cf. Orientações do Grupo de Trabalho do Art. 29 sobre o Encarregado de Proteção de Dados, p. 8.

O RTD pode comprovar o cumprimento do RGPD pela adoção de códigos de conduta ou mediante procedimento de certificação junto de organismos acreditados, incluindo obtenção de selos e marcas de proteção de dados, aprovados pela Comissão Europeia ou pelo Autoridade de controlo, consoante os casos.

As transferências para países terceiros ou organizações internacionais podem ser feitas com base: a) numa decisão de adequação da Comissão ou, na falta disso, b) em regras vinculativas aplicáveis às empresas, c) cláusulas-tipo de proteção de dados adotadas pela Comissão, d) código de conduta ou procedimento de certificação aprovados em conformidade com o regulamento, i.e., acompanhados de compromissos vinculativos e com força executiva.

O RGPD prevê ainda derrogações para tratamentos de dados para fins jornalísticos, expressão literária, artística ou científica, aquivo de interesse público, investigação científica ou histórica, ou estatísticos, beneficiam de derrogações aos princípios de tratamento de dados.

Finalmente, o RGPD consagra a possibilidade de aplicação privada dos direitos sobre dados pessoais, no sentido de que o RTD deve indemnizar integral e efetivamente os titulares de dados pelos danos sofridos, sendo solidária a responsabilidade no caso de tratamento conjunto por vários responsáveis ou subcontratante, sem prejuízo de ação de regresso. Além disso, o RTD fica sujeito ao pagamento de avultadas coimas, que podem a 4% do seu volume de negócios, e de um modo geral deve cumprir as determinações das autoridades competentes.

## REFERÊNCIAS

APARÍCIO VAQUERO, Juan Pablo, Alfredo Batuecas Caletrío (coord.), **En torno a la privacidad y la protección de datos en la sociedad de la información**, Granada. Comares, 2015

BARBOSA, Mafalda Miranda - "Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil", **Revista Bolsa, Banca e Seguros** 3 (2018) 147-216

BISHNOI, Vijay - "Data protection law: An inhibition in enforcement and promotion of competition law", **European Competition Law Review** 40/1 (2019) 34-40

BLUME, P. - "Data Protection in the Cloud", **Computer Law Review International** 2011/3, 76-80.

CALVÃO, Filipa Urbano - "A protecção de dados pessoais na internet: desenvolvimentos recentes", **Revista de Direito Intelectual**, 2015/2, 67-84

CANOTILHO, J.J. Gomes, Vital Moreira, **Constituição da República Portuguesa Anotada**, vol. 1, 4.ª ed., Coimbra, Coimbra Editora, 2007

CASIMIRO, Sofia de Vasconcelos - "O direito a ser esquecido pelos motores de busca: o Acórdão Costeja", **Revista de Direito Intelectual**, 2014/2, 307-353

CASTRO, Catarina Sarmento e - **Direito da informática, privacidade e dados pessoais**, Coimbra, Almedina, 2005

CORDEIRO, A. Barreto Menezes - "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", **Revista da Ordem dos Advogados** 78/I-II (2018) 17-38 - "O tratamento de dados pessoais fundado em interesses legítimos", Revista de Direito e Tecnologia 1/1 (2019) 1-31

CRAM, Ian - *The right to respect for private life: digital challenges, a comparative-law perspective – The United Kingdom*, **European Parliamentary Research Service**, Brussels, October 2018

FIDALGO, Vítor Palmela - "O direito à portabilidade de dados pessoais", **Revista de Direito e Tecnologia** 1/1 (2019) 89-135.

FRANCESCHI, A., A. Lehmann - "Data as tradeable commodity and new measures for their protection", **The The Italian Law Journal** 1/1 (2015) 51-72

GONÇALVES, Maria Eduarda - **Direito da Informação - Novos Direitos e Formas de Regulação na Sociedade da Informação**, 2.ª ed., Coimbra, Almedina, 2003

GREGORIO, Giovanni de - "From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society", **European Journal of Legal Studies** 11/2 (2019) 65-103

GRUPO DE TRABALHO do Artigo 29.º para a Proteção de Dados, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determi-

nam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Adotadas em 4 de abril de 2017, Revistas e adotadas pela última vez em 4 de outubro de 2017, WP 248 rev.01

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, Orientações sobre os encarregados da proteção de dados (EPD). Adotadas em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017, WP 243 rev.01

HON, W.K., J. Hörnle, C. Millard, "Data protection jurisdiction and Cloud Computing – when are cloud users and providers subject to EU Data protection law? The Cloud of Unknowing", **International Review of Law, Computers & Technology,** 26/2-3 (2012) 129-164

LOPES, J. Seabra - "A proteção da privacidade e dos dados pessoais na sociedade de informação", **Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa,** UCP, Lisboa, 2002, 779

LÓPEZ CALVO, J. - **Comentarios al Reglamento Europeo de Protección de Datos,** Madrid, Sepin, 2017

MARQUES, Garcia, Lourenço Martins - **Direito da Informática**, 2.ª ed., Coimbra, Almedina, 2006

MATOS, Filipe Miguel Cruz de Albuquerque - "O Regulamento de Protecção de Dados Pessoais (2016/679) no contexto dos desafios da actividade seguradora — o caso particular dos seguros de saúde", **Revista Bolsa, Banca e Seguros** 3 (2018) 51-122

MONIZ, Helena - "Notas sobre a protecção de dados pessoais perante a informática: o caso especial dos dados pessoais relativos à saúde"; **Revista Portuguesa de Ciência Criminal** 7/2 (1997) 231-298

PEREIRA, Alexandre Libório Dias - "A proteção dos dados pessoais no direito português, em especial no setor da saúde", in Algunos desafios en la proteccion de datos personales, org. Alfredo Batuecas Caletrio, Juan Pablo Aparicio Vaquero, Madrid, Comares, 2018 - "Proteção do consumidor e segurança informática no comércio eletrónico", **Revista Bolsa, Banca e Seguros** 3 (2018) 303-329

PINHEIRO, Alexandre Sousa - Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional, Lisboa, AAFDL, 2015 -

Coord.., **Comentário ao Regulamento Geral de Proteção de Dados**, Almedina, Coimbra, 2018.

PINTO, Paulo Mota - "O direito à reserva sobre a intimidade da vida privada", **Boletim da Faculdade de Direito de Coimbra** 64 (1993) 479-586

RIBEIRO, Joaquim de Sousa - "A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas", in **Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho**, vol. III, Coimbra Editora, 853-859

ROUVROY, Antoinette, Yves Poullet,- "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", in **Reinventing Data Protection?**, ed. Gutwirth (et al.), Springer, Dordrecht, 2009, 45-76

SEDGEWICK, Margaret Byrne, "Transborder data privacy as trade", **California Law Review** 105/5 (2017) 1513-1542

SLOOT, B., F.Z. Borgesius - "Google and Personal Data Protection", in **Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models**, ed. In A. Lopez-Tarruela, Hague: Asser/Springer, 2012, 75-111.

SPIECKER, Indra - "A new framework for information markets: Google Spain", **Common Market Law Review**, 52 (2015) 1033-1058

TIKKINEN-PIRI, Christina, Anna Rohunen, Jouni Markkula - "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies", **Computer Law & Security Review** 34 (2018) 134–153

VICENTE, Dário Moura, Sofia de Vasconcelos Casimiro - "A proteção de dados pessoais na Internet à luz do Direito Comparado", **Revista de Direito Intelectual,** 2018/2, 45-90

WEIGL, Michaela - "The EU General Data Protection Regulation's Impact on Website Operators and eCommerce", **Computerrecht-international** 2016/4, 102-108.

# Seção II

## As novas fronteiras tecnológicas e os desafios para a proteção dos dados pessoais

# Capítulo 1

# NOVAS GUERRAS EM NOVOS CAMPOS DE BATALHA: o RGPD EUROPEU e as gigantes tecnológicas NORTE-AMERICANAS

*Sofia de Vasconcelos Casimiro*[1]

## SUMÁRIO



## RESUMO

Este texto apresenta o RGPD como um instrumento da União Europeia para reconquistar o controlo dos dados pessoais no contexto internacional. Dadas as suas ambições extraterritoriais, o RGPD desafia a supremacia dos Estados Unidos da América, que tem tirado proveito das suas gigantes tecnológicas. São analisados três casos de estudo, passando em revista temas como a CLOUD Act, Safe Harbor, Privacy Shield, os casos Schrems I e II, bem como os bloqueios ao TikTok e WeChat de forma a ilustrar como a legislação, acordos internacionais e ordens executivas são as armas das novas guerras que se travam em novos campos de batalha.

**Palavras-chave:** dados pessoais; RGPD; âmbito territorial; extraterritorialidade; CLOUD Act; Schrems; Porto Seguro; Escudo de Proteção da Privacidade; ordens executivas; TikTok; WeChat

*"A suprema arte da guerra é*
*de subjugar o inimigo sem lutar"*
*SUN TZU, A Arte da Guerra, Universo*
*dos Livros, São Paulo, 2010, p. 12*

[1] Doutorada por Queen Mary, University of London, Intellectual Property Research Institute. Mestre em Direito pela Faculdade de Direito da Universidade de Lisboa. Professora da Faculdade de Direito da Universidade de Lisboa. Professora da Academia Militar.

## 1 O RGPD E O SEU ÂMBITO DE APLICAÇÃO TERRITORIAL

O Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, abreviadamente designado Regulamento Geral sobre a Proteção de Dados ou pelas siglas RGPD, surge como uma oportunidade ímpar para a União Europeia exercer supremacia num novo domínio de poder: o domínio dos dados pessoais, considerados o novo petróleo[2].

Ao reforçar o controlo dos dados pessoais associados ao espaço da União Europeia, iniciado com a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (adiante designada simplesmente "Diretiva de Proteção de Dados Pessoais"), o RGPD devolve à União Europeia algum controlo sobre novas atividades que proliferam no ciberespaço e que assentam sobretudo no tratamento de dados pessoais.

Com efeito, o ciberespaço tem-se revelado um terreno fértil para o desenvolvimento de novos modelos de negócio que, sob uma aparente gratuitidade de produtos e, sobretudo, de serviços oferecidos, procede à recolha massiva de dados pessoais dos seus utilizadores. A gratuitidade é aparente, uma vez que os dados pessoais são comercializados diretamente a terceiras entidades que deles retiram enorme valor, quer pela criação de um perfil de consumidor que lhes permite direcionar ofertas de produtos e serviços, quer pela comercialização de serviços de direcionamento de outros conteúdos destinados a influenciar os utilizadores nas mais diversas áreas, quer ainda pela criação e comercialização de estudos com base nos dados recolhidos, entre muitos outros. Os utilizadores dos serviços pagam, assim, e bem, os serviços que utilizam. Os utilizadores pagam com dados pessoais.

---

[2] Veja-se, entre muitas outras obras com essa referência, LOGAN KUGLER, "The war over the value of personal data", **Communications of the ACM,** volume 61, 2, fevereiro 2018, pp. 17-19.

Com vista a ampliar, na maior extensão possível, o controlo sobre os dados pessoais, a União Europeia atribuiu ao RGPD um amplo âmbito de aplicação territorial. Esta matéria encontra-se prevista no artigo 3.º do RGPD, que estabelece vários critérios de aplicação do Regulamento. Um dos critérios assenta no local onde se desenvolve a atividade, do responsável pelo tratamento dos dados ou do subcontratante, que justifica o tratamento dos dados pessoais. Caso esse local se situe na União Europeia, o tratamento dos dados ficará sujeito ao RGPD, ainda que seja efetuado fora do espaço da União. Outro critério assenta no local onde os titulares dos dados residem, devendo ser aplicado o RGPD se residirem na União, desde que o tratamento seja efetuado para oferecer produtos ou serviços na União ou para monitorizar o seu comportamento na União. Por fim, enquanto terceiro e último critério, o RGPD aplica-se quando o responsável pelo tratamento esteja fora da União, num lugar em que se aplique o Direito de um Estado-Membro por força do Direito Internacional Público.

Analisados os três critérios, verifica-se que houve uma clara intenção de alargar os critérios de fixação do âmbito territorial vigentes na legislação europeia de proteção de dados anterior ao RGPD, correspondente à Diretiva de Proteção de Dados Pessoais, que foi revogada pelo Regulamento.

## 2 A APLICABILIDADE DO RGPD A GIGANTES TECNOLÓGICAS SEDEADAS NOS ESTADOS UNIDOS DA AMÉRICA

A aplicabilidade do RGPD a entidades sedeadas fora da União Europeia seria previsível e expectável. Tal já se verificava durante a vigência da Diretiva de Proteção de Dados Pessoais[3] quando o tratamento fosse

[3] Durante a vigência desta Diretiva, os critérios de âmbito territorial referiam-se à aplicação do Direito nacional de cada Estado-Membro, uma vez que o instrumento legislativo utilizado, a Diretiva, não é diretamente aplicado e necessita de ser transposto para o Direito nacional. Pelo contrário, o RGPD, sendo diretamente aplicável sem carecer de transposição, dispõe quanto ao âmbito territorial da sua própria aplicação.

efetuado no âmbito de uma atividade desenvolvida por um estabelecimento situado no espaço da União[4].

A maior extensão do âmbito territorial operada pelo RGPD verifica-se em relação a tratamentos efetuados por entidades sedeadas fora da União Europeia no âmbito de atividades desenvolvidas por estabelecimentos situados fora do espaço da União. Este critério tem permitido a aplicação do RGPD a tratamentos de dados pessoais efetuados por gigantes tecnológicas que, numa primeira análise, fugiriam às malhas da legislação europeia. Neste ponto, o RGPD demonstra ambições de extraterritorialidade que poderão ser, por vezes, de difícil execução.

Uma grande parte das gigantes tecnológicas tem sede nos Estados Unidos da América, podendo, assim, ser referenciadas como empresas norte-americanas, ainda que tenham estabelecimentos no território da União Europeia[5]. É o caso da Amazon.com, Inc., Apple, Inc., Alphabet, Inc. (empresa-mãe da Google LLC. e outras subsidiárias), Facebook, Inc., e Microsoft Corporation.

Estas gigantes tecnológicas são responsáveis pelo tratamento de muitos milhões de milhões de dados pessoais de titulares de dados europeus. Com o tratamento de dados de cidadãos europeus, estas gigantes tecnológicas lucram triliões[6]. Com efeito, estas e muitas ou-

---

4 Esta previsão encontrava-se no artigo 3.º da Diretiva. Este artigo previa ainda a extensão do âmbito de aplicação aos responsáveis pelo tratamento que, tendo embora o estabelecimento fora do território da Comunidade, recorressem a meios situados nesse território, exceto quando esses meios só fossem utilizados para trânsito dos dados. Estes critérios somavam-se ao da aplicabilidade quando o responsável do tratamento tivesse o estabelecimento num lugar fora da Comunidade em que se aplicasse o Direito de um Estado-Membro por força do Direito Internacional Público. Sobre a interpretação deste artigo 3.º pelo Comité Europeu para a Proteção de Dados, veja-se o documento intitulado "Diretrizes 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3.º)", disponível em https://edpb.europa.eu.

5 A maioria das gigantes tecnológicas norte-americanas tem estabelecimento na Irlanda, por causa da política fiscal extremamente vantajosa deste país.

6 Vejam-se, por exemplo, os valores de lucro da Facebook, Inc., por cada utilizador na União Europeia no artigo de JOHN NAUGHTON, "Can democracies stand up to Facebook? Ireland may have the answer", **The Guardian**, 26 de setembro de 2020, disponível em www.theguardian.com.

tras empresas tecnológicas norte-americanas procedem à recolha de dados dos utilizadores dos seus serviços, quer quando estes ativamente tomam a iniciativa de fornecer os seus dados, enviando-os para essas empresas, quer quando, mais habitualmente, ao aderirem a esses serviços aceitam que lhes sejam recolhidos os dados que geram com a utilização dos mesmos. Neste último caso, o comportamento do utilizador é passivo e a recolha resulta, geralmente, do facto de o utilizador não desativar as opções de recolha de dados gerados pela utilização dos serviços[7]. Neste exemplo, muito usual, a informação não é ativamente fornecida pelo utilizador, mas é gerada por este e automaticamente recolhida para diversas finalidades.

Uma vez que os utilizadores são pessoas singulares, ainda que possam em algumas situações atuar em representação de pessoas coletivas, quando a recolha de informação permita identificar, direta ou indiretamente, o utilizador a quem se refira a informação, essa recolha consistirá inevitavelmente num tratamento de dados pessoais à luz do RGPD[8].

A recolha de dados pessoais através das tecnologias de informação tem vindo a tornar-se mais complexa, sofisticada e devidamente planificada. Nas décadas anteriores, a recolha era feita de forma um pouco limitada ou caótica. Alternava-se entre processos de recolha de muitos poucos dados, como o nome e o endereço eletrónico do utilizador, retirando pouca utilidade da recolha, ou, pelo contrário, processos de recolha de praticamente todos os dados gerados, tornando impraticável a extração de qualquer utilidade desses dados, face à sua grande quantidade. As atuais ferramentas especificamente desenvolvidas para o tratamento dos grandes bancos de dados eletrónicos, designados *big data*, alteraram diametralmente o cenário. Estas ferramentas permitem extrair todo

7 As técnicas habitualmente utilizadas para recolha de dados procuram aproveitar a passividade do titular dos dados, muito embora, na maioria das vezes, seja exigido o consentimento ativo desse titular para que o tratamento de dados tenha lugar de uma forma lícita.

8 Sobre o conceito de dados pessoais e tratamento de dados pessoais, veja-se o artigo 4.º do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

o tipo de informação a partir de uma imensidão desorganizada de dados informatizados[9]. Estas ferramentas conferiram utilidade a milhões de *terabytes*, onde se incluem dados pessoais, permitindo o seu processamento e organização de forma a conhecer perfis psicológicos e antecipar tendências de opinião, tipo de estímulos que possibilitam alterações de opinião e até de comportamento.

Com o aperfeiçoamento das tecnologias que procedem ao tratamento dos dados pessoais, aperfeiçoaram-se igualmente as técnicas de direcionamento dessa recolha. Para além de se conseguir conhecer quais os conteúdos acedidos pelo utilizador, quando foram acedidos, durante quanto tempo foram acedidos, a partir de onde foram acedidos, consegue-se também conhecer qual a reação do utilizador aos conteúdos, quais os sentimentos nele gerados e, nomeadamente, se determinaram mudança de humor e o comportamento que se seguiu, entre outra informação.

O quadro legal europeu relativo à proteção de dados pessoais estabelece, como um dos seus alicerces, o consentimento do titular dos dados como o principal fundamento de legitimidade para o tratamento de dados pessoais. Por outras palavras, para que um tratamento de dados pessoais tenha lugar será necessário, por regra, obter o prévio consentimento da pessoa singular a quem respeitam os dados pessoais.

Para que esteja em conformidade com o RGPD, o consentimento do titular dos dados tem de corresponder a uma manifestação de manifestação de vontade livre, específica, informada e explícita[10]. Cada um destes adjetivos carrega consigo exigências distintas que devem ser rigorosamente observadas e que merecem uma atenção particular. Por exemplo, só existirá liberdade de consentir num tratamento de dados caso não seja imposta ao titular de dados uma penalidade quando

---

9 Veja-se, por todos, VOLKER BRUHL, **Big Data, Data Mining, Machine Learning and Predictive Analytics – A Conceptual Overview,** CFS Working paper, n.º 617, 2019, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3321195.

10 *Vide* os artigos 4.º/11) e 7.º do RGPD, bem como o respetivo considerando 32.

se oponha ao tratamento de dados, a não ser que essa penalidade seja uma consequência incontornável da falta de tratamento dos dados. Ilustrando com casos da vida real, seria admissível impedir o acesso a um serviço de localização das farmácias mais próximas de um condutor se esse condutor recusasse dar o seu consentimento para o tratamento dos seus dados de geolocalização. Contudo, já não seria admissível impedir o acesso a esse mesmo serviço caso o condutor consentisse no tratamento dos seus dados de geolocalização mas recusasse que, adicionalmente, se tratassem os dados sobre os seus rendimentos anuais ou sobre o tipo de programas televisivos que assiste. Conforme determina o n.º 4 do artigo 7.º do RGPD, que dá um importante contributo para a interpretação do que seja um consentimento livre, "Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato".

O consentimento tem ainda de ser específico, no sentido em que não poderá ser dado de forma geral, para qualquer finalidade e abrangendo quaisquer dados pessoais. O titular dos dados tem de consentir para cada tipo de tratamento, para cada grupo de dados, para cada transmissão, entre outros.

As exigências de liberdade e especificidade do consentimento encontram-se intimamente ligadas à exigência de um consentimento informado. Para que possa dar o seu consentimento, o titular dos dados tem de ser devidamente esclarecido em relação aos vários aspetos do tratamento dos dados. Esta exigência assume uma relevância tal que o RGPD lhe dedica inteiramente os artigos 13.º e 14.º, para descrever pormenorizadamente as informações que devem ser prestadas e as condições dessa prestação.

O consentimento tem ainda, de ser explícito, exigindo um ato positivo claro, não se bastando com uma omissão de atuação. Ao contrário do que se tornou prática habitual em muitos *websites*, não se poderá presumir que a mera navegação consubstanciará um consentimento para

o tratamento de dados, assim como não se deverá aceitar a utilização de uma opção pré-validada que o titular dos dados deva desmarcar para recusar o seu consentimento. Este aspeto foi destacado por um Acórdão do Tribunal de Justiça da União Europeia (TJUE) de outubro de 2019[11].

Estas exigências impostas pelo RGPD, que são apenas algumas das que decorrem deste instrumento legal, impõem complexidades e despesas acrescidas aos processos de recolha de dados e constituem-se, inevitavelmente, como obstáculos a essa recolha, levando à diminuição do volume de dados pessoais que, cumprindo todas as exigências, podem ser licitamente tratados.

Entende-se, pois, que as gigantes tecnológicas norte-americanas demonstrem alguma resistência ao cumprimento do RGPD, à semelhança do que se verificou em relação ao cumprimento da legislação nacional dos Estados-Membros durante a vigência da Diretiva de Proteção de Dados Pessoais. Ainda durante a vigência desta Diretiva assinalaram-se alguns braços de ferro entre aquelas gigantes tecnológicas e alguns Estados-Membros em matéria respeitante à lei aplicável.

A este propósito, é ilustrativo o processo que opôs a autoridade de controlo alemã à Facebook, Inc., pela forma como esta empresa violava, no entender da autoridade de controlo, a lei alemã. A Facebook, Inc., invocou que a lei alemã não era aplicável, sustentando que se sujeitava antes à lei irlandesa, correspondente à lei do local onde a empresa tinha um estabelecimento no espaço da Comunidade. Num tribunal inferior a Facebook, Inc., saiu vencedora, tendo-se entendido que a lei aplicável ao tratamento de dados realizado por esta sociedade na Alemanha era a lei irlandesa[12]. Contudo, em sede de recurso, o tribunal superior alemão inverteu a decisão e, argumentando que o tratamento de dados em causa não era realizado no âmbito das atividades do estabelecimento da Facebook, Inc., situado na Irlanda, mas da sede nos Estados Unidos da Améri-

[11] Ac. do TJUE de 1 de outubro de 2019, proferido no âmbito do processo C-673/17, que envolveu a empresa alemã Planet49 GmbH.

[12] Decisão de 22 de abril de 2013, do tribunal alemão administrativo (*Oberverwaltungsgericht Schleswig*).

ca, e uma vez que a empresa utilizava meios automatizados situados na Alemanha para efetuar o tratamento de dados nesse país, determinou que a lei alemã era a lei aplicável[13].

Durante a vigência da Diretiva de Proteção de Dados Pessoais as leis nacionais da Comunidade divergiam ainda substancialmente entre si, pelo que a luta nos tribunais incidia muitas vezes sobre qual, de entre as leis nacionais da Comunidade seriam aplicáveis ou, como geralmente pretendiam as empresas norte-americanas, sobre se não seriam antes aplicáveis as leis do lugar da respetiva sede.

As empresas norte-americanas que procedam ao tratamento de dados pessoais têm um evidente interesse na aplicabilidade da lei do lugar da sede, por contraposição à aplicação da Diretiva de Proteção de Dados Pessoais ou, atualmente, do RGPD. Com efeito, a legislação dos Estados Unidos da América nesta matéria é tradicionalmente muito mais permissiva para os que pretendam proceder ao tratamento de dados, não comungando do extremo rigor das exigências do RGPD[14], ainda superior ao da Diretiva. Se é verdade que a Diretiva oferecia alguma margem, ainda que mínima, para que se entendesse que a legislação dos Estados-Membros não era aplicável, sobretudo quando o tratamento dos dados não fosse efetuado no âmbito da atividade de um estabelecimento situado num desses Estados-Membros, o RGPD tem a ambição de se aplicar a todos os tratamentos de dados que tenham uma conexão com a União Europeia, ainda que efetuados noutro território por um empresa com sede ou estabelecimento fora da União. Empresas norte-americanas como a Amazon.com, Inc., a Apple, Inc., a Alphabet, Inc. (Google), a Facebook, Inc., e a Microsoft Corporation ficam necessariamente sujeitas à aplicação do RGPD e devem cumpri-lo rigorosamente.

---

13 Acórdão de 12 de fevereiro de 2014 proferido pelo tribunal de recurso de Berlim (*Langericht Berlin*) no âmbito do processo 5 U 42/12.

14 Para uma visão abrangente e aprofundada de Direito Comparado em matéria de proteção de dados pessoais, no contexto específico da Internet, incluindo uma análise do regime de proteção de dados nos Estados Unidos da América e em vários Estados-Membros da União Europeia, vide DÁRIO MOURA VICENTE e SOFIA DE VASCONCELOS CASIMIRO (Coord.), **Data Protection in the Internet,** volume 38 da coleção Ius Comparatum - Global Studies in Comparative Law, Springer, Suíça, 2020.

## 3 A GUERRA PELOS DADOS; O NOVO PROTECIONISMO

A aprovação do RGPD representou um importante marco numa guerra silenciosa que se tem vindo a travar a nível internacional. A referência à Sociedade da Informação reflete uma sociedade que elege a informação como o seu mais valioso recurso. Entende-se, por isso, que os Estados procurem estimular a criação e a obtenção de informação e, sobretudo, o seu domínio sobre a informação na maior extensão possível. Este propósito tem gerado uma verdadeira guerra pelos dados, nas mais diversas vertentes. A oposição entre protecionismo e liberalismo volta a estar atual neste contexto. Se os conceitos se referiam tradicionalmente à transação de produtos materiais, direcionam-se agora, sobretudo, para a transação de produtos imateriais.

O RGPD representa, em nosso entender, um claro pendor protecionista da União Europeia na forma de gerir os seus dados, alicerçado embora em direitos fundamentais. A força da aplicabilidade do RGPD é mais forte ao atender à aceção europeia do direito à privacidade e ao que se tem vindo a desenvolver como um direito à proteção dos dados pessoais[15], ao abrigo da Carta dos Direitos Fundamentais da União Europeia[16]. Estes fundamentos têm justificado uma aplicação apertada ao cumprimento do RGPD e uma forte censura social a atividades que contrariem os princípios nele plasmados. Várias gigantes tecnológicas norte-americanas têm vindo a ser sancionadas ao abrigo deste Regulamento e há investigações em curso quanto à conformidade das suas atividades com o mesmo. A multa que foi aplicada à Google pela Commission Nationale de l'Informatique et des Libertés (CNIL), a autoridade francesa de proteção de dados, em 2019, no valor então recorde de 50

[15] A questão de saber se este direito se autonomizou face ao direito à privacidade tem vindo a ser alvo de estudos. Veja-se, entre outros, MARIA TZANOU, "Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right", **International Data Privacy Law**, 2013, Vol. 3, 2, pp. 88-99, e, ainda, DÁRIO MOURA VICENTE e SOFIA DE VASCONCELOS CASIMIRO, *op.cit*..

[16] Vejam-se os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia.

milhões de euros[17], é disso ilustrativa, bem como a multa aplicada à Facebook, Inc., pelo Information Commissioner's Office (ICO), a autoridade britânica de proteção de dados, também em 2019, no valor de 500.000 euros pelo papel desta empresa no escândalo resultante do tratamento de dados de milhões dos seus utilizadores, sem o seu consentimento, pela empresa Cambridge Analytica, Ltd., para a utilização em campanhas políticas[18].

Os Estados Unidos, por sua vez, apostam num aparente liberalismo, cientes de que as maiores gigantes tecnológicas são norte-americanas e beneficiam desse liberalismo que, desejavelmente, aplicariam universalmente. Este liberalismo não significa, contudo, que os Estados Unidos abram mão do controlo sobre a informação. Significa apenas que pretendem que a informação circule livremente a partir de todos os Estados de forma a poderem ser captadas pelas grandes gigantes tecnológicas. A partir destas, sabendo que a maioria tem sede nos Estados Unidos ou depende grandemente do mercado norte-americano, os Estados Unidos poderão, então, aceder aos dados.

Os casos de estudos que a seguir se analisam permitem ilustrar o que aqui se refere.

## 3.1 O primeiro caso de estudo: CLOUD Act

O acesso a dados eletrónicos armazenados nos servidores de prestadores de serviços de comunicações sempre se revelou muito valioso, mormente no contexto da investigação criminal. No entanto, e apesar da sua inegável importância, o acesso a esses dados apresenta, muitas vezes, grandes dificuldades. As dificuldades poderão advir da falta de

[17] Veja-se a notícia divulgada pela própria CNIL em 21 de janeiro de 2019 intitulada "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC", disponível em https://www.cnil.fr.

[18] Veja-se a notícia divulgada pela própria ICO em 25 de novembro de 2018 intitulada "ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information", disponível em https://ico.org.uk.

enquadramento legal para esse acesso ou, como sucede também habitualmente, do facto de os prestadores de serviços de comunicações já terem eliminado os dados, não se encontrando os mesmos disponíveis no momento em que se pretende aceder aos mesmos.

O acesso aos dados eletrónicos pode, ainda, revelar uma dificuldade adicional: os servidores onde os dados se encontram alojados podem estar localizados fora das fronteiras do Estado onde se encontra a entidade que pretende aceder aos dados. Nesta eventualidade, e ainda que o prestador de serviços de comunicações em causa tenha sede no Estado onde se encontra a entidade que pretende aceder aos dados, esse prestador terá de cumprir o quadro legal do Estado onde os servidores se situam. Ora, este quadro legal poderá proibir ou colocar sérias restrições no acesso aos dados.

Estas questões estão longe de serem meramente hipotéticas. Com efeito, são inúmeros os pedidos de acesso a dados que se encontram em servidores localizados noutros Estados. Um dos pedidos foi particularmente mediático, uma vez que despoletou um processo que opôs a Microsoft Corporation aos Estados Unidos da América e que, através de recursos sucessivos, acabou por subir até ao Supremo Tribunal dos Estados Unidos[19]. Este processo teve origem num outro processo relativo a uma investigação da prática do crime de tráfico de estupefacientes. No âmbito deste processo, um juiz norte-americano emitiu um mandado judicial para que a Microsoft Corporation fornecesse vários dados eletrónicos, incluindo certas mensagens de correio eletrónico relevantes para o processo. A Microsoft Corporation forneceu dados que estavam alojados nos servidores do Estados Unidos da América, mas recusou-se a fornecer as mensagens de correio eletrónico, invocando que as mesmas se encontravam alojadas em servidores situados fora do território dos Estados Unidos, na República da Irlanda. De acordo com a empresa, o mandado judicial norte-americano não poderia sujeitar as empresas ao

[19] United States v. Microsoft Corp., 584 U.S., 138 S. Ct. 1186 (2018). Para encontrar documentação sobre este processo, veja-se o *website* do Supremo Tribunal dos Estados Unidos, no endereço www.supremecourt.gov.

fornecimento de dados alojados fora do território. Depois de uma decisão desfavorável à empresa, pelo tribunal inferior, e de uma decisão favorável, pelo tribunal de recurso, o processo foi submetido ao Supremo Tribunal dos Estados Unidos.

Este processo acabou por não ter seguimento, uma vez que as partes chegaram a acordo perante a aprovação de uma nova lei federal, designada Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), de 2018, que , entre outras previsões, estabelece a obrigação de os prestadores de serviços de comunicações norte-americanos fornecerem às autoridades norte-americanas os dados eletrónicos que lhes sejam solicitados no âmbito de uma investigação criminal, independentemente do local onde os mesmos se encontrem alojados. De acordo com esta lei federal, os prestadores de serviços de comunicações têm a possibilidade de invocar que a transmissão dos dados os levaria a violar uma lei estrangeira, como forma de procurarem evitar essa transmissão. Contudo, em última análise, após apreciação desse argumento, as autoridades podem decidir-se por avançar com o pedido e exigir que, ainda assim, o prestador de serviços de comunicações forneça os dados.

A CLOUD Act prevê ainda a celebração de acordos internacionais bilaterais com vista a facilitar o fluxo de dados com outros Estados, no âmbito de investigações criminais. Nesse âmbito, em março de 2020 foi celebrado o primeiro acordo bilateral nestes termos, entre os Estados Unidos da América e o Reino Unido, designado US-UK CLOUD Act, que facilita a livre circulação de dados entre os dois países no âmbito de investigações criminais.

A postura aparentemente liberal dos Estados Unidos da América perante os dados pessoais torna-se evidente neste primeiro caso. Com efeito, os Estados Unidos procuram alargar a sua hegemonia internacional sobre os dados pessoais. Procuram fazê-lo, num primeiro momento, ao pressionar as empresas norte-americanas para fornecer os dados que detenham, independentemente do local onde esses dados se encontrem armazenados. Verifica-se aqui uma manifesta tentativa de extrapolação da autoridade norte-americana sobre os dados para além das fronteiras.

Ao enfrentar alguma oposição, procuram, num segundo momento, alcançar esses mesmos objetivos através de uma nova legislação que torna mais claras as obrigações de fornecimento dos dados e limita as possibilidades de recusa.

## 3.2 O segundo caso de estudo: Privacy Shield

Fora do contexto das investigações criminais, o próprio desenrolar de relações comerciais entre os vários Estados torna imprescindível a transferência internacional de dados pessoais, nomeadamente para concluir vendas de produtos ou serviços a titulares de dados que se encontrem noutro Estado daquele onde se encontra o vendedor. Por esta razão, o RGPD estabelece regras sobre a transferência de dados pessoais para fora da União Europeia. Em particular, este Regulamento estabelece que essa transferência só poderá verificar-se caso determinadas condições, que garantam a proteção dos dados, estejam reunidas.

A posição mais liberal - ou aparentemente liberal, como referimos *supra* - dos Estados Unidos da América perante os dados pessoais tem gerado dificuldades na transferência de dados pessoais desde a União Europeia para o território norte-americano.

A anterior Diretiva de Proteção de Dados Pessoais criava exigências específicas para a transferência internacional de dados pessoais, que vieram a ser aprofundadas com o RGPD. Quer à luz da anterior Diretiva, quer à luz do RGPD, na eventualidade de os dados pessoais serem transferidos a partir do espaço da União Europeia para entidades localizadas em países terceiros ou para organizações internacionais, o nível de proteção dos titulares dos dados deve continuar a ser garantido, incluindo em posteriores transferências dos dados[20]. Para assegurar o devido controlo do cumprimento desta exigência, as transferências internacionais de dados pessoais ficam sujeitas, por regra, a uma prévia autorização específica, num processo que poderá ser moroso. Cabe à

[20] *Vide* considerando 101 e artigo 44.º do RGPD.

Comissão Europeia a listagem dos países e das organizações internacionais que oferecem um nível adequado de proteção de dados e que, por essa razão, estão dispensadas da referida autorização, assim possibilitando que as transferências de dados para esses países ou organizações sejam efetuadas sem burocracias adicionais[21]. Ora, face à menor proteção dos dados pessoais, os Estados Unidos da América não foram automaticamente integrados entre esses países, o que significa que as várias transferências de dados pessoais para entidades aí situadas teriam, por regra, de se sujeitar a um processo de solicitação, análise e concessão de autorização, que não se compadece com a celeridade das transações comerciais. Esta exigência criaria sérios entraves à circulação de informação e, a manter-se, conduziria a um congestionamento das próprias transações entre os dois blocos. Com vista a superar esta dificuldade, em 2000, ainda durante a vigência da Diretiva de Proteção de Dados Pessoais, o Departamento de Comércio dos Estados Unidos elaborou, em estreita colaboração com a Comissão Europeia e com a autoridade federal suíça responsável pela proteção de dados pessoais nesse país, um documento intitulado *Safe Harbor Privacy Principles*. Este documento continha um conjunto de regras e princípios que deveriam ser observados para que se assegurasse a proteção de dados pessoais. Qualquer entidade norte-americana que pretendesse efetuar o tratamento de dados pessoais oriundos da União Europeia teria de se comprometer a cumprir aqueles princípios e regras. A Comissão Europeia, na sua Decisão 2000/520/CE, entendeu que a aplicação deste sistema de vinculação das entidades norte-americanas ao documento assegurava um nível de proteção adequado dos dados pessoais transferidos da União para entidades situadas nos Estados Unidos.

As revelações de Edward Snowden, em 2013, sobre o sistema de vigilância global desenvolvido pela agência norte-americana National Security Agency (NSA) e sobre o acesso, pelas autoridades dos Estados Unidos da América a dados pessoais sem mandados judiciais, incluindo os dados pessoais em formato eletrónico detidos pelas gigantes tecnoló-

21 *Vide* artigo 45.º do RGPD.

gicas norte-americanas Google, Facebook, Apple e outras[22], determinaram uma viragem na posição da União Europeia em relação aos receios de indevido tratamento dos dados dos cidadãos europeus[23].

Num Acórdão de 6 de outubro de 2015, o TJUE invalidou a Decisão 2000/520/CE da Comissão Europeia, assim deitando por terra a transferência de dados pessoais da União Europeia para os Estados Unidos da América ao abrigo do *Safe Harbor Privacy Principles*[24]. Entre outros argumentos, as revelações relativas ao acesso a dados geridos pelas empresas norte-americanas por parte dos serviços de informações dos Estados Unidos da América demonstravam que os dados pessoais dos cidadãos europeus não se encontravam devidamente protegidos nesse país, sendo manifestamente insuficientes, para o efeito, as regras e os princípios plasmados no referido documento.

Ainda durante a vigência da Diretiva da Proteção de Dados, a Comissão Europeia e o Departamento de Comércio dos Estados Unidos recomeçaram conversações para encontrar uma solução que reforçasse a proteção dos dados pessoais que fossem transferidos para os Estados Unidos a América. Foram elaborados novos princípios de privacidade, que, em conjunto com compromissos e declarações oficiais de várias autoridades dos Estados Unidos da América, constituem o *Escudo de Proteção da Privacidade UE-EUA* ou, como é mais habitualmente referido, na língua inglesa, *Privacy Shield EU-USA*.

---

22 Veja-se, entre outros, BARTON GELLMAN e LAURA POITRAS, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", **The Washington Post,** 7 de junho 2013, disponível em https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1, e EWEN MACASKILL e GABRIEL DANCE, "NSA files' decoded", **The Guardian**, 1 de novembro de 2013, https://www.theguardian.com/us-news/the-nsa-files.

23 Veja-se a Resolução do Parlamento Europeu, de 12 de março de 2014, sobre o programa de vigilância da Agência Nacional de Segurança dos EUA (NSA), os organismos de vigilância em diversos Estados-Membros e o seu impacto nos direitos fundamentais dos cidadãos da UE e na cooperação transatlântica no domínio da justiça e dos assuntos internos (2013/2188(INI)).

24 Acórdão proferido pelo TJUE no âmbito do processo C-362/14, disponível em http://curia.europa.eu, que tem vindo a ser referido como o caso Schrems I.

Na sua Decisão de Execução (UE) 2016/1250, de 12 de julho de 2016, a Comissão Europeia entendeu que as transferências de dados pessoais a partir da União para entidades autocertificadas nos Estados Unidos da América ao abrigo do *Privacy Shield EU-USA* asseguravam um nível de proteção adequado a esses dados pessoais.

No entanto, num Acórdão de 16 de julho de 2020, o TJUE voltou a entender que os mecanismos estabelecidos para a transferência de dados da União para os Estados Unidos da América eram insuficientes, não acautelando devidamente a proteção dos dados pessoais e, consequentemente, invalidou a Decisão de Execução (UE) 2016/1250, esvaziando de sentido o *Privacy Shield EU-USA*[25].

Este segundo caso é ilustrativo da postura protecionista da União Europeia perante os dados pessoais. A União Europeia levanta dificuldades na transferência dos dados pessoais para os Estados Unidos com fundamento no nível baixo de proteção dos dados por este país. Os Estados Unidos procuram aceder aos dados para os fins que entendem relevantes, assumindo o habitual controlo desses dados e procurando aproveitar a posição privilegiada das gigantes tecnológicas norte-americanas, mas a União Europeia retalia com a ameaça de não permitir a transferência caso não sejam dadas garantias suficientes de que os valores subjacentes à legislação europeia serão acolhidos.

## 3.3 O terceiro caso de estudo: ordens executivas contra TikTok e WeChat

O terceiro e último caso a abordar, muito brevemente, tem vários pontos de contacto com o caso anterior. Como foi descrito, a União Europeia tem-se oposto à transferência de dados pessoais para os Estados Unidos da América com o receio de que esses dados sejam indevidamente tratados, nomeadamente pelos respetivos serviços de informações.

[25] Acórdão proferido pelo TJUE no âmbito do processo C-311/18, disponível em http://curia.europa.eu, que tem vindo a ser referido como o caso Schrems II.

Ora, utilizando este mesmo argumento, os Estados Unidos têm vindo a opor-se à hegemonia de empresas tecnológicas chinesas.

Com efeito, o Presidente norte-americano Donald Trump tem vindo a adotar várias medidas contra as aplicações móveis de sucesso a operar nos Estados Unidos da América pertencentes a empresas com sede na China: TikTok e WeChat. Considerando que essas aplicações poderão representar um risco para a segurança nacional, permitindo que os serviços de informações da China acedam a dados recolhidos por essas aplicações nos Estados Unidos, este Presidente decretou, em 6 de agosto de 2020, uma ordem executiva contra cada uma dessas aplicações móveis[26], a que se seguiu, em 18 de setembro de 2020, uma proibição por parte do Departamento de Comércio dos Estados Unidos da América de se proceder a transações financeiras através dessas aplicações[27].

Entendemos que este último caso evidencia que o liberalismo dos Estados Unidos da América face aos dados pessoais é um liberalismo meramente aparente. Os dados poderão circular livremente entre países através de gigantes tecnológicas desde que essas gigantes tecnológicas sejam, pelo menos maioritariamente, norte-americanas. O facto de as gigantes tecnológicas serem norte-americanas permite que os Estados Unidos controlem os dados. Num contexto em que o controlo dos dados possa pertencer a outro Estado, os Estados Unidos reagem, procurando impedir a sua atividade.

---

[26] Ordens executivas números 13942 e 13943, de 6 de agosto de 2020, ambas disponíveis em https://www.federalregister.gov/presidential-documents/executive-orders/donald-trump/2020. Estas ordens executivas fundamentam-se numa ordem executiva anterior, número 13873, de 15 de maio de 2019.

[27] Numa declaração intitulada **Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States,** o gabinete de relações públicas do Departamento de Comércio dos Estados Unidos da América anunciou, em 18 de setembro de 2020, ter proibido transações comerciais envolvendo essas aplicações (disponível em https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect).

## 4 REFLEXÕES FINAIS

A guerra pelo controlo da informação verifica-se desde tempos imemoriais. Num momento histórico em que a informação se tornou o principal recurso da sociedade, entende-se que esta guerra se tenha intensificado, tornando-se mais complexas as formas de a empreender.

As guerras hodiernas são travadas em campos de batalha muito diversos dos de antigamente. Um novo campo de batalha consiste no ciberspaço, onde circulam vários tipos de dados. Entre estes, merecem destaque os dados pessoais, que apresentam um valor exponencial à medida que evoluem as ferramentas de tratamento desses dados. As gigantes tecnológicas norte-americanas tornaram-se os senhores feudais dos novos tempos, acumulando os feudos dos dados pessoais e detendo os meios de, a partir deles, produzir riqueza. Beneficiando da posição privilegiada e única das gigantes tecnológicas norte-americanas, os Estados Unidos apresentavam todas as condições para alcançar a hegemonia, de forma isolada e bem destacada, no domínio dos dados pessoais.

A aprovação do RGPD surge como uma oportunidade para romper com aquela hegemonia. Ao impor uma visão protecionista na gestão dos dados pessoais, que já decorria da anterior Diretiva da Proteção de Dados Pessoais mas que surge agora reforçada, o RGPD apresenta sérias restrições ao tratamento desses dados alicerçadas na defesa dos direitos fundamentais. Estas restrições podem ter impacto na hegemonia dos Estados Unidos da América, uma vez que o RGPD tem efeitos extraterritoriais, decorrentes da sua aplicabilidade a situações que apresentam um mínimo de conexão com a União Europeia.

Ao abrigo do quadro legal de proteção de dados pessoais, a União Europeia tem procurado reconquistar algum domínio sobre os dados pessoais. Os Estados Unidos, por sua vez, não estão dispostos a abrir mão da sua hegemonia e lançam mão de várias frentes de batalha, quer pressionando as gigantes tecnológicas para lhes fornecer dados, quer celebrando acordos internacionais para obter esses dados diretamente dos outros Estados, quer ainda bloqueando gigantes tecnológicas de outros

Estados que possam vir a ameaçar a posição das gigantes tecnológicas norte-americanas, com fundamento na segurança nacional.

Nestas breves linhas, analisámos alguns dos movimentos de peças nesta complexa estratégia. Num primeiro caso de estudo, verificámos que os Estados Unidos sufragam uma livre circulação de dados para fins de investigação criminal com vista a poder beneficiar do acesso a esses dados. Unilateralmente, aprovaram uma legislação que determina o fornecimento de dados para fins de investigação criminal independentemente do local geográfico onde se encontram armazenados. Verifica-se, sem dúvida, um aproveitamento da posição privilegiada das gigantes tecnológicas norte-americanas no acesso aos dados. Ao abrigo desta legislação, CLOUD Act, estimulam-se ainda acordos internacionais que permitam desbloquear eventuais obstáculos àquele fornecimento de dados.

Num segundo caso, ilustrou-se a legislação protecionista da União Europeia que coloca entraves à transferência de dados pessoais para os Estados Unidos da América, uma vez que este país, no entender da União Europeia, não oferece garantias suficientes de proteger esses dados. Esta posição ficou evidente na jurisprudência do TJUE, quer no Acórdão no caso Schrems I, quer no Acórdão no caso Schrems II.

No terceiro caso, verificamos que a posição liberal dos Estados Unidos perante os dados pessoais recua face à ameaça de gigantes tecnológicas chinesas. Nesse contexto, atento o sucesso de plataformas como a TikTok e a WeChat, os Estados Unidos apelam a argumentos assentes na segurança nacional e replicam a posição protecionista que a União Europeia tem vindo a esgrimir contra os próprios Estados Unidos.

O círculo fecha-se com este terceiro e último caso, permitindo vislumbrar que as posições adotadas pela União Europeia e pelos Estados Unidos, ainda que por vezes se toquem, assentam em valores diametralmente diversos em ambos os lados do Atlântico. De ambos os lados encontramos visões diversas perante os dados pessoais e uma forte intenção de fazer vingar essas visões além-fronteiras. As intenções de extraterritorialidade de ambos os lados do Atlântico posicionam-nos numa guerra silenciosa, atirando-os também para lados opostos da trincheira.

A aprovação de legislação regional ou nacional de reforço da posição de cada lado, a invocação repetida de direitos fundamentais como argumento de bloqueio de transferências internacionais de dados, a celebração de acordos e parcerias internacionais para transferências de dados e a aprovação de ordens executivas com fundamentos em segurança nacional para impedir o tratamento de dados por Estados terceiros são apenas diferentes expressões das novas formas de travar uma guerra sem que haja o efetivo uso da força e sem que haja uma retórica inflamada e bélica, seguindo a máxima de Sun Tzu: "*A suprema arte da guerra é de subjugar o inimigo sem lutar*"[28]. Não deixa, porém, de ser uma guerra.

## REFERÊNCIAS

BARTON GELLMAN; LAURA POITRAS, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", **The Washington Post,** 7 de junho 2013, disponível em https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1,

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. Artigos 7.º e 8.º.

CNIL. 21 de janeiro de 2019 , **The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC**", disponível em https://www.cnil.fr.

DÁRIO MOURA VICENTE; SOFIA DE VASCONCELOS CASIMIRO (Coord.), **Data Protection in the Internet,** volume 38 da coleção Ius Comparatum - Global Studies in Comparative Law, Springer, Suíça, 2020.

DEPARTAMENTO DE COMÉRCIO DOS ESTADOS UNIDOS DA AMÉRICA. **Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States,** 18 de setembro de 2020**.** Disponível em: https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect

[28] SUN TZU, *A Arte da Guerra,* Universo dos Livros, São Paulo, 2010, p. 12.

EWEN MACASKILL; GABRIEL DANCE, "NSA files' decoded", **The Guardian**, 1 de novembro de 2013, https://www.theguardian.com/us-news/the-nsa-files.

ICO. 25 de novembro de 2018, "**ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal informatio**n", disponível em https://ico.org.uk.

JOHN NAUGHTON, "Can democracies stand up to Facebook? Ireland may have the answer", **The Guardian**, 26 de setembro de 2020, disponível em www.theguardian.com.

LOGAN KUGLER, "The war over the value of personal data", **Communications of the ACM,** volume 61, 2, fevereiro 2018, pp. 17-19.

VOLKER BRUHL, **Big Data, Data Mining, Machine Learning and Predictive Analytics – A Conceptual Overview,** CFS Working paper, n.º 617, 2019, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3321195.

PARLAMENTO EUROPEU. **Resolução de 12 de março de 2014**.

SUN TZU, **A Arte da Guerra**, Universo dos Livros, São Paulo, 2010, p. 12.

SUPREMO TRIBUNAL DOS ESTADOS UNIDOS, United States v. Microsoft Corp., 584 U.S., 138 S. Ct. 1186 (2018), disponível em: www.supremecourt.gov.

TRIBUNAL ALEMÃO ADMINISTRATIVO (*Oberverwaltungsgericht Schleswig*). Decisão de 22 de abril de 2013.

TRIBUNAL DE RECURSO DE BERLIM (*Langericht Berlin*). **Acórdão de 12 de fevereiro de 2014**, processo 5 U 42/12.

RGPD.

TJUE. **Acórdão processo C-362/14**, disponível em http://curia.europa.eu, caso Schrems I.

TJUE. **Acórdão processo C-311/18,** disponível em http://curia.europa.eu, caso Schrems II.

# Capítulo II

## NA BORDA: dados pessoais e não pessoais nos dois Regulamentos da União Europeia

*Manuel David Masseno*[1]

### SUMÁRIO



### RESUMO

No contexto regulatório da sua Economia dos Dados, a União Europeia dispõe de regras distintas para os tratamentos de dados pessoais e de dados não pessoais, embora com níveis de densidade diferentes. Porém, a evolução das técnicas de anonimização e de personalização dos dados tornaram instáveis os limites entre aos âmbitos de aplicação material de cada um dos regimes jurídicos, o que acabou por ser assumido pelo Legislador. Assim, este texto explora os critérios normativos subjacentes a tais fronteiras, em especial no que se refere à personalização potencial de dados anónimos ou anonimizados e procura identificar os riscos inerentes, assim como os instrumentos técnicos e normativos disponíveis para os minimizar, desde as avaliações de impacto em proteção de dados até às certificações previstas, incluído as relativas à cibersegurança.

**Palavras-chave:** Anonimização, Certificação, Dados, Risco, União Europeia

[1] Professor Adjunto do IPBeja - Instituto Politécnico de Beja, onde também integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança Informática, sendo ainda o seu Encarregado da Proteção de Dados. Pertence à EDEN – Rede de Especialistas em Proteção de Dados da Europol – Agência Europeia de Polícia e ao Grupo de Missão "Privacidade e Segurança" da APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação, em Portugal, ao Grupo de Estudos de Direito Digital e *Compliance* da FIESP – Federação das Indústrias do Estado de São Paulo, à Comissão Estadual de Direito Digital da Ordem dos Advogados do Brasil, Seção de Santa Catarina e à Comissão de Direito Digital da Subseção de Campinas da OAB.

*"Assistimos a uma nova revolução industrial induzida pelos dados digitais, a informática e a automatização. As atividades humanas, os processos industriais e a investigação conduzem, todos eles, à recolha e ao tratamento de dados numa escala sem precedentes, favorecendo o surgimento de novos produtos e serviços, assim como de novos processos empresariais e metodologias científicas [e] Desde que as regras relativas à proteção dos dados pessoais, quando aplicáveis, sejam cumpridas, os dados, uma vez registados, podem ser reutilizados muitas vezes sem perda de fidelidade. Esta geração de valor agregado está no cerne do conceito de cadeia de valor dos dados. [tendo sempre presente que] O direito fundamental à proteção dos dados pessoais aplica-se aos grandes volumes de dados no caso de se tratar de dados pessoais: o seu tratamento tem de respeitar todas as regras aplicáveis em matéria de proteção de dados." (COM/2014/0442 final, de 2 de julho).*

## 1 AS REFERÊNCIAS[2-3-4]

Antes de mais, é necessário ter presente que, uma vez operada a *constitucionalização* da Proteção de Dados operada em 2009 com a entrada em vigor do *Tratado de Lisboa*, com a inclusão da mesma no *Tratado sobre o Funcionamento da União Europeia* (Art.º 16.º) e com a receção da *Carta dos Direitos Fundamentais* (Art.º 8.º) no Direito Primário da União (*Ex vi*, Art.º 6.º do *Tratado da União Europeia*), o respetivo microssistema ficou consolidado, ainda que não completo, com a adoção do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento

---

2 Versão em Língua Portuguesa da Comunicação apresentada no *IV Congreso Interactivo Virtual - Humanos Máquinas Derecho ¿amigos ou inimigos?*, sediado na *Universidad Nacional de Lanús*, (Argentina), a 20 de novembro de 2019, antes exposta como "On the Waterfront: 'Personal' and 'Non-Personal' Data at Both EU Regulations", na *Nordic Conference on Legal Informatics 2019 - Digital Rights, Digital Lawyers, Digital Courts*, realizada na *Lapin yliopisto* (Universidade da Lapónia, Finlândia) dia 14 de novembro de 2019.

3 Apenas serão indicadas referências bibliográficas disponíveis na Internet e em Acesso Aberto, assumindo as consequências resultantes de não o fazer com outras, mais marcantes, apenas publicadas em papel ou sujeitas a pagamento.

4 Artigo publicado na *Cyberlaw by CIJIC* – Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, n. 9, 2020, e na Revista Eletrônica *Disciplinarum Scientia* | Sociais Aplicadas, Vol. 16 n. 1, 2020.

de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/C (*Regulamento Geral sobre a Proteção de Dados*) – o *RGPD*[5].

Ao mesmo tempo e enquanto ainda decorria o processo legislativo correspondente ao *RGPD*, a *Comissão* [presidida por Jean-Claude] *Juncker* avançou com a "Estratégia para o Mercado Único Digital na Europa" (COM/2015/192 final, de 6 de maio), dando continuidade a orientações que vinham da *Comissão* [presidida por José Manuel Durão] *Barroso* e constavam da Comunicação "Para uma economia dos dados próspera" (COM/2014/0442 final, de 2 de julho)[6].

O que foi explicitado através de uma sua nova Comunicação, "Construir uma Economia Europeia dos Dados" (COM/2017/9 final, de 10 de janeiro), agora centrada na necessidade de avançar com disciplinas para os "dados em bruto", com uma especial ênfase na sua portabilidade em todo o Mercado Interno da União[7]. Daí que a Comissão tenha avançado com a *Proposta* (COM/2017/0495 final, de 13 de setembro) do que veio a ser o

5 Os estudo sobre o RGPD são hoje multidão. Mas, sempre podemos referir os estudos de Angelina TEIXEIRA (2016), de Alfonso ORTEGA JIMÉNEZ e Juan José Gonzalo DOMENECH (2018) e ainda de Chris HOOFNAGLE, Bart van der SLOOT e Fredrik ZUIDERVEEN BORGESIUS (2019).

6 Aliás, na sua "Estratégia para o Mercado Único Digital na Europa" a Comissão acentua que "As empresas e os consumidores continuam a não se sentirem suficientemente confiantes para adotar serviços de computação em nuvem transfronteiras para fins de armazenamento ou processamento de dados, devido a preocupações relacionadas com a segurança, o respeito dos direitos fundamentais e a proteção de dados em termos mais gerais. A adoção do Pacote Reforma da Proteção de Dados assegurará que o tratamento de dados pessoais seja regido por regras atualizadas e uniformes em toda a União. No entanto, frequentemente os contratos excluem, ou limitam de forma significativa, a responsabilidade contratual do prestador de serviços de computação em nuvem caso os dados deixem de estar disponíveis ou fiquem inutilizáveis, ou dificultam a rescisão do contrato. Isso significa que não existe, de facto, uma portabilidade dos dados. No domínio da proteção de dados, tanto o atual como o futuro quadro legislativo impede as restrições à livre circulação de dados pessoais na União. As restrições à livre circulação de dados por outros motivos não são abordadas. [Pelo que] A Comissão irá propor em 2016 a Iniciativa Europeia «Livre Circulação de Dados» que aborda a questão das restrições à livre circulação de dados por motivos não relacionados com a proteção de dados pessoais na UE e das restrições injustificadas sobre a localização de dados para fins de armazenamento ou de tratamento. A iniciativa abordará as questões emergentes de propriedade, interoperabilidade, utilizabilidade e acesso aos dados nomeadamente em situações entre empresas, entre empresas e consumidores e dados gerados por máquinas e máquina-a-máquina. Incentivará o acesso aos dados públicos a fim de contribuir para dinamizar a inovação."

7 Sobre estes Documentos e em termos gerais sobre o Mercado Único Digital e por todo, é de atender à exposição de Fernanda Ferreira DIAS (2016).

Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho de 14 de novembro de 2018 relativo a um regime para o livre fluxo de dados não pessoais na União Europeia – o *Regulamento LFD*[8].

No entanto e entre outras, voltou a ser colocada questão a necessitar de respostas jurídicas tão robustas quanto possível, a de existir uma borda, mutável de acordo com a evolução das tecnologias, entre os âmbitos de aplicação material de ambos os Regulamentos, isto é, entre os dados pessoais e os dados não pessoais. A determinação dessa borda, e um breve esboço do que fazer, constitui o objeto desta intervenção.

## 2 ATÉ MESMO NOS LIMITES

Para começar, temos que o *RGPD* "aplica-se ao tratamento de dados pessoais" (Art.º 2.º n.º 1), não só a uma "pessoa singular [física] identificada", mas também a uma que venha a ser "identificável", em termos potenciais e através de meios técnicos, incluindo os indiretos[9]-[10].

---

8 Para uma perspetiva geral do *Regulamento LFD*, embora tratando essencialmente de outras questões, Pedro DE MIGUEL ASENSIO (2019).

9 Ou seja "[…] que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;" (Art.º 4.º 1). O que incluí os quase-identificadores e os metadados, ao ser certo que, "As pessoas singulares podem ser associadas a identificadores por via eletrónica […] tais como endereços IP (protocolo internet) ou testemunhos de conexão (*cookie*) ou outros identificadores como as etiquetas de identificação por radiofrequência." (*Considerando* 30). Diversamente, a propósito da reindentificação de dados pseudonimizados, o *RGPD* acrescenta que "[…] importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica." (*Considerando* 26).

10 Neste particular, há ainda que atender ao conteúdo do Parecer 4/2007 sobre o conceito de dados pessoais, de 20 de junho de 2007, do *Grupo de Trabalho do 29.º* [o qual antecedeu o CEPD – Comité Europeu para a Proteção de Dados], assim como à Jurisprudência do Tribunal de Justiça da União Europeia, a qual culminou no Acórdão proferido no Processo C-582/14, *Patrick Breyer*, de 19 de outubro de 2016. Quanto a estas referências, são de

Consequentemente, do *RGPD* resulta que: "[…] Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação." (*Considerando* 26 *in fine*)

Por sua vez, o *Regulamento LFD* veio esclarecer que o mesmo "aplica-se ao tratamento de dados eletrónicos que não sejam dados pessoais" (Art.º 2.º n.º 1), entendendo estes "na aceção do artigo 4.º, ponto 1, do Regulamento (UE) 2016/679 [o *RGPD*]" (Art.º 3.º n.º 1)[11].

Assim, ao *Regulamento Geral sobre Proteção de Dados* é conferida uma *vis atractiva*, sempre que não seja possível identificar os dados em presença como, exclusivamente, não pessoais. Pelo que, "No caso de um conjunto de dados compostos por dados pessoais e não pessoais, o presente regulamento aplica-se aos dados não pessoais do conjunto de dados. Caso os dados pessoais e não pessoais de um conjunto de dados estejam indissociavelmente ligados, o presente regulamento não prejudica a aplicação do Regulamento (UE) 2016/679" (Art.º 2.º n.º 2 do *Regulamento LFD*).

## 3 MAS, AFINAL, NADA É PARA SEMPRE

No que concerne a distinção que nos ocupa, temos que a Diretiva 95/46/CE, que precedeu o *Regulamento sobre Proteção de Dados*,

atender os estudos, complementares entre si, de Rossana DUCATO (2016), de Nadezhda PURTOVA (2018), de A. Barreto MENEZES CORDEIRO (2018) e ainda de Lorenzo dalla CORTE (2019), inclusive quanto a referências bibliográficas adicionais.

[11] Isto, porque "A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. Exemplos concretos de dados não pessoais incluem conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados, os dados relativos à agricultura de precisão que podem ajudar a controlar e a otimizar a utilização de pesticidas e de água ou ainda dados sobre as necessidades de manutenção de máquinas industriais." (*Considerando* 9).

assentara numa *fictio iuris*, ao abstrair-se da evolução da técnica, ainda que previsível. Daí, na mesma constar que "[…] os princípios da proteção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável [os quais são, também] conservados sob uma forma que já não permita a identificação da pessoa em causa." (*Considerando* 26).

O que já não ocorre com o *RGPD*, ao ser assumido que "As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos [e também que] Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares." (*Considerando* 30).

Por sua vez, o *Regulamento LFD* é transparente, ao explicitar que "Se os progressos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados como dados pessoais, e o Regulamento (UE) 2016/679 deve ser aplicado em conformidade" (*Considerando* 9 *in fine*), o mesmo valendo para os dados originariamente anónimos, por identidade de razão.

Porém, é necessário ter presente que não estamos face a algo verdadeiramente novo. Aliás, as Instituições da União Europeia foram ficando cientes desta realidade, como mostram os Pareceres do *Grupo de Trabalho do Art.º 29.º*.

Assim e num primeiro momento, tal ocorreu a propósito dos riscos para a proteção dos dados dos administrados que poderiam advir da transposição da Diretiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de Novembro de 2003, relativa à reutilização de informações do sector público, designadamente, o Parecer n.º 7/2003 sobre a reutilização de informações do setor público e a proteção dos dados pessoais, de 12 de dezembro. A que se seguiu o Parecer n.º 6/2013 sobre dados abertos e reutilização de informações do setor público (ISP), de 5 de junho, suscitado pela adoção da Diretiva 2013/37/UE do Parlamento Europeu

e do Conselho, de 26 de junho de 2013, que altera a Diretiva 2003/98/CE relativa à reutilização de informações do setor público[12].

Mas, uma análise detalhada destas questões, tanto desde o ponto de vista técnico quanto numa perspetiva jurídica, constituiu o objeto do Parecer n.º 5/2014 sobre técnicas de anonimização, de 10 de abril[13].

Por isso mesmo, algumas autoridades nacionais avançaram com orientações destinadas a mostrar padrões aos respetivos responsáveis pelo tratamento de dados, como no Reino Unido com a ICO - *Information Commissioner's Office*, que aprovou o *Anonymisation: managing data protection risk code of practice*, em novembro de 2012, ou com a *Agencia Española de Protección de Datos*, com as suas *Orientaciones y garantías en los procedimientos de anonimización de datos personales*, de outubro de 2016.

Entretanto e a propósito da entrada em vigor do *Regulamento LFD*, a Comissão Europeia publicou as suas "Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados não pessoais na União Europeia" (COM/2019/250 final, de 29 de maio), com referências específicas e desenvolvidas quanto a esta questão[14], concluindo que "[…] se determi-

[12] Sobre esta tensão entre as políticas de dados abertos e a proteção de dados, criticamente, temos também o artigo de Katleen JANSSEN e Sara HUGELIER (2013).

[13] No qual é afirmado, precisamente, que "A anonimização de dados pessoais pode ser uma boa estratégia para manter os benefícios e atenuar os riscos. Quando um conjunto de dados se encontra verdadeiramente anonimizado e as pessoas deixam de ser identificáveis, a legislação europeia de proteção de dados deixa de ser aplicável.
No entanto, estudos de casos e publicações de investigação evidenciam que criar um conjunto de dados verdadeiramente anónimo a partir de um conjunto substancial de dados pessoais mantendo, simultaneamente, as informações subjacentes exigidas para a tarefa não é um desafio simples. Por exemplo, um conjunto de dados considerado anónimo pode ser combinado com outro conjunto de dados de modo a que uma ou mais pessoas sejam passíveis de ser identificadas."

[14] "Todos os dados que não sejam «dados pessoais», na aceção do Regulamento Geral sobre a Proteção de Dados, são dados não pessoais. Os dados não pessoais podem ser classificados segundo a origem:
Desde o início - dados originalmente não relacionados com uma pessoa singular identificada ou identificável, tais como dados sobre as condições meteorológicas gerados por sensores instalados em turbinas eólicas ou dados sobre as necessidades de manutenção de máquinas industriais.
Em segunda fase - dados inicialmente pessoais, mas posteriormente anonimizados. A «anonimização» de dados pessoais é diferente da pseudonimização (ver supra), uma vez que os

nados dados não pessoais puderem ser associados a uma pessoa de qualquer forma, tornando-os direta ou indiretamente identificáveis, devem ser considerados dados pessoais. [e, do mesmo modo] Aplicam-se as mesmas regras [as relativas ao tratamento de dados pessoais] quando a evolução da tecnologia e da análise de dados torna possível a conversão de dados anonimizados em dados pessoais."

Acrescente-se que preocupações idênticas, em especial motivadas pela disponibilização de informações do Setor Público destinadas à sua reutilização por privados num contexto tecnológico de acesso generalizado às analíticas de *Big Data*, enformaram o Anexo II do Relatório de 24 de novembro de 2016 (A/HRC/31/64) do Relator Especial para a Privacidade do Conselho dos Direitos Humanos das Nações Unidas, Joseph A. Cannataci.

Adicionalmente e como resulta também dos Documentos antes referidos, diversos estudos académicos foram mostrando as dificuldades de manter distinções claras, consistentes e, mais ainda, irreversíveis entre dados pessoais e dados não pessoais. O que se concretiza na explicitação dos limites das técnicas de anonimização disponíveis em cada momento, assim como nas possibilidades de personalização de dados anónimos ou anonimizados.

A título exemplificativo, logo em 2010 e desde uma perspetiva jurídica, Paul OHM expôs as insuficiências das técnicas então disponíveis. Entretanto, em julho último, seguindo uma metodologia de natureza matemática, Luc ROCHER, Julien M. HENDRICKX e Yves-Alexandre de MONTJOYE

dados devidamente anonimizados não podem ser atribuídos a uma determinada pessoa, nem sequer pela utilização de dados adicionais, pelo que se tratam de dados não pessoais. Aferir da correta anonimização dos dados depende de circunstâncias específicas e únicas de cada caso. Os vários exemplos detetados de reidentificação de conjuntos de dados supostamente anonimizados demonstraram que essa avaliação pode ser exigente. Para determinar se uma pessoa é identificável, é necessário ter em conta todos os meios suscetíveis de serem razoavelmente utilizados por um responsável pelo tratamento ou qualquer outra pessoa para identificar uma pessoa direta ou indiretamente.
No entanto, se determinados dados não pessoais puderem ser associados a uma pessoa de qualquer forma, tornando-os direta ou indiretamente identificáveis, devem ser considerados dados pessoais."

demonstraram como a reidentificação de dados anónimos ou anonimizados pode ser alcançada, com níveis muito altos de eficácia e uma relativa facilidade técnica[15]-[16].

## 4 E "QUE FAZER?" ...ANTES DO TRATAMENTO DE DADOS, PESSOAIS E NÃO PESSOAIS

Atendendo a este contexto técnico e regulatório, também resultante do Princípio da responsabilidade proativa (*Accountability*)[17] e por força da aplicação dos Princípios e regras constantes do *RGPD*, o Responsável pelo Tratamento deverá promover a realização de análises de risco, previamente à anonimização de dados pessoais ou aos tratamento de dados não pessoais[18]. O que o afastará de incorrer em qualquer uma das res-

[15] Depois das conclusões de Paul OHM, a questão continuou a sem debatida na Doutrina de ambas margens do Atlântico, procurando uma compatibilização, porventura impossível, entre uma tecnologia crescentemente mais poderosa no sentido de viabilizar a repersonalização de dados anonimizados e as regras pressupondo a correspondente irreversibilidade, sobretudo durante o processo legislativo que culminou na adoção do *Regulamento Geral sobre Proteção de Dados*, ou logo após, como ocorreu com Paul SCHWARTZ e Daniel SOLOVE (2011) e (2014), Samson Y. ESAYAS (2015) ou ainda com Sophie STALLA-BOURDILLON e Alison KNIGHT (2017).

[16] Quanto à utilização de analíticas de *Big Data* para a "definição de perfis" (isto é, uma "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações", Art.º 4.º 4) do *RGPD*) e para a personalização, também a partir de dados anónimos ou anonimizados, são de referir os estudos de Benjamin HABEGGER *et al*. (2014), de Alessandro MANTELERO (2016) e de Elena GIL (2016, *maxime* pp. 86-110) ou, desde uma perspetiva técnica de, Nils GRUSCHKA *et al*. (2018) e ainda o meu trabalho e de Cristiana Teixeira SANTOS (2019), tal como as reflexões críticas de Lorenzo COTINO HUESO (2017).

[17] Havendo sido objeto do Parecer n.º 3/2010 sobre o princípio da responsabilidade, adotado em 13 de julho de 2010 pelo *Grupo de Trabalho do Art.º 29*, o mesmo ficou explicitado n.º 2 do Art.º 5.º do *RGPD*, em cujos termos, "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 [, isto é, pelo cumprimento dos "Princípios relativos ao tratamento de dados pessoais] e tem de poder comprová-lo", sobre o mesmo, além das considerações de Teresa Vale LOPES (2018) e de Emanuele LUCCHINI GUASTALLA (2018), tem muito interesse o recente estudo de Lachlan URQUHART, Tom LODGE e Andy CRABTREE (2019).

[18] Isto, porque "Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos,

ponsabilidades previstas nas tipologias constantes do *RGPD* em resultado da personalização de dados, mesmo se apenas potencial ou realizada por terceiros[19].

Aliás, embora se nos afigure evidente, deve ficar claro que a anonimização de dados pessoais pressupõe a presença dos inerentes requisitos no que respeita à "Licitude do tratamento" (Art.ºs 6.º a 11.º), assim como a observância dos "Princípios relativos ao tratamento de dados pessoais" (Art.º 5.º). O mesmo valendo para a personalização, ou a repersonalização, de dados anónimos ou anonimizados.

Especificamente, deverão ser seguidos os critérios indicados no *RGPD* a propósito tanto da "Proteção de dados desde a conceção e por defeito [omissão…]" (Art.º 25), em particular no que se refere à "Segurança do tratamento" (Art.º 32.º), ou seja, "Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas […]."[20].

---

como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica." (*Considerando* 26 do *RGPD*). A propósito das análises de risco neste contexto, em termos gerais, são de referir os estudos de Niels van DIJK, Raphaël GELLERT e Kjetil ROMMETVEIT (2016), de Alessandro MANTELERO (2017), assim como as considerações de Teresa Vale LOPES (2018).

19 Como ocorre com o "direito de indemnização e responsabilidade", objetiva e solidária (Art.º 82.º), com as "coimas" [sanções administrativas], que podem atingir montantes muito elevados (Art.ºs 58.º n.º 1 i) e 83.º), e, sendo o caso, com outras "sanções", designadamente de ordem penal (Art.º 84.º). Para uma melhor compreensão destes preceito e por todos, atente-se no estudo Brendan Van ALSENOY, (2017) e na síntese de Pedro Miguel FREITAS (2018).

20 Quanto ao conteúdo e ao sentido destas previsões, são sobretudo os estudos encomendados pela ENISA – agora, Agência da União Europeia para a Cibersegurança, antes da adopção do *RGPD*, a George DANESIS *et a*l. (2014) e a Giuseppe D'ACQUISTO *et al*. (2015), e, depois, a Marit HANSEN e Konstantinos LIMNIOTIS (2018), sendo ainda de considerar os contributos de Simone CALZOLAIO (2017), de Lee A. BYGRAVE (2017), de Irene KAMARA

E ainda, se isso resultar da análise de risco ou for necessário por a mesma ser obrigatória para tratamentos de dados pessoais análogos aos pretendidos (Art.º 35.º n.º 3)[21], deverá também ser efetuada uma "Avaliação de impacto sobre a proteção de dados", com especial ênfase no acompanhamento da evolução das técnicas de personalização ou de repersonalização de dados anónimos ou anonimizados, isto é, "Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares […]." (Art.º 35.º n.º 1)[22].

Por outras palavras, essas Avaliações devem realizar-se periodicamente ou sempre que se verifique a emergência de novas técnicas neste domínio, não apenas para a anonimização mas também para a personalização[23].

Adicionalmente, o enquadramento de tais tratamentos de dados no âmbito de "um procedimento de certificação aprovado nos termos do artigo 42.º" (tal como referido no Art.º 25.º n.º 3 a propósito da "proteção de dados desde a conceção e por defeito" e no Art.º 32.º n.º 2 no que se refere à "segurança do tratamento") poderá assumir uma grande

(2017), este centrado na definição e aplicação de normas técnicas neste domínio, assim como de Teresa Vale LOPES (2018).

21 Especificamente, "a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º; ou c) Controlo sistemático de zonas acessíveis ao público em grande escala."

22 A este propósito e em geral, são de assinalar as referências breves de Luís PICA (2018) e as considerações de Teresa Vale LOPES (2018), bem como e sobretudo os estudos de Niels van DIJK, Raphaël GELLERT e Kjetil ROMMETVEIT (2016) e de Bruno PEREIRA e João ORVALHO (2019)

23 Para tanto, cumprirá seguir as Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 (Revistas e adotadas pela última vez em 4 de outubro de 2017), do Comité Europeu para a Proteção de Dados.

importância para evitar males maiores no que se refere às várias responsabilidades nas quais os responsáveis pelos tratamentos podem incorrer, embora não as afastem, pelo menos por inteiro[24].

Neste mesmo sentido, a aprovação de "critérios de certificação", contendo parâmetros objetivos e detalhados quanto às técnicas de anonimização mais robustas, pelo Comité Europeu para a Proteção de Dados, conduzindo a um "Selo Europeu de Proteção de Dados", reveste-se da maior relevância (Art.ºs 42.º n.º 5 e 70.º n.º 1 p)[25].

Sempre a propósito da certificação das técnicas de anonimização e do tratamento de dados anónimos ou anonimizados, ferramentas complementares poderiam resultar do novel "sistema europeu de certificação da cibersegurança", tal como previsto no Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 abril de 2019 relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (*Regulamento Cibersegurança*)[26]. O que teria consequências, pelo menos no que se refere à segurança no tratamento dos dados, sobretudo perante uma "violação de dados pessoais"[27], com implicações quanto à presença e conteúdo do dever de notificação da mesma aos titulares dos dados (Art.º 34.º do *RGPD*).

---

[24] No que se refere a este regime, atente-se nos estudos de Giovanni Maria RICCIO e Federica PEZZA, (2018) e de Jorge A. VIGURI CORDERO (2018), assim como nos apontamentos de Luís PICA (2018) e de Teresa Vale LOPES (2018).

[25] Aliás, essa mesma preocupação já consta, ainda que como referências muitos sintéticas, das Orientações 1/2018 relativas à certificação e à definição de critérios de certificação de acordo com os artigos 42.º e 43.º do Regulamento (Versão 3.0, de 4 de junho de 2019), adotadas pelo CEPD.

[26] A propósito destas questões, em termos gerais, é de atender aos estudos de Helena CARRAPIÇO e André BARRINHA (2017), na expetativa de uma próxima publicação de trabalhos específicos, embora estas questões não sejam novas, como mostra o estudo de Roksana MOORE (2013), por exemplo.

[27] Por "«Violação de dados pessoais», [entende-se] uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;" (Art.º 4.º 12) do *RGPD*). No que se refere a esta matéria, é de atender ao conteúdo do muito recente artigo de Stephanie von MALTZAN (2019).

Em especial, estaria em causa uma certificação facultando um 'nível de garantia' 'substancial'[28] ou, até mesmo, um 'alto'[29] (Art.º 52), relativamente a ameaças por parte de terceiros, no sentido de afastar no tempo os riscos resultantes da evolução das tecnologias e da redução dos respetivos custos, pelo menos.

## 5 E PARA PREVENIR RESPONSABILIDADES, PELO MENOS EM PARTE.

Como acabámos de ver, a minimização dos riscos de incumprimento do *RGPD* resultantes de personalizações futura de dados anónimos ou anonimizados, de forma a manter até aos limites do possível a liberdade de tratamento dos mesmo, incluindo a respetiva negociação, implica acompanhar de perto a evolução do estado da técnica, assim como da ações das autoridades, de proteção de dados ou de cibersegurança, no que se refere às certificações de ferramentas ou de procedimentos. Porém, os riscos de incumprimento estarão sempre presentes, apenas podendo ser contidos.

---

28 "6. Um certificado europeu de cibersegurança que ateste um nível de garantia «substancial» dá garantia de que os produtos, serviços e processos de TIC objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos conhecidos para a cibersegurança e do risco de incidentes e ciberataques levados a cabo por autores com competências e recursos limitados. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público e a realização de ensaios para demonstrar que os produtos, serviços ou processos de TIC aplicam corretamente as funcionalidades de segurança necessárias."

29 "7. Um certificado europeu de cibersegurança que ateste um nível de garantia «elevado» dá garantia de que os produtos, serviços e processos de TIC objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos de ciberataques sofisticados levados a cabo por autores com competências e recursos significativos. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público, a realização de ensaios para demonstrar que os produtos, serviços ou processos de TIC aplicam corretamente as funcionalidades de segurança necessárias, ao nível tecnológico mais avançado, e uma avaliação da sua resistência a atacantes competentes através de ensaios de penetração. […]"

No entanto, o procedimento mais eficaz para afastar tais riscos, ainda que inviável em muitos casos, pela própria *natureza das coisas*, passaria pela aplicação da disciplina constante do *RGPD* a todos os tratamentos de dados, pessoais e não pessoais, pelo menos quando fossem empregues tecnologias como as inerentes à "internet das coisas, a inteligência artificial e a aprendizagem automática" (*Considerando* 9 do *Regulamento LFD*)[30]. Designadamente e pelo menos, com a cifragem de tais massas de dados, de modo a prevenir as consequências e responsabilidades resultantes de eventuais "violações de dados"[31].

## REFERÊNCIAS

(Todas as hiperligações foram verificadas no dia 20 de agosto de 2020)

ALSENOY, Brendan Van (2017), "Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation", **JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law**, Vol. n. 7 <https://www.jipitec.eu/issues/jipitec-7-3-2016/4506>

BYGRAVE, Lee A. (2017), "Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements", **Oslo Law Review**, Vol 4. n. 2, pp. 105-120 <https://www.idunn.no/file/pdf/66974311/data_protection_by_design_and_by_default_deciphering_the_.pdf>;

CALZOLAIO, Simone (2017), "*Privacy by design*. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679", **Federalismi.it – Rivista di diritto pubblico ita-**

30 Em síntese, trata-se de observar os "Princípios relativos ao tratamento de dados pessoais" - em especial no que se refere à "limitação das finalidades", à "minimização dos dados" e à sua "integridade e confidencialidade" (Art.º 5.º n.º 1 b) e c) e n.º 2), de acatar os requisitos de licitude que couberem (Art.ºs 6.º a 11.º ), de respeitar pelos "direitos dos titulares dos dados" (Art.ºs 12.º a 22.º), bem como cumprir as obrigações impostas aos responsáveis pelo tratamento (Art.ºs 24.º a 39.º), em especial formulando e seguindo políticas de privacidade (Art.º 24.º n.º 2), metodicamente. A este propósito, vejam-se as considerações breves de Lurdes Alves DIAS (2018), os artigos de Dag Wiese SCHARTUM (2017) e de Filippo A. RASO (2018), os estudos temáticos realizados por mim e por Cristiana Teixeira SANTOS (2018) e (2019), e ainda as reflexões críticas de Miguel MORENO MÚNÕZ (2017).

31 No que se refere à utilização desta técnica no âmbito do *RGPD*, é de referir o trabalho de Gerald SPINDLER e Philipp SCHMECHEL (2016), sendo ainda de muito interesse as reflexões contextuais de Samson Y. ESAYAS (2015).

**liano, comparator e europeo**, n. 24, pp. 2-21 <https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=35361&dpath=document&dfile=22122017172932.pdf&content=%3Ci%3EPrivacy%2Bby%2Bdesign%2E%3C%2Fi%3E%2BPrincipi%2C%2Bdinamiche%2C%2Bambizioni%2Bdel%2Bnuovo%2BReg%2E%2BUe%2B2016%2F679%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B>;

CARRAPIÇO, Helena; BARRINHA, André (2018), "European Union cyber security as an emerging research and policy field", **European Politics and Society**, Vol. 19, n. 3, pp. 299-303 <https://www.tandfonline.com/doi/full/10.1080/23745118.2018.1430712;

CORTE, Lorenzo dalla (2019), "Scoping personal data: Towards a nuanced interpretation of the material scope of EU data protection law", **European Journal of Law and Technology**, Vol. 10 n. 1 <http://ejlt.org/index.php/ejlt/article/view/672/909>;

COTINO HUESO, Lorenzo (2017), "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", **Dilemata – Revista internacional de éticas aplicadas**, n. 24, pp. 131-150 <Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales>;

DANESIS, George *et al*. (2014). **Privacy and Data Protection by Design – from policy to engineering**, ENISA - Agência da União Europeia para a Cibersegurança <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>;

D'ACQUISTO, Giuseppe *et al*. (2015). **Privacy by design in big data - An overview of privacy enhancing technologies in the era of big data analytics**, ENISA - Agência da União Europeia para a Cibersegurança <https://www.enisa.europa.eu/publications/big-data-protection>;

DE MIGUEL ASENSIO, Pedro A. (2019), "Servicios de almacenamiento y tratamiento de datos: el Reglamento (UE) 2018/1807 sobre libre circulación de datos no personales", **La Ley Unión Europea**, n. 66, pp. 1-6 <https://eprints.ucm.es/51323/1/PADemiguelAsensio%20LaLey%20UE%20n%2066%201.19.pdf>;

DIAS, Lurdes Alves (2018), "RPGD: Principais Dificuldades e Dúvidas das Organizações e dos Titulares de Dados Pessoais na Adaptação ao Atual Regime", **Cyberlaw by CIJIC**, n. 6 <https://www.cijic.org/wp-content/uploads/2018/10/RGPD--principais-dificuldades-e-duvidas.pdf>;

DIAS, Fernanda Ferreira (2016), "O Mercado Único Digital Europeu", **Análise Europeia - Revista da Associação Portuguesa de Estudos Europeus**, n. 2, pp. 17-41 <http://www.tfra.pt/wp-content/uploads/an%C3%A1lise_europeia_2__1_.pdf>;

DIJK, Niels van; GELLERT, Raphaël; ROMMETVEIT, Kjetil (2016), "A risk to a right? Beyond data protection risk assessments", **Computer Law & Security Review**, Vol. 32 n. 2, pp. 286-306 <https://www.researchgate.net/publication/294577405_A_risk_to_a_right_Beyond_data_protection_risk_assessments>;

DUCATO, Rossana (2016), "La crisi della definizione di dato personale nell'era del web 3.0", **Quaderni della Facoltà di Giusrisprudenza dell'Università di Trento**, n. 26, pp. 143-178 <https://www.academia.edu/31629227/La_crisi_della_definizione_di_dato_personale_nellera_del_web_3_0_Una_lettura_civilistica_in_chiave_comparata>;

ESAYAS, Samson Yoseph (2015), "The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach", **European Journal of Law and Technology**, Vol. 6 n. 2 <https://ejlt.org/index.php/ejlt/article/view/378/568>;

FREITAS, Pedro Miguel (2018), "The General Data Protection Regulation: an overview of the penalties' provisions from a Portuguese standpoint". **UNIO - EU Law Review**, Vol. 4 n. 2 <http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%204%20.%20Vol%201/Unio%204%20n.%202%20PT/Unio%204%20n.%202%20EN/Pedro%20Miguel%20Freitas%20(1).pdf>;

GIL, Elena (2016), **Big data, privacidad y protección de datos**. Madrid: Agencia Española de Protección de Datos / Boletín Oficial del Estado <https://www.aepd.es/sites/default/files/2019-10/big-data.pdf>;

GRUSCHKA, Nils *et al*. (2018), "Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR", **Proceedings of the 2018 IEEE International Conference on Big Data**, Seattle <https://arxiv.org/pdf/1811.08531.pdf>;

HABEGGER, Benjamin *et al*. (2014), "Personalization vs. Privacy in Big Data Analysis", **International Journal of Big Data**, n. 1, pp. 25-35 <https://perso.liris.cnrs.fr/omar.hasan/publications/habegger_2014_bigdata.pdf>;

HANSEN, Marit; LIMNIOTIS, **Konstantinos (2018), Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default**, ENISA – Agência da União Europeia para

a Cibersegurança <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2>;

HOOFNAGLE, Chris J.; SLOOT, Bart van der; ZUIDERVEEN BORGESIUS, Frederik (2019), "The European Union general data protection regulation: what it is and what it means", **Information & Communications Technology Law**, Vol. 28 n. 1, pp. 65-98 <https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501?src=recsys&>;

JANSSEN, Katleen; HUGELIER, Sara (2013), "Open data as the standard for Europe? A critical analysis of the European Commission's proposal to amend the PSI Directive", **European Journal of Law and Technology**, Vol. 4 n. 3 <https://ejlt.org/index.php/ejlt/article/view/238/411>;

KAMARA, Irene (2017), "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'". **European Journal of Law and Technology**, Vol. 8 n. 1 <http://ejlt.org/index.php/ejlt/article/view/545/725>;

LOPES, Teresa Vale (2018), "Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados", **Anuário da Proteção de Dados 2018**, pp. 45-69 <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>;

LUCCHINI GUASTALLA, Emanuele (2018), "Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori", **Contratto e Impresa**, n. 1, pp. 106-125 <http://www.digiec.unirc.it/documentazione/materiale_didattico/697_2017_1376_29541.pdf>;

MALTZAN, Stephanie von (2019), "No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protection Compliant Incident Response System", **European Journal of Law and Technology**, Vol. 10 n. 1 <http://ejlt.org/index.php/ejlt/article/view/665/894>;

MANTELERO, Alessandro (2016), "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection", **Computer Law & Security Review**, Vol. 22 n. 2, pp. 238-255 <https://www.academia.edu/25657426/Personal_data_for_decisional_purposes_in_the_age_of_analytics_From_an_individual_to_a_collective_dimension_of_data_protection>;

_____ (2017), "Responsabilità e rischio nel Reg. UE 2016/679", **Le nuove leggi civili commentate**, Vol. XL n. 1, pp. 144-164 <https://www.academia.edu/34660169/Responsabilit%C3%A0_e_rischio_nel_Reg_UE_2016_679>;

MASSENO, Manuel David; SANTOS, Cristiana Teixeira (2018), "Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations", **MediaLaws – Rivista di diritto dei media**, n. 2, pp. 251-266 <http://www.medialaws.eu/rivista/assuring-privacy-and-data-protection-within-the-framework-of-smart-tourism-destinations/>;

_____ (2019), "Personalization and profiling of tourists in smart tourism destinations - a data protection perspective", **International Journal of Information Systems and Tourism**, Vol. 4 n. 2, pp. 7-23 <http://www.uajournals.com/ijist-tourism/journal/4/2/1.pdf>;

MENEZES CORDEIRO. A. Barreto (2018), "Dados pessoais: conceito, extensão e limites", **Revista de Direito Civil**, A. 3 n. 2, pp. 297-321 <https://blook.pt/publications/publication/e38a9928dbce/> ;

MORENO MUÑOZ, Miguel (2017), "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", **Dilemata – Revista internacional de éticas aplicadas**, n. 24, pp. 1-23 <https://www.dilemata.net/revista/index.php/dilemata/article/view/412000098/488>;

MOORE, Roksana (2013), "The Case for Regulating Quality within Computer Security Applications". **European Journal of Law and Technology**, Vol. 4 n. 3 <http://ejlt.org/index.php/ejlt/article/view/272/412>;

ORTEGA JÍMENEZ, Alfonso; GONZALO DOMENECH, Juan José (2018), "Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea", **Revista de la Faculdad de Derecho de la Universidad de la República**, n. 44 <http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S2301-06652018000100031&lng=es&nrm=iso>;

PEREIRA, Bruno; ORVALHO, João (2019), "Avaliação de Impacto sobre a Protecção de Dados", **Cyberlaw by CIJIC**, n.º 7 <https://www.cijic.org/wp-content/uploads/2019/05/Bruno-Pereira-e-Joao-Orvalho_RGPD_Avalia%C3%A7%C3%A3o-de-Impacto-sobre-a-Prote%C3%A7%C3%A3o-de-Dados.pdf>;

PICA, Luís (2018). "As Avaliações de Impacto, o Encarregado de Dados Pessoais e a Certificação no Novo Regulamento Europeu de Proteção de Dados Pessoais", **Cyberlaw by CIJIC**, n.º 5 <https://www.cijic.org/wp-content/uploads/2018/03/3_AS-AVALIA%C3%87%C3%95ES-DE-IMPACTO-O-ENCARREGADO-DE-DADOS-PESSOAIS-E-A-CERTIFICA%C3%87%C3%83O-NO-NO-

VO-REGULAMENTO-EUROPEU-DE-PROTE%C3%87%C3%83O-DE-DADOS-PESSOAIS.pdf>;

PURTOVA, Nadezhda (2018), "The law of everything. Broad concept of personal data and future of EU data protection law", **Law, Innovation and Technology**, Vol. 10 n. 1, pp. 40-81 <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176?src=recsys>;

RASO, Filippo A. (2018), "Innovating in Uncertainty: Effective Compliance and the GDPR", **Harvard Journal of Law & Technology Digest** <https://jolt.law.harvard.edu/assets/digestImages/PDFs/Raso_2018-08.pdf>;

RICCIO, Giovanni Maria; PEZZA, Federica (2018), "Certification Mechanism as a Tool for the Unification of the Data Protection European Law", **MediaLaws – Rivista di diritto dei media**, n.º 1, pp. 249-260 <http://www.medialaws.eu/wp-content/uploads/2019/05/18.-Riccio-Pezza.pdf>;

SCHARTUM, Dag Wiese (2017), "Intelligible Data Protection Legislation: A Procedural Approach", **Oslo Law Review,** Vol 4. n. 1, pp. 48-59 <https://www.duo.uio.no/bitstream/handle/10852/61212/intelligible_data_protection_legislation_a_procedural_appr.pdf>;

SCHWARTZ, Paul; SOLOVE, Daniel (2011), "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", **New York University Law Review,** Vol. 86, pp. 1814-1894 <https://fpf.org/wp-content/uploads/2011/07/The%20PII%20Problem%20Privacy%20and%20a%20New%20Concept%20of%20Personally%20Identifiable%20Information.pdf>;

_____ (2014), "Reconciling Personal Information in the United States and European Union", **California Law Review**, Vol. 102, pp. 877-916 <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2103&context=faculty_publications>;

SPINDLER, Gerald; SCHMECHEL, Philipp (2016), "Personal Data and Encryption in the European General Data Protection Regulation", *JIPITEC* - **Journal of Intellectual Property, Information Technology and E-Commerce Law**, Vol. 7 <https://www.jipitec.eu/issues/jipitec-7-2-2016/4440/spindler_schmechel_gdpr_encryption_jipitec_7_2_2016_163.pdf>;

STALLA-BOURDILLON, Sophie; KNIGHT, Alison (2017), "Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymization, Pseudonymiza-

tion and Personal Data", **Wisconsin International Law Journal**, Vol. 34 n. 2, pp. 285-322 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927945>;

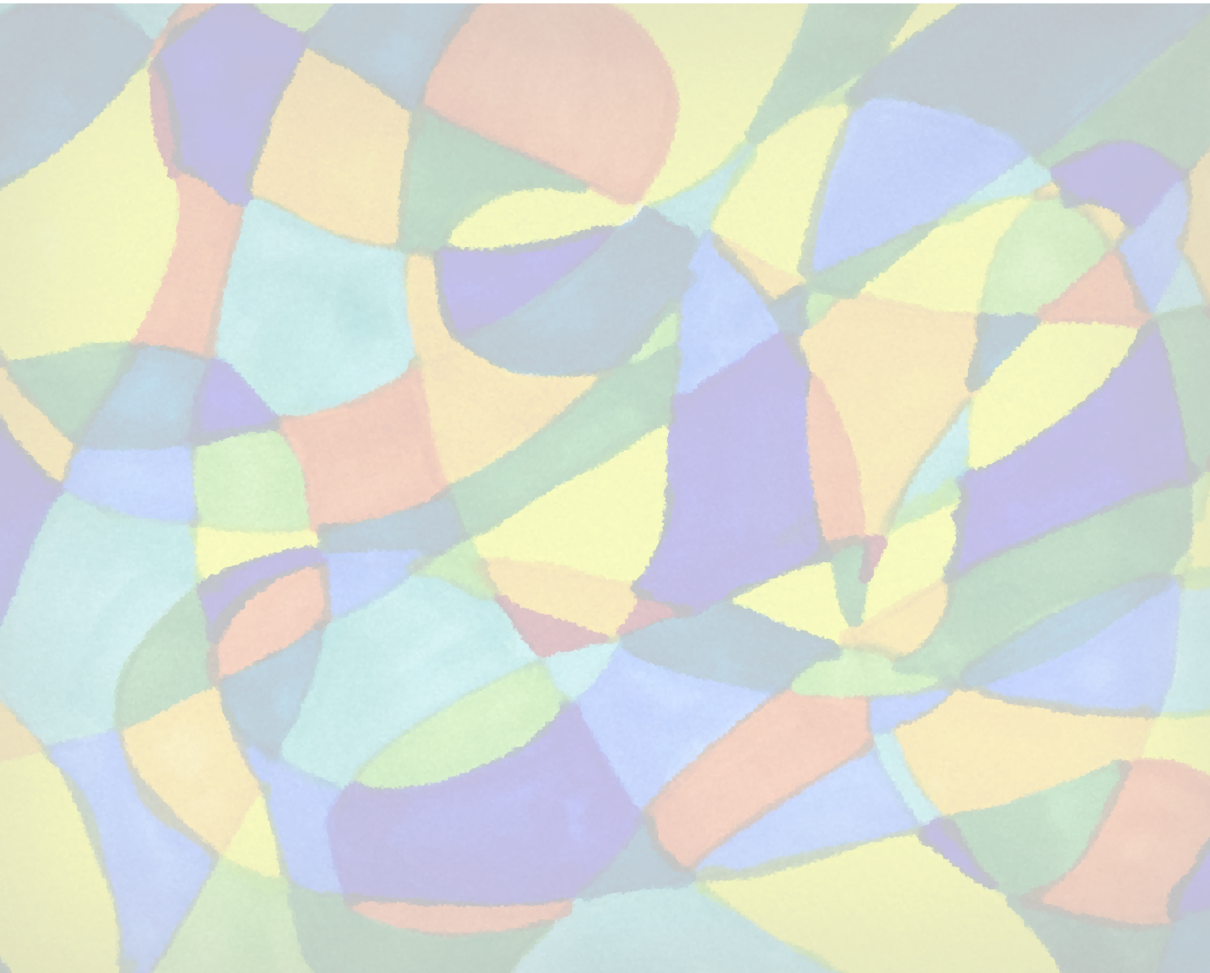
TEIXEIRA, Angelina (2016), "A Chave para a Regulamentação da Protecção de Dados (Das pessoas singulares)", **Data Venia - Revista Jurídica Digital**, n.º 6, pp. 6-32 <https://www.datavenia.pt/ficheiros/edicao06/datavenia06_p005-032.pdf>;

URQUHART, Lachlan; LODGE, Tom; CRABTREE, Andy (2019), "Demonstrably doing accountability in the Internet of Things", **International Journal of Law and Information Technology**, Vol. 27 n. 1, pp. 1-27 <https://academic.oup.com/ijlit/article/27/1/1/5259368>;

VIGURI CORDERO, Jorge A. (2018), "La Certificación en el Nuevo Reglamento Europeo de Protección de Datos y Anteproyecto de Ley Orgánica de Protección de Datos", **El Tiempo de los Derechos**, n. 11 <https://redtiempodelosderechos.files.wordpress.com/2018/01/wp11-certificacion-protecciondedatos.pdf>.

# PARTE II

## *UMA PERSPECTIVA DE DIREITO COMPARADO SOBRE A PROTEÇÃO DE DADOS*



# Seção I

## Princípios jurídicos de tratamento de dados pessoais

# Capítulo I

# OS "PRINCÍPIOS JURÍDICOS" DA LGPD E DO RGPD: uma leitura a partir da Teoria dos Princípios de Humberto Ávila

*Matheus Falk*[1]

**SUMÁRIO**



**RESUMO**

Operadores e teóricos do direito parecem pensar que a distinção entre princípios e regras esteja na "natureza das coisas". Isto é, que certas normas são regras e certas outras princípios, por virtude própria. No entanto, consoante defende Humberto Ávila, não há regras e princípios antes da interpretação. Pelo contrário, tudo depende, nas palavras de Ávila, de uma "interpretação constitutiva do intérprete", já que, ao fim e ao cabo, qualquer enunciado normativo pode ser considerado uma formulação, seja de uma regra, seja de um princípio. Pautado nessas premissas, pretende-se analisar os denominados "princípios" elencados pela Lei Geral de Proteção de Dados (LGDP) e pelo Regulamento Geral de Proteção de Dados, a fim de desvelar as potenciais funções de cada um desses textos normativos nos respectivos ordenamentos jurídicos, de maneira a permitir, ao final, uma interpretação comparada desses institutos.

**Palavras-chave:** Princípios e regras; Teoria dos Princípios; Lei Geral de Proteção aos Dados Pessoais (LGPD); Regulamento Geral Sobre a Proteção de Dados.

## 1 INTRODUÇÃO

Wayne Morrison, em tentativa de conceituar a filosofia do direito, a ela atribui duas possíveis definições: um sentido mais simples, como o

[1] Bacharel e Mestre em Direito das Relações Sociais pela Universidade Federal do Paraná (UFPR). Assessor de Juiz de Direito no Estado do Paraná.

*corpus* de respostas à pergunta *"o que é o direito?"*, e um mais complexo, em que a filosofia jurídica pode ser definida como *a sabedoria em matéria de direito, ou como o entendimento da natureza e do contexto do "empreendimento jurídico"* (MORRISON, 2012, p. 2).

Um conceito de teoria do direito, ou melhor, uma filosofia do direito, tomada em seu sentido mais complexo, é essencial para que o profissional destinado a trabalhar com a juridicidade compreenda o material e as ferramentas a si disponíveis. Sem clareza teórica e o apoio em uma compreensão sólida do empreendimento jurídico, submete-se o jurista a um sem-número de equívocos, desde os mais fundamentais aos mais intrincados. Exemplo do que se diz repousa na distinção entre regras e princípios jurídicos: a ausência de um entendimento aprofundado desses conceitos faz com que os juristas os afirmem como *imanentes*[2], e não como *valores*[3]. Ou seja, advogam a presença intrínseca de um princípio ou de uma regra em determinados textos normativos, enquanto que a melhor técnica, derivada de uma compreensão filosófica do fenômeno jurídico, ensina que só se pode afirmar a presença de uma regra ou princípio como produto da interpretação do texto normativo, em atividade criativa, e não apenas descritiva (ÁVILA, 2016).

Ciente desses conceitos, como interpretar um texto normativo que afirma expressamente cuidar de princípios jurídicos? Tais textos encerram, verdadeiramente, e tão somente, princípios, ou há neles espaço para a criação de regras? Dessas indagações gerais decorre uma particular, tema propriamente do presente trabalho: tanto o ordenamento brasileiro quanto o europeu, em suas legislações protetivas de dados pessoais,

---

2 Nicola Abbagnano apresenta o conceito de imanente como *tudo que, fazendo parte da substância de uma coisa, não subsiste fora dessa coisa.* (ABBAGNANO, 2007, p. 540).

3 Novamente de acordo com Nicola Abbagnano, *a melhor definição de V. é a que o considera como possibilidade de escolha, isto é, como uma disciplina inteligente das escolhas, que pode conduzir a eliminar algumas delas ou a declará-las irracionais ou nocivas, e pode conduzir (e conduz) a privilegiar outras, ditando a sua repetição sempre que determinadas condições se verifiquem. Em outros termos, uma teoria do V., como crítica dos V., tende a determinar as autênticas possibilidades de escolha, ou seja, as escolhas que, podendo aparecer como possíveis sempre nas mesmas circunstâncias, constituem pretensão do V.* à *universalidade e à permanência*. (ABBAGNANO, 2007, p. 993).

encerram o que denominam de *princípios relativos ao tratamento de dados pessoais*. Tais textos normativos são verdadeiramente, e tão somente, princípios, ou deles se podem extrair também regras?

A análise simultânea e comparativa dos ordenamentos brasileiro e europeu se justifica muito em razão da similaridade existente entre seus textos. Nesse contexto, deve-se esclarecer que tal similitude não é acidental, mas deriva da exigência europeia de que um país terceiro ou um organismo internacional assegure um nível de proteção adequado, ou seja, compatível com aquele que é conferido pelo regulamento europeu, a fim de que a transferência de dados pessoais ocorra de maneira legítima[4]. Em decorrência disso, o Brasil, de maneira expedita, tratou de editar uma legislação inspirada no modelo europeu, precipuamente para que as relações comerciais que exijam o intercâmbio de dados pessoais entre os territórios possam ser regularmente mantidas[5].

A própria análise comparativa entre os modelos jurídicos exige, por fim, clareza metodológica. Por essa razão é que se adota o método funcional de direito comparado, na forma desenvolvida por Zweigert e Kötz, apresentada por Paula Maria Nasser Cury (CURY, 2014, p. 178). Procura-se, desse modo, respeitar o núcleo desse método, que pressupõe a compatibilidade do que se compara, isto é, de elementos que preencham as mesmas funções jurídicas. No caso, ao se autodenominarem *princípios relativos ao tratamento de dados pessoais*, e ostentarem franca similaridade entre os textos normativos e os objetivos a que se propõe, tanto as disposições constantes no ordenamento brasileiro quanto no europeu pa-

---

4 Nesse sentido as previsões do Capítulo V do RGPD, bem como o contido no considerando nº 103 desse Regulamento. Sobre o assunto VIOLA, 2019.

5 Nesse sentido a afirmação de Cíntia Rosa Pereira de Lima, ao prefaciar a obra *Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo*, afirmando que*: quanto aos aspectos relacionados à circulação transfronteiriça dos dados pessoais, o modelo estabelecido na União Europeia é a partir do juízo de adequação. Em outras palavras, os dados pessoais de europeus somente podem ser enviados para países que tenham um nível adequado aos padrões europeus de proteção de dados pessoais. De sorte que o Brasil conta com uma lei de proteção de dados pessoais inspirada no modelo europeu, o que se concretizará com a criação da ANPD e sua implantação e atuação de maneira independente, o que colaborará positivamente para a inserção do Brasil no capitalismo informacional.* (TEIXEIRA, 2019, p. 9).

recem objetos destinados a desempenhar funções similares, razão pela qual, presumindo-se a similitude, ciente de que a função cumpre o papel de elemento externo, e pretendendo-se a neutralidade na análise, permite-se a comparação dos direitos, valorando-se, no fim, os resultados obtidos (CURY, 2014, p. 179).

## 2 PRINCÍPIOS E REGRAS: DEFINIÇÃO E APLICAÇÃO DAS ESPÉCIES NORMATIVAS NA TEORIA DE HUMBERTO ÁVILA

O mundo natural é exterior ao Direito. Ainda que a compreensão acerca da existência das coisas e da realidade admita múltiplas versões, advindas de correntes filosóficas, científicas e religiosas distintas, integrada, ainda, por diferentes perspectivas sensoriais, certo é que ela, em si, se difere do Direito. Não há, por assim dizer, amálgama entre o que podemos denominar de "natureza" e o sistema normativo: enquanto aquela se desenvolve de maneira independente das categorizações humanas, nesse, a deôntica conferida pelos imperativos linguísticos a ela atribuídos fornece aos atos e fatos naturais significação jurídica, fazendo com que assim pertençam ao domínio da normatividade[6].

A juridicidade, portanto, é característica atribuída artificialmente à realidade. Mais do que isso, ela é necessária à sustentação de um Estado

[6] Acerca da relação existente entre os planos do ser e do dever ser, imperiosa a citação do que prescreve Hans Kelsen: "O fato externo que, de conformidade com o seu significado objetivo, constitui um ato jurídico (lícito ou ilícito), processando-se no espaço e no tempo, é, por isso mesmo, um evento sensorialmente perceptível, uma parcela da natureza, determinada, como tal, pela lei da causalidade. Simplesmente, este evento como tal, como elemento do sistema da natureza, não constitui objeto de um conhecimento especificamente jurídico – não é, pura e simplesmente, algo jurídico. O que transforma este fato num ato jurídico (lícito ou ilícito) não é sua faticidade, não é o seu ser natural, isto é, o seu ser tal como determinado pela lei da causalidade e encerrado no sistema da natureza, mas o sentido objetivo que está ligado a esse ato, a significação que ele possui. O sentido jurídico específico, a sua particular significação jurídica, recebe-a o fato em questão por intermédio de uma norma que a ele se refere por seu conteúdo, que lhe empresta a significação jurídica, por forma que o ato pode ser interpretado segundo esta norma. A norma funciona como esquema de interpretação". (KELSEN, 2009, p. 4).

que se autodenomine democrático, ou seja, cuja existência e soberania se sustentem baseadas na titularidade do poder político pelo povo, responsável, ainda que indiretamente, pela própria produção normativa a que deve obediência. Por essa razão é que Neil MacCormick, ao tratar do Poder Judiciário, afirma ser "um importante aspecto do Estado de Direito que os tribunais e juízes levem a sério as regras estabelecidas na ordem normativa institucional que constitui os sistemas contemporâneos de Direito das nações" (MACCORMICK, 2008, p. 105).

A seriedade com que é empreendido o mister jurisdicional perpassa por um conhecimento arraigado de sua matéria-prima: as normas jurídicas. E sobre o assunto há, nas palavras de Humberto Ávila, uma "falta da desejável clareza conceitual na manipulação das espécies normativas" (ÁVILA, 2016, p. 44). Com efeito, a fim de que juristas possam regularmente se utilizar do arcabouço normativo à disposição, e que juízes e tribunais possam validamente emitir seus vereditos, devem, em seus processos discursivos e institucionais, manipular os textos normativos de maneira a extrair-lhes regras e princípios. Somente assim, conscientes das possibilidades e limites de cada gênero normativo e das nuances semânticas que lhe são admissíveis, é que podem tanto observar os ditames normativos quanto controlar, apropriadamente, *v.g.*, a atividade voltada ao tratamento de dados pessoais.

A premissa básica estabelecida por Humberto Ávila em sua teoria do Direito é a de que os textos normativos não se confundem com as normas[7]. Ou seja: o fenômeno jurídico, representado pelos atos de interferência na realidade apoiados na linguagem empregada nos dispositivos legais, não é algo mecânico nem instantâneo. Sua exteriorização depende da interpretação manejada por um operador linguístico, que, ao construir (ou *reconstruir*, em termo mais acurado empregado pelo próprio autor, a partir do reconhecimento de uma "autonomia semân-

[7] Nesse sentido, Ávila: *Normas não são textos nem o conjunto deles, mas os sentidos construídos a partir da interpretação sistemática de textos normativos. Daí se afirmar que os dispositivos se constituem no objeto da interpretação; e as normas, no seu resultado*. (ÁVILA, 2016, p. 50).

tica da linguagem"[8]) um sentido a partir do texto normativo, criará a norma, ao aplicá-la consoante esse entendimento. Esse ato de concretização do texto normativo, de convolação da linguagem em facticidade, depende da composição de sentido manobrada pelo intérprete[9]. Dessa forma, de um dispositivo normativo podem exsurgir nenhuma, uma ou várias normas, a depender da interpretação engendrada. Nas palavras do autor: "não há correspondência biunívoca entre dispositivo e norma – isto é, onde houver um não terá obrigatoriamente de haver o outro" (ÁVILA, 2016, p. 51).

Isso ocorre porque a produção legislativa não é fruto de um autor determinado, nem de uma vontade inequívoca na formação do texto. O processo legislativo é complexo, e recebe múltiplas contribuições até a definitiva conformação do texto a ser promulgado. Dessa forma, não há como se falar em significação única e prévia da legislação, porquanto não resulta da vontade de um autor individual. A interpretação não se limi-

---

8 Tal expressão é retirada dos escólios de Frederick Schauer. Nesse sentido a lição do jurista americano: *El contraste entre los modelos conversacional y atrincheirado centra nuestra atención en la autonomía semántica del linguaje, esto es, en la aptitud que poseen los símbolos – palavras, frases, oraciones, párrafos – para portar significados independientes de los propósitos comunicativos que persigan sus usuários em ocasiones particulares. El fundamento de la autonomía semántica podría explicarse em* términos de reglas *linguísticas, de convenciones, de uma referencia socialmente determinada o incluso de otras diversas maneras. Pero ni el nombre ni la fuente del fenómeno son relevantes aquí. Pues cualquiera que sea el nombre que le demos, hay al menos algo - no importa cómo se lo llame - que comparten todos los hablantes de um lenguaje y que les permite ser compreendidos por otros hablantes de ese mismo lenguaje, incluso em aquellos casos en los que el hablante y su interlocutor no tienen nada em común, salvo su lenguaje. Sea lo que fuere aquello que me permite entender algo de lo escrito en un periódico australiano de 1836, pero nada de lo que podría haber escrito em chino em 1991 algún académico del derecho estadounidense de cuarenta e cinco años de edad interesado em las reglas, se trata de algo que se localiza en la comprensión de los usos de los símbolos y que no resulta completamente reducible a lo que um hablante podría desear comunicar em una ocasión particular*. (SCHAUER, 2004, p. 115-116).

9 *Ocorre que a aplicação do Direito depende precisamente de processos discursivos e institucionais sem os quais ele não se torna realidade. A matéria bruta utilizada pelo intérprete – o texto normativo ou o dispositivo constitui uma mera possibilidade de Direito. A transformação dos textos normativos em normas jurídicas depende da construção de conteúdos de sentido pelo próprio intérprete. Esses conteúdos de sentido, em razão do dever de fundamentação, precisam ser compreendidos por aqueles que os manipulam, até mesmo como condição para que possam ser compreendidos por seus destinatários*. (ÁVILA, 2016, p. 44).

ta, portanto, a descrever o sentido dado pelo legislador ao texto legal; ela verdadeiramente constitui o sentido desses textos, deles extraindo os elementos necessários para construir a significação (ÁVILA, 2016, p. 52).

No entanto, não é correto afirmar que as locuções empregadas nos textos normativos sejam despidas de qualquer significado. A construção de sentido pelo intérprete verdadeiramente compõe a norma jurídica, não existindo norma sem essa atividade intelectiva; contudo, a significação estruturada pelo jurista não pode ser completamente desvinculada de um conteúdo mínimo incorporado ao uso técnico ou usual da linguagem. A correlação entre os vocábulos (e suas associações) e os elementos reais que os representam apresenta-se como condição de uso da própria linguagem, e devem ser observados pelo intérprete para uma (re)construção válida das normas a partir dos textos normativos[10].

A construção das normas a partir da composição de sentidos dos textos normativos pelo intérprete é a razão invocada por Ávila para concluir que nem regras, nem princípios são intrínsecos aos dispositivos. Nenhum excerto normativo contém, *a priori,* uma regra ou um princípio: tal qualificação normativa depende dos valores considerados e empregados pelo intérprete no processo de significação do texto, a depender dos fins a cuja realização as normas erigidas servem.

Com isso não quer dizer, entretanto, que um dispositivo possa, ao talante do intérprete, ser reconstruído como regra ou como princípio; apenas esclarece a possibilidade teórica de que se construírem regras e princípios a partir dos mesmos textos normativos[11]. Desse modo, quan-

[10] É o que Ávila define como "uso comunitário da linguagem". (ÁVILA, 2016, p. 53).

[11] Sobre a diferença entre princípios e regras assim pode ser resumida a teoria de Humberto Ávila: *Em vez do modo de aplicação e de conflito, os critérios de diferenciação entre as espécies normativas passam a ser os seguintes: natureza da descrição normativa (as regras descrevem condutas não permitidas, obrigatórias ou permitidas, e os princípios estados ideais a serem promovidos ou conservados); natureza da justificação (as regras exigem um exame de correspondência conceitual, centrado na sua finalidade subjacente, entre a descrição normativa e os atos praticados ou fatos ocorridos, e os princípios exigem uma avaliação da correlação positiva entre os efeitos da conduta adotada e o estado de coisas que deve ser promovido); natureza da contribuição para a decisão (as regras têm pretensão de decidibilidade, pois visam a dar uma solução provisória para um problema conhecido, e os princípios pretensão de*

do o texto normativo privilegiar o caráter descritivo de determinado comportamento, estará o intérprete diante de uma regra, cuja aplicação demanda um exame de correspondência entre a construção conceitual dos fatos e a construção conceitual da norma e da finalidade que lhe dá suporte (ÁVILA, 2016, p. 64). Por outro lado, quando favorecer a descrição de fins normativamente relevantes ou um estado de coisas a ser promovido, colocará o intérprete na presença de um princípio (ÁVILA, 2016, p. 86), cuja concretização exigirá a adoção de comportamentos necessários à sua promoção (ÁVILA, 2016, p. 81).

A teoria de Ávila apresenta o seguinte conceito para a categoria normativa das regras: "as regras são normas imediatamente descritivas, primariamente retrospectivas e com pretensão de decidibilidade e abrangência, para cuja aplicação se exige a avaliação da correspondência, sempre centrada na finalidade que lhes dá suporte ou nos princípios que lhes são axiologicamente sobrejacentes, entre a construção conceitual da descrição normativa e a construção conceitual dos fatos" (ÁVILA, 2016, p. 102).

A regras são *imediatamente descritivas* porquanto estabelecem obrigações, permissões e proibições mediante a descrição da conduta a ser adotada, ou ainda atribuem efeitos jurídicos a determinados atos, fatos ou situações. São *primariamente retrospectivas* na medida em que precipuamente descrevem uma situação de fato conhecida pelo legislador.

A eficácia das regras é *preliminarmente decisiva*, dado que pretendem oferecer uma solução provisória para determinado conflito de interesses já detectado pelo Poder Legislativo. Desse modo, ao descrever a conduta a ser adotada ou a parcela de poder a ser exercida por seu destinatário, afastam considerações de ordem moral que poderiam surgir no momento de sua aplicação, dissuadindo-a ou alterando-a. A própria regra, nesse contexto, se torna uma razão para agir, ou uma razão para de-

*complementaridade, pois servem de razões a serem conjugadas com outras para a solução de um problema). Reitere-se: o ponto central da distinção entre as espécies normativas deixa de ser o conflito e a força normativa nele exteriorizada, e passa a ser a justificação e os elementos a serem considerados*. (ÁVILA, 2016, p. 158).

cidir. A obediência ao seu comando não deve, ainda, se dar tão somente porque editada por uma autoridade competente: a produção de efeitos relativos a valores prestigiados pelo próprio ordenamento jurídico, como segurança, paz e igualdade, permitindo, ainda, uma previsibilidade do comportamento social, se revelam motivos tão importantes quanto a legitimidade de sua fonte produtiva. Por essa razão não devem ser facilmente afastadas, visto que tais situações ocasionariam, caso o distanciamento de seus comandos fossem recorrentes e infundados, custos a um modelo de soluções previsíveis, eficientes e equânimes dos conflitos sociais. A rigidez da regra é bem resumida pelo doutrinador gaúcho: "A opção legislativa pela regra reforça sua insuperabilidade preliminar" (ÁVILA, 2016, p. 130).

Não se negligencia, porém, que os textos normativos cristalizam o resultado de generalizações feitas pelo legislador, existindo, todavia, espaços inicialmente não previstos, ou, caso previstos, dotados de maior ou menor grau de abertura ante a extensão conceitual do texto – conceitos jurídicos indeterminados ou cláusulas gerais – ou pelo uso de fórmulas alternativas – discricionariedade propriamente dita. Nesses hipóteses deverá o aplicador analisar a finalidade da regra, e somente a partir da ponderação de todos os elementos do caso concreto é que pode decidir qual elemento de fato tem prioridade para definir a prioridade normativa (ÁVILA, 2016, p. 68). Sua influência na reconstrução da regra, nesses casos, é ainda maior; entretanto, sempre estará vinculado a um campo semântico de maior ou menos densidade, que deverá ser respeitado a fim de que validamente construa a norma para o caso concreto.

Haverá, ainda, hipóteses em que a superação das regras se fará necessária. Tais situações são excepcionais, e dependem da implementação de condições formais e materiais para sua efetivação[12]. Para tanto, ostenta três requisitos procedimentais: demanda uma *justificativa condizente*,

[12] É o que o autor chama de "eficácia de trincheira". Nesse sentido a lição de Humberto Ávila: "as regras tem eficácia de trincheira, pois, embora geralmente superáveis, só o são por razões extraordinárias e mediante um ônus de fundamentação maior". (ÁVILA, 2016, p. 146).

mediante a conjugação de dois fatores – a demonstração de incompatibilidade da hipótese da regra e sua finalidade específica no caso concreto e a demonstração de que o afastamento da regra não provocará expressiva insegurança jurídica[13], ou seja, "que a justiça individual não afeta substancialmente a justiça geral" (ÁVILA, 2016, p. 147). Exige, ainda, uma *fundamentação condizente*, mediante a exteriorização das razões que permitem a superação, até para que sejam passíveis de controle. Por esse motivo é que "a fundamentação deve ser escrita, juridicamente fundada e logicamente estruturada" (ÁVILA, 2016, p. 147). Por fim, carece de uma *comprovação condizente*, traduzida na constatação, pelos meios de prova adequados, de que a superação não acarretará o "aumento excessivo das controvérsias, da incerteza e da arbitrariedade e a inexistência de problemas de coordenação, altos custos de deliberação e graves problemas de conhecimento" (ÁVILA, 2016, p. 147).

Os princípios, por sua vez, são assim definidos pelo doutrinador: "os princípios são normas imediatamente finalísticas, primariamente prospectivas e com pretensão de complementaridade e de parcialidade, para cuja aplicação se demanda uma avaliação da correlação entre o estado de coisas a ser promovido e os efeitos decorrentes da conduta havida como necessária à sua promoção" (ÁVILA, 2016, p. 102).

Os princípios são *imediatamente finalísticos* na medida em que estabelecem um estado ideal de coisas a ser atingido. Estado ideal de coisas, explica o autor, "pode ser definido como uma situação qualificada por determinadas qualidades. O estado de coisas transforma-se em fim quando alguém aspira conseguir, gozar ou possuir as qualidades presentes naquela situação" (ÁVILA, 2016, p. 95). São *primariamente prospectivos* ao justamente determinar, especialmente, um estado de coisas a ser construído; dessa forma, orienta tanto as ações diretamente praticadas por seus destinatários (indivíduos e poderes estatais), que

[13] Sobre o assunto arremata Ávila: "a decisão individualizante de superar uma regra deve sempre levar em conta seu impacto para aplicação das regras em geral. A superação de *uma regra* depende da aplicabilidade geral *das regras* e do equilíbrio pretendido pelo sistema jurídico entre a justiça geral e a justiça individual". (ÁVILA, 2016, p. 146).

tem o verdadeiro dever de adotar comportamentos necessários à realização de um determinado estado de coisas (ÁVILA, 2016, p. 161), como a compreensão do sentido das regras.

E eficácia dos princípios é bifronte: incide, por um lado, sobre a compreensão do sentido das regras, restringindo ou ampliando seus sentidos a partir da interpretação dos textos normativos e bloqueando a influência de conceitos contrários ao ordenamento, buscando, precipuamente, a promoção de um estado ideal de coisas a ser atingido. Nesse contexto pode ainda integrar ao ordenamento elementos normativos não previstos expressamente em regras codificadas, mas necessários à operacionalização do sistema e à regulação da vida social.

Além dessa faceta há o que Ávila chama de *eficácia externa dos princípios*, que se reporta à *seleção dos fatos considerados pertinentes à solução de uma controvérsia* e ao ônus argumentativo para restrição ou aplicação direta dos *princípios*. No primeiro caso, assume que a escolha dos fatos juridicamente relevantes para o deslinde dos conflitos ocorre, em boa parte, no curso da própria cognição do intérprete, ou seja, em momento concomitante ao da construção da norma. Nesse sentido, "não se interpreta a norma e depois o fato, mas o fato de acordo com a norma e a norma de acordo com o fato, simultaneamente" (ÁVILA, 2016, p. 126). E define que "pertinente será o evento cuja representação factual seja necessária à identificação de um bem jurídico protegido por um princípio constitucional. Com efeito, os princípios protegem determinados bens jurídicos (ações, estados ou situações cuja manutenção ou busca é devida) e permitem avaliar os elementos de fato que lhe são importantes" (ÁVILA, 2016, p. 126).

Quanto ao ônus argumentativo, leciona que sobre os princípios incide o *postulado da justificabilidade crescente*, traduzido na premissa de que, quanto maior for o efeito, direto ou indireto, na preservação e realização de bens e interesses jurídicos protegidos por princípios constitucionais, mais intensa deverá ser a justificação para eventual restrição por parte do Poder Público. A decisão pautada em princípios, por sua vez, deve guiar sua aplicabilidade por meio da ponderação equitativa entre

os princípios concretamente colidentes, porquanto os princípios não trazem, diferentemente das regras, uma solução previamente formatada para o conflito de interesses que pode surgir no processo de aplicação, necessitando, no mais das vezes, da complementação de outros valores, informados por outros princípios, para a efetiva construção da solução[14].

Decidir diretamente baseado em princípios, portanto, acarreta ônus argumentativo inafastável ao intérprete, porquanto deve, sem escusas, justificar ou a ausência de regra para o caso concreto, ou, caso exista, sua inadequação para solucionar o conflito, superando-a de maneira a invocar, diretamente e por meio da ponderação equitativa, princípios para a elucidação da controvérsia. Restringir a aplicação dos princípios, por sua vez, mitiga a implementação de condições necessárias à promoção de um estado ideal de coisas, o que desencadeia, igualmente, forte ônus argumentativo ao operador, seja ele integrante do Poder Público ou integrante de órgão responsável por seu controle. Consoante leciona Ávila: "O Poder Público, se adotar medida que restrinja algum princípio que deve promover, deverá expor razões justificativas para essa restrição, em tanto maior medida quanto maior for a restrição" (ÁVILA, 2016, p. 127).

Sem qualquer pretensão de esgotar a riqueza teórica dos estudos empreendidos por Humberto Ávila, tentou-se demonstrar, a partir de seus escólios doutrinários, como os intérpretes validamente constroem normas e princípios a partir de textos normativos. Conhecer tais premissas é de fundamental importância a quem tem o mister de, eventualmente, controlar atos que afrontem a teia normativa de proteção aos dados pessoais. Mais especificamente, ao se deparar com as atividades de tratamento de dados pessoais, devem os intérpretes discernir se os agentes de tratamento se submetem, em razão das diferentes con-

[14] Nesse sentido Ávila: "Porque os princípios não estabelecem, de antemão, o meio de atuação do Poder Público, eles deixam de vincular o aplicador a uma operação de correspondência entre o conceito da hipótese normativa e o conceito dos fatos do caso. Ao invés disso, o aplicador está incumbido de fazer uma ponderação concretamente orientada entre os princípios conflitantes, ele próprio encontrando os meios adequados, necessários e proporcionais à consecução do fim cuja realização é determinada pela positivação dos princípios". (ÁVILA, 2016, p. 127-128).

sequências, a regras ou princípios, uma vez que, no Brasil, vinculados à observância do que prescreve o art. 6º da LGDP, e, na Europa, ao que dispõe o art. 5º do RGPD, consoante adiante se observa.

## 3 LEI GERAL DE PROTEÇÃO DE DADOS E REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

O Parlamento Europeu e o Conselho da União Europeia foram responsáveis pela edição do Regulamento 679/2016, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Referido regulamento teve sua aplicação iniciada em 25 de maio de 2018[15], substituindo a Diretiva 95/46/CE, que correspondia, até então, ao Regulamento Geral sobre a Proteção de Dados.

Por meio da União Europeia – formação política estabelecida com a assinatura do Tratado de Maastricht, em 7 de fevereiro de 1992, pelos membros da Comunidade Europeia, cuja aglutinação em um bloco internacional para congregação de interesses comuns vinha se avultando desde o término da 2ª guerra mundial – na qual se aglutinam a maioria dos países Europeus, estabelecem-se normativas, na forma de diretivas, recomendações, pareceres, entre outros[16], a fim de, respeitando a inde-

[15] Consoante o texto normativo do Regulamento:
*Artigo 99.º*
*Entrada em vigor e aplicação*
*1. O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia.*
*2. O presente regulamento é aplicável a partir de 25 de maio de 2018.*

[16] Consoante a explanação de Danilo Doneda acerca do tema: *a Diretiva é um instrumento normativo típico da União Europeia. No sistema de fontes do direito comunitário, existem as fontes primárias, que são os tratados que a instituem, ao lado da normativa diretamente derivada deles; e as fontes secundárias, que são basicamente os regulamentos, as diretivas e as decisões, além de outros como as recomendações e pareceres. Em relação exclusivamente à Diretiva, a sua função básica é de uniformização legislativa. A aprovação de uma diretiva implica que cada país-membro adapte, em um certo período de tempo, seu próprio ordenamento jurídico aos moldes estabelecidos pela diretiva, em um processo que leva o nome de transposição – e sua eficácia é tanto maior se levarmos em conta que a falha de um país-membro a transpô-la*

pendência das nações que a compõe, as obrigar, com maior ou menor grau de vinculação, ou à obediência imediata às disposições regulamentares, ou à internalização desses dispositivos nas legislações domésticas.

Ao justificar a edição de uma nova normativa para proteção dos dados, o Parlamento Europeu e o Conselho da União Europeia indicaram que a anterior, constituída na forma de Diretiva, não se mostrava suficiente para tutelar os habitantes de seus Estados-membros, mormente ante os diferentes níveis de internalização do regramento, não adotado em plenitude por todos os Países, e o poderio de captação e tratamento de dados admitido pelas novas tecnologias. Desse modo, optou-se pela redação de um novo texto normativo, constituído na forma de Regulamento, cujo nível de vinculação e aplicação é superior ao da Diretiva[17].

A exposição de motivos do Regulamento 679/2016, redigida na forma de considerandos, deixa claro os objetivos da nova normativa, de incremento do nível de proteção aos dados pessoais[18]. As notas explica-

*tempestivamente acarreta um certo grau de eficácia direta da diretiva e também leva o país a responder pela mora perante a Corte Europeia de Justiça.* DONEDA, 2013, p. 224).

17 Nesse sentido a explicação apresentada pela própria União Europeia, por meio de informação contida em seu sítio eletrônico: *Para alcançar os objetivos estabelecidos nos Tratados, a UE adota diferentes tipos de atos legislativos. Alguns desses atos são vinculativos outros não. Alguns são aplicáveis a todos os países da UE, outros apenas a alguns deles. Regulamentos - Um «regulamento» é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países da UE. Por exemplo, quando a UE quis garantir a aplicação de medidas comuns de salvaguarda aos produtos importados de fora da UE, o Conselho adotou um regulamento. (...) Diretivas - Uma «diretiva» é um ato legislativo que fixa um objetivo geral que todos os países da UE devem alcançar. Contudo, cabe a cada país elaborar a sua própria legislação para dar cumprimento a esse objetivo. É disso exemplo a Diretiva sobre direitos dos consumidores, que reforça esses direitos em toda a UE através designadamente da eliminação de encargos e custos ocultos na Internet e da extensão do período de que os consumidores dispõem para se retirar de um contrato de venda.* Disponível em: https://europa.eu/european-union/eu-law/legal-acts_pt. Acesso em: 12 set. 2020.

18 Nesse sentido os considerandos nº 9, 10 e 11, assim redigidos:
*(9) Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses*

tivas explicitam, ainda, o interesse do Regulamento em normatizar questão que impede o tráfego internacional de dados pessoais com países e organizações não dotados de sistema protetivo de acordo com o da União Europeia, não permitindo, portanto, o endereçamento e a circulação de dados pessoais a quaisquer ambientes e destinatários.

Nesse contexto é que foi aprovada, em 14 de agosto de 2018, no Brasil, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados, com entrada em vigor no mês de setembro de 2020. Em que pese derivada do Projeto de Lei nº 4.060, de 2012, apenas em 22 de maio de 2018 – ou seja, três dias antes do início da eficácia do RGPD – é que recebeu, de seu relator, requerimento de urgência para tramitação[19].

---

*dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças e*
*(10) A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. No que diz respeito ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento. Em conjugação com a legislação geral e horizontal sobre proteção de dados que dá aplicação à Diretiva 95/46/CE, os Estados-Membros dispõem de várias leis setoriais em domínios que necessitam de disposições mais específicas. O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»). Nessa medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais.*
*(11) A proteção eficaz dos dados pessoais na União exige o reforço e a especificação dos direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento e pela definição do tratamento dos dados pessoais, bem como poderes equivalentes para controlar e assegurar a conformidade das regras de proteção dos dados pessoais e sanções equivalentes para as infrações nos Estados-Membros.*

[19] Nesse sentido, a íntegra do requerimento: *https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=7940B2663EF5BB140A428FF22B66F40F.proposicoesWebExterno2?codteor=1662254&filename=Tramitacao-PL+4060/2012*

É inegável o interesse brasileiro na tutela dos dados pessoais, já que sua proteção posiciona-se com corolário do princípio da dignidade da pessoa humana; além disso, apresenta-se como direito e garantia individual implícita, nos termos do art. 5º, IV, X e XII[20], da Constituição da República Federativa do Brasil[21]. O amparo constitucional do direito à proteção de dados[22] é preconizada explicitamente por Danilo Doneda, ao afirmar que *a Constituição Federal de 1988 ocupou-se do assunto e incluiu, entre as garantias e direitos fundamentais de seu artigo 5º, a proteção da 'intimidade' e da 'vida privada' (inciso X), deixando claro que a proteção da pessoa humana abrange estes aspectos"* (DONEDA, 2006, p. 107-108).

---

[20] *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*

*...*

*IV - é livre a manifestação do pensamento, sendo vedado o anonimato;*

*...*

*X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;*

*...*

*XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;*

[21] Consoante a redação empregada na própria Constituição Federal, o rol de direitos e garantias previstos na Carta Política é exemplificativo, e não exaustivo. Nesse sentido o art. 5º, §2º, CF:

*Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*

*...*

§ 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.

[22] A própria potencialidade dos meios informáticos para a publicidade e propagação de informações privadas é objeto de análise pelos constitucionalistas, conforme se observa da reflexão feita por José Afonso da Silva, ao lecionar que: *O intenso desenvolvimento de complexa rede de fichários eletrônicos, especialmente sobre dados pessoais, constitui poderosa ameaça à privacidade das pessoas. O amplo sistema de informações computadorizadas gera um processo de esquadrinhamento das pessoas, que ficam com sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão dos fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento.* (AFONSO DA SILVA, 2011, p. 212).

No entanto, ainda que se reconheça a estatura constitucional do direito que se pretende tutelar com a LGPD, e mesmo a exigência da edição de lei específica contida no art. 3º, III, da Lei nº 12.965/2014 - considerando que um dos pilares que sustentam o Marco Civil da Internet[23] diz respeito justamente à privacidade dos usuários, na qual estão contidos os dados pessoais por eles produzidos (GUERRA FILHO, W. S.; CARNIO, H. G., 2014, p. 24) - , é evidente que a exigência europeia de um nível de proteção adequado para a transferência legítima de dados pessoais foi o verdadeiro propulsor da promulgação da lei brasileira, confirme se verifica, extensamente, do voto do então relator do PL, apresentado em 24 de maio de 2018, um dia antes do início da eficácia do Regulamento europeu[24].

---

[23] Texto integral da Lei n.º 12.965/2014 disponível em: *http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm*. Acesso em: 12 set. 2020.

[24] *Importante pontuar que as propostas se inserem em um contexto mundial, portanto, maior, em que legislações nacionais são introduzidas em cada país, de forma a tratar da questão dos dados pessoais e garantir a proteção das pessoas de maneira harmônica. Ao mesmo tempo, a construção de um arcabouço similar entre os países gera um ambiente propício aos negócios, principalmente globais, oriundos do manuseio de dados. De fato, a Mensagem do Poder Executivo, ao PL nº 5.276/16, ressalta que a proposta é fruto da Resolução da ONU, de 25 de novembro de 2013, sobre "Direito à Privacidade na Era Digital", e que "109 países possuem normas nesse sentido e mais de 90 destes têm uma autoridade pública específica especializada no tema".*
*Grande fonte de inspiração para os projetos advém do arcabouço europeu. O primeiro instrumento daquele bloco na temática é a Convenção do Conselho da Europa nº 108, de 1981, "Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais". O segundo instrumento geral é a Diretiva Europeia nº 46, de 1995, conhecida como Diretiva de Proteção de Dados. Em terceiro lugar, citamos a Diretiva nº 58, de 2002, focada na proteção da privacidade no âmbito das comunicações eletrônicas. Esse conjunto de normas está devidamente internalizado nos países que compõem o bloco.*
*Em 2016, o sistema europeu foi revisado com a aprovação do Regulamento no 679, de 2016, do Parlamento Europeu e do Conselho, de 27/04/2016, que trata da proteção das pessoas naturais com respeito ao processamento de dados pessoais e ao livre movimento desses dados. A Regulação revoga a Diretiva 95/46 e entra em vigência em 25 de maio de 2018. O objetivo da nova regulação é dar resposta apropriada aos rápidos avanços tecnológicos e à globalização, que trouxeram novos níveis de escala da coleta e de compartilhamento de dados pessoais, inclusive transferidos internacionalmente. O novo instrumento fortalece o papel fiscalizatório dos órgãos de controle, bem como entrega às pessoas naturais o poder efetivo sobre seus próprios dados, detalhando os conceitos de transparência e de consentimento destacado. A norma adentra em questões como dados sensíveis, genéticos, anonimização e pseudonimização, legítimo interesse e tratamento global (transferência internacional) dos dados pessoais.*

Muito em razão da clara inspiração brasileira no Regulamento europeu, entre vários dos aspectos comuns a ambas as normativas, encontram-se as disposições indicadas nos art. 6º da Lei Geral de Proteção de Dados e art. 5º da *General Data Protection Regulation*, que afirmam tratar dos princípios inerentes ao tratamento de dados pessoais. Conscientes da definição de princípios e regras a partir do que leciona Humberto Ávila, há como se afirmar que algum dos ordenamentos, ou ambos, disciplinam realmente princípios? Ou também regras? É do que se tratará nos tópicos a seguir.

## 3.1 Princípios e regras na Lei Geral de Proteção de Dados

A Lei nº 13.709/2018, comumente denominada de Lei Geral de Proteção de Dados, garante os seguintes (supostos) princípios a serem observados pelas atividades de tratamento de dados pessoais: princípio da finalidade; princípio da adequação; princípio da necessidade; princípio do livre acesso; princípio da qualidade dos dados; princípio da transparência; princípio da segurança; princípio da prevenção; princípio da não discriminação; e princípio da responsabilização e prestação de contas.

Para que se analise, com responsabilidade teórica, se tais textos normativos podem se amoldar a regras e/ou princípios, imperioso que se rememore, em poucas linhas, os principais atributos que caracterizam cada uma dessas espécies normativas.

---

*Nesta contextualização internacional é importante observar que a Diretiva Europeia, extensamente detalhada e que possui 99 artigos e 173 notas explicativas, não permite a transferência internacional de dados para países que não possuam legislação que garanta a mesma proteção dada pela Lei Europeia. (...)*
*Esse ponto, de a legislação do país estar de acordo com a legislação europeia, é extremamente pertinente neste julgamento, pois indica, como questão de fundo, a atratividade comercial do setor de TIC (Tecnologia da Informação e das Comunicações) dos países. Em tempos de computação em nuvem, um país que atenda à legislação europeia possui condições de atrair processamento de dados daquele bloco. E atrair o tratamento de dados implica não só a possibilidade de instalação de data centers, mas das próprias empresas de TIC, incluindo as gigantes ponto com. Por isso, a necessidade de o Brasil possuir, sem abrir mão de suas especificidades e soberania, uma legislação harmônica com o mundo e com os principais blocos organizados, como a União Europeia.*

De um lado, as regras, de caráter imediatamente descritivo, primariamente retrospectivas e com pretensão de decidibilidade e abrangência, para cuja aplicação se exige a avaliação da correspondência, sempre centrada na finalidade que lhes dá suporte ou nos princípios que lhes são axiologicamente sobrejacentes, entre a construção conceitual da descrição normativa e a construção conceitual dos fatos.

De outro, os princípios, normas imediatamente finalísticas, primariamente prospectivas e com pretensão de complementaridade e de parcialidade, para cuja aplicação se demanda uma avaliação da correlação entre o estado de coisas a ser promovido e os efeitos decorrentes da conduta havida como necessária à sua promoção.

Por fim, deve-se relembrar que a atividade de construção de sentido pelo intérprete compõe a norma jurídica, não existindo norma sem essa atividade intelectiva; contudo, a significação estruturada pelo jurista não pode ser completamente desvinculada de um conteúdo mínimo incorporado ao uso técnico ou usual da linguagem. A correlação entre os vocábulos (e suas associações) e os elementos reais que os representam apresenta-se como condição de uso da própria linguagem, e devem ser observados pelo intérprete para uma (re)construção válida das normas a partir dos textos normativos. Isso significa que, quando o texto normativo privilegiar o caráter descritivo de determinado comportamento, estará o intérprete diante de uma regra, cuja aplicação demanda um exame de correspondência entre a construção conceitual dos fatos e a construção conceitual da norma e da finalidade que lhe dá suporte, enquanto que, quando favorecer a descrição de fins normativamente relevantes ou um estado de coisas a ser promovido, colocará o intérprete na presença de um princípio, cuja concretização exigirá a adoção de comportamentos necessários à sua promoção.

Ciente desses pressupostos, passa-se à análise do texto normativo empregado no art. 6º da LGPD, escandindo-o, após, para escorreita investigação, em cada um de seus incisos. Confira-se, portanto, o texto normativo:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

O primeiro dos anunciados "princípios" indicados no art. 6º da LGPD vem assinalado em seu inciso I, que trata do princípio da finalidade, conceituado da seguinte forma: *realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.*

Verificando a redação empregada ao texto normativo, estamos diante, em tese, de um princípio ou de uma regra? Ao interpretá-lo a partir de um conteúdo semântico mínimo incorporado ao uso técnico, e mesmo usual, da linguagem, não há dúvidas de que o texto não nos apresenta um princípio, mas uma regra. Isso porque não estabelece um *estado ideal de coisas a ser atingido*, mas sim *permissões e proibições*, mediante a descrição da conduta a ser adotada a partir de uma situação de fato conhecida pelo legislador.

Volvendo ao texto normativo, se observa que a norma *permite* que os agentes promovam o tratamento de dados pessoais *apenas* para propósitos legítimos, específicos, explícitos e informados ao titular, e *proíbe* que um tratamento posterior se dê de forma incompatível com essas finalidades. Não estabelece, portanto, um fim a ser perseguido, como se gradativamente se pudesse alcançar o estado ideal indicado pela norma; ao revés, impõe que o tratamento de dados pessoais ocorra, tão somente, para tais finalidades e dentro de referidas balizas, sem o qual o tratamento se mostrará ilegal.

Ademais, em que pese a ausência de previsão, no próprio art. 6º da LGPD, de sanções aplicáveis em decorrência da inobservância de quaisquer de seus incisos, deve-se ter em mente que o art. 52 do mesmo diploma normativo é responsável pela previsão das penalidades administrativas incidentes aos agentes de tratamento de dados em razão das infrações cometidas às normas previstas na Lei nº 13.709/2018[25].

Idêntica conclusão – de que se trata de uma regra e não, precipuamente, de um princípio – se chega ao se analisar as definições apresentadas nos incisos II, III, V, IX e X do art. 6º da LGPD, que tratam, respectivamente, da adequação, da necessidade, da qualidade e da não discriminação no tratamento de dados pessoais.

O primeiro desses textos normativos, ao tratar da adequação, exige que o tratamento dos dados pessoais seja compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento. Desse modo, *proíbe* os agentes de tratarem dados para finalidades não informadas ao titular, o que corresponde não a um estado ideal de coisas a ser

[25] *Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)*
*I - advertência, com indicação de prazo para adoção de medidas corretivas;*
*II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;*
*III - multa diária, observado o limite total a que se refere o inciso II;*
*IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;*
*V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;*
*VI - eliminação dos dados pessoais a que se refere a infração;*
*VII - (VETADO);*
*VIII - (VETADO);*
*IX - (VETADO).*
*X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)*
*XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)*
*XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)*

atingido, mas sim a um modal deôntico característico da regras, preliminarmente decisivas.

O segundo, ao se referir à necessidade, limita o tratamento ao mínimo necessário para a realização das finalidades legítimas do agente. Repete, portanto, uma proibição, ao não admitir que os agentes tratem dados para além do necessário a suas finalidades legítimas, o que corresponde a um enunciado imediatamente descritivo, primariamente retrospectivo e com pretensão de decidibilidade – a uma regra, portanto[26].

O terceiro se remete à qualidade dos dados. Ao prescrever a necessidade de os agentes de tratamento garantirem, aos titulares, exatidão, clareza, relevância e a atualização de seus dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento, *obriga* a esses agentes que observem tal conduta, desvelando tanto a importância sobre o conhecimento da existência de tratamento dos dados pessoais quanto a de que tais dados correspondam à realidade contemporânea. Isso se dá sob pena de correção coercitiva, realizada por meio de ação própria em caso de bancos de dados mantidos por particulares, ou, quando de caráter público ou mantidos por entidades governamentais, por meio de *habeas data*[27], motivo pelo qual não pode ser confundido com um estado ideal de coisas a ser atingido – com um princípio, portanto – mas representa uma clara hipótese de regra.

Quanto ao *habeas* data, integrado ao rol de direitos fundamentais da Constituição Federal, na qualidade de remédio constitucional presente no art. 5º, LXXII[28], CF, e posteriormente regulamentado pela Lei n.º

---

26 *Seria possível apontar, para esse inciso, ainda que com âmbito de aplicação diminuído em relação ao da regra, uma interpretação conforme um princípio, no sentido de os agentes de tratamento envidarem esforços para, cada vez mais, minimizarem a necessidade de tratarem dados, diminuindo a quantidade e extensão do tratamento, considerando suas finalidades legítimas.*

27 Sobre a questão TEIXEIRA, 2019, p. 48-49.

28 *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*

*...*

*LXXII - conceder-se-á habeas data:*

9.507/1997, possui como objetivo assegurar, à pessoa física ou jurídica, o conhecimento de registros a eles concernentes e constantes em repartição pública ou particular acessível ao público, dele podendo, ainda, se valer para retificação, caso necessário, dos dados encontrados[29]. Sua utilização é destinada exclusivamente à tutela dos dados da pessoa física ou jurídica, com vistas ao fornecimento de informações ou correção de dados, não se prestando para outros fins[30]. Há, inclusive, quem defenda que o *habeas data* se confunde com o próprio *direito de autodeterminação informativa*[31].

O quarto diz respeito à impossibilidade de o tratamento de dados pessoais se dar para fins discriminatórios ou abusivos, ou seja, *proíbe* aos agentes tratarem dados com o objetivo de portarem-se de forma injusta ou desigual com uma pessoa ou um grupo de pessoas, por motivos relacionados com suas características pessoais específicas, como cor de pele, nível social, religião, sexualidade, entre outros. Não há, aqui também, estado ideal de coisas a ser atingido ou caráter primariamente prospectivo, próprio dos princípios, mas verdadeira regra a ser obedecida, no aqui e no agora, sendo peremptoriamente proibido o tratamento discriminatório possibilitado mediante a coleta e tratamento de dados pessoais.

---

*a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;*
*b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;*

29 Nesse sentido ver: MEIRELLES, 2013, p. 339.

30 Nesse contexto, novamente a lição de Hely Lopes Meirelles: *os dados e informações a serem obtidos ou corrigidos pelo habeas data devem ter caráter pessoal. Trata-se de garantia constitucional decorrente da chamada liberdade de informática, dando acesso aos bancos de dados para controle das informações neles constantes a respeito da pessoa, do indivíduo, em todos os seus aspectos, políticos, econômicos, sanitários, familiares, etc., segundo entendem a melhor doutrina e a jurisprudência. Assim, não cabe resolver, por exemplo, problemas vinculados ao Registro de Imóveis. (*MEIRELLES, 2013, p. 341).

31 Nesse sentido o escólio de Gilmar Ferreira Mendes e Paulo Gustavo Gonet Branco: *embora formulado de maneira pouco clara, é certo que o habeas data destina-se a proteger aspecto autônomo do direito de personalidade, o chamado direito de autodeterminação sobre informações – Recht auf informationelle Sebstbestimmung –, que assegura a cada indivíduo o poder de decidir quando e em que medida informações de índole pessoal podem ser fornecidas ou utilizadas por terceiros.* (MENDES; BRANCO. 2012, p. 1150-1151).

Por fim, a responsabilização e a prestação de contas reclamam aos agentes de tratamento que adotem medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais. Esse inciso também parece não apontar para um estado ideal de coisas a ser atingido, mas a uma exigência de que os agentes sejam capazes de comprovar que cumprem, efetivamente, as normas protetivas dos dados pessoais.

Por sua vez, os incisos IV, VI, VII e VIII do art. 6º da LGPD, que tratam, respectivamente, do livre acesso, da transparência, da segurança, da prevenção e da responsabilização e prestação de contas no tratamento de dados pessoais, ainda que devam ser conceituados, no mais das vezes, como regras, também podem, em determinadas situações, a depender do contexto da interpretação, serem interpretados como princípios.

Assim se dá, *v.g.*, com o que preceitua o livre acesso, enquanto garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Referido dispositivo, de maneira indubitável, deve ser interpretado como regra, mormente ao obrigar que a consulta sobre a forma, a integralidade e a duração do tratamento dos dados pessoais seja disponibilizada de forma gratuita. Admite, no entanto, interpretação também como princípio, na medida que a facilitação da consulta pode ser também examinada como um crescente investimento no incremento da qualidade das ferramentas disponíveis para consulta aos registros de dados pessoais. Isso porque nem todos os mantenedores de bancos de dados gozam da mesma estrutura tecnológica, e mesmo o acelerado desenvolvimento dessas aplicações pode apontar para uma adoção necessária de novas técnicas de consulta no futuro. Caso o agente não disponha, no momento específico da análise do caso concreto, da mais avançada funcionalidade disponível do mercado, mas apenas de outra mais incipiente, desde que com o objetivo de facilitar a consulta do titular dos dados pessoais, não há como se admitir infração à norma, que

atua em parte como regra, mas também, nesse caso, em caráter prospectivo, como princípio.

A transparência, prevista pelo inciso VI, observa o mesmo destino dado ao inciso IV, referente ao livre acesso, já que deve ser interpretada como regra ao obrigar aos agentes que observem os segredos comercial e industrial ao fornecer informações claras, precisas e facilmente acessíveis aos titulares sobre a realização do tratamento e sobre os respectivos agentes de tratamento; no entanto, ainda que obrigue a prestação de informações claras, precisas e facilmente acessíveis, também pode ter seu texto normativo interpretado como princípio em relação à facilidade de acesso às informações, nos mesmos moldes defendidos para o que a normativa conceitua como livre acesso, mencionado alhures.

A segurança exige aos agentes de tratamento que se utilizem de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, o que, novamente, se remete a um caráter imediatamente descritivo, primariamente retrospectivo e com pretensão de decidibilidade e abrangência próprio das regras, e não a um estado ideal de coisas conectado aos princípios. No entanto, há de se admitir a leitura da segurança também como princípio, ao se compreender, como objetivo de todos os que tratam dados pessoais, o incremento, sempre sob a observância do desenvolvimento tecnológico e do custo de suas aplicações, de seus dispositivos de proteção, mediante adoção das melhores funcionalidades para prevenir – e, quando impossível, mitigar – os danos decorrentes de intercorrências e uso ilegítimo dos dados pessoais. A leitura desse texto normativo como princípio vai ao encontro, ainda, do explicitado para o inciso art. 6º, IV, LGPD.

A prevenção demanda a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. A interpretação do texto normativo como regra é simples: obriga-se aos agentes que adotem medidas para evitar a ocorrência de danos em detrimento do tratamento de dados pessoais. No entanto, há de se interpretar

o texto normativo, em certo contexto, também como princípio, já que não os agentes não devem se limitar à adoção de quaisquer protocolos para obstar a ocorrência de danos. Ao se objetivar uma proteção cada vez mais eficaz aos titulares dos dados pessoais, persegue-se um estado ideal de coisas, ou seja, uma eficácia preventiva máxima, para que danos nunca ocorram aos titulares de dados pessoais – situação que não pode ser exigida, nesses moldes, no caso concreto, mas pode, e deve, ser perseguida pelos responsáveis pelo tratamento de dados pessoais. Sua conceituação guarda importante similaridade com o previsto pelo inciso VII, supramencionado.

De todo o exposto, se verifica que, no ordenamento brasileiro, em que pese a nomenclatura utilizada pelo *caput* do art. 6º da LGPD, os denominados "princípios jurídicos", no mais das vezes, podem – e devem – ser lidos como regras, porquanto submetidos, quando comparados ao âmbito de aplicação no caso concreto, a essa espécie normativa, de caráter imediato e cogente, e não como princípios, já que não representam fins a serem atingidos ou estados ideais de coisas a serem alcançadas.

O ordenamento europeu, de redação similar ao brasileiro, pode ser submetido à mesma análise, a partir da teoria apresentada por Humberto Ávila, a fim de desvelar se seu texto normativo corresponde, submetidos à interpretação, efetivamente a princípios, ou também a regras.

## 3.2 Princípios e regras no Regulamento Geral de Proteção de Dados

Os anunciados princípios garantidos pelo RGPD são: princípio da licitude, lealdade e transparência; princípio da (adequação) limitação das finalidades; princípio da (necessidade) minimização; princípio da (qualidade dos dados) exatidão; princípio da limitação da conservação; princípio da (segurança) integridade e confidencialidade; e princípio da (prestação de contas) responsabilidade, assim descritos em seu art. 5º, *in verbis*:

Artigo 5.º

Princípios relativos ao tratamento de dados pessoais

*1. Os dados pessoais são:*

*a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);*

*b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»);*

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);

f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);

2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo

(«responsabilidade»).

O *caput* do art. 5º do RGPD afirma que o texto de seus incisos tratará de *princípios relativos ao tratamento de dados pessoais*. No entanto, logo ao se analisar a alínea *a*, ciente das premissas obtidas a partir da leitura dos escólios de Humberto Ávila, se verifica que a licitude exigida pela norma não corresponde a um princípio, mas a uma regra, na exata medida em que determina que os dados pessoais sejam tratados dentro da legalidade, não havendo espaço para se considerar um tratamento fora do âmbito legal como legítimo, sob o argumento de que a licitude figura como um estado ideal a ser atingido, na forma de princípio, e não de uma regra. O mesmo se pode dizer em relação à lealdade, já que não podem os agentes de tratamento falsearem informações sobre suas atividades para com os titulares dos dados pessoais, sob pena de ilicitude.

A transparência, por sua vez, deve ser interpretada como regra enquanto dever do agente de tratamento em fornecer informações precisas, verdadeiras e acessíveis aos titulares dos dados pessoais sobre as características e os responsáveis pelo tratamento. Admite, no entanto, clara interpretação como princípio, já que deve guiar as ações dos agentes de tratamento de dados sempre a um maior nível de transparência de suas ações de tratamento de dados, a partir do desenvolvimento tecnológico disponível.

A limitação das finalidades determina que os agentes de tratamento recolham dados, tão somente, para finalidades determinadas, explícitas e legítimas, não podendo trata-los posteriormente de uma forma incompatível com essas finalidades. Referido dispositivo se amolda, com perfeição, à espécie normativa das regras, porquanto subentende-se, de seu texto, o condicionamento da atitude dos agentes de tratamento por meio de modais deônticos: *proíbe* que dados pessoais sejam tratados para finalidades indeterminadas, sub-reptícias e ilegítimas, ainda que a *posteriori*.

A alínea *c* estabelece o dever de minimização dos dados, em que o tratamento de dados deve ser adequado, pertinente e limitado ao que é necessário relativamente às finalidades para as quais são tratados. A hipótese, portanto, também é de uma leitura do dispositivo como regra,

ao impor, no caso concreto, uma proibição ao não admitir que os agentes tratem dados para além do necessário e de suas finalidades legítimas.

A exatidão, referenciada na alínea *d* do art. 5º do RGPD, cuida da chamada exatidão, em que os dados pessoais devem ser exatos e atualizados sempre que necessário, adotando-se as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados. Novamente a melhor interpretação do texto normativo frente ao que se acredita exigir a realidade informa que a hipótese se amolda a uma regra, e não a um princípio, já que *obriga* aos agentes de tratamento que mantenham os dados pessoais da forma como apresentados pelos titulares, o que se coaduna com a pretensão de veracidade. Além disso, os dados devem sempre refletir a verdade contemporânea, e os agentes de tratamento devem permitir que os dados inverídicos sejam apagados ou retificados. O enunciado do texto normativo, porquanto imediatamente descritivo, primariamente retrospectivo e com pretensão de decidibilidade, se refere, portanto, com franca primazia, a uma regra.

O texto normativo vinculado à limitação da conservação também corresponde, interpretado conforme as exigências dos termos que o compõe e a realidade que procura tutelar, a uma regra, ainda que redigida com certa vagueza. O caráter imperativo da norma, ao *proibir* que se mantenham dados armazenados por período superior ao necessário para as finalidades para as quais são tratados não corresponde a uma finalidade, mas a uma obrigação. Tanto o é que estabelece, expressamente, exceção à regra, ao afirmar que os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89º, nº 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados. A própria previsão de exceção à regra serve, portanto, como forte indício à confirmá-la, ao se interpretar o texto normativo.

A integridade e confidencialidade dos dados, presente na alínea *f* do art. 6º do RGPD, permite, por sua vez, de maneira mais facilitada, uma leitura dúplice de seu texto normativo – ora como regra, ora como princípio. De um lado, como regra, exige que os dados pessoais sejam tratados de uma forma que se garanta a sua segurança, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas. Desse modo, obriga que os agentes adotem medidas capazes de proteger os dados pessoais de ingerências ilegais, e mesmo de situações acidentais capazes de causar destruição, perda ou danificação dos dados pessoais. Como princípio, aponta para uma postura dos agentes voltada a uma paulatina melhora de suas ferramentas de proteção aos dados pessoais, vislumbrando um estado ideal de coisas a ser promovido, ou seja, um ambiente totalmente seguro, capaz de impedir qualquer intromissão e utilização indevida dos dados pessoais, e mesmo a danificação, ainda que acidental, de qualquer dos componentes de seu banco de dados.

Por fim, a responsabilidade prevista pelo texto normativo que compõe o item nº 2 se coaduna, indubitavelmente, com uma regra, ao ser interpretada como a *obrigação* do intérprete em cumprir todas as disposições presentes nas alíneas que integram o item nº 1, exigindo que assim possam comprová-lo. Não há, portanto, *prima facie*, largo espaço para adoção de um princípio a partir desse texto normativo, já que expressamente preliminarmente, e não prospectivamente, quem tem o dever de observar os ditames do item nº 1, e, mais do que isso, impõe o dever de que o responsável por tal observância seja capaz de comprovar que agiu de acordo com a norma jurídica.

Ante o exposto, se verifica que o regulamento europeu, ainda que preveja, no *caput* de seu art. 5º, a presença de princípios aplicáveis ao tratamento de dados pessoais, o seu conteúdo, quando interpretado em face do que deve ser realizado pelos destinatários da norma, não se coaduna, no mais das vezes, com a classe normativa correspondente aos princípios, mas sim com a das regras, cujo grau de coercibilidade e forma

de aplicação ostentam um caráter mais rígido e direto na exigência de seu cumprimento.

Há, ainda, um último ponto a ser destacado: o papel da sanção. A exemplo do regulamento brasileiro, os dispositivos constantes no art. 5º do RGPD também devem ser colmatados por outros textos presentes no mesmo diploma jurídico, mormente aquele indicados no art. 83º e ss., que preveem as consequências para o descumprimento das regras indicadas no Regulamento. Essa leitura conjunta dos dispositivos revela que a interpretação dos textos normativos extraídos do art. 5º do RGPD, como regra, respeita a teoria dos princípios apresentada por Ávila, já que se revelam, em consonância com o que defende o teórico gaúcho para as regras, preliminarmente decisivas.

## 3.3 Comparação entre os regulamentos brasileiro e europeu

Consoante se verificou ao se analisar o texto normativo que compõe o art. 6º da Lei Geral de Proteção de Dados, em que pese o *caput* do artigo fazer referência a princípios que devem ser observados nas atividades de tratamento de dados pessoais, seus incisos encerram, em muitos momentos, em interpretação voltada à realidade, regras a serem observadas pelos agentes de tratamento, e não propriamente princípios, com as diferenças inerentes a cada uma das classes normativas.

Da mesma forma, o texto normativo do art. 5º do Regulamento Geral de Proteção de Dados, por mais que apresente, em seu *caput*, supostos princípios relativos ao tratamento de dados pessoais, ao se analisar as alíneas que o compõe, se verifica que a melhor interpretação conduz, na maior parte do tempo, à reconstrução dos textos como regras, e não como princípios.

Há, ademais, franca correspondência entre as normas construídas a partir dos textos prescritos pelo art. 6º da LGPD e pelo art. 5º do RGPD, conforme se pode observar dos conceitos apresentados nos itens ante-

riores. De início, o instituto da finalidade, presente na LGPD, se coaduna com o da limitação das finalidades previsto pelo RGPD, e, em ambos os casos, se concluiu que a espécie normativa correspondente à norma obtida com a interpretação condiz com a classe das regras.

Da mesma forma, a adequação indicada na LGPD se conecta às mesmas peculiaridades inerentes à limitação das finalidades do RGPD, na medida em que ambos os textos normativos, ao serem interpretados para construção da norma, indicam uma proibição, ou seja, uma regra que impede os agentes de tratarem dados para finalidades não informadas ao titular.

A necessidade prevista pela lei brasileira possui correspondente europeu na minimização dos dados, em que ambos os textos normativos, quando interpretados, proíbem que o tratamento vá além do mínimo necessário para a realização das finalidades legítimas do agente. Consoante sobredito, ao corresponder a um enunciado imediatamente descritivo, primariamente retrospectivo e com pretensão de decidibilidade, a interpretação do dispositivo informa sua qualidade precípua de regra, ainda que se possa admitir, com menos frequência para solução de casos concretos, a interpretação como princípio, no sentido de que os agentes de tratamento busquem sempre minimizar a necessidade de tratamento de dados, considerando suas finalidades legítimas.

A qualidade dos dados, consignada no art. 6º, V, LGPD, pode ser comparada à exatidão prevista pelo art. 5º, *1, d*, RGPD, já que ambos preconizam a necessidade de os dados tratados serem fiéis à realidade contemporânea, admitindo-se, quando preciso, o esclarecimento sobre seu conteúdo, e mesmo a correção e a exclusão dos dados que estiverem em desacordo com a facticidade. Ambos os textos, nos ordenamentos brasileiro e europeu, devem ser interpretados como regra, ao obrigarem aos agentes de tratamento que mantenham os dados pessoais da forma como apresentados pelos titulares. A interpretação do texto normativo ostenta tanto o caráter de regra que, no Brasil, a própria Constituição da República prevê ação específica para conhecimento e eventual correção de dados presentes em bancos de caráter público ou mantidos por entidades governamentais, por meio de *habeas data*.

Na LGPD ainda se prevê a segurança no tratamento dos dados, cujo paralelo pode ser feito com a integridade e confidencialidade dos dados do RGPD. No Brasil, a segurança exige aos agentes de tratamento que se utilizem de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Na Europa, a integridade e confidencialidade dos dados exige que os dados pessoais sejam tratados de uma forma que se garanta a sua segurança, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas. Desse modo, obriga que os agentes adotem medidas capazes de proteger os dados pessoais de ingerências ilegais, e mesmo de situações acidentais capazes de causar destruição, perda ou danificação dos dados pessoais. Tais interpretações, no entanto, são as admissíveis aos dispositivos como regra. Há, todavia, que se admitir uma interpretação de ambos, de maneira facilitada, como princípio, ao se compreender, para ambos os ordenamentos, como objetivo de todos os que tratam dados pessoais, o incremento, sempre sob a observância do desenvolvimento tecnológico e do custo de suas aplicações, de seus dispositivos de proteção, mediante adoção das melhores funcionalidades para prevenir e, se necessário, mitigar os danos decorrentes de intercorrências e uso ilegítimo dos dados pessoais.

O último dos dispositivos normativos que admite a comparação entre os ordenamentos é o previsto no art. 6º, X, LGPD e no art. 5º, *2*, RGPD: o primeiro, que trata da responsabilização e prestação de contas, no ordenamento brasileiro, e o segundo, referente à responsabilidade, no ordenamento europeu. Ambos os textos normativos, quando interpretados, merecem ser entendidos como regra, pois obrigam aos agentes que cumpram, e que possam comprovar o cumprimento, de todas as normas protetivas de dados pessoais vigentes em seus respectivos sistemas normativos. Não correspondem, portanto, a um estado ideal de coisas a ser atingido, mas uma regra moldada por um modal deônticos.

Os demais textos normativos não encontram exata correspondência quando comparados os dispositivos consignados no art. 6º da LGPD e art. 5º do RGPD. Deve-se considerar, no entanto, a possibilidade de corresponderem a outros dispositivos indicados nas leis protetivas de dados; tal análise, no entanto, fugiria do escopo do presente trabalho, que busca analisar os dispositivos que expressamente atribuíram a característica de princípio a normas que, consoante a interpretação apresentada, nem sempre correspondem a essa categoria normativa.

De maneira global, portanto, uma análise crítica a partir do que permite o direito comparado informa que a técnica de redação utilizada tanto pelo legislador europeu quanto pelo brasileiro não se coaduna com uma visão contemporânea de filosofia e de teoria do direito, que não enxerga, à priori, regras e princípios nos textos normativos, mas extrai tais espécies normativas enquanto produto da interpretação – justamente o empreendimento que se tentou realizar para desvelar o conteúdo precípuo, pós-interpretação, dos textos informados pelo art. 6º da LGPD e art. 5º do RGPD.

De forma particular, por sua vez, ao se confrontar cada um dos institutos específicos, constantes em incisos e alíneas que supostamente anunciariam a presença de princípios de tratamento de dados pessoais previstos pelo *caput* dos artigos constantes no ordenamentos brasileiro e europeu, se verifica que a interpretação obtida a partir dos textos normativos ostentam correspondências muito próximas, entendendo-se ora como regra, ora como princípio, disposições muito semelhantes, de onde se pode afirmar que muitas das normas obtidas cumprem a mesma função jurídica, mormente a de servir como regras, e não como princípios, a fim de obrigar os agentes de tratamento de dados pessoais à observância coercitiva de comportamentos exigidos pelas legislações.

## 4 CONSIDERAÇÕES FINAIS

A partir da teoria do direito de Humberto Ávila, verificamos que os princípios indicados no art. 6º da LGPD e no art. 5º do RGPD, ainda que

assim nomeados pelo *caput* dos respectivos artigos, não correspondem, intrinsecamente, tão somente, a princípios jurídicos.

Ao escandir os conceitos em cada um dos incisos que compõe os respectivos dispositivos, verifica-se que ambas as legislações estabelecem, em vários momentos, comandos a serem seguidos pelos operadores de dados pessoais, cujas normas não são imediatamente finalísticas, primariamente prospectivas e com pretensão de complementaridade e de parcialidade, mas sim imediatamente descritivas, primariamente retrospectivas e com pretensão de decidibilidade e abrangência – o que se coaduna com a definição teórica de *regra*, e não de *princípio*.

Preliminarmente decisivas, as regras não significam estados ideais a serem alcançados ou modelos a serem perseguidos, mas sim modais deônticos (proibições, permissões e obrigações) a serem observados. São, por esse motivo, de observância cogente aos atores sociais.

A similitude das legislações, ocasionada pela inspiração brasileira na normativa europeia, e o trânsito internacional de dados pessoais permitido pelas atuais tecnologias da informação, admita a partir do que prevê o capítulo V do RGPD, demonstra a importância de uma análise teórica conjunta dos assim chamados "princípios" presentes nos ordenamentos jurídicos brasileiro e europeu. Ao se verificar que tais princípios podem corresponder, em verdade, a regras a partir da interpretação do jurista, resta claro que a nomenclatura indicada pelo legislador brasileiro e o europeu a seus respectivos textos normativos não vincula o tipo de eficácia nem a forma de aplicação daquilo que encerram os artigos ora analisados.

Admite-se, assim, a partir de uma visão apoiada em teoria que compreende o empreendimento jurídico levado a cabo na atualidade, a possibilidade, a capacidade e a necessidade de uma interpretação que aplique, em várias situações concretas, em seus respectivos sistemas, os ditames do art. 5º do RGPD e do art. 6º da LGPD, na forma de regra, e não de princípio.

Tal conclusão, de maneira alguma, mostra-se deletéria aos jurisdicionados, brasileiros ou estrangeiros. Ao revés. O próprio Humberto Ávila reforça a importância e a força das regras frente aos princípios e seu caráter cogente mais imediato e decisivo[32]. Desse modo, ao se advogar a necessidade de se promover, em diversos momentos a leitura dos "princípios" da LGPD e do RGPD, não como princípios, mas como regras, se está fortalecendo o sistema de proteção aos titulares dos dados pessoais de cada um dos sistemas de Direito, ao tempo em que se atua com responsabilidade teórica e clareza conceitual em um ambiente jurídico que demanda, na esteira do que exige o Estado Democrático de Direito, transparência e objetividade de seus atores e de suas ações.

## REFERÊNCIAS

ABBAGNANO, Nicola. **Dicionário de filosofia.** 5ª ed. São Paulo: Martins Fontes, 2007.

AFONSO DA SILVA, José. **Curso de Direito Constitucional Positivo**. 34. ed. rev. e atual. São Paulo: Malheiros, 2011.

ÁVILA, Humberto. **Teoria dos Princípios - Da definição à aplicação dos princípios jurídicos**. 16ª ed. São Paulo: Malheiros Editores, 2016.

CURY, Paula Maria Nasser. Métodos de Direito Comparado: desenvolvimento ao longo do século XX e perspectivas contemporâneas. **Revista de Estudos Constitucionais**, Hermenêutica e Teoria do Direito (RECHTD). UNISINOS. Julho-setembro/2014, p. 176-185.

[32] Consoante os escólios de Ávila: *Até porque, sem outro argumento a modificar a equação, o ônus de superar uma regra é maior do que aquele exigido para superar um princípio. Ao contrário do que se crê, portanto, a opção legislativa pela regra reforça sua insuperabilidade preliminar. Essas considerações revelam, pois, a* diferente funcionalidade *dos princípios e das regras: as regras consistem em normas com pretensão de solucionar conflitos entre bens e interesses, por isso possuindo* caráter "prima facie" forte e superabilidade mais rígida *(isso é, as razões geradas pelas regras, nos confrontos com razões contrárias, exigem um ônus argumentativo maior para serem superadas); os princípios consistem em normas com pretensão de complementaridade, por isso, tendo* caráter "prima facie" fraco e superabilidade mais flexível *(isto é, as razões geradas pelos princípios, no confronto com razões contrárias, exigem um ônus argumentativo menor para serem superadas.* (ÁVILA, 2016, p. 130-131).

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

GUERRA FILHO, W. S.; CARNIO, H. G. Metodologia jurídica político-constitucional e o marco civil da internet: contribuição ao direito digital. *in* Fabiano Del Masso; Juliana Abrusio; Marco Aurélio Florêncio Filho. (Org.). **Marco Civil da internet lei 12.965/2014 e garantias aos usuários**. 1ª ed. São Paulo: Revista dos tribunais, 2014.

KELSEN, Hans, **Teoria Pura do Direito**, 7ª ed. Coimbra: Almedina, 2008.

MACCORMICK, Neil. **Retórica e o estado de direito**. Rio de Janeiro: Elsevier, 2008.

MEIRELLES, Hely Lopes. **Mandado de Segurança e Ações Constitucionais (atualizado por Arnoldo Wald e Gilmar Ferreira Mendes)**. 35ª ed. São Paulo: Malheiros, 2013.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 7. ed. rev. e atual. São Paulo: Saraiva, 2012.

MORRISON, Wayne. **Filosofia do direito:** dos gregos ao pós-modernismo. 2ª ed. São Paulo: Editora WMF Martins Fontes, 2012.

SCHAUER, Frederick. **Las reglas em juego. Un examen filosófico de la toma de decisiones basada en reglas en el derecho y en la vida cotidiana.** Madrid, Espanha: Marcial Pons Ediciones Jurídicas y Sociales, 2004.

VIOLA, Mário. **Transferência de dados entre Europa e Brasil:** Análise da Adequação da Legislação Brasileira. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2019. Disponível em: https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azu l_INTERACTIVE_Justificado.pdf. Acesso em: 10/09/2020.

TEIXEIRA, Tarcísio. **Lei geral de proteção de dados:** Comentada artigo por artigo. Salvador: Editora JusPodivm, 2019.

# Capítulo II

# A SOCIEDADE DE VIGILÂNCIA DIGITAL: o controle da informação e o princípio da autodeterminação informativa

*Rodrigo Otávio Cruz e Silva*[1]

*Laísa Fernanda Alves Vieira*[2]

## SUMÁRIO



## RESUMO

A pesquisa propõe a leitura crítica das relações de poder e contrapoder calcadas em uma sociedade de vigilância com o direito à autodeterminação informativa. O estudo centra-se na dicotomia da vigilância com as prerrogativas de controle dos indivíduos sobre os seus próprios dados pessoais, cotejando esse cenário com a legislação europeia e a legislação brasileira de proteção de dados. A partir do método funcional de direito comparado, busca-se revisitar autores que abordaram a questão do controle e fenômenos como vigilância, internet, informação, liberdades e sujeitos que sucumbem a problemática do tratamento de dados pessoais. A conclusão estrutura-se no sentido da necessidade de melhoria constante do regulamento dos dados pessoais, principalmente pelo seu poder de garantir a autonomia dos indivíduos em relação aos seus dados pessoais.

Palavras-chave: Autodeterminação informativa. Sociedade de Vigilância. Lei Geral de Proteção de Dados. Regulamento Geral de Proteção de Dados da União Europeia.

[1] Doutorando em Direito pela Universidade Federal do Paraná - UFPR. Mestre em Direito pela Universidade Federal de Santa Catarina - UFSC. Bacharel em Direito pela Universidade Federal de Santa Catarina - UFSC. Pesquisador do Grupo de Estudos em Direito Autoral e Industrial (GEDAI/PPGD-UFPR). Advogado. E-mail: rodrigoocs@hotmail.com.

[2] Mestre em Direito das Relações Sociais da Universidade Federal do Paraná/UFPR. Advogada. Pesquisadora do Grupo de Estudos em Direito Autoral e Industrial - GEDAI/UFPR e do Grupo Direito. E-mail: laisafvieira@gmail.com

## 1 INTRODUÇÃO

A informação como elemento de transformação individual e coletivo se tornou central para a vida social e econômica no contexto do paradigma pós-industrial. É a informação apropriada pelo indivíduo que origina a criatividade, e esta, ao conceber e sugerir o novo, contribui para o desenvolvimento em todas as suas dimensões. A relação entre informação, novas tecnologias, ambiente digital e propriedade intelectual, concebeu uma realidade que alterou as formas de acesso e de apropriação da cultura, trazendo à tona o debate sobre o controle da informação.

## 2 A SOCIEDADE DE VIGILÂNCIA DIGITAL: INTERSEÇÃO ENTRE A SOCIEDADE INFORMACIONAL E A SOCIEDADE DE CONTROLE, UMA CRÍTICA AO CONTROLE DA INFORMAÇÃO

É inegável que a evolução tecnológica produziu transformações utilitárias em diferentes aspectos da vida social. Nesse sentido, o fator utilização da tecnologia está ligado à satisfação de interesses de ordens de naturezas diversas, como econômica, política, ideológica, religiosa e militar. É nesse cenário que a apropriação das tecnologias exige uma observação para além da análise reducionista de seus efeitos positivos e negativos enquanto bem intelectual, isso porque o seu domínio repercute sobre os interesses conflitantes dos diversos atores atingidos – como Estados, governos, sociedade, empresas, terceiro setor e indivíduos.

No presente tópico pretende-se estabelecer uma relação crítica entre sociedade informacional e a sociedade de controle e apresentar o pensamento de Byung-Chul Han sobre a sociedade de vigilância digital. Na perspectiva que o domínio da informação, orientado por interesses econômicos e políticos, tende a levar ao controle abusivo das dinâmicas sociais e dos indivíduos, incluído, nesse ponto, a restrição de acesso à propriedade intelectual, apresenta-se o exercício desse poder como entrave ao desenvolvimento e ao progresso humano.

Contudo, antes de apresentar a crítica à soberania do poder político - a partir da visão de Foucault e Deleuze -, para então abordar a relação entre poder, controle, informação e novas tecnologias, mostra-se relevante a relação entre Imprensa, Poderes e Democracia na sociedade informacional. O sociólogo e jornalista francês Ignacio Ramonet desconstrói a ideia de a imprensa continuar a ser considerada o "quarto poder", isto é, o poder proveniente dos meios de comunicação em massa. Na visão do autor, a própria concepção de poder idealizada por Montesquieu já não mais se revela válida na atualidade e, em razão disso, não há que se falar em "quarto poder".

Nessa linha de raciocínio, para Ramonet, é perceptível a existência de três poderes, sendo, porém, o primeiro poder "claramente exercido pela economia. O segundo (cuja imbricação com o primeiro se mostra muito forte) é certamente o midiático – instrumento de influência, de ação e de decisão incontestável – de modo que o poder político só vem em terceiro lugar" (RAMONET, 2001, p. 40).

Nesse ponto, a crítica à soberania do poder político é ressaltada na obra de Michel Foucault. A existência de um poder não estatal nas sociedades disciplinares dos séculos XIX e XX é entendida por Foucault como norma de dominação existente fora do direito, uma espécie de dominação exercida de múltiplas formas no interior da sociedade, e inversa do poder político. Essa dominação fora do poder político foca "não portanto, o rei em sua posição central, mas os súditos em suas relações recíprocas; não a soberania em seu edifício único, mas as múltiplas sujeições que ocorreram e funcionam no interior do corpo social" (FOUCAULT, 2010, p.24).

Para Foucault é nítida a existência de um poder diverso do âmbito jurídico da soberania, dos aparelhos estatais, orientado para as formas de sujeição dos sistemas locais. É quando surge a perspectiva de poder disciplinar, "injustificável, nos termos da teoria soberania, radicalmente heterogêneo". Assim, nas sociedades modernas há de um lado uma legislação que articula o "princípio da soberania do corpo social e da delegação", a soberania estatal, e de outro, "ao mesmo tempo, uma trama cerrada de coerções disciplinares que garante, de fato a coesão desse mesmo corpo social".

Assim, fica superada a ideia do Poder do Estado como fonte única de autoridade. Ressalta-se, portanto, que "o discurso da disciplina é alheio ao da lei", de modo que "as disciplinas vão trazer um discurso que será o da regra; não o da regra jurídica derivada da soberania, mas o da regra natural, isto é, da norma" (FOUCAULT, 2010, p. 31).

A partir das ideias de Foucault, Gilles Deleuze, filósofo da pós-modernidade, anunciou a nova realidade normalizadora sob a ideia da *sociedade de controle*, sentido em "que no novo paradigma da sociedade de controle as novas tecnologias de poder são realizadas como reino do biopoder" (FOUCAULT, 2010, p. 204). A antiga sociedade disciplinar *foucaultiana* estaria dando lugar à sociedade de controle[3], na qual as antigas instituições de confinamento vivem uma crise generalizada – a prisão, a escola, os hospitais, a fábrica e a família. Os muros de confinamento das instituições disciplinares vão sendo superados pelos fluxos contínuos, por espaços abertos, porém controlados.

A saída da sociedade disciplinar foucaultiana – na qual a indústria cultural de massa era um poderoso instrumento de dominação – entra no que Gilles Deleuze, filósofo da pós-modernidade, chamou de sociedade de controle, onde as formas de mobilização das populações para a extração de mais-valia, objetivo último do capitalismo, apresentam-se mais interligadas e em níveis mais infrapessoais. A sociedade de controle é a denominação utilizada para dar conta desse novo tipo de atuação do sistema capitalista sobre a massa da população.

É nesse ponto que a sociedade informacional encontra a sociedade de controle. Enquanto o crescente fluxo de informação sujeita a vida das pessoas, determina a consciência social (MARX, 2008, p. 47), e promove uma nova forma de capitalismo de valorização da informação e da criati-

[3] "Os ministros competentes não param de anunciar reformas supostamente necessárias. Reformar a escola, reformar a indústria, o hospital, o exército, a prisão; mas todos sabem que essas instituições estão condenadas, num prazo mais ou menos longo. Trata-se apenas de gerir sua agonia e ocupar as pessoas, até a instalação das novas forçar que se anunciam. São as *sociedades de controle* que estão substituindo as sociedades disciplinares". DELEUZE, Gilles. Postt-scriptum sobre as sociedades de controle. In **L'Autre Journal,** n. 1º, maio de 1990. Trad. Peter Pál Pelbart. Conversações: 1972-1990. Rio de Janeiro: Ed. 34, 1992. p. 220.

vidade humana, a necessidade contínua de apreensão de seu conteúdo ilimitado, a necessidade de acesso e de domínio das tecnologias informacionais, bem como o monitoramento dos fluxos de informação e de indivíduos pelas máquinas informacionais, observa-se uma nova forma de dominação pelo controle social informacional. Isso porque "o poder agora é exercido mediante máquinas que organizam diretamente o cérebro (em sistemas de comunicação, redes de informação, etc.) e os corpos (em sistemas de bem-estar, atividades monitoradas, etc.) no objetivo de um estado de alienação independente do sentido da vida e do desejo de criatividade"[4].

É assim que as novas tecnologias das sociedades informacionais são vistas em operação nas sociedades de controle idealizadas por Deleuze:

> É fácil fazer corresponder a cada sociedade certos tipos de máquina, não porque as máquinas sejam determinantes, mas porque elas exprimem as formas sociais capazes de lhes darem nascimento e utilizá-las. As antigas sociedades de soberania manejavam máquinas simples, alavancas, roldanas, relógios; mas as sociedades disciplinares recentes tinham por equipamento máquinas energéticas, com o perigo passivo da entropia e o perigo ativo da sabotagem; as sociedades de controle operam por máquinas de uma terceira espécie, máquinas de informática e computadores, cujo perigo passivo é a interferência, e o ativo a pirataria e a introdução de vírus (DELEUZE, 1990, p. 223).

Portanto, para o controle social, o uso das novas tecnologias informacionais é tido como uma expressão do exercício do poder na sociedade contemporânea, sendo ferramentas de afirmação da sociedade de controle.

---

[4] HARDT, M. Negri, A. **Império**. Rio de Janeiro, Record, 2001. APUD FONSECA, Ricardo Marcelo. O poder entre o direito e a 'norma': Foucault e Deleuze na Teoria do Estado "in" FONSECA, Ricardo Marcelo (org.). **Repensando a teoria do Estado**. Belo Horizonte: Fórum, 2004.

A partir desse pensamento, surgem novos e complexos problemas, dentre os quais se destacam a tutela da privacidade e a resistência ao controle informacional, numa lógica contrária ao "dever" de fornecimento de informações pelo indivíduo ao poder público e ao setor privado como contrapartida de benefícios sociais.

Assim, Stefano Rodotà destaca dois pontos de atenção: a) a dificuldade de individuar quais tipos de informação poderia o cidadão renunciar ao controle; b) o problema do controle sobre os sujeitos recebedores de informações, ou seja, o problema do controle relativo ao uso das informações coletadas pelas organizações públicas e privadas para desenvolver seus programas, o que permitem o surgimento de novas concentrações de poder ou o fortalecimento de poderes existentes (RODOTÀ, 2008).

Essa relação entre poder e controle ganha dimensão mundial por meio do domínio da informação e das novas tecnologias. A evolução da sociedade informacional não se deu de maneira neutra, isenta de juízos de valor, e a tecnologia da informação "como todas as tecnologias, foi escolhida e moldada de conformidade com certos e determinados interesses sociais e políticos" (KUMAR, 1997, p. 46).

As recentes tecnologias desenvolvidas pelos grandes provedores de conteúdo, destinadas a monitorar na internet as atividades dos usuários e impedir infrações a direitos autorais, promoveram um amplo debate sobre os limites da tecnologia e a tutela da privacidade. Pamela Samuelson ao indagar se as empresas da internet deveriam notificar os usuários sobre as tecnologias de proteção dos direitos autorais, entende que os usos da tecnologia – monitoramento e a coleta de dados – ao permitir a discriminação de preços e a utilização do perfil dos consumidores para fins comerciais, configura invasão à privacidade. Assim, a pesquisadora defende uma política de transparência pelas empresas de internet em prol de seus usuários, e que "*should be required to give their customers effective notice of any such monitoring and of uses that they intend to make of such data*" (SAMUELSON, 2019).

Ademais, para Klaus Schawab, o problema do acesso à informação pode levar à assimetria de informações que possibilitam o surgimento de assimetrias de poder. Nesse ponto, a questão da titularidade ou mesmo da oportunidade de acesso ao conhecimento necessário para o domínio das novas tecnologias, está ligado ao surgimento de desigualdades entre "indivíduos conhecedores da tecnologia – que compreendem e controlam essas tecnologias – e aqueles que a conhecem menos – os usuários passivos de uma tecnologia que não entendem"(SCHWAB, 2016, p. 77).

É nessa linha que o que se observa é a concentração cada vez maior do poder nas mãos dos titulares da informação, cuja relação muitas vezes é direta com o domínio da tecnologia e da informação e da propriedade intelectual[5]. Nas palavras de Coelho, o próprio processo de globalização pode ser visto sob essa ótica de estandardização e controle, cujo poder transcende Estados e nações, para além do âmbito militar e econômico, compreendendo inclusive o plano social – ciência, cultura e ideologia[6]. Assim, a realização da cibernética permite o controle dos comportamentos sociais pela manipulação da informação, ao promover todo tipo de controle das máquinas sobre os seres humanos, afastando-se assim da finalidade coletivista de conferir autonomia individual e emancipação social, superados pela progressiva "colonização cultural e virtual dos povos" (COELHO, 2001, p. 25).

---

5 "Esses acontecimentos caracterizaram uma segunda revolução industrial, não menos importante que a primeira, que tem sido denominada de *revolução informática* ou *revolução cibernética*. É que o aperfeiçoamento e extrema sofisticação dos computadores, como máquinas que controlam outras máquinas, possibilita também o controle dos comportamentos individuais e coletivos para muito além do que a ficção jamais imaginara, com evidentes repercussões nos estudos sociais em geral. E assim, pode-se descrever o paradigma da transmodernidade como consistindo basicamente numa visão da realidade através dos programas de computador". (COELHO, 2001. p. 21).

6 "Em suma, a globalização pode ser definida como um poderoso processo de estandardização da cultura a nível mundial. Só que isso ocorre segundo os padrões e critérios de quem detém a maior parcela de poder na sociedade pelo domínio da informação, da ciência e da tecnologia; e um tal poder hoje transcende a nação e o Estado, projetando-se como poder mundial, não somente militar e econômico, mas científico, cultural e ideológico. Ou seja, o poder está como nunca jamais se vislumbrou nas mãos de quem domina o saber, que hoje se identifica com o crescente domínio da tecnologia e da informação" (COELHO, 2001. p. 20).

O filósofo sul-coreano Byung-Chul Han em suas recentes obras, como em "Sociedade do Cansaço" (2015) e "No enxame: perspectivas do digital" (2017), apresenta a lógica do controle como a lógica do capitalismo neoliberal contemporâneo. O autor analisa fenômenos como internet, informação, comunicação digital, hipercomunicação, vigilância, liberdade, redes sociais, individualismo, e o novo sujeito do desempenho. Eis o problema do presente no encontro entre a sociedade informacional e a sociedade do controle, o problema da vigilância, do psicopoder, do controle das liberdades e dos fluxos de informação pelos detentores do domínio das tecnologias informacionais.

Para Byung-Chul Han, fazendo alusão ao panóptico de Jeremy Bentham (1785)[7] e a ideia de Big Brother superada pelo Big Data, a sociedade atual vive a realidade de um panóptico digital. A confiança, como práxis social, torna possível as relações entre indivíduos num quadro de desconhecimento recíproco. A conexão digital e a facilidade no acesso a informações tornam, de certa forma obsoleta, ou melhor dizendo, desnecessária a confiança, posto que "onde se pode adquirir muito rápido e facilmente informações, o sistema social muda da confiança para o controle e para a transparência"[8].

No panóptico digital, diferente da ideia de células isoladas, o que se observa é uma intensa comunicação entre os indivíduos. O panóptico digital é abastecido em tempo real com as informações geradas voluntariamente pelos indivíduos. Vive-se a ilusão da liberdade. E é justamente a liberdade de "conexão e a hipercomunicação que tornam o controle total

[7] Representante do Utilitarismo, o projeto de Bentham concebeu a planta de uma penitenciária ideal. Pelo projeto, um único vigilante pode observar todos os prisioneiros sem que estes saibam se estão sendo observados. (BENTHAM, 2008).

[8] "No panóptico digital não é possível nenhuma confiança – ela não chega nem mesmo a ser necessária. [...]. A conexão digital facilita a aquisição de informações de tal modo que a confiança, como práxis social, perde cada vez mais em significado. Ela dá lugar ao controle. Assim, a sociedade da transparência tem uma proximidade estrutural à sociedade de vigilância. [...]. Todo clique que eu faço é salvo. Todo passo que eu faço é rastreável. Deixamos rastros digitais em todo lugar. Nossa vida digital se forma de modo exato na rede. [...]. No lugar do Big Brother, entra o Big Data". (HAN, 2018, p. 122).

possível"[9]. A vigilância é feita não apenas por governos, mas inclusive por empresas de tecnologia, buscando a máxima exploração da informação. É quando o "mercado de vigilância no Estado democrático tem uma proximidade perigosa do Estado de vigilância digital"[10].

Uma contribuição relevante do pensamento de Han é a ideia de superação do biopoder de Foucault pelo *psicopoder*. O panóptico digital, diferente da sociedade disciplinar (biopoder), transforma a sociedade em sociedade da transparência psicopolítica (psicopoder). O psicopoder vigia, controla e influencia o indivíduo não de fora, mas a partir de dentro. Essa sociedade digital de vigilância, "que tem acesso ao inconsciente-coletivo, ao comportamento social futuro das massas, desenvolve traços totalitários"[11].

---

9 "A sociedade da vigilância digital apresenta uma estrutura especial panóptica. O panóptico de Bentham consiste de células isoladas umas das outras. [...]. Os habitantes do panóptico digital, em contrapartida, se conectam e se comunicam intensamente uns com os outros. Não o isolamento espacial e comunicativo, mas sim a conexão e a hipercomunicação que tornam o controle total possível. Os habitantes do panóptico digital não são prisioneiros. Eles vivem a ilusão da liberdade. Eles abastecem o panóptico digital com informações que eles emitem e expõem voluntariamente". (HAN, Op. cit, 2018, p. 122).

10 "A vigilância e o controle são uma parte inerente da comunicação digital. [...]. Aqui, todos observam e vigiam a todos. Não são apenas serviços secretos do governo que nos espionam. Empresas como o Facebook ou o Google trabalham elas mesmas com serviços secretos. Elas expõem a nossa vida para conseguir capital em troca das informações espionadas. Firmas espionam os seus funcionários. Bancos examinam a fundo potenciais clientes de crédito. [...]. O mercado de vigilância no Estado democrático tem uma proximidade perigosa do Estado de vigilância digital. Na sociedade de informação contemporânea, na qual o Estado e o mercado se fundem cada vez mais, as atividades da Acxionm, do Google e do Facebook se aproximam das atividades de um serviço secreto. [...]. Aspira-se em todo lugar a uma exploração máxima da informação. [...]. Todos são o Big Brother e o presidiário simultaneamente. Essa é a consumação digital do panóptico de Bentham". (HAN, Byung-Chul. Op. cit, (2018). p. 124, 126-127).

11 "Hoje uma nova mudança de paradigma se realiza. O panóptico digital não é uma sociedade disciplinar Biopolítica, mais sim uma sociedade da transparência psicopolítica. E, no lugar do biopoder, entra o psicopoder. [...]. O psicopoder é mais eficiente do que o biopoder na medida em que vigia, controla e influencia o ser humano não de fora, mas sim a partir de dentro. A psicopolítica se empodera do comportamento social das massas ao acessar a sua lógica inconsciente. A sociedade digital de vigilância, que tem acesso ao inconsciente-coletivo, ao comportamento social futuro das massas, desenvolve traços totalitários. Ela nos entrega à programação e ao controle psicopolíticos. A era da Biopolítica está, assim, terminada. Dirigimo-nos, hoje, à era da psicopolítica digital". (HAN, Op. cit, 2018, p. 130).

Outro autor contemporâneo, crítico da vigilância e controle dos indivíduos pelas novas tecnologias e pela coleta de dados, é Bernard E. Harcourt. Em sua obra "Exposed: desire and disobedience in the digital age", o autor fala que a economia digital derrubou as clássicas fronteiras e promoveu o colapso do Estado, economia e sociedade. Fato é que as empresas de tecnologia promovem vigilância, comercializam dados pessoais e influenciam posições políticas. O grande volume de dados produzidos na rede no Big Data está fundindo política, economia e sociedade, criando um enorme mercado de dados, que permite a empresas e governos "to identify and cajole, to stimulate our consumption and shape our desires, to manipulate us politically, to watch, surveil, detect, predict, and, for some, punish"[12].

Para Harcourt, as fronteiras entre governo, comércio e vida privada entraram em colapso, circunstância que está impedindo os indivíduos serem indivíduos. Resistir ao excesso de Estado – seus órgãos oficiais de controle e vigilância – pode ser difícil, mas tentar controlar um gigante voraz, que inclui a NSA, Google, Facebook, Netflix, Amazon, Samsung, Target, Skypes e Microsoft, compreendendo governo, comércio, vigilância e esfera privada, é ainda mais assustador. Governar está entrando no comércio, pois Estados como China, Rússia e EUA procuram garantir a "soberania digital" por meio da regulamentação de legislações comerciais voltadas ao regime da proteção de dados de seus cidadãos, impondo a empresas armazenamento de dados em servidores locais ou restrição de

[12] "THE DIGITAL ECONOMY has torn down the conventional boundaries between governing, commerce, and private life. In our digital age, social media companies engage in surveillance, data brokers sell personal information, tech companies govern our expression of political views, and intelligence agencies free-ride off ecommerce. The customary lines between politics, economics, and society are rapidly vanishing, and the three spheres are melding into one—one gigantic trove of data, one colossal data market, that allows corporations and governments to identify and cajole, to stimulate our consumption and shape our desires, to manipulate us politically, to watch, surveil, detect, predict, and, for some, punish. In the process, the traditional limits placed on the state and on governing are being eviscerated, as we turn more and more into marketized malleable subjects who, willingly or unwittingly, allow ourselves to be nudged, recommended, tracked, diagnosed, and predicted by a blurred amalgam of governmental and commercial initiatives". (HARCOURT, 2015. p. 404).

atuação a provedores de Internet. Também o comércio está entrando na vigilância com a política de coletas de dados pessoais das empresas. Ainda, o comércio está entrando na esfera do governo na medida em que surgem novos mercados de dados, permitindo que empresas, vendedores, burocratas, anunciantes e a polícia coletem dados sobre os hábitos dos indivíduos: vigilância sobre os movimentos diários, físicos e digitais, sobre consumo, a comunicação, os gostos, as opiniões e os pensamentos (HARCOURT, 2015, p. 404).

Na raiz do problema está a busca por soberania em assuntos de interesses globais estratégicos, na concorrência econômica e comercial, cujo impulso principal culminou na conhecida espionagem econômica denunciada por Glenn Greenwald, a partir de documentos vazados da NSA por Eduard Snowden. Nessa grande fusão entre o público e privado, o fim das fronteiras e a perda de soberania oficial numa realidade em que os interesses econômicos orientam os movimentos planetários, apenas em último plano, aparece os interesses dos indivíduos, a proteção da vida privada e de seus dados.

A presente crítica se mostra relevante na medida em que se observa que o desenvolvimento social é profundamente influenciado pelo domínio e pelo acesso à informação, além das novas tecnologias.

Acrescenta-se, também, o debate sobre a regulamentação da internet. A narrativa das últimas décadas sobre a internet focou no tema das inovações e implicações para a indústria digital, já para a próxima década o debate será sobre encontrar a melhor política, regulamentação e governança para o desenvolvimento econômico e social[13].

[13] "It is increasingly clear, however, that while the narrative of the last decades has been one around the driving forces of technical innovations and their implications for the Internet industry, the narrative of the next decade will be around the forces of policy, regulation and governance. With this emerging push for more regulatory control of the Internet, it is not only critical to address governance structures, but also to find appropriate models for regulating a technology that is significantly different from older media governed by old regulatory models. Finding the best structures, processes and models for governance over the coming decade will shape the future vitality of the Internet and the overall vitality of local and global economic and social development". (DUTTON, 2016).

O controle de toda a rede é "a ambição dos novos colossos das indústrias da informação que, para chegar lá, continuam a multiplicar as fusões, as aquisições e as concentrações" (RAMONET, 2001, p. 128). Tais movimentos reforçam a lógica da informação e da comunicação como uma mercadoria a ser produzida às massas. E não pode passar despercebido que a concentração de mercado e de poder desses gigantes da internet elevam o problema do controle da informação, os conteúdos criados e disponibilizados, opondo em grande parte das vezes, de um lado, os interesses econômicos dos grupos de domínio da informação e, de outro, o interesse político e cultural da sociedade e seus indivíduos.

O fenômeno do deslocamento do controle da informação para além das fronteiras e do domínio dos Estados é uma realidade que deve ser vista com preocupação pela comunidade internacional, com atenção a temas como proteção de dados, regulamentação de setores tecnológicos e da internet, e, para o presente trabalho, o acesso à propriedade intelectual.

Apresentado o encontro da sociedade informacional com a crítica da sociedade do controle, verifica-se no centro do problema o controle da informação como uma expressão do exercício do poder na sociedade, bem como a importância das TICs para a retomada democrática do exercício de controle social (vigilância cidadã) sobre as condutas dos agentes públicos[14].

Feita essa análise, passa-se ao estudo da informação e da propriedade intelectual na perspectiva econômica da sociedade informacional.

[14] "[...], as TIC podem facilitar o acesso à informação e à transparência e, assim, contribuir para que a população exerça um poder efetivo de ação e controle. Por meio do conhecimento das informações públicas, pode haver um controle social sobre as condutas dos atores políticos responsáveis pela administração e o uso dos recursos públicos.". (SÁNCHES, 2019. p. 9).

## 3 A INFORMAÇÃO NA SOCIEDADE INFORMACIONAL: UMA VISÃO DO FENÔMENO DA SINGULARIDADE DA INFORMAÇÃO E O RECONHECIMENTO DO SEU VALOR ECONÔMICO

A informação é o mais importante elemento de transformação do ser humano. O seu poder está no seu potencial de transformar culturalmente o indivíduo, o ambiente social e a própria humanidade. A importância da informação está no papel de difundir o conhecimento com o propósito transformador e, consequentemente, contribuir para o desenvolvimento. Portanto, ao reconhecer a informação como fator desenvolvimento individual e coletivo, a decisão de privilegiar o seu acesso a determinados indivíduos e instituições implica em tornar a informação instrumento de dominação e controle, compreendido nesse ponto a centralidade também do acesso à propriedade intelectual como elemento informacional.

A respeito da perspectiva econômica, a informação ganhou contornos de mercadoria no sistema capitalista. Como informado anteriormente, a partir da década de 1980 a revolução das TICs implementou um importante processo de reestruturação do sistema capitalista. Na visão de Castells, o final do século XX está associado ao surgimento do informacionalismo, um modo de desenvolvimento associado à nova estrutura social. O surgimento das tecnologias da informação exerceu grande influência na transformação dos modos de desenvolvimento capitalista. Enquanto o industrialismo persegue o crescimento econômico e a maximização da produção, o informacionalismo tem no desenvolvimento tecnológico a sua essência, a partir dele ocorre a acumulação de conhecimento e o surgimento de novos meios de processamento da informação. A diferença entre os modos de desenvolvimento agrário, industrial e informacional, pode ser vista nas palavras de Castells, que ressalta:

> "[...]. Cada modo de desenvolvimento é definido pelo elemento fundamental à promoção da produtividade no processo produtivo. Assim, no modo agrário de desenvolvimento, a fonte do incremento de

> excedente resulta dos aumentos quantitativos da mão-de-obra e dos recursos naturais (em particular) no processo produtivo, bem como da dotação natural desses recursos. No modo de desenvolvimento industrial, a principal fonte de produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo dos processos produtivo e de circulação. No novo modo informacional de desenvolvimento, a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos. [...], o que é específico ao modo informacional de desenvolvimento é a ação de conhecimentos sobre os próprios conhecimentos como principal fonte de produtividade. O processamento da informação é focalizado na melhoria da tecnologia do processamento da informação como fonte de produtividade, em um círculo virtuoso de interação entre as fontes de conhecimentos tecnológicos e a aplicação da tecnologia para melhorar a geração de conhecimentos e o processamento da informação." (CASTELLS, 2011, p. 53-54).

Feita a diferenciação entre os modos de desenvolvimento e destacada a centralidade da informação, é possível afirmar que as TICs foram determinantes para a evolução do capitalismo e a sua atual dimensão planetária.

Na década de 1970 a virada cibernética selou "a aliança entre o capital e a ciência e a tecnologia, e conferiu à tecnociência a função de motor de uma acumulação que vai tomar todo o mundo existente como matéria-prima à disposição do trabalho tecnocientífico". O fenômeno da virada cibernética não se limita à nova lógica da técnica informática, mas ressalta também a "perspectiva de uma dominação irrestrita da natureza pelo homem, inclusive da natureza humana" (SANTOS, 2003. p. 10-11), levando à concepção do "estado de natureza cibernético", em que a natureza é natureza como informação, sujeita ao processamento e ao armazenamento pelo computador.

Numa visão capitalista, o estado de natureza informacional sugere um modelo "dadocêntrico" de economia, onde tudo pode ser traduzido em informação apropriável como matéria-prima a ser processada pelas

tecnologias com valor para o capitalismo global, ou seja, todos os aspectos da existência humana passam a ter relevância econômica com potencial para se tornar ativo rentável. E nesse aspecto a ideia de encontro das sociedades informacional e de controle sugerem o fundamento do "capitalismo dadocêntrico". Para esses novos mercados informacionais é relevante apreender um perfil e monitorar a personalidade, os gostos e os movimentos diários dos indivíduos, independente da relação com atividade profissional ou pessoal (MOROZOV, 2018. p. 33).

Ora, a fonte ideal, o suprassumo do modelo capitalista de coleta de informação desse novo mercado de coleta e tratamento de dados estaria no carro autônomo operado pelo Google, que "não seria apenas um veículo autônomo, mas também um santuário à vigilância – sobre rodas!" (MOROZOV, 2018, p.31).

Uma crítica ao modelo de capitalismo dadocêntrico em que todas as informações têm relevância econômica é vista nas palavras de Evgeny Morozov:

> O modelo de capitalismo 'dadocêntrico' adotado pelo Vale do Silício busca converter todos os aspectos da existência cotidiana em ativo rentável: tudo aquilo que costumava ser o nosso refúgio contra os caprichos do trabalho e as ansiedades do mercado. Isso não ocorre apenas pela atenuação da diferença entre trabalho e não trabalho, mas também quando nos faz aceitar tacitamente a ideia de que nossa reputação é uma obra em andamento – algo a que podemos e devemos nos dedicar 24 horas por dia, sete dias por semana. Dessa maneira, tudo vira um ativo rentável: nossos relacionamentos, nossa vida familiar, nossas férias e até nosso sono (agora você é convidado a rastrear o sono, a fim de aproveitá-lo ao máximo no menor tempo possível)" (MOROZOV, 2018, p.31).

Essa apropriação das informações dos indivíduos para alimentar o novo mercado informacional reafirma o ditado que se popularizou no meio digital que, "se o serviço na web é gratuito é porque você é o produto". Essa afirmação destaca a falta de transparência na atuação das gigan-

tes da internet, e o desconhecimento público do alcance da monetização das informações pessoais para o mercado mundial.

A visão de Evgeny Morozov ressalta a crítica ao poderio alcançado por empresas de tecnologia como o Google[15] que, quando sujeitas ao debate público promovido por ativistas da *web* sobre a necessária quebra do monopólio tecnológico, apresenta em sua defesa argumentos estritamente técnicos do debate digital, excluindo de forma proposital a inafastável relação de suas atividades com o debate político e econômico. Defende o autor como crítica ao atual capitalismo global concentrado nas mãos das gigantes da tecnologia que "o verdadeiro inimigo não é a tecnologia, mas o atual regime político e econômico"[16].

Assim, para o autor defende o futuro tecnológico depende da desvinculação do neoliberalismo, e para que os indivíduos retomem a soberania sobre a tecnologia, é necessário a compreensão emancipadora da conquista sobre a economia e a política (MOROZOV, 2018, p.24-25).

Para José de Oliveira Ascensão, apesar da tomada de "consciência que a *informação é o elemento estratégico do processo social*", a exponencial disponibilidade de informação no seio sociedade da informação não traduz necessariamente em informação assimilada, em conhecimento gerado. Apesar da aparente diversidade, quando os dados são

---

15 Visão crítica ao poderio informacional do Google: "[...]. Não seria ótimo que um dia, diante da afirmativa de que a missão do Google é 'organizar as informações do mundo e torná-las acessíveis e úteis para todos', pudéssemos ler nas entrelinhas e compreender o seu verdadeiro significado, ou seja, 'monetizar toda a informação do mundo e torna-la universalmente inacessível e lucrativa'? Esse ato de interpretação subversiva eventualmente nos possibilitaria alcançar a maior de todas as compreensões emancipadoras: deixar o Google organizar todas as informações do mundo faz sentido quanto deixar Halliburton lidar com todo o petróleo do planeta" (MOROZOV, 2018. p. 28-29).

16 "Há um motivo simples para o debate digital parecer tão vazio e inócuo: definido como 'digital' em vez de 'político' e 'econômico', desde o princípio o debate é conduzido em termos favoráveis às empresas de tecnologia. Sem o conhecimento da maioria de nós, a natureza aparentemente excepcional das mercadorias em questão – desde a 'informação', passando pelas 'redes', até a 'internet' – está codificada em nossa linguagem. É essa excepcionalidade oculta que permite ao Vale do Silício descartar seus críticos, chamando-os de ludistas, os quais, ao se oporem à 'tecnologia', à 'informação' ou à 'internet' – não se usam plurais no Vale do Silício, pois toda nuance traz o risco de confundir seus cérebros -, também devem ser opositores do 'progresso'" (MOROZOV, 2018, p. 29-30).

filtrados e controlados "não há informação, há *desinformação*" (ASCENSÃO, 2003, p. 24)[17].

Esse problema decorre do interesse empresarial e do tratamento da informação como mercadoria, o que leva ao movimento de "monopolização e privatização" da informação. Quando o acesso à informação apresenta cada vez mais restrições, "esses gravames servem as empresas de informação, mas não a informação e o conhecimento das pessoas" (ASCENSÃO, 2003, p. 24).

Na ideia da "informação em risco na sociedade da informação", transcreve-se a posição do autor sobre a relação entre informação e mercado, e o efeito negativo do controle da informação sobre o desenvolvimento social:

> Mas se se abandonam todas as considerações qualitativas e o critério passa a ser dado pelo mercado; se os entes públicos se demitem de qualquer função orientadora; então a informação será produto de supermercado, mas não conduzirá a uma sociedade de conhecimento ou ao desenvolvimento da cultura(ASCENSÃO, 2003, p. 25).

A partir desse novo estágio da tecnociência o armazenamento e o processamento de todas as informações existentes, traduzidas como matéria-prima com valor, passou a ser a realidade do novo modo de desenvolvimento informacional. É através desse garimpo e, especialmente, do processamento das informações existentes – o mundo como um banco de dados – que se estimula o surgimento de inovações.

Ocorre que, apesar do indiscutível reconhecimento econômico e da centralidade que a informação - compreendida a propriedade intelectual - alcançou nos mercados, tal realidade deve ser tratada com responsabilidade e presença dos governos por meio de políticas públicas que garantam o acesso à informação e objetive o desenvolvimento social pautado na diversidade cultural. A liberdade econômica não pode ser si-

[17] Disponível em: http://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Ascensao-Jose-PROPRIEDADE-INTELECTUAL-E-INTERNET.pdf. Acesso em: 04 dez. 2019.

nônimo de controle e desinformação, pelo contrário, a mercantilização da informação deve encontrar harmonia com o desenvolvimento e o respeito à diversidade cultural.

Diante desse breve panorama, observa-se o desenvolvimento do paradigma informacional está atrelado à singularidade da informação, e ao reconhecimento da propriedade intelectual como ato criativo decorrente da gestão da informação. As tecnologias informacionais para além de dominar os elementos naturais, operar máquinas, controlar a produção, aumentar a produtividade e os lucros, têm como finalidade viabilizar a humanidade (LÉVY, 2000. p. 42). Portanto, as novas tecnologias ao propagar a informação e o conhecimento estimulam o surgimento de novas técnicas que podem beneficiar a sociedade como um todo.

Hoje, o domínio da natureza, o extrativismo, a pecuária, a agricultura e a pesca não são mais centrais na economia, é a informação e seu produto, a criatividade, que ditam os novos rumos do desenvolvimento seja econômico ou social. E nessa conta, tanto informações pessoais e empresariais, que podem ser objeto de tratamento como os bens da propriedade intelectual, se tornaram elementos de fundamental importância na complexa nova economia.

## 4 O PRINCÍPIO DA AUTODETERMINAÇÃO INFORMATIVA: ENTRE A LGPD E O RGPD

Nesse quadrante de ideias, onde a informação toma um papel central na nova dinâmica social, imperioso se faz falar das tentativas de forma de controle dos indivíduos sobre as suas próprias informações. A autodeterminação informativa surge como forma de se conferir ao sujeito uma postura ativa no exercício de seus dados pessoais, dando-lhes formas de contrapoder e controle oponíveis contra o Estado e particulares.

Tal circunstância advém como um instrumento de defesa da realização da personalidade. Portanto, a autodeterminação informativa é

entendida como a autonomia do indivíduo em controlar o fluxo de suas informações, tendo uma forma de controle acerca do modo como a sua personalidade será exposta para a sociedade (SCHWABE, 2005, p. 202).

Fato é que a autodeterminação informativa não é uma garantia ilimitada das pessoas contra a ingerência externa sobre o fluxo de suas próprias informações, entretanto, é uma forma de lhe conferir o gerenciamento de sua autoexposição social.

Nesse compasso, surgem legislações na tentativa de normatizar e contribuir com a autodeterminação informativa como expressão de proteção da privacidade. No âmbito Europeu, os dados pessoais são normatizados pelo Regulamento Geral de Proteção de Dados 2016/679 (RGPD), o qual influenciou os debates para a aprovação da Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/2018).

Em essência, ambas as legislações vêm assegurar aos cidadãos o direito à autodeterminação informativa em relação aos seus dados pessoais fornecidos a terceiros. Em que pese as suas diferenças estruturais, a principiologia das legislações é conferir aos sujeitos – cidadãos europeus e brasileiros - um empoderamento digital no que trata à coleta e tratamento desses dados.

As legislações possibilitam perceber uma tendência mundial em se tutelar a proteção da privacidade e dos dados pessoais, consolidando no direito positivo mecanismos para os indivíduos garantirem um nível adequado de oposição contra os controladores de dados. Nesses termos, apesar de não serem legislações à prova de críticas, já que apresentam problemas práticos em diversos aspectos, deve-se reconhecer o esforço político e social empregado em tutelar os dados pessoais na sociedade de controle.

Como visto, o indivíduo titular dos dados pessoais deve ter controle, ou ao menos *plena transparência*, sobre a destinação dada às suas informações pessoais, bem como das metodologias utilizadas para tanto. A autodeterminação informativa abriga a filosofia de que o indivíduo titular de dados pessoais deve ser o protagonista das matérias relaciona-

das ao tratamento de seus dados pessoais, trazendo ao sujeito o foco das operações em preocupação perpétua com a privacidade.

Diante desta noção é que surge o direito do titular de opor-se a operações de tratamento de seus dados pessoais realizadas sem o sem consentimento e que também não encontrem respaldo em nenhuma outra modalidade de base legal, ou seja, é o direito de impedir ou requerer a interrupção de operações ilícitas de seus dados pessoais.

Na LGPD, a autodeterminação informativa encontra guarida expressa no art. 18, onde constam direitos conferidos ao titular como a confirmação da existência do tratamento, acesso aos dados, correção de dados incompletos, inexatos ou desatualizados, anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei, dentre outros. Verifica-se como a normativa confere ao titular um contrapoder em relação a utilização de seus dados pessoais.

No RGPD, vislumbra-se a autodeterminação informativa de modo expresso na parte que trata dos direitos do titular dos dados, a exemplo da Secção 2, artigo 13º, 2: o titular possui o direito de se opor ao tratamento, bem como solicitar a sua retificação, apagamento ou o seu apagamento. Tais regras são especificas em conceder formas de controle ao titular dos dados.

Tais prerrogativas aglutinam-se na tendência de o consentimento do titular dos dados admitir o tratamento dos dados pessoais. Essa via enseja que será permitido o tratamento dos dados pessoais havendo manifestação inequívoca do titular pra determinada finalidade. A natureza do objeto aqui é personalíssima, onde não pode pairar qualquer tipo de vício, sendo ela dada para um fim concreto. Observe-se, pois, como o consentimento é fruto da autodeterminação informativa. Tanto a LGPD quanto o RGPD preveem condições e qualificações aplicáveis pra efetivação do consentimento, sendo ele protagonista no liame regulatório.

Se outrora a privacidade se comunicava com o direito de manter-se anônimo, em maior ou menor grau, o conceito hoje se comunica mais com o nível de controle que o indivíduo tem sobre as operações realiza-

das com a sua autorização, e com o nível de transparência e segurança daquelas realizadas sem a sua autorização mas com base em outro autorizador legal.

## 5 CONSIDERAÇÕES FINAIS

Assim, temos que o princípio da autodeterminação informativa confere ao titular dos dados a palavra final no que diz respeito às operações de tratamento dos seus dados pessoais, via de regra, e, mesmo quando não puder opor-se ao tratamento, nos casos em que este se der com base em outros interesse, confere ao menos o direito de informação sobre a limitação de finalidade desses dados e quanto à segurança conferida a eles.

## REFERÊNCIAS

RAMONET, Ignacio. **A Tirania da Comunicação**. 2ª ed. Trad. Lúcia Mathilde Endlich Orth. Petrópolis, RJ: Vozes, 2001. p. 40.

FOUCAULT, Michel. **Em defesa da sociedade**. São Paulo: Martins Fontes, 2010. p. 24.

FONSECA, Ricardo Marcelo. O poder entre o direito e a 'norma': Foucault e Deleuze na Teoria do Estado "in" FONSECA, Ricardo Marcelo (org.). **Repensando a teoria do Estado**. Belo Horizonte: Fórum, 2004, págs, 269-270.

DELEUZE, Gilles. Postt-scriptum sobre as sociedades de controle. In **L'Autre Journal**, n. 1º, maio de 1990. Trad. Peter Pál Pelbart. Conversações: 1972-1990. Rio de Janeiro: Ed. 34, 1992. p. 220.

DELEUZE, Gilles. Conversações. Post-Scriptum sobre as Sociedade de Controle, in **L´Autre Journal**, n. 1, maio de 1990. Trad. Peter Pál Pelbert. Rio de Janeiro: ed. 34, 1998 p. 223. (DELEUZE, 1990, o. 223)

MARX, Karl. **"Prefácio" à Contribuição à Crítica da Economia Política**. Trad. Florestan Fernandes. São Paulo: Expressão Popular, 2008. p. 47

RODOTÀ, Stefano**. A vida na sociedade da vigilância**: a privacidade hoje. Trad. Danilo Doneda e Luciana C. Doneda. Rio de Janeiro: Renovar, 2008. p. 36-37

KUMAR, Krishan. **Da sociedade pós-industrial à pós-moderna**: novas teorias sobre o mundo contemporâneo. Trad. Ruy Jungmann. Rio de Janeiro: Jorge Zahar Editor, 1997. p. 46.

SAMUELSON, Pamela. **Should Copyright Owners Have to Give Notice About Their Use of Technical Protection Measure**s?, 6 J. Telecom. & High Tech. L. 41 (2007). Disponível em: http://people.ischool.berkeley.edu/~pam/papers.html. Acesso em: 21/10/2019.

SCHWAB, Klaus. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016. p. 77.

COELHO, Luiz Fernando. **Saudade do futuro**. Florianópolis: Fundação Boiteux, 2001. p. 21.

BENTHAM, Jeremy [et al]. **O Panóptico**. Trad. Guacira Lopes Louro, M. D. Magno, Tomaz Tadeu. 2. ed. Belo Horizonte: Autêntica Editora, 2008. O panóptico, ou, a casa de inspeção.

HAN, Byung-Chul. **No enxame**: perspectivas do digital. Trad. Lucas Machado. Petrópolis-RJ, Vozes, 2018. p. 122

HARCOURT, Bernard E. **Exposed: desire and disobedience in the digital age**. Cambridge, Massachusetts: Harvard University Press, 2015. p. 404

DUTTON, Willian H. **Multistakeholder Internet Governance**? Background Paper for World Development Report 2016 Digital Dividens, Michigan State University. 2016.

RAMONET, Ignacio. **A Tirania da Comunicação**. 2ª ed. Trad. Lúcia Mathilde Endlich Orth. Petrópolis, RJ: Vozes, 2001. p. 128.

SÁNCHES, Olga Del Rio *et al*. **TIC para o desenvolvimento sustentável**: recomendações de políticas públicas que garantem direitos. Montevidéu, UNESCO, 2019. p. 9

CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia, sociedade e cultura. v. 1. São Paulo: Paz e Terra, 2011. pp. 53-54.

SANTOS, Laymert Garcia dos [et. al.]. **Revolução tecnológica, internet e socialismo**. São Paulo: Ed. Fundação Perseu Abramo, 2003. p. 10-11 e 14.

MOROZOV, Evgeny. **Big Tech**: a ascensão dos dados e a morte da política. Trad. Claudio Marcondes. São Paulo: Ubu Editora, 2018. p. 33.

ASCENSÃO, José de Oliveira. **Propriedade Intelectual e Internet**. Texto apresentado na Conferência II Ciberética, Florianópolis, 14.11.2003. p. 24 Disponível em: http://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Ascensao-Jose-PROPRIEDADE-INTELECTUAL-E-INTERNET.pdf. Acesso em: 04/12/2019.

LÉVY, Pierre. **A inteligência coletiva**: por uma antropologia do ciberespaço. Trad. Luiz Paulo Rouanet. 3. ed. São Paulo: Loyola, 2000. p. 42

SCHWABE, Jürgen. **Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. MARTINS, Leonardo (org. e introdução). Tradução de Beatriz Henning et al. Montevideo: KonradAdenauer-Stiftung E. V., 2005, p. 202. Disponível em: https://www.kas.de/c/document_library/get_file?uuid=c0b-3d47d-beba-eb55-0b11-df6c530ddf52&groupId=252038. Acesso em: 12 nov. 2019, p. 189.

# Seção II

## Dados pessoais e seu tratamento sob perspectiva técnica e multissetorial

# Capítulo I

# A CLÁUSULA ABERTA DOS INTERESSES LEGÍTIMOS E AS AUTORIDADES NACIONAIS: análise comparativa entre LGPD e RGPD

*Marcus Paulo Röder*[1]

*Pedro Perdigão Lana*[2]

## SUMÁRIO



## RESUMO

O presente artigo é fruto de pesquisa que se valeu da metodologia de direito comparado, precisamente do método funcional de comparação, realizada no intuito de comparar ordenamentos jurídicos de países europeus - notadamente a partir de orientações de autoridades nacionais e casos concretos - em aplicação do Regulamento Geral da Proteção de Dados da União Europeia (RGPD) em perspectiva comparada com o ordenamento jurídico brasileiro, em razão do recente advento da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) e que, tal qual o RGPD, também prevê a hipótese dos interesses legítimos como base legal para tratamento de dados, visando identificar bases e diretrizes que poderão nortear a aplicação do instituto e da legislação protetiva de dados pessoais no Brasil.

**Palavras-chave:** Proteção de dados pessoais; Bases legais para tratamento; Interesses legítimos; Autoridade Nacional de Proteção; Regulamento Geral de Proteção de dados da União Europeia.

[1] Advogado. Mestrando em Direito no Programa de Pós-Graduação da Universidade Federal do Paraná (PPGD/UFPR). e-mail: mp.roder@gmail.com

[2] Advogado. Mestrando em Direito Empresarial na Universidade de Coimbra e graduado em Direito pela UFPR. Pesquisador do GEDAI/UFPR. Membro do conselho diretor do Youth SIG/Internet Society.

## INTRODUÇÃO

A Sociedade Informacional em que vivemos, fruto da revolução tecnológica eclodida vigorosamente a partir do final do século XX, cada vez mais se baseia no modelo econômico denominado de economia movida a dados ("*data-driven economy*"), onde as informações (sejam dados pessoais ou não) são insumos essenciais para praticamente todas as atividades econômicas (CASTELLS, 2005, *passim*; SRNICEK, 2018, p. 39).

A utilização de dados e informações[3] pessoais é inegavelmente essencial para o desenvolvimento da maior parte das atividades econômicas - seja para as que já estão em exercício e desenvolvimento ou para as atividades que ainda surgirão futuramente no mercado.

Ocorre que, se por um lado os contributos do desenvolvimento tecnológico são positivos para este novo modelo econômico - na medida em que proporciona a capacidade de processamento de informações em grande escala e permite a interação simultânea entre indivíduos com uma comunicação global e em rede (superando o problema de barreiras geográficas) -, por outro também surgem externalidades negativas decorrentes deste monitoramento e vigília constante que tais tecnologias permitem sobre o dia-a-dia e a própria vida das pessoas.

Vale dizer: o constante monitoramento da vida das pessoas em busca de dados como matéria prima deste novo modelo econômico, faz surgir um modelo de *sociedade de vigilância* (ZUBOFF, 2019 p. 8).

---

[3] Apesar da frequente utilização dos termos "dado" e "informação" como sinônimos (e o presente texto poderá intercambiar tais termos em diversos momentos), cabe aqui apresentar uma diferenciação técnica: "*[o] dado é o estado primitivo da informação, pois não é algo per se que acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação*" (BIONI, 2019, p. 36). Caminha no mesmo sentido ASCENSÃO, ao apontar que: "*A sociedade de massas oferece uma quantidade fantástica de informação disponível, mas de que não resulta informação assimilada(...). São hoje visíveis as ambiguidades que se ocultam na referência, já de si indefinida, à 'sociedade da informação (...) Quando, na aparente diversidade, os dados são filtrados e controlados de formas mil, não há informação, há desinformação*" (2006, p. 23-24)

A consequência disso é a possibilidade de que os agentes de tratamento (controladores e operadores[4]) promovam "*a classificação das pessoas em categorias de acordo com a avaliação de seus riscos e a discriminação do acesso a determinados bens e serviços, de modo a afetar significativamente as suas chances de vida*" (MENDES, 2015, p. 24).

É por isso que, a reboque do desenvolvimento tecnológico acelerado e das constantes ou iminentes violações à privacidade e a outros direitos e liberdades individuais, vislumbramos o surgimento de uma onda de iniciativas legislativas (em diversos países, mas, mais notadamente por influência das normas oriundas do continente europeu) que visam garantir a proteção dos indivíduos (titulares desses dados) e regulamentar regras para coleta e tratamento de dados pessoais.

No Brasil, após um longo período de *vacatio legis* (prorrogado por diversas vezes por um emaranhado de iniciativas legislativas, tanto pelo Congresso quanto pelo Executivo), a Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018) finalmente teve sua vigência em 18/09/2020, ainda que parcialmente com algumas insuficiência, como a ausência de uma concreta e efetiva estruturação da Autoridade Nacional de Proteção de Dados (ANPD).

Ainda há muito o que ser construído (pela doutrina, jurisprudência e pela autoridade administrativa) para preencher as lacunas e incertezas em relação ao modo correto de interpretar e aplicar corretamente a nova legislação. Exemplo disso é que, dentre as hipóteses legais para tratamento de dados pessoais, os interesses legítimos aparecem como uma cláusula aberta bastante polêmica, sem um conteúdo suficientemente definido pela legislação. Isso não é uma característica exclusiva das regras brasileiras, mas a ausência da ANPD se torna especialmente problemática por fragilizar e limitar a eficácia e aplicação da norma de proteção de dados pessoais, notadamente na base legal mencionada.

[4] A definição e distinção entre controlador e operador consta no art. 5º, incisos VI e VII, da LGPD. Em apertada síntese, controlador é aquele a quem competem as decisões referentes ao tratamento; enquanto que operador é quem efetivamente realiza o tratamento de dados pessoais, em nome do controlador.

Não só por ser, na prática, uma das bases mais utilizadas no meio empresarial, mas também por sua acentuada abertura às interpretações diversas. A hipótese do interesse legítimo parece inclusive ter sido pensada para abranger os casos que não poderiam ser taxativamente previstos no texto legal, a fim de evitar uma rápida defasagem. Sem orientações claras e objetivas, no entanto, empresas e indivíduos ficam sem uma base certa para consultar e ter segurança jurídica sobre seus direitos ou deveres.

A proposta deste artigo é verificar o papel e os parâmetros decisórios definidos por autoridades nacionais de proteção de dados européias (e também judicial em casos concretos) na aplicação do RGPD, visando ressaltar a importância dessas diretrizes para nortear a utilização da base legal do legítimo interesse, e no que podemos aprender para aplicá-las à LGPD no Brasil. As similaridades entre legislações justificam essa busca, embora seja igualmente importante apontar os pontos em que cabem diferenciações, a fim de se evitar o erro, tão comum nas regras brasileiras, de importar institutos estrangeiros sem o necessário cuidado.

## 1 A REGULAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS - BASES NORMATIVAS

Em razão do crescente ganho de relevância das questões relacionadas à temática da privacidade e proteção de dados pessoais, notadamente pelo inegável valor econômico, cada vez mais surgiram correntes políticas que defendiam a necessidade de heterorregulação do assunto.

Ainda existem partidários do modelo da desregulação e aqueles que são totalmente contrários a qualquer tipo de intervenção legislativa sobre o tema, especialmente por defenderem a capacidade de autorregulação entre os atores envolvidos nas atividades de tratamento; ou porque sustentam discursos com forte estímulo para um retorno às regras de mercado (dentro de uma lógica estritamente proprietária). Essa posição surge, comumente, do argumento de que "*as disciplinas demasiadamente rígidas de circulação transnacional de informações*

*podem causar dificuldades à produção e ao comércio internacional*" (RODOTÀ, 2008, p. 51).

Inobstante, é facilmente perceptível que este não é mais o modelo que vem sendo adotado pela maior partes dos países do mundo. De modo a comprovar tal afirmação, referenciamos levantamento recente, no qual se apurou que em pelo menos 142 países do mundo existem legislações versando sobre privacidade e proteção de dados pessoais (GREENLEAF e COTTIER, 2020).

Cabe ressaltar, entretanto, que muito embora o modelo da heterorregulação seja fundamental para endereçar os diversos riscos decorrentes das atividades de tratamento de dados pessoais, isso não nos permite dizer (ou ao menos seria ingênuo pensar desta forma) que a simples aprovação de legislações, que contenham normas e regras para regular e disciplinar o tratamento de dados, seja o suficiente para resolver o problema (FRAZÃO, 2019, p. 116). Neste sentido, referencia-se a compreensão de Ana Frazão acerca do papel da heterorregulação:

> "(...) o papel da heterorregulação é de ser o fio condutor que deve orientar e conformar as demais formas de regulação, até para evitar que as regras de mercado, impostas unilateralmente pelos agentes mais poderoso, de forma direta ou pela via da tecnologia, dominem todas as outras formas de regulação dos dados, tornando inócua ou sem sentido a proteção de dados implementada pela lei" (2019b, p. 128).

Vale dizer: existe a possibilidade que nos desprendermos da lógica simplória e maniqueísta (que apenas rivalize os modelos da *deregulation*, heterorregulação e autorregulação) para pensar em uma alternativa que implique em um modelo de *corregulação*. Este novo modelo busca conformar o que há de melhor entre os modelos anteriores, a partir de uma perspectiva que é possível uma interação e harmonização entre os modelos da heterorregulação estatal e da autorregulação pelo mercado, além de alternativas apresentadas pela via da própria

tecnologia[5]. É neste preciso sentido que a aprovação de uma *lei geral de proteção* "*pretende ser a base normativa para tratamento de dados, sem prejuízo de que os agentes de tratamento, por iniciativa própria, possam ir além dos padrões de cuidado e segurança previstos pela lei*" (FRAZÃO, 2019b, p. 118).

Isto posto, avançaremos na análise para tratar do conceito e no que consistem as bases normativas.

## 1.1 O que são as bases normativas?

O conceito de base normativa (ou "base legal") corresponde às hipóteses nas quais a legislação protetiva autoriza a realização do tratamento de um dado pessoal e que deverão ser indicadas expressamente pelos agentes de tratamento (controlador ou operador), como o fundamento legal da atividade e dos processos adotados, antes mesmo do efetivo início de qualquer tratamento[6] e que também deverão constar nos relatórios de impacto[7-8].

---

5 Há ferramentas de tecnologia que buscam preservar e reforçar a proteção da privacidade dos usuários, bastante conhecidas como *Privacy Enhancing Technologies* (PETs). Neste sentido, recomenda-se leitura das obras de Lawrence Lessig e Joel R. Reidenberg.

6 No contexto brasileiro, a definição de tratamento consta no art. 5º, incisos VI e VII, da LGPD (Lei 13.709/18), *in verbis*: "*toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração*".

7 A definição de relatório de impacto consta no art. 5º, inciso XVII, da LGPD, qual seja: "*documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco*".

8 Nos termos dos artigos 37 e 38 da LGPD, controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem e a ANPD poderá determinar que o controlador elabore relatórios de impacto à proteção de dados pessoais. Ainda, conforme o parágrafo único do art. 38, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

No contexto brasileiro, a LGPD traz dez hipóteses em que o tratamento de dados pessoais será legalmente admitido (*vide* art. 7º e, para o caso de tratamento de dados sensíveis, aplicar-se-á o art. 11). A primeira base legal é o famigerado[9] *consentimento* fornecido pelo titular (art. 7, inc. I), passando outras hipóteses como para cumprimento de obrigação legal (inc. II), execução de contrato (inc. V) até a proteção do crédito (inc. X). A hipótese do interesses legítimos encontra-se prevista no inciso IX do art. 7.

A consequência do tratamento de dados pessoais sem o devido enquadramento nas bases normativas supramencionadas - seja pelo Operador ou por determinação do Controlador - é que a atividade será considerada como irregular e o Controlador poderá ser punido administrativamente ou processado judicialmente pelo ato (OLIVEIRA; COTS, 2020, p. 50).

O foco desta pesquisa não é tratar sobre todas as bases legais previstas na legislação, razão pela qual não parece profícuo esmiuçarmos explicações específicas para cada uma, razão pela passamos imediatamente a tratar sobre a hipótese dos interesses legítimos.

## 1.2 Os interesses legítimos

A hipótese dos interesses legítimos é comumente apresentada como a mais flexível das bases legais para tratamento de dados pessoais. Conforme observa BIONI, "*ainda que sob o mesmo nível hierárquico, o legítimo interesse serve como uma válvula de escape para que as demais bases legais não sejam "sobrecarregadas*" (BIONI, 2019, p. 248-249).

A grande preocupação, diante da enorme carga subjetiva para se preencher o conteúdo da hipótese do legítimo interesse, era de que fosse uma "*nova carta coringa regulatória para abraçar uma miríade de possíveis usos dos dados*" (*Idem*, p. 249). De outro lado, há aqueles que defendem

[9] Bruno Bioni é autor brasileiro que melhor aborda a temática da "função e os limites do consentimento", com obra que é resultado de dissertação na USP. Cf. BIONI, 2019.

que "*a criação era medida essencial para que o empreendedorismo e a inovação não sofressem ainda mais os impactos da nova lei*" OLIVEIRA; COTS, 2020, p. 65).

No contexto brasileiro, a temática do legítimo interesse é mencionado em três diferentes momentos. Primeiramente, dentro as bases legais previstas no já mencionado art. 7º; na sequência está previsto no art. 10 da lei - que estabelece os requisitos para adoção da base normativa da legítimo interesse para tratamento de dados pessoais; e por fim, no art. 37 que dispõe sobre a obrigação dos Controladores e Operadores de registrarem as operações de tratamento de dados pessoais que realizarem, destaque especial para o trecho final do dispositivo "*(...) especialmente quando baseado no legítimo interesse*".

Frisa-se que muito embora o art. 10 e seus parágrafos busquem fornecer os requisitos para adoção da base legal do legítimo interesse, a redação persiste na utilização de cláusulas abertas e de conceitos que não são suficientemente bem definidos em nenhuma parte da LGPD.

Na tentativa de preencher o conteúdo e de modo a permitir a aplicação da base legal em comento, a doutrina nacional invariavelmente teve de se socorrer da experiência europeia para verificar como os países europeus utilizam os conceitos jurídicos indeterminados de "legítimo interesse" e "legítima expectativa".

Exemplo que merece ser referenciado é a obra de Bruno Brioni, que apresenta e trabalha com o "*Teste de Proporcionalidade*", composto de quatro etapas e inspirado na opinião do Grupo de Trabalho do artigo 29 (WP29) na União Europeia (*vide* cap. 4.1 abaixo), sobre o teste de balanceamento.

O autor afirma que o teste consiste em "balancear" os direitos em jogo - as *legítimas expectativas* dos titulares dos dados (cidadãos) e *interesse legítimo* dos agentes de tratamento (controlador). Em análise das disposições da LGPD, BIONI apresenta as etapas do teste: **a)** verificação da legitimidade do interesse: situação concreta e finalidade legítima (art. 10, *caput* e I, da LGPD); **b)** Necessidade: minimização e outras bases

legais (art. 10, §1º da LGPD); **c)** Balanceamento: impactos sobre o titular dos dados e legítimas expectativas (art. 10, II, da LGPD) e **d)** Salvaguardas: transparência e minimização dos riscos ao titular do dado (art. 10, §§2º e 3º, da LGPD). (BIONI, 2019, p. 253-256).

Ainda, conforme também afirma BIONI, "[a] *aplicação da base legal do legítimo interesse não se dá no vazio, demandando-se uma análise contextual*[10] *para verificar se o tratamento dos dados está de acordo como as 'legítimas expectativas' do seu titular*" (BIONI, 2019, p. 267).

Não obstante o bom e avançado trabalho doutrinário sobre a matéria, permanece incerto se os delineamentos extraídos da experiência europeia serão válidos e aplicáveis ao contexto brasileiro. Neste sentido, cabe apontar que a LGPD define como sendo de competência da ANPD deliberar, na esfera administrativa e em caráter terminativo, sobre a interpretação da lei (art. 55, inc. XX).

Deste modo, para compreender melhor o papel da ANPD, cumpre estudar o papel das autoridades nacionais de proteção de dados pessoais.

## 2 O PAPEL DAS AUTORIDADES NACIONAIS DE PROTEÇÃO DE DADOS

A opção pela institucionalização da proteção de dados pessoais na figura de uma autoridade administrativa independente foi o caminho trilhado pela maior parte dos países que adotaram uma adequada regulação jurídica sobre o tema, especialmente pelos países europeus.

A instituição de autoridades administrativas responsáveis pela fiscalização e proteção de dados tem origem em normativas européias da década de 1970, a exemplo do *Datenschutzbeauftragen* na Alemanha, da Comissão Nacional de Proteção de Dados portuguesa e da *Commission National Informatique et Libertés* (CNIL) na França. Esse modelo se consolidou na Europa a partir da obrigatoriedade estabelecida pela Diretiva 46/95/CE,

[10] Cf. NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford, California: Stanford University Press, 2010.

que passou a vincular todos os países-membros da União Europeia (DONEDA, 2019, p. 308).

Não obstante a origem no contexto europeu, atualmente a instituição de organismos deste gênero (autoridades administrativas responsáveis pela fiscalização) estão presentes na maior parte dos países que possuem legislações protetivas que versam sobre privacidade e tratamento de dados pessoais[11].

## 2.1 Função das Autoridades

A instituição de órgãos, comumente denominados de "autoridade nacional de proteção" ou "autoridade de garantia", é parte fundamental para definição de uma adequada estrutura administrativa e jurídica para cada país onde se pretenda estabelecer uma política real e efetiva de proteção de dados pessoais.

Para compreender o papel e as funções desses órgãos, tomemos como exemplo a definição trazida pelo art. 5º, inciso XIX da LGPD, que dispõe que "*a Autoridade Nacional de Proteção de Dados é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da legislação em todo o território brasileiro*". Ainda, nos termos do art. 55-B, consta expressamente no texto da LGPD que "[é] *assegurada a autonomia técnica e decisória à ANPD*".

Assim, além de suas funções de fiscalização do cumprimento da legislação protetiva, autoridades nacionais desempenham um importante papel de aproximação entre as esferas do mercado e do setor público

[11] Referencia-se o trabalho do professor da Universidade de Nova Gales do Sul (UNSW), em Sydney - Austrália, Graham Greenleaf, que realiza pesquisas sobre legislações que versam sobre privacidade e proteção de dados pessoais no mundo. Em seu último levantamento feito até o final de 2019, Greenleaf aponta a existência de 142 países - sendo que a maior parte prevê a instituição de autoridade legislativa. Cf. Greenleaf, Graham and Cottier, Bertil, 2020 Ends a Decade of 62 **New Data Privacy Laws** (January 29, 2020). 163 Privacy Laws & Business International Report 24-26, Available at SSRN: https://ssrn.com/abstract=3572611

com o cidadão, nos mais diversos contextos. Além disso, conforme afirma Danilo Doneda, as autoridades nacionais "t*ambém proporcionam uma forma de tutela, em certa medida inovadora, dos direitos fundamentais*" (DONEDA, 2019, p. 309-310).

Ainda, uma das características desses órgãos - pelo menos que é comum na maior parte dos países que adotam boas legislações protetivas -, é que são dotados de substancial independência[12] em relação aos demais órgãos do governo (sem controle e sujeição ao poder Executivo), possuindo, como exemplo, uma maior autonomia organizativa, finaceira e nos procedimentos de nomeação e mandatos de seus membros. (DONEDA, 2019, p. 311-312).

Além disso, as autoridades nacionais são geralmente descritas pela marcante característica de possuírem caráter eminentemente técnico e que devem ser integrada por especialistas que deverão ser capazes de atender satisfatoriamente às demandas advindas da crescente complexidade das relações sociais e da organização do Estado, no contexto da Sociedade Informacional.

Assim, as autoridades nacionais são importantes não apenas para tutela do cidadão, mas enquanto órgãos responsáveis por implementar e fiscalizar o cumprimento de todo o sistema normativo de proteção de dados, bem como por definir os padrões de aplicação da lei. Revelam-se, assim, bastante útil ao setor privado na medida em que esses padrões decisórios poderão servir como diretrizes a serem aplicáveis no exercício das atividades empresariais, de forma preventiva e potencialmente evitando a orientação de natureza punitiva de decisões dos Tribunais. Nesses casos, se julgam situações particulares e que serão aplicáveis, a princípio, apenas entre os envolvidos no caso concreto (especialmente no pouco harmônico sistema judicial brasileiro, não há segurança jurídica de que a decisão formará um precedente e que será efetivamente vinculante).

[12] Para melhor compreensão da importância dessas autoridades como atributo para que sua missão seja exitosa, cf. DONEDA, 2019, p. 314-318.

Ainda, as autoridades nacionais possuem o condão de serem protagonistas na garantia da concorrência, na medida em que tem o dever de fiscalizar e penalizar condutas anticompetitivas e discriminatória (FRAZÃO; CARVALHO, 2019, *passim*).

Por fim, cabe ressaltar que as autoridades também servem para evitar o risco de fragmentação da lei entre tribunais e outros órgãos administrativos com competências eventualmente concorrentes, visando à garantia da uniformidade dos direitos dos titulares e maior segurança jurídica na aplicação da legislação (DONEDA, 2019, p. 315).

Compreendidas as principais funções e o papel das autoridades nacionais, passamos a tratar especificamente do contexto brasileiro, onde o texto final da LGPD - após alterações sobre a versão originalmente aprovada no Congresso Nacional em 2018 - acabou por fragilizar bastante a estrutura e suscitar suspeitas acerca da efetiva independência da desditosa Autoridade Nacional de Proteção de Dados.

## 2.2 O caso brasileiro

No contexto brasileiro, a criação da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados Pessoais e de Privacidade foi um tema bastante controvertido desde o momento da promulgação da Lei nº 13.709, em 14 de agosto de 2018. Isto porque, todo do Capítulo IX da redação original da lei (que tratava sobre o tema) foi integralmente vetado pelo ex-Presidente da República Michel Temer.

Ato contínuo, em 27 de dezembro de 2018, o ex-Presidente Michel Temer editou a Medida Provisória nº 869/2018 que, para além de tratar de outras matérias da LGPD, recriou a ANPD. Por sua vez, a MP 869/2018 foi convertida na Lei Federal nº 13.853, de 8 de julho de 2019, dando lugar à redação atual.

As razões dos vetos indicavam que os dispositivos incorriam em inconstitucionalidade do processo legislativo (por violação à competência privativa do Presidente da República, nos termos do art. 61 da Constitui-

ção Federal de 1988). Fato é que, na prática, as alterações operadas após o veto implicaram em menor independência do que se pretendia na redação original da LGPD.

Isto porque, muito embora o art. 55-B afirme que será assegurada autonomia técnica e decisória à ANPD, por esta fazer parte da administração direta, a ANPD não terá a autonomia administrativa nem personalidade jurídica própria, enquanto parte integrante da Presidência da República (é o que se extrai da atual redação do art. 55-A).

Ressalva-se, entretanto, que nos termos dos parágrafos do mesmo artigo 55-A, tal natureza jurídica é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida ao regime autárquico especial e vinculada à Presidência da República. A avaliação quanto à transformação deverá ocorrer em até dois anos da entrada em vigor da estrutura regimental da autoridade nacional.

Mais recentemente, em 26 de agosto de 2020, o Executivo Federal, o Presidente da República, Jair Messias Bolsonaro, editou o Decreto nº 10.474 que aprovou a estrutura regimental e o quadro de cargos e funções para a futura composição da ANPD. Não obstante, conforme dispõe o art. 6º do referido Decreto, as suas disposições só entram em vigor na data de publicação da nomeação do Diretor-Presidente da Autoridade Nacional de Proteção de Dados no Diário Oficial da União. Fato que não ocorreu ainda.

Assim, apesar da vigência da LGPD, a autoridade administrativa que será responsável por zelar, fiscalizar, editar normas e orientações para o exercício das atividades de tratamento de dados pessoais, sequer está em funcionamento. Em suma, ainda pairam muitas dúvidas e incertezas acerca de como será concretizada a estrutura e como se dará a atuação da ANPD no Brasil.

Apesar disso, na tentativa de encontrar parâmetros que poderão nortear a aplicabilidade da LGPD e a atuação da ANPD no Brasil, passamos a realizar um comparativo com a experiência advinda de países europeus.

## 3 UM COMPARATIVO COM A EXPERIÊNCIA EUROPEIA

Como nosso foco é no método comparativo funcional (LEGRAND, 2018, *passim*), não pretendemos fazer uma reconstrução histórica do conceito de legítimo interesse no âmbito europeu. É importante perceber que o "interesse legítimo" ou "legítimo interesse" não é um termo unívoco, sendo bastante comum inclusive em outras áreas do direito[13]. A ordem das palavras no conceito é inclusive alternada sem modificação do significado, tanto na LGPD[14] quanto no RGPD[15].

Bem similar à forma que conhecemos hoje, a base legal do legítimo interesse vai expressamente aparecer no art. 7º da Diretiva 95/46/CE de 1995[16]:

> Artigo 7º Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se: (...)
>
> f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º

---

13 Vide o CC/02, onde se fala sobre o "interesse legítimo" do segurado em contratos securitários (art. 757), do proprietário de imóvel sobre a interferência em atividades no subsolo ou espaço aéreo (art. 1.229) e do titular de direito empenhado em relação ao credor pignoratício (art. 1452, parágrafo único).

14 Cf., na LGPD, o art. 7º, IX em comparação com o art. 10 ou o art 37.

15 Cf., no RGPD, o art. 40º, 2, d) em comparação com o art. 6º, f) ou o art. 13º, 1, d), dentre outros. Mas aqui o texto demonstra uma preferência por "interesses legítimos" quando se refere ao responsável pelo tratamento (ou outros que estarão utilizando os dados sem seres seus titulares), e "legítimos interesses" quando se refere ao titular dos dados, existindo uma notável exceção no art. 88º, 2.

16 Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=-CELEX:31995L0046&from=PT

O texto da norma permaneceu essencialmente o mesmo durante todo o procedimento legislativo, mesmo passando por diversas emendas, e não tinha a pretensão de prover indicadores ou critérios de como fazer o balanceamento descrito (entre os interesses do responsável pelo tratamento e os direitos e liberdades fundamentais do titular). Mas o maior grau de discricionariedade aos Estados-Membros, característico das Diretivas, fez com que a implementação do artigo 7º fosse insatisfatória e com sérias divergências entre os países europeus (WP29, 2010, p. 5; KAMARA & DE HERT, 2018, p. 9)

Abrimos aqui um parênteses para esclarecer a diferença entre Diretivas e Regulamentos, considerando que ambos são atos normativos comunitários de caráter vinculante. O Regulamento tem caráter geral, é obrigatório em todos seus elementos e é diretamente aplicável em todos os Estados-membros[17]. Já as Diretivas vinculam os Estados-membros quanto ao resultado a alcançar, deixando, em larga medida (e ao menos em tese, porque às vezes essa margem discricionário é estreita), às instâncias nacionais a competência quanto à forma e os meios (artigo 288º, par. 3º do TFUE), com possibilidade de aplicação imediata dos dispositivos comunitários em situações bem limitadas (PAIS, 2013, p. 30).

Essas divergências e insuficiências em uma base legal com enorme potencial flexível, capaz de abarcar os mais diversos tipos de tratamentos de dados, ensejava uma brecha na Diretiva que poderia torná-la inócua (FERRETTI, 2014). Isso foi um forte estímulo para aprimorar as normas de proteção de dados em nova proposta, dessa vez com aplicabilidade direta em toda a UE.

Não à toa, o Regulamento Geral de Proteção de Dados[18], de 27 de abril de 2016, apesar de não definir precisamente o conceito de "interesse legítimo" ou "interesse" (CORDEIRO, 2019, p. 12), foi muito mais a fundo no

[17] Artigo 288º, par. 2º do Tratado de Funcionamento da União Europeia

[18] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT

tema, embora esse aprofundamento não tenha avançado sem alguma instabilidade. A título de exemplo, a norma sobre os legítimos interesses chegou a excluir os interesses de terceiros na primeira proposta da Comissão de 2012, que também propunha que fosse ela a responsável por densificar em atos posteriores, e relatório de um dos comitês do Parlamento sugeriu uma lista exaustiva de situações que poderiam ser enquadradas nessa base legal (KAMARA & DE HERT, 2018, p. 10-11)[19].

Enquanto na Diretiva 95/46 essa questão foi breve e superficialmente tratada na seção de Considerandos, no RGPD há uma abordagem extensa e reiterada (especialmente no Considerando 47) antes mesmo de começar o texto da lei, inovando especialmente no maior cuidado com dados infantis e na restrição dessa base para autoridades públicas. O conceito também é abordado em diversos dispositivos[20], para além da determinação fundamental do art. 6º, 1, f):

> (47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. (...) De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. (...) Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. (...) **[Nota: para sintetizar, excluímos do trecho, os diversos exemplos de interesse legítimo expostos]**

[19] Para mais detalhes do desenvolvimento legislativo dos interesses legítimos no RGPD, ver CORDEIRO, 2019, p. 6--9.

[20] Vide, dentre vários, os Considerandos 50 e 69, e os artigos 14º e 40º, 2, b).

> Artigo 6º Licitude do Tratamento
>
> 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: (...)
>
> f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Mesmo com maior detalhamento e alguns exemplos, percebe-se que o Regulamento continua se baseando fortemente em conceitos indeterminados e abertos. Uma densificação deles, portanto, era indispensável para uma melhor eficácia das normas de proteção de dados.

## 3.1 WP29 e EDPB

A publicação da Diretiva 95/46 da UE trouxe consigo um dispositivo particularmente importante para a formação do direito comunitário de proteção de dados da forma que existe hoje. É o artigo 29, que criou um "g*rupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais*", de caráter consultivo e independente, formado pelas autoridades nacionais (ou conjuntos delas de cada país). Além de permitir uma troca e acúmulo de conhecimentos, a iniciativa também possibilitava orientar a regulamentação em um caminho harmonizado para os diferentes contextos culturais e tecnológicos que existem nos estados-membros.

Esse grupo ficou conhecido como "Grupo de Trabalho do artigo 29" (ou *Working Party 29,* originando a sigla WP29). Sua importância não foi apenas a de consolidar e unificar alguns entendimentos divergentes sobre proteção de dados das últimas décadas, mas principalmente um exemplar trabalho no apoio à construção do RGPD e a elaboração de orientações sobre a melhor interpretação dessas regras entre a publicação em 2016 e a entrada em vigor em 2018.

Nesse momento, a WP29 encerrou seus trabalhos e foi substituída por uma outra instituição, com maiores e mais detalhadas atribuições, o Comité Europeu para a Proteção de Dados (ou *European Data Protection Board,* conhecido pela sigla *EDPB).* Este era previsto nos artigos 68º a 76º do RGPD, além de ser citada em diversos outros dispositivos do Regulamento.

Apesar de não ser exatamente uma relação formal de continuidade, é possível notá-la pela coincidência do momento de encerramento e início de cada instituição e pela composição extremamente similar, ressaltando ainda que o Comitê não se confunde com a Autoridade Europeia para a Proteção de Dados (*European Data Protection Supervisor* - EDPS), cujo representante compõe o EDPB.

O caráter consultivo do WP29 e do EDPB não são apenas para casos concretos e não secundarizam essas instituições perante outras como a AEPD ou com o Tribunal de Justiça da União Europeia (TJUE). Pelo contrário, as orientações do WP29 permanecem hoje como uma das principais fontes de interpretação para as aplicações práticas do RGPD, inclusive com ratificação pelo EDPB de boa parte dos documentos relativos ao Regulamento provenientes de sua antecessora, logo em sua primeira reunião plenária[21].

Ocorre que a Opinião/Parecer 06/2014 do WP29, que trata especificamente sobre legítimos interesses do controlador (conhecida também como WP217), foi adotada em 9 de abril de 2014, antes da publicação do RGPD. Referia-se, assim, ao conceito firmado no art. 7º da Diretiva 95/46, embora mencione por diversas vezes discussões sobre a proposta de Regulamento que estava então em andamento (cf. WP29, 2014, p. 8-9).

Em outras palavras, esse documento não estava entre aqueles ratificados pelo EDPB, que já tratavam diretamente das regras do RGPD. Mas como há também um compartilhamento de conceitos (e um significativo grau de continuidade) entre a Diretiva e o Regulamento, esse documento

[21] Cf. https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_pt

continuou sendo extensamente utilizado como base tanto para julgamentos do TJUE quanto para novas orientações do Comitê, vide a nota de rodapé n. 20 das Diretrizes 2/2018, a nota de rodapé 7 das Diretrizes 2/2019 e, destacadamente, o ponto 30 e as notas de rodapé 3, 10 e 23 das Diretrizes 5/2020, todas da EDPB.

Assim, as orientações europeias nesse âmbito parecem ser largamente baseadas na Opinião 06/2014/WP217, com adições em outros documentos geralmente sobre a incidência de requisitos gerais (como a transparência[22]) ou relativas à atividades específicas, como a interpretação dos interesses legítimos no caso de dispositivos de vídeos (Diretrizes 3/2019 da EDPB).

A Opinião 06/2014 é clara ao apontar que essa base legal não deve ser utilizada como último recurso ou para preencher lacunas, e nem como uma alternativa prioritária por ser menos restritiva[23]. Pelo contrário, ela teria um campo natural e específico de relevância, com a observância obrigatória de certos requisitos, em especial o teste de balanceamento/ponderação, que coloca de um lado os interesses do controlador e de outro o impacto sobre interesses e direitos dos titulares (WP, 2014, p. 9). O documento também aborda extensivamente a relação da regra dos interesses legítimos com outros artigos da Diretiva, em especial os casos em que outras bases legais devem ser utilizadas.

Para os fins do presente trabalho, há duas seções do documento do WP29 que merecem destaque. A primeira são os detalhamentos da base legal dos interesses legítimos, onde o Grupo de trabalho orienta que:

---

22 Cf. as Diretrizes sobre transparência no Regulamento 2016/679 do WP29 (WP260 rev.01), adotado em 2017 e revisado em 2018. Elas orientam, no ponto 66 (p. 32) e na tabela da p. 36, como o controlador deve deixar claro na sua política de privacidade, sugerindo ainda como expor essas informações, qual é o interesse legítimo, como é feito o teste tripartite do balanceamento e que este pode ser consultado a pedido do titular. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

23 Assim como o RGPD, contudo, não é clara ao definir o que seria um "interesse legítimo" ou mesmo um "interesse" em termos conceituais, preferindo densificar essa noção por meio de exemplos (CORDEIRO, 2019, p. 12)

- Embora sejam conceitos próximos, há uma distinção entre propósito/finalidade do controlador, que é a razão pela qual um dado é processado, dos seus interesses, que significam os benefícios que ele (ou a sociedade) pode retirar daquele processamento (2014, p. 24).
- A legitimidade é fluída e não depende apenas da legalidade, clareza e imediatez do ato, mas também dos interesses e direitos do titular (p. 25-26).
- A (então) proposta de Regulamento veda a utilização da base legal pelas autoridades públicas (p. 26-27).
- Os interesses de terceiros podem ser reivindicados para tratamento dos dados, vide aspectos de transparência, fiscalização, pesquisa e interesse público (p. 27-28).
- O teste de balanceamento caminha ao lado do requisito da necessidade, pois o tratamento precisa ser necessário, fundamentado na noção técnica de necessidade firmada no ordenamento comunitário (p.11 e 29).
- Os "interesses e direitos fundamentais" do titular devem ser interpretados de forma ampla e extensiva, com a ausência do adjetivo "legítimos" sendo significativa para a correta hermenêutica (p. 29-30, ver também CORDEIRO, 2019, p. 17-18).

A segunda é uma lista de fatores chaves que devem ser considerados no teste de balanceamento[24], onde o Grupo orienta que:

- Ao avaliar se há um interesse legítimo do controlador, é importante notar que alguns direitos fundamentais do titular serão quase sempre afetados (como o de privacidade), mas que eles podem ser contrabalanceados com direitos fundamentais do controlador e de terceiros (como o de acesso a documentos, li-

[24] Vale também a pena conferir a sugestão de sistematização deste teste proposta por Barreto Menezes CORDEIRO, na esteira de Constantin Herfurth e mantendo a essência daquela avançado pelo WP29 (CORDEIRO, 2019, p. 18-28)

berdade comercial ou liberdade de expressão), além de ser útil destacar qual o valor cultural dado a cada um desses direitos ou interesses (p.34-36).

- Ao avaliar os impactos do tratamentos dos dados, não se pode limitá-los aos danos causados, pois abrangem todas possíveis consequências, inclusive as de efeitos positivos, as psicológicas e as em potencial. Deve-se também levar em consideração: a natureza dos dados (quão sensíveis eles são); a maneira como eles são processados; as expectativas razoáveis dos titulares; e a condição do controlador e do titular, como, por exemplo, se são empresas grandes e se o tratamento é sobre dados de empregados (p. 36-41).
- Essas avaliações nem sempre serão determinantes para um enquadramento claro na base legal, e sim indicarão a probabilidade de correta utilização dela. Nos casos mais dúbios, vale a pena para o controlador implementar medidas que favoreçam a interpretação a seu favor (p. 41)[25].
- No sentido do ponto anterior, pode-se criar protocolos de tratamento ou ferramentas tecnológicas que diminuam o impacto negativo ou reforcem a importância do interesse do titular, como apagar os dados imediatamente após o tratamento ou aumentar significativamente a transparência da empresa (p. 42).

A WP217 ainda detalha obrigações de transparência e fiscalização, ressaltando o papel das normas consumeristas, e a importância de efetivar a opção do titular de impedir o tratamento de seus da-

[25] Existem duas formas de ver a ponderação proposta tanto na Diretiva quanto no Regulamento. A primeira uma leitura literal da regra, o que excluiria qualquer consideração de medidas tomadas para afetar o balanceamento, mas a proposição do WP29 parece se adequar mais à teleologia dessas normativas de proteção de dados (KAMARA & DE HERT, 2018, p. 16)

dos[26], e de ter alternativas aos serviços que têm como seu modelo de negócio a comercialização direta ou indiretas de dados pessoais (p. 43-48). Ao final, resume com grande clareza o texto (p. 48-51), faz algumas recomendações que foram largamente adotadas na elaboração do RGPD (p. 51-54) e no seu Anexo I apresenta um didático passo-a-passo de como fazer o teste de balanceamento na prática, com diversos exemplos (p. 55-68).

As outras diretrizes e orientações mostram como o que é considerado um interesse legítimo pode variar de acordo com a atividade. Vide o caso de proteção de dado em gravações de vídeos, onde questões se segurança e existência de perigos concretos assumem centralidade[27].

Confirmando que as orientações do WP29 continuaram de primeira relevância após a publicação do Regulamento, podemos consultar os documentos amplamente utilizados hoje como base para implementações práticas do RGPD. Encontramos vários exemplos em documentos respaldados e indicados pela respeitada Associação Internacional de Profissionais de Privacidade (*International Association of Privacy Professionals* - IAPP), como o elaborado pela *Data Privacy Network*[28], de natureza essencialmente prática e que talvez seja o guia de acesso aberto mais útil para implementação do RGPD por empresas, ONG e indivíduos.[29]

---

[26] O direito de oposição firmado no artigo 21º do RGPD é particularmente voltado para a base legal dos interesses legítimos, conforme expressamente mencionado no item 1 desse artigo. Por outro lado, o Regulamento trouxe consigo a oportunidade do controlador se defender ao expor razões imperiosas e legítimas para continuar o tratamento.

[27] Cf. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf, especialmente pgs. 9 e 10.

[28] Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation de 2017, cf. https://iapp.org/media/pdf/resource_center/DPN-Guidance-A4-Publication.pdf

[29] Podemos ver também, em outro exemplo, o documento preparatório para *workshop* promovido pelo *Centre for Information Policy Leadership,* que evidencia como programas de proteção de dados baseados nos interesses legítimos já estavam implementados por diferentes organizações. Cf. https://iapp.org/media/pdf/resource_center/final_cipl_

## 3.2 CASOS JUDICIAIS DO TJUE SOBRE A BASE LEGAL DOS INTERESSES LEGÍTIMOS

Nos focaremos aqui nos entendimentos firmados pelo Tribunal de Justiça da União Europeia, por ser a autoridade última para definir a interpretação da legislação comunitária, e ter exercido essa competência frequentemente em relação aos atos normativos de proteção de dados. No entanto, não é o único órgão judicial que cumpre esse papel, pois as Cortes nacionais também tiveram importante julgados relativos ao objeto de nossa investigação (ver extensa lista, incluindo decisões de autoridades nacionais, em ZANFIR-FORTUNA & TROESTER-FALK, 2018, p. 32-40).

Há vários acórdãos importantes para a base legal dos interesses legítimos ainda na vigência da Diretiva 95/46[30]. Antes da publicação do RGPD, foram proferidos três acórdãos de maior relevância para a nossa análise.

O primeiro foi relativo aos casos *ASNEF* e *FECEMD* (C-468/10 e C-469/10[31]) em 24 de novembro de 2011, determinando que a Espanha não teria internalizado o art. 7º, f) da Diretiva corretamente, porque estabeleceu um requisito extra para além do balanceamento com os direitos e liberdades fundamentais do titular (que deveria ser feito caso-a-caso). Firmou-se que o artigo das bases legais tinha efeitos diretos nos ordenamentos nacionais que deveriam ser seguidos, mas os estados-membros poderiam definir orientações oficiais próprias para aplicação, priorizando alguns parâmetros dentro dos limites fixados na Diretiva.

O segundo, de 13 de maio de 2014, foi o famoso *Google Spain v. AEPD and Mario Gonzalez* (C-131/12[32]), onde se estabeleceu o direito à

examples_of_legitimate_interest_grounds_for_processing_of_personal_data_16_march_2017.pdf

30 Com mais detalhes, cf. KAMARA & DE HERT, 2018, p. 21-26 e ZANFIR-FORTUNA & TROESTER-FALK 2018, p. 10-20

31 Cf. http://curia.europa.eu/juris/liste.jsf?num=C-468/10&language=pt

32 Cf. http://curia.europa.eu/juris/liste.jsf?language=pt&num=c-131/12

desindexação (ou, imprecisamente, "direito ao esquecimento"), com uma importante opinião do Advogado Geral sobre o interesse legítimo dos provedores de busca. Essa opinião foi apenas parcialmente adotado pelo Tribunal, que novamente ressaltou a necessidade de uma análise casuística e a apontou que, na situação concreta, o direito dos usuários da Internet em obter a informação não se sobrepunha aos direitos do proponente da ação

Por fim, o caso *Rynes* (C-212/13)[33], julgado em 11 de dezembro de 2014, tratava de uma filmagem de uma câmara de segurança de uma residência particular que captava um pouco da rua e seus transeuntes. Apesar de não se aprofundar no teste de balanceamento, o Tribunal decidiu que a abrangência dos legítimos interesses seria larga o suficiente para abarcar essa situação, que, ao envolver a filmagem parcial um espaço público, não estava abarcada pela exceção domiciliar do art. 3, 2 da Diretiva. A defesa da segurança, vida e propriedade do dono da casa e de sua família foi vista como um claro interesse legítimo.

Depois de publicado o RGPD, em 19 de outubro de 2016, o TJUE julgou o caso *Breyer* (C-582/14)[34], confirmando os entendimentos dos casos *ASNEF* e *Rynes*. Pouco tempo depois, em 9 de março de 2017, decidiu-se sobre caso *Manni* (C-398/15[35]), onde um cidadão italiano quis remover registros seus, danosos à sua reputação, da Câmara de Comércio do país. O Tribunal negou esse pedido entendendo que no ambiente comercial o interesse de terceiros em conhecer os registros passados de uma empresa deveria ser considerado, que as bases legais podem cumular entre si e que todos os aspectos do caso concreto devem ser levado em consideração (quem são os titulares e controlados, quais os tipos de dados, as finalidades do processamento, dentre outros).

Dali a poucas semanas, em 4 de maio 2017, foi julgado aquele que é possivelmente o caso mais importante para a base legal dos interesses

33 Cf. http://curia.europa.eu/juris/liste.jsf?language=pt&num=C-212/13

34 Cf. http://curia.europa.eu/juris/liste.jsf?language=pt&num=C-582/14

35 Cf. http://curia.europa.eu/juris/liste.jsf?language=pt&num=C-398/15

legítimos, *Rīgas satiksme* (C-13/16)[36]. Os fatos tratavam de uma busca de uma empresa de transporte público para identificar e processar judicialmente o passageiro de uma companhia de táxi que havia danificado um bondinho, o que foi entendido pela Corte como um interesse legítimo. O TJUE entendeu que a mencionada base legal não estabelece uma obrigação de tratamento, mas sim uma possibilidade, embora a Diretiva não seja um impedimento para que a lei nacional estabeleça essa obrigação. Ainda mais importante, detalhou as três condições cumulativas para recorrer à essa base, nomeadamente a busca de um interesse legítimo, a necessidade do tratamento e o balanceamento relativo ao caso concreto (realçando que a disponibilidade das informações em fontes públicas deve ser um fator importante a ser levado em consideração.

Depois da entrada em vigor do RGPD, destacam-se dois julgados, embora ambos abordassem situações ocorrida sob a vigência da (e regidas normativamente pela) Diretiva. O caso *Fashion ID* (C-40/17[37]) tratou da co-responsabilidade de controlador que usava um *plugin* do botão "curtir" do Facebook em seu próprio site, e dentre vários temas importantes, o Tribunal decidiu que, nos casos de uma atuação conjunta de controladores (que aqui eram o Facebook e o dono do site), ambos deveriam demonstrar os seus respectivos legítimos interesses no tratamento dos dados, mas só podiam ser responsabilizados em relação ao processamento de dados que de fato realizavam.

Para finalizar, também foi de grande relevância, apesar de menos inovador, a decisão naquele que ficou conhecido como o caso CCTV (*TK v. Asociaţia de Proprietari bloc M5A-Scara*A, C-708/18[38]), do final de 2019. O contexto fático era a de um morador que se recusou a aceitar que instalassem câmeras de vigilâncias nas áreas comuns do condomínio onde morava, e a decisão do TJUE foi importante por reafirmar vários dos pontos que foram avançados ou detalhados em decisões anteriores, deixan-

36 Cf. http://curia.europa.eu/juris/liste.jsf?language=pt&num=C-13/16

37 Cf. http://curia.europa.eu/juris/liste.jsf?language=pt&num=C-40/17

38 Cf. http://curia.europa.eu/juris/liste.jsf?language=pt&num=C-708/18

do para a corte nacional decidir se os critérios do interesse legítimo haviam sido preenchidos.

## 3.3 ALGUNS EXEMPLOS DE ORIENTAÇÕES DAS AUTORIDADES NACIONAIS

Embora os principais detalhamentos sobre os interesses legítimos estejam nos âmbitos acima citados, as autoridades nacionais também fornecem suas próprias informações sobre essa base legal. Os documentos mais genéricos de orientação são caracterizadas por serem sintéticos e voltados para uma leitura facilitada dos controladores ou titulares dos dados, refletindo ainda valores culturais característicos de cada estado-membro da União Europeia.

Possivelmente, o melhor exemplo dessa capacidade de sintetizar didaticamente é o *Information Commissioner's Office* (ICO) do Reino Unido. Apesar do *Brexit,* o país ainda está sob regramento do RGPD até o final de 2020, e há uma clara pretensão de incorporar as regras do direito comunitário ao ordenamento britânico (em sua totalidade ou ao menos em todos os pontos essenciais), com algumas adições relativas ao diálogo de dados entre UE e Reino Unido. Essas novas regras funcionariam ao lado do já vigente *Data Protection Act* 2018[39].

O ICO tem um documento geral sobre legítimos interesses aparentemente voltado para controladores e operadores, que se inicia com um resumo de frases curtas e um *checklist* e indica as mudanças que o RGPD trouxe em relação à Diretiva. Aponta, em seguida, como funciona o teste tripartite de balanceamento e quando é possível recorrer ao interesse legítimo, focando na sua flexibilidade mas no aumento dos ônus de responsabilidade. Desenvolve um passo-a-passo de como realizar a ponderação com perguntas que devem ser respondidas, mencionando

[39] Essas informações podem ser encontradas na seção de perguntas frequentes do site do ICO: https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/information-rights-at-the-end-of-the-transition-period-frequently-asked-questions/

que, por ser essa a base com menor segurança jurídica, a prioridade deve ser dada para outras bases legais quando elas são aplicáveis. Ressalta, ao fim, a ausência de direito de portabilidade e o fortalecimento do direito de objeção (pelo titular) ao tratamento dos dados[40].

A *Commission nationale de l'informatique et des libertés* (CNIL) também é notória por forte atuação e tem uma página de seu site voltada para esclarecimentos sobre os interesses legítimos. Sua prioridade, no entanto, parece ser tornar a questão mais acessível ao cidadão comum, usando uma linguagem simples e de fácil leitura, com alguns curtos exemplos. Os pontos mais importantes são abordados, com orientações concretas mais escassas que no caso da ICO, embora se recomende que as empresas documentem a metodologia utilizada para os testes de balanceamento[41].

Algumas Autoridades Nacionais preferem abordar os interesses legítimos ao lado das outras bases legais, em explicações mais completas do sistema como um todo, que se refletem em comentários um pouco mais genéricos sobre cada base legal especificamente considerada. Na Irlanda, o *Data Protection Commissioner* (DPC, ou *An Coimisinéir Cosanta Sonraí* em irlandês) segue esse caminho, e na parte dos interesses legítimos dá especial relevo aos Considerandos do RGPD e levanta os principais pontos da base legal[42]. A *Garante per la protezione dei dati personali* italiana também parece caminhar nesse sentido, mas sendo um pouco mais específica e trabalhando sobre as categorias de atividades, como a relativa aos dados pessoais de informações comerciais[43].

---

40 Apesar de quase todos os documentos oficiais da UE terem uma versão sua em inglês, o ICO é uma das poucas Autoridades que disponibiliza orientações gerais, em explicações avulsas e específicas, sobre diversos pontos relativos à proteção de dados. Vide, nos interesses legítimos:: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests-1-0.pdf

41 Cf. https://www.cnil.fr/fr/linteret-legitime-comment-fonder-un-traitement-sur-cette-base-legale

42 Cf. o Guidance Note: Legal Bases for Processing Personal Data: https://www.dataprotection.ie/sites/default/files/uploads/2019-12/Guidance%20on%20Legal%20Bases_Dec19_1.pdf, especialmente p. 21-24 sobre os interesses legítimos

43 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9119868

Podemos também encontrar, como no caso da *Agencia Española de Protección de Datos* (AEPD), orientações relevantes sobre os legítimos interesses em documentos públicos relativos a consultas sobre casos específicos[44], o que ajuda o público a entender como funciona o processo em casos realmente existentes e a partir deles abstrair para suas próprias aplicações. Por fim, há também a opção, como parece ter feito a Comissão Nacional de Proteção de Dados (CNPD) portuguesa, de priorizar orientações mais precisas sobre questões concretas[45], confiando nas diretrizes genéricas já existentes a nível europeu.

Cumpre deixar claro que essas as posições acima apontadas não são mutuamente excludentes, e podem refletir apenas o estado atual dos sites dessas autoridades ou o grau de publicidade e facilidade de acesso às informações. Por exemplo, nada impede que uma Autoridade que não tenha documentos trabalhando detalhadamente o tópico dos interesses legítimos o crie em um futuro próximo. O que essas diferenças mostram é que, apesar dos entendimentos firmados no âmbito comunitário aplicáveis aos cidadãos da UE, é ainda possível obter um maior reforço informativo (por vezes na forma de explicações mais compreensíveis e contextualizadas) junto com a autoridade nacional de seu país.

## 4 CONCLUSÃO

O objetivo deste artigo não foi apresentar a metodologia mais adequada de avaliações de impacto ou de ponderação de direitos e interesses para justificar o tratamento de dados na base legal dos legítimos interesses[46]. Também não foi prover um passo-a-passo genérico do que fazer, o que, se for o desejo do autor, pode ser obtido de forma didática a partir das referências indicadas no texto.

---

44 https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-interes-legitimo.pdf

45 Cf. https://www.cnpd.pt/home/orientacoes/orientacoes.htm

46 Para exemplos de metodologias concretamente utilizadas, ver KAMARA & DE HERT, 2018, p. 15.

O que procuramos demonstrar é que, pela base legal dos legítimos interesses ser acentuadamente aberta/flexível mas também exigir um maior grau de responsabilidade, orientações confiáveis sobre ela são absolutamente necessárias para possibilitar um ambiente de proteção de dados seguro para todos os atores envolvidos, incluindo os tribunais.

Na falta de uma organização oficial capaz de prover respostas sólidas às dúvidas existentes, como foi o WP29 ou é o EDPB da União Europeia, espera-se que uma Autoridade Nacional possa cumpri-lo em sua função consultiva. No Brasil, essa papel é indispensável porque, apesar de termos alguns critérios de proteção de dados no Marco Civil da Internet, não há uma legislação anterior próxima à LGPD (como existia a Diretiva 95/46 antes do RGPD na União Europeia), e não temos assim julgados capazes de indicar caminhos a serem seguidos, fora de teor mais genérico como o julgamento pelo Supremo Tribunal Federal das Ações Diretas de Inconstitucionalidade nº 6.387, 6.388, 6.389, 6.390 e 6.393, em 07/05/2020.

Isso é grave porque as informações já divulgadas sobre a Autoridade Nacional da Proteção de Dados mostram que se caminha para um órgão que: i) não terá a independência desejada, sendo vinculada à Casa Civil; ii) terá um número de funcionários (indicados pelo governo) reduzido em relação ao que foi considerado desejável por especialistas; iii) em um contexto de crise econômica, terá poucos recursos disponíveis para seu pleno funcionamento e realização das pesquisas e avaliações necessárias; iv) não há qualquer garantia legal, ainda, que a escolha dos dirigentes da ANPD seguirá os parâmetros de exigência técnica desejáveis, o que enseja o risco de serem indicados poucos reais especialistas, capazes de legitimar as orientações para obter uma plena aceitação quando avaliadas pelo Poder Judiciário pátrio, que invariavelmente permanecerá com a última palavra.

Nos basearmos nas orientações já consolidadas no âmbito da União Europeia pode ser (como de fato está sendo na prática atual) uma solução "tapa-buraco". Contudo, além do permanente risco de desconsi-

deramos o contexto jurídico e cultural do país, que é inclusive ressaltado pelas instituições e institutos jurídicos da UE sobre proteção de dados em relação aos estados-membros, há diferenças objetivas no texto da lei que podem afetar a interpretação sistêmica dos interesses legítimos no caso concreto, considerando que, no teste de balanceamento, todos os elementos devem ser minuciosamente levados em conta.

A inexistência de uma autoridade nacional devidamente estruturada, mesmo após a vigência quase integral da LGPD, nos faz presumir por uma certa dificuldade em prover de forma célere as orientações necessárias para construir uma boa cultura de proteção de dados no Brasil.

Sugerimos, para endereçamento do problema, embora reconhecendo que não é a ideal, que se realizem encontros cujo foco seja apresentar orientações genéricas. Seriam espaços de debate entre especialistas de proteção de dados[47] e de magistrados que se proponham a ser protagonistas nesse tema, tanto dos Tribunais quanto do Ministério Público (preferencialmente com todos os níveis da federação e com representantes de todas as unidades federativas), além de procuradores dos órgãos públicos relevantes.

Esses encontros teriam o propósito de firmar orientações não-vinculativas, mas com respaldo de uma construção multisetorial e notoriamente técnica, seguindo o exemplo e os moldes dos já consagrados enunciados publicados pelo Fórum Permanente de Processualistas Civis ou nas Jornadas de Direito organizadas pelo Conselho da Justiça Federal. Vale lembrar, a título de encerramento, que o reconhecimento formal da ANPD desse tipo de orientações, na forma de boas práticas ou de códigos de conduta, é expressamente previsto no art. 4º, XV[48] do Decreto n. 10.474 de 2020.

---

47 Não exclusivamente de juristas e operadores do direito, mas também de especialistas em tecnologia da informação e tantos profissionais de áreas correlatas, incluindo representantes do mercado e do terceiro setor.

48 Art. 4º Ao Conselho Diretor, órgão máximo de direção da ANPD, compete: (...)
XV - reconhecer e divulgar regras de boas práticas e de governança estabelecidas por controladores e operadores relacionadas ao tratamento de dados pessoais;

## REFERÊNCIAS

ASCENSÃO, José de Oliveira. Propriedade intelectual e internet. **Direito da Sociedade da Informação,** v. VI, p. 1–25, 2006.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Editora Forense, 2019.

CASTELLS, Manuel. **A sociedade em rede.** Vol. I. - 8. ed. São Paulo: Editora Paz e Terra, 2005.

CORDEIRO, A. Barreto Menezes. O tratamento de dados pessoais fundado em interesses legítimos. **Revista de Direito e Tecnologia,** v. 1, n. 1, p. 1-31, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei geral de proteção de dados - 2. ed. - São Paulo: Thomson Reuters Brasil, 2019.

FERRETI, Federico. Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights? **Common Market Law Review**, v. 51, n. 3, pp. 843-868, 2014

ZANFIR-FORTUNA, Gabriela; TROESTER-FALK, Teresa. **Processing Personal Data on the Basis of Legitimate Interests under the GDPR:** Practical Cases**.** Relatório de Future of Privacy Network (FPF) e NIMITY, 2018. Disponível em: http://www.ejtn.eu/PageFiles/17861/Deciphering_Legitimate_Interests_Under_the_GDPR%20(1).pdf

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais - Noções introdutórias para compreensão da importância da Lei Geral de Proteção de Dados. p. 23-52. 2019a. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo. OLIVA, Milena Donato. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. - 1. ed. - São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana. Objetivos e alcances da Lei Geral de Proteção de Dados. p. 99-129. 2019b. In: FRAZÃO, Ana; TEPEDINO, Gustavo. OLIVA, Milena Donato. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** - 1. ed. - São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana; CARVALHO, Angelo Gamba Prata de (Coord). **Empresa, mercado e tecnologia** - Belo Horizonte: Fórum, 2019.

GREENLEAF, Graham and COTTIER, Bertil, 2020 Ends a Decade of 62 New Data Privacy Laws (January 29, 2020). (2020) 163 **Privacy Laws & Business International** Report 24-26, Available at SSRN: https://ssrn.com/abstract=3572611.

KAMARA, Irene; DE HERT, Paul. Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. **Brussels Privacy Hub,** Vol. 4, No. 12, 2018.

LEGRAND, Pierre. **Como ler o direito estrangeiro.** Tradução de Daniel Wunder Hachem. São Paulo: Editora Concorrente, 2018.

MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de Dados Pessoais. **Revista de Direito do Consumidor.** vol. 102/2015. p. 19 - 43. Nov.- Dez./2015

MENDES, Laura Schertel. DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**. Vol. 120/2018. p. 469 - 483. Nov.-Dez./2018.

NISSENBAUM, Helen Fay. **Privacy in context: technology, policy, and the integrity of social life**. Stanford, California: Stanford University Press, 2010.

PAIS, Sofia Oliveira. **Estudos de direito da União Europeia**. 2.ª ed. Coimbra: Almedina, 2013.

RODOTÀ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. – Rio de Janeiro: Renovar, 2008.

SRNICEK, Nick. **Platform Capitalism.** Cambridge: Polity Press, 2018.

WERTHEIN, Jorge. **A sociedade da informação e seus desafios.** Ci. Inf., Brasília, v. 29, n. 2, p. 71-77, maio/ago. 2000. ISSN 0100-1965. http://dx.doi.org/10.1590/S0100-19652000000200009.

ZUBOFF, Shoshana. **The age of surveillance capitalism**. The fight for a human future at the new frontier of power. New York: Public Affairs, 2019.

# Capítulo II

# A PROTEÇÃO DE DADOS SENSÍVEIS E AS INOVAÇÕES DA ÁREA DA SAÚDE

*Caroline Salah Salmen*[1]
*Cathiani M. Belle*[2]



**RESUMO**

A pesquisa analisa a proteção dos dados pessoais sensíveis a partir da sua coleta dentro das instituições hospitalares até a sua anonimização para aplicação em estatísticas e prospecções tecnológicas. Com base na dinâmica entre o processamento de dados, o direito à privacidade dos doentes clínicos e a evolução dos produtos na área da saúde é que a investigação almeja circunscrever um cenário plural e delicado que subjaz esse debate. Para tanto, apresenta as especificidades da Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil, em discussão com a União Europeia e os Estados Unidos. Para, por fim, observar a efetividade dos serviços prestados na área da saúde no que tange à proteção dos dados pessoais e a sua prospecção de uso na indústria das tecnologias para a saúde. Por meio de método dedutivo e de pesquisa bibliográfica, foi possível concluir que no Brasil, assim como na União Europeia e nos Estados Unidos, há uma crescente preocupação com a proteção dos dados pessoais e que as normas vigentes para o tratamento dos dados dos pacientes em hospitais antes da aprovação da LGPD apresentavam critérios de seguridade.

**Palavras-chave:** Lei Geral de Proteção de Dados; LGPD; Direito da Saúde; dados sensíveis.

[1] É Advogada, pós-graduada em Direito Civil, do Consumo e Processo pela Universidade Positivo. Advogada. Pesquisadora e membro do Grupo de Estudos em Direito Autoral e Industrial (GEDAI) da Universidade Federal do Paraná (UFPR). E-mail: carolinesalmen@gmail.com.

[2] Doutoranda em Filosofia, na área de Ética e Política, pela Universidade Federal do Paraná - UFPR. Mestra e graduada em Filosofia pela Universidade Federal do Paraná - UFPR. Pesquisadora e membro do Grupo de Estudos em Direito Autoral e Industrial (GEDAI) da Universidade Federal do Paraná (UFPR). E-mail: cathibelle.07@gmail.com.

## 1 INTRODUÇÃO

O crescimento do uso da internet, das grandes redes e dos sistemas de informação tem mudado a forma como as mais diversas atividades humanas são realizadas. Um dos grandes fatores que justificam essa revolução é o crescimento exponencial no tratamento e compartilhamento de dados.

O intercâmbio de dados é realizado para as mais diversas finalidades, como no caso de empresas privadas que adquirem grande quantidade de bancos de dados pessoais para estudar a assertividade no lançamento de um novo produto ou serviço, com base no perfil dos indivíduos que a empresa tem interesse em prospectar. A complexidade do ser humano resta reduzida a certo perfil comportamental gerada por meio de tratamento de dados (SCHREIBER, 2014).

Não é diferente na área da saúde, especialmente nas grandes estruturas, com coleta de dados em proporções elevadas, que inviabilizam a comparação de dados de saúde e de indivíduos nas mais diversas localidades e revisões do tratamento assistencial proposto.

A coleta de dados na saúde e sua comparabilidade fomentará uma revisão constante de protocolos clínicos e dos tratamentos propostos, conforme a faixa etária, o sexo, a idade e demais características que se considere relevante (BONAFÉ, 2019, p. 46). A congregação de resultados de exames por imagens, por exemplo, tem permitido diagnósticos mais corretos do que aqueles realizados por profissionais médicos experientes, incapazes de processar milhares de resultados de exames em um mesmo momento.

Se a captação e tratamento de dados em outros setores proporciona melhoria dos resultados e eficiência, no setor da saúde não é diferente, mas há sempre a sensibilidade de enfoque, pois a atuação é sempre orientada pelo direito à vida. Paralelamente, temos o direito à privacidade do paciente, da escolha e da participação do melhor tratamento.

Vivemos no período da Sociedade Informacional, na qual a proteção integral da pessoa passa pelas dimensões do seu corpo que se apresenta em duas perspectivas: o corpo é físico, mas também é eletrônico a partir dos dados pessoais, que se referem a informações relativas a uma pessoa, incluindo-se os dados sensíveis (RODOTÀ, 2004).

Portanto, a proteção de dados sensíveis de pacientes em tratamento nas instituições hospitalares no Brasil permite debater a seriedade desse amparo legal, por um lado, e a necessidade da divulgação de alguns desses dados para o mapeamento, pesquisa e inovação na área da saúde, por outro lado. Nesse contexto, o problema é o de como discriminar o processo de uso compartilhado entre o recolhimento dos dados sensíveis desde o registro para cadastro em um consultório até a entrada em um hospital e de como esses dados passam a ser acolhidos pela indústria de tecnologia na área da saúde.

Nesse cenário é que subjaz as seguintes questões: i) A legislação brasileira assegura a proteção de dados pessoais sensíveis na área da saúde? ii) Como ocorre o tratamento dos dados pessoais sensíveis desde a primeira coleta até a anonimização para utilização e divulgação pelo Ministério da Saúde? iii) Existe diferença entre o tratamento de dados pessoais sensíveis na área da saúde apresentado pela legislação brasileira e em relação as leis da União Europeia e dos Estados Unidos? iv) A utilização de dados pessoais sensíveis por indústrias que trabalham com inovação e novas tecnologias na área da saúde pode configurar uma violação da LGPD?

A partir da análise dos dados sensíveis e do tratamento dessas informações até a sua anonimização é que a pesquisa almeja ponderar as interrogações em torno da responsabilidade dos hospitais na proteção de dados pessoais sensíveis e o direito à privacidade dos doentes clínicos. Portanto, o intuito da investigação é ampliar o entendimento a respeito de dados da saúde e circunscrever uma nova finalidade para a dinâmica de coleta desses dados e, com isso, poder apresentar possibilidades a expansão da inovação na área da saúde.

## 2 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O TRATAMENTO DE DADOS NA SAÚDE

Os dados possuem um inestimado valor, visto que, por meio deles, torna-se viável a formação de perfis de comportamento, consumo e até mesmo sobre características genéticas. Assim como muitos outros, o setor de saúde é dependente de dados e análises para proporcionar serviços mais rápidos e melhores. É um dos setores que atravessa um momento de grande inovação e transformação digital, utilizando-se da Inteligência Artificial, *Big Data, Machine Learning*, plataformas em nuvem, etc.

Ao longo dos anos, antes mesmo da LGPD sequer começar ser debatida, foram editadas normas e instituídos critérios técnicos para o compartilhamento de dados nos sistemas de saúde vigentes no país, tais como o Sistema de Saúde Único (SUS), a Saúde Suplementar e a Saúde Privada. Isso porque, segundo Bonafé (2019, p.47), "o compartilhamento de dados em saúde é essencial para reduzir os custos assistenciais, seja ao disponibilizar dados mínimos do paciente aos que integram a cadeia de assistência à saúde, seja para viabilizar um tratamento mais assertivo".

O Ministério da Saúde instituiu regras para os Sistemas de Informação, por meio da Portaria de Consolidação nº 01, de 28 de setembro de 2017 ("Portaria"), com um capítulo específico regulamentando o uso de padrões, informações em saúde e de interoperabilidade entre os sistemas de informação do SUS, incluindo também os sistemas privados e de saúde suplementar[3], com objetivo de permitir o compartilhamento de informações em saúde e a cooperação de todos os profissionais e de estabelecimentos de saúde. Dentre os principais itens na instituição de sistemas de informação, foi instituído a criação e padronização de codificação de dados, de forma a tornar célere o acesso a informações relevantes e fidedignas ao usuário dos serviços de saúde.

A referida Portaria também estabelece que o sistema e informação permitirá a identificação dos usuários das ações e serviços em todo o país

[3] Portaria de consolidação nº 1, de 28 de setembro de 2017, art. 230, parágrafo único.

por meio do Sistema Cartão Nacional de Saúde[4] que, dentre vários benefícios, permite que (i) a apuração do perfil epidemiológico dos usuários de acordo com seu domicílio residencial, (ii) a possibilidade de o usuário ter acesso aos seus dados de forma unificada e, (iii) a garantia de que os dados pessoais dos usuários sejam tratados de forma a respeitar os princípios constitucionais da intimidade, da integralidade das informações e da confidencialidade. Além disso, essas informações e dados dos usuários do SUS compõem uma base de dados que poderão ser compartilhados entre os entes federativos e demais órgãos que executem políticas públicas, desde que sejam respeitadas as normas de segurança da informação. O DATASUS é o responsável por administrar a Base de Dados e encarregado de proporcionar um sistema que possibilite a transferência de informações para outros sistemas utilizados pelo poder público, privado contratado e de saúde complementar. (BONAFÉ, 2019, p. 48).

A portaria de Consolidação nº 01/2017 previu uma série de critérios e requisitos que deverão ser cumpridos por todos os envolvidos na cadeia, por exemplo, o nível de segurança mínimo que deverá ser observado para possibilitar a transmissão de dados de saúde, o órgão responsável pelo armazenamento e a necessidade de individualização da responsabilização do agente público ou privado que teve acesso aos dados, no caso de uma possível infração.

De igual forma, a Agência Nacional de Saúde Suplementar (ANS)[5] também necessita de compartilhamento de informações a fim de que os serviços ofertados pelas operadoras de planos privados de assistência à saúde possam ser prestados aos seus beneficiários. Assim, através da Resolução Normativa nº 305/2012, estabeleceu parâmetros para Troca de Informações na Saúde Suplementar (TISS), sendo um deles, dentre outros, compor o registro eletrônico dos dados de atenção à saúde entre as operadoras, prestadores de serviço de saúde, o beneficiário de plano privado de assistência à saúde e a própria ANS.

---

4 Portaria de consolidação nº 1, de 28 de setembro de 2017, arts. 255 e 256.

5 Instituída pela Lei nº 9.961/200 com objetivo de normatizar, controlar e fiscalizar as atividades das operadoras de planos privados de assistência à saúde.

Assim, é possível verificar que antes mesmo da edição da LGPD o setor da saúde, pública e privada, já era pautado pelos princípios constitucionais de privacidade e intimidade, inclusive tratando de níveis de segurança da informação e regulamentação de ferramentas de tecnologia da informação. Para Bonafé (2019, p. 50), o setor de saúde será fortemente impactado com as obrigações dispostas na LGPD, principalmente no tocante ao direito do usuário do sistema ter informações sobre o uso de seus dados.

## 2.1 O tratamento dos Dados Sensíveis

A LGPD diferencia e tutela de maneira distinta os dados pessoais e os dados pessoais sensíveis. Enquanto o dado pessoal é compreendido por informações relacionadas a pessoa natural identificada ou identificável (artigo 5º, I), o dado pessoal sensível se refere à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II). Ou seja, é um rol taxativo e, portanto, restrito a situações jurídicas objetivas.

O dado pessoal relativo à saúde necessita ser classificado como dado sensível e, assim, receber um regime jurídico próprio, mais protetivo em vista dos riscos que envolvem o seu tratamento receber um distinto tratamento de dados. Tratamento de dados é toda operação feita com dados pessoais, como: coleta, produção, classificação, arquivamento, eliminação (art. 5º, X). Portanto, é possível perceber que há uma ampla conceituação de tratamento de dados pessoais, visto que parte da coleta e termina em seu descarte, englobando todas as possibilidades de manipulação dos dados, independentemente do meio utilizado.

O debate em torno do tratamento de dados pessoais sensíveis ressalta o fato de que a LGPD compreende tanto o tratamento de dados digitais ou como os não digitais, tanto aquele que ocorrem dentro da internet como aqueles que ocorrem fora dela. A LGPD também

apresenta dez princípios fundamentais para a realização das atividades de tratamento de dados pessoais, a saber: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização. Princípios estes que estão sob a égide do princípio da boa-fé[6] e que refletem "a formação de um sistema, pois nenhum deles representa uma novidade em si, mas a cristalização de avanços que foram alcançados pelas leis anteriores, muitas vezes com viés mais pragmático do que principiológico" (OLIVEIRA e LOPES, 2019, p. 82)[7].

Mulholland (2018, p. 163) defende que "deve-se visar a um tratamento limitado desses dados sensíveis, para evitar o seu eventual uso para propósitos que não atendam aos fundamentos republicanos do Estado Democrático de Direito". Nesse sentido, o princípio da finalidade[8] (art. 6º, I) possui destaque pois determina que a utilização dos dados pessoais se restringe "propósitos legítimos, específicos, explícitos e informados ao titular", que, no caso dos dados sensíveis, demandaria hipóteses de tratamento objetivas e limitadas (MORAES, 2008).

Nos termos do artigo 11 da LGPD, as hipóteses de tratamento de dados pessoais sensíveis pode ocorrer (i) com o consentimento do titular; ou (ii) sem o consentimento do titular, nas hipóteses listadas de forma exaustiva. Considerando o seu caráter protetivo e seus fundamentos, prescritos no artigo 2º, notadamente o respeito à privacidade e autodeterminação informativa (que consiste no poder do indivíduo de definir e inspecionar como seus dados pessoais são utilizados), a LGPD determina que o consentimento do titular dos dados sensíveis não poderá ser reali-

6 Lei 13.709/2018. Art.6°.

7 OLIVEIRA, Marco Aurélio Bellizze. LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2019.

8 Doneda (2011, p. 100) aponta que "este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade)".

zado de forma genérica ou para finalidades não especificadas. O consentimento será entendido como específico, desde que ele seja manifestado em relação a propósitos claramente determinados pelo controlador, anteriormente ao procedimento de coleta dos dados pessoais (LIMA, 2019, p.198)[9]. O consentimento poderá ser nulo se as informações fornecidas ao titular possuam um conteúdo enganoso ou abusivo ou sem ter sido apresentadas previamente com transparência, de forma clara e inequívoca (TEFFÉ, VIOLA, 2020, p. 10)

De acordo com a LGPD, os dados pessoais sensíveis podem resultar em danos imediatos quando divulgados de forma indevida, por isso, requerem cuidados especiais e só podem ser solicitados para finalidades específicas, uma vez que poderão "implicar riscos e vulnerabilidades potencialmente mais gravosas aos direitos e liberdades fundamentais de titulares" (VAINZOF, 2019, p.92)[10].

Nesse contexto, o debate em torno do tratamento e da proteção dos dados pessoais sensíveis referente à área da saúde pode apresentar indícios de uma leitura dicotômica, uma vez que, por um lado, existe o titular do direito e seus dados e, por outro lado, o Estado e a possibilidade de tratamentos diversificados desses dados.

No Brasil, a LGPD determina que o tratamento de dados pessoais poderá ocorrer, dentre outras hipóteses, com o fornecimento do consentimento do titular desses direitos[11]. Porém, considerando as peculiaridades dos dados sensíveis, em especial os dados de saúde, a LGPD previu uma relação de hipóteses em que estes poderão ser tratados sem que haja o consentimento do titular[12]. De acordo a Lei, esses dados podem

---

9 **LGPD:** Lei Geral de Proteção de Dados comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 2019.

10 **LGPD:** Lei Geral de Proteção de Dados comentada. / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 2019.

11 Lei 13.709/2018. Art. 7°, I - mediante o fornecimento de consentimento pelo titular; Art. 11, I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

12 Art. 11, II. Lei Federal nº 13.709/2018.

ser tratados a partir da anonimização, isto é, na "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento do dado pessoal, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo"[13]. Desse modo, os dados anonimizados são "dados relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento"[14], ou seja, podem ser descritos como aqueles dados os quais o titular não está inscrito com uma identificação direta e que podem ser utilizados para pesquisas e políticas públicas.

Sendo assim, "referidos conceitos são de extrema relevância na proteção de dados pessoais, para a defesa da livre-iniciativa e a manutenção de inovadores modelos de negócio, pois, conforme já apontado anteriormente, a LGPD não considera dano anonimizado, ou seja, dado relativo a titular que não possa ser identificado, dado pessoal, o que resulta na inaplicabilidade da legislação em estudo para tal tipo de dado" (VAINZOF, 2019, p.95). Devido a sua importância, trazemos as hipóteses em que a lei autoriza o compartilhamento dos dados sensíveis sem o consentimento do titular de forma mais especificada.

### 2.1.1 Cumprimento de obrigação legal ou regulatória

Bonafé (2019, p. 56) alega que o setor da saúde é um dos mais impactados com essa previsão, pois a esfera de atuação do Poder Público é enorme, tanto na Saúde Suplementar quanto no SUS. Além disso, traz como exemplo o caso das notificações compulsórias que, a depender do evento de saúde registrado, cabe ao serviço de saúde notificá-lo à Vigilância Sanitária, a fim de garantir um sistema de controle epidemiológico[15]. Esta notificação compulsória é obrigatória para os médicos e demais profissionais de saúde responsáveis pelos serviços públicos e privados, quando houver

[13] Lei 13. 709/2018. Art. 5°, XI.

[14] Lei 13. 709/2018. Art. 5°, III.

[15] Portaria de Consolidação SUS nº 04, de 28 de setembro de 2017. Anexo V.

suspeita ou a confirmação de doença ou agravo previsto na relação[16] publicada pelo Ministério da Saúde. Assim, a autoridade de saúde tem até 24 (vinte e quatro) horas para ser informada para que, em posse dessas informações, divulgue os dados públicos para os profissionais da saúde, órgãos de controle social e população em gera, mesmo sem o consentimento do titular dos dados, pois decorre de obrigação legal ou regulatória.

Outro exemplo de tratamento de dados que se enquadra nessa hipótese, citado por Bonafé (2019, p. 56), é o de Ressarcimento ao SUS. Nesse caso, o serviço de saúde, público ou privado, presta atendimento em regime de complementariedade ao SUS e colhe os dados do paciente. O SUS e a ANS trocam esses dados, a fim de verificar se, dentre esses pacientes, há beneficiários de Planos Privados de Assistência à Saúde[17]. Realizada a consolidação dessas informações, a ANS remete às Operadoras de Planos Privados de Assistência à Saúde um aviso de beneficiário identificado (ABI), que avaliam os tratamentos prestados ao beneficiário. Verifica-se que o Ressarcimento ao SUS engloba uma troca de dados de saúde bem relevante, o que possibilita, inclusive, que a Operadora tenha acesso ao prontuário do paciente para impugnar tecnicamente o pedido de ressarcimento formulado pela ANS, independentemente de qualquer consentimento.

Como é possível observar, o setor da saúde contempla diversas hipóteses de tratamento de dados sensíveis sem o consentimento do titular para o cumprimento da obrigação legal ou regulatória, considerando o caráter ímpar dessas informações à sociedade como um todo.

### 2.1.2 Execução de Políticas Públicas

Conforme a redação constante na LGPD, desde que em cumprimento de política pública, verifica-se que há ampla possibilidade à Admi-

[16] Há uma extensa lista de doenças e agravos, contudo, destacamos: a) doenças com suspeita de disseminação intencional (Antraz pneumônico, tularemia, varíola); b) doenças febris hemorrágicas emergentes/reemergentes; c) doenças exantemáticas (sarampo e rubéola) e; d) casos de violência sexual e tentativa de suicídio.

[17] Resolução normativa nº 358, de 27 de novembro de 2014, arts. 3º e 4º.

nistração Pública tratar dados sensíveis sem o consentimento do titular. Não há uma definição legal do que é considerado uma política pública e, para Bonafé (2019, p. 57), a regulação da Saúde Suplementar promovida pela AND, a assistência ofertada pelo SUS, as parcerias de desenvolvimento para oferta de medicamentos, dentre outras ações, constituem políticas públicas.

Com o objetivo de subsidiar a formulação, o monitoramento e a avaliação das políticas de saúde, foi instituído, pela Comissão Intergestores Tripartite, o Conjunto Mínimo de Dados da Atenção à Saúde[18] que, de acordo com a normativa, é composto de: (i) dados administrativos, relacionados com a gestão de recursos dos estabelecimentos de saúde; (ii) dados clínico-administrativos, referentes à gestão dos pacientes, e (iii) dados clínicos, relacionados ao estado de saúde ou doença dos indivíduos, expressos em diagnósticos, procedimentos e tratamentos realizados. Ou seja, um pacote completo para qualquer gestor que queira implementar uma política de saúde baseada em dados.

Bonafé (2019, p. 57) entende que a ANPD deverá expedir orientação e normativa acerca do alcance que a hipótese poderá ser utilizada, justamente pela ampla capacidade de tratamento de dados sensíveis sem o consentimento do titular pela Administração Pública.

### 2.1.3 Realização de Estudos por Órgão de Pesquisa

Incialmente, destaca-se que a LGPD define que apenas podem ser enquadrados como órgãos de pesquisa, órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico[19].

[18] Resolução nº 06, de 25 de agosto de 2016.

[19] Art. 5º, XVIII. Lei Federal nº 13.709/2018.

Bonafé (2019, p.59) acredita que a restrição a caracterização de pesquisa a estudos em saúde pública é indevida, pois não é incomum a Administração Pública contratar terceiros para produzir nessas pesquisas, defendendo que, por este motivo, na tramitação da MP nº 869/2018, foram propostas emendas que visavam excluir a definição "sem fins lucrativos" da redação, justamente para autorizar que qualquer pessoa jurídica possa ser enquadrada como órgão de pesquisa, quando atestada sua capacidade técnica e cumpridos os requisitos legais aplicáveis.

### 2.1.4 Exercício Regular de Direitos

A LGPD estipula que não há a necessidade de consentimento do titular dos dados pessoais, caso o tratamento de dados se torne indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral.[20] Portanto, um prestador de serviços pode compartilhar dados para a execução de atividades contratualmente estipuladas, sem necessidade de consentimento do titular dos dados.

Um exemplo desta hipótese seria um titular dos dados pessoais realizar um exame em um laboratório de análise clínicas, dessa forma, não haveria, necessariamente, a obrigatoriedade de o titular dos dados consentir de forma expressa que seus dados sejam transferidos a uma empresa de transporte terceirizada que realiza o deslocamento do material coletado (BONAFÉ, 2019, p. 60).

É necessário que os princípios da LGPD sejam respeitados, principalmente o princípio da finalidade e da necessidade, que estabelecem que os dados serão tratados para fins legítimos e específicos, com a limitação ao mínimo de tratamento necessário para a realização de suas finalidades[21]. Isso demonstra que, conforme as diretrizes e os princípios da LGPD, a Lei não objetiva inviabilizar a execução de contratos e a pres-

[20] Art. 11º, II. Lei Federal nº 13.709/2018.

[21] Art. 6º, I e III, Lei Federal nº 13.709/2018.

tação de serviços, contudo, os agentes de tratamento deverão atuar com boa-fé e adotar medidas para prevenir a ocorrência de danos em decorrência do tratamento de dados pessoais.

### 2.1.5 Proteção da vida ou da incolumidade física

Embora a legislação não defina o conceito do que é considerado como "proteção da vida", contudo, valendo-se dos conceitos previstos no RGPD, de uma maneira ampla, é possível entender que o conceito está adstrito à proteção da vida e à segurança pública.

Assim, torna-se evidente a necessidade de tratamento de dados pessoais diante de uma situação que demande a atuação imediata da Administração Pública para salvar vidas. Um exemplo que possibilita o tratamento de dados com base na proteção da vida é a utilização destas informações para a prevenção, a investigação e a repressão de infrações penais pelos agentes públicos responsáveis (BONAFÉ, 2019)

Nessa perspectiva, o RGPD preceitua que não será necessário o consentimento do titular nos casos de prevenção de ameaças à segurança pública ou violações de deontologia de profissões regulamentadas, como no caso de médicos que estão submetidos aos preceitos éticos dispostos no Código de Ética Médica.

### 2.1.6 Tutela da saúde

A princípio, com a redação inicial da Lei 13.709/2018, o conceito somente abarcava os casos de urgência e emergência, ou seja, nos quais o titular de dados apresenta risco eminente de vida e, assim, não haveria a possibilidade de se obter o consentimento em tais casos.

Porém, houve alteração da LGPD e, em virtude das peculiaridades do setor de saúde, o texto final preceitua que não será obrigatório o consentimento do titular dos dados pessoais sensíveis para as hipóteses em que, o tratamento, for indispensável para a tutela da saúde, em procedi-

mento realizado por profissionais de saúde, serviços de saúde, ou autoridade sanitária.[22]

Contudo, permite a realização de acesso a esses dados pessoais sensíveis para a prática de estudos em saúde pública, desde que observado critérios específicos de segurança e, se possível, o trabalho possa ser desenvolvido com dados anonimizados ou pseudoanonimizados, mas, nunca, relevando os dados pessoais em si mesmos[23].

## 3 A UNIÃO EUROPEIA E OS ESTADOS UNIDOS: UMA AMPLIAÇÃO NA LEITURA DA PROTEÇÃO DOS DADOS SENSÍVEIS

A LGPD apresenta disposições a respeito do tratamento de dados pessoais sensíveis em consonância com a garantia de proteção dos direitos fundamentais. Debate este anteriormente suscitado pela União Europeia nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho[24], relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Lei esta que preconiza a seguridade da proteção das liberdades e dos direitos fundamentais das pessoas singulares[25].

A Diretiva 95/46/CE apresenta, em seu art. 8º, a ponderação do tratamento para certas categorias especificas de dados e, assim como no Brasil[26], discrimina de forma diferenciada os dados referentes à informação "racial ou étnica, as opiniões políticas, as convicções religiosas ou fi-

22 Art. 11, II, "f" Lei Federal nº 13.709/2018.

23 Lei 13.709/2018. Art.13. § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

24 De 24 de Outubro de 1995.

25 Diretiva 95/46/CE. Art. 1º. Objeto da Diretiva: 1. Os Estados-membros assegurarão, em conformidade com a presente Diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.

26 Lei 13.709/2018. Art. 5° II.

losóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual"[27]. Nesses termos, tanto a Diretiva 95/46/CE como a LGPD, demonstram relevante proximidade em relação as especificidades em referência a um o tratamento diferenciado dos dados pessoais sensíveis como uma categoria específica. Em 23 de abril de 2016, a União Europeia apresenta o Regulamento (UE) nº 2016/679 do Parlamento e do Conselho Europeu, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e revoga a Diretiva 95/46/CE. Mas o RGPD[28] mantém as diretrizes de seguridade pautada nos direitos fundamentais de proteção a certos tipos dos dados pessoais.

Os Estados Unidos, distintamente da União Europeia, abordam a discussão em torno da proteção dos dados pessoais a partir da possibilidade de uma relação com o mercado econômico, discriminando uma dinâmica utilitarista. Todavia, o problema é que os EUA não apresentam um conjunto de leis sistematizadas de proteção dos dados pessoas e da privacidade, ou seja, não há um regulamento geral capaz de ser aplicável a todas as atividades de processamento de dados no país. Em 2018, foi apresentada a *Consumer Data Protection Act*, projeto de lei que prevê sanções para as empresas que violarem a privacidade dos usuários, dispondo sobre impactos eficazes na proteção e na privacidade das informações pessoais dos usuários. É no debate em torno das perspectivas de proteção que a pesquisa inscreve a Quarta e Quinta Emenda Constitucional americana, com o intuito de elucidar como é possível discriminar, na compreensão dos EUA, um tratamento de dados pessoais expansivo, mas, também, protetivo.

Portanto, a questão da proteção de dados pessoais, especificamente de dados pessoais sensíveis, inscreve-se em termos de uma análise de

---

27 Diretiva 95/46/CE. Art. 8º. 1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.

28 Regulamento (UE) nº 2016/679 do Parlamento e do Conselho Europeu, nomeadamente conhecida como *General Data Protection Regulation* (GDPR).

aspectos específicos das legislações supracitadas, com o intuito de debater uma alternativa que preserve os direitos de proteção e de privacidade, mas que, ao mesmo tempo, possibilite a extensão das pesquisas e produtos tecnológicos na área da saúde, nos termos do artigo primeiro da Lei 13.243/2016[29] no que tange aos estímulos ao desenvolvimento científico, à pesquisa, à capacitação científica e tecnológica e à inovação[30].

## 3.1 A União Europeia e a defesa dos direitos fundamentais

A vigência do Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho apresenta alterações legislativas distintas da Diretiva 95/46/CE, mas não altera a compreensão da União Europeia a respeito da proteção e do tratamento dos dados pessoais em termos de significativa defesa dos direitos fundamentais do titular desses dados. O RGPD elabora, em seu art. 9º, os termos para o processamento de dados pessoais sensíveis na categoria especial de dados pessoais, ou seja, "é proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa"[31]. Mas, para além da incorporação dos dados da saúde na categoria dos dados especiais, o RGPD discrimina, especificamente, o que são esses dados relativos à saúde como aqueles "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde"[32].

---

29 Marco Legal de Ciência, Tecnologia e Inovação, de 11 de janeiro de 2016.

30 Lei 13.243/2016. Art. 1º.

31 Regulamento (UE) 2016/679. Art.9º, nº1.

32 Regulamento (UE) 2016/679. Art. 4°, nº15.

Entretanto, o RGPD permite ponderar que esta categoria não é aplicável para fins da medicina preventiva, para a prestação de cuidados ou tratamentos de saúde, para a gestão de sistemas e serviços para a saúde[33]. Para os casos em que há um evidente interesse público no domínio da saúde pública, como garantia à elevação da qualidade nos cuidados em saúde, medicamentos e outros dispositivos[34]. E, ainda, quando o tratamento desses dados pessoais específicos for para fins de investigação científica ou estatística[35]. Desse modo, assim como a Diretiva 95/46/CE permitia ao Estado intervir no tratamento dos dados pessoais sensíveis, em termos de saúde pública, quando o manifesto interesse público em correspondência com as questões de investigação científica[36], o RGPD afirma que os Estado-Membros possuem "margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensí-

[33] Regulamento (UE) 2016/679. Art. 9° (h) Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 3;

[34] Regulamento (UE) 2016/679. Art. 9° (i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;

[35] Regulamento (UE) 2016/679. Art. 9° (j) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, nº 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.

[36] Diretiva 95/46/CE. (34) Considerando que, sempre que um motivo de interesse público importante o justifique, os Estados-membros devem também ser autorizados a estabelecer derrogações à proibição de tratamento de categorias de dados sensíveis em domínios como a saúde pública e a segurança social - em especial para garantir a qualidade e a rentabilidade no que toca aos métodos utilizados para regularizar os pedidos de prestações e de serviços no regime de seguro de doença - e como a investigação científica e as estatísticas públicas; que lhes incumbe, todavia, estabelecer garantias adequadas e específicas para a proteção dos direitos fundamentais e da vida privada das pessoas;

veis»). Nessa medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais"[37], mas, sempre resguardando o respeito aos direitos fundamentais e a privacidade dos titulares.

A compreensão do consentimento do titular dos dados assume relevante importância nos termos de tratamento desses dados quando sensíveis, tanto no Brasil como na União Europeia, uma vez que "o Regulamento Geral sobre a Proteção de Dados, criado para atender a uma necessidade de modernização do sistema de proteção de dados pessoais europeu, também reflete grande preocupação em torno do consentimento" (LANA e D'ALMEIDA, 2019, p.72). Portanto, é possível observar uma linha tênue entre as predisposições atribuídas ao consentimento do titular dos dados e a intervenção estatal, mas é preciso investigar em que medida essa divergência não pode compreender uma solução passível ao interesse público, em termos nos quais o interesse público manifesta uma parcela coincidente de interesses dos indivíduos como membros de uma coletividade (BACELLAR FILHO, 2010, p.91).

## 3.2 Os Estados Unidos e a compreensão utilitarista no tratamento dos dados pessoais

A formulação da *Consumer Data Protection* (2018) como projeto de lei, objetiva alterar a Lei da Comissão Federal do Comércio[38] e estabelecer requisitos e responsabilidades para entidades que usam, armazenam ou compartilham informações pessoais[39]. Nesse contexto é que ela almeja

37 Regulamento (UE) 2016/679. (10).

38 *Federal Trade Commission* <https://www.ftc.gov/>

39 *"To amend the Federal Trade Commission Act to establish requirements and responsibilities for entities that use, store, or share personal information, to protect personal information, and for other purposes"* <https://assets.documentcloud.org/documents/5026543/Wyden-Privacy-Bill.pdf>

ampliar os poderes da *Federal Trade Comission* (FTC), como uma agência reguladora que defende os interesses dos consumidores e capaz de regular as questões em torno da privacidade dos dados pessoais. Contudo, um aspecto de relevância fundamental à proteção desses dados presente no projeto é a criação do cadastro "*Do Not Track*"[40]. Este cadastro permite que a pessoa que não deseja ver seus dados sendo repassados a terceiros, possa manifestar a sua opção e ter suas informações "deixadas de fora" do compartilhamento de dados. Nesse sentido é que se manifesta um potencial interesse americano na avaliação do impacto da proteção de dados, em termos de um estudo que avalia em que medida um sistema da informação protege a privacidade e a segurança das informações pessoais que são processadas[41].

Todavia, é preciso observar que os Estados Unidos desenvolvem uma posição utilitarista em relação ao tratamento e a proteção dos dados pessoais, postura esta que está voltada à expansão do mercado econômico. Para Pamela Samuelson, a Quarta Emenda[42] fornece proteção contra invasões não autorizadas nas propriedades reais ou pessoais de alguém, que o fazem com o intuito de obter acesso a informações que possam estar escondidas, por outro lado, a Quinta Emenda[43] representa a proteção contra as ações da própria pessoa que pode acabar por revelar certas informações sobre si mesma a outrem (SAMUELSON, p.5). Entretanto, tanto uma proteção como a outra não incorrem no direito de propriedade sobre os dados pessoais, ou seja, é possível reconhecer o direito à privacidade, mas não o direito à propriedade das informações pessoais no direito americano.

---

40 Projeto 2018: SEC. 6. *"DO NOT TRACK" DATA SHARING OPT OUT.*

41 Projeto 2018: 6)" *DATA PROTECTION IMPACT ASSESSMENT.— The term "data protection impact assessment" means a study evaluating the extent to which an in formation system protects the privacy and security of personal information the system processes"*

42 *"**The Fourth Amendment** protects citizens from unreasonable search and seizure. The government may not conduct any searches without a warrant, and such warrants must be issued by a judge and based on probable cause"* <https://www.whitehouse.gov/>.

43 *"**The Fifth Amendment** provides that citizens not be subject to criminal prosecution and punishment without due process. Citizens may not be tried on the same set of facts twice, and are protected from self-incrimination (the right to remain silent). The amendment also establishes the power of eminent domain, ensuring that private property is not seized for public use without just compensation"* <https://www.whitehouse.gov/>.

No Brasil, a LGPD não apresenta referência à propriedade, em verdade, o termo "propriedade" é expresso somente uma vez na LGPD e não faz menção a uma relação direta com os dados pessoais[44]. Nesse ínterim, o conceito de titular pode ser analisado como aquele que compreende a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"[45]. Sendo assim, é possível observar como a lei não reconhece o direito de um titular livre para controlar a utilização dos seus dados pessoais. No projeto de lei americano, as informações pessoais são definidas como qualquer informação, transferida ou obtida e que possa ser vinculada a um consumidor específico[46], demonstrando, mais uma vez, como o dado ou informação pessoal apresenta vínculo necessário com as atribuições especificas de um titular.

A análise dos dados pessoais sensíveis, discriminados na LGPD, permite elucidar os casos específicos em que é possível ocorrer o tratamento desses dados sem o consentimento do seu titular[47]. Portanto, por mais intuitivamente intensa que possa parecer a ideia de direitos de propriedade nos dados pessoais, esses dados não são observados nesses termos, mesmo nos EUA a existência de proteção em relação aos dados pessoais não corresponde ao direito de uma pessoa ter a propriedade de seus dados pessoais (SAMUELSON, p.6). Mesmo constatando a possibilidade de haver um pensando voltado para o mercado econômico, uma vez que os EUA apresentam propensões a desenvolver a ideia de comercialização dos dados pessoais pelas empresas[48], não há previsão legal para tanto. Contudo, é preciso ressalvar que "determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto

44 Lei 13.709/2018. Art. 55-L. III.

45 Lei 13.709/2018. Art 5°, V.

46 Projeto 2018: *"(12) PERSONAL INFORMATION.—The term "personal information" means any information, regardless of how the information is collected, in ferred, or obtained that is reasonably linkable to a specific consumer or consumer device"*.

47 Lei 13.709/2018. Art. 11, II. c), f).

48 *"A property rights approach to solving the information privacy problem may also be consistent with survey evidence suggesting that most Americans are willing to disclose personal data to businesses and allow them to use these data as long as the individuals obtain a discernible benefit from this disclosure and use"* (SAMUELSON, p.8).

grau, que não pode ser conferida exclusivamente a uma decisão individual – como é o caso para certas modalidades de utilização de dados sensíveis" (DONEDA, 2011, p. 98).

O debate em torno da questão da propriedade dos dados pessoais, a partir de uma leitura americana, enseja a questão da possibilidade de as pessoas obterem alguma forma de retorno pessoal com esta dinâmica, principalmente no que tange as questões da área da saúde. Projetos como o do Robô Laura[49], que apresenta um monitoramento contínuo dos sinais vitais dos pacientes, permitem que estes recebam um benefício direito a partir da sua intervenção. Desse modo, mesmo havendo um tratamento direto do quadro clínico dos pacientes para ocorrer o monitoramento desses dados e dos protocolos assistenciais necessários à manutenção do processo, esses dados são utilizados com uma finalidade específica[50] e não incorre em uma vantagem econômica[51], mas no auxílio e redução de custos à saúde pública. Todavia, é preciso observar que:

> Em primeiro lugar, direitos fundamentais não podem estar sujeitos exclusivamente, a juízos de custo-benefício, uma vez que são deontológicos e vinculantes. Em segundo lugar, não necessariamente existe o trade-off entre eficiência e privacidade, diante da multiplicidade de técnicas e ferramentas que podem ser utilizadas para movimentar a economia digital, mas preservando as situações existenciais dos titulares de dados. Em terceiro lugar, ainda que sempre houvesse o trade-off, seria preciso ponderar que a inovação não é um valor absoluto e que, exatamente por isso, não pode ser perseguida de forma irrestrita e às custas do sacrifício das situações existenciais mais elementares dos titulares de dados[52].

---

49 Realiza o monitoramento e análise preditiva dos riscos de sepse nos hospitais com a aplicação de Inteligência Artificial. Disponível em: https://www.laura-br.com/. Acesso em: 11 set. 2020.

50 Lei 13.709/2018. Art. 9°, I - finalidade específica do tratamento;

51 Lei 13.709/2018. Art. 11. II, g) §4°.

52 FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2019, p.110-111.

Desse modo, ao ensejar uma prospecção tecnológica para a saúde em termos de flexibilização dos dados pessoais sensíveis, não se pode incorrer em um retrocesso em relação aos avanços e direitos apresentados pela LGPD. A questão das vantagens decorrentes do acesso e tratamento desses dados devem estar circunscritas em termos de valor para uma melhora no quadro clínico dos pacientes em tratamento e, ainda, no valor agregado ao redirecionamento dos gastos públicos à uma maior eficiência de aplicação ao suprimir problemas e investir em soluções.

O debate entre a interpretação do tratamento dos dados pessoais referente a União Europeia e os Estados Unidos, permite ponderar prospecções distintas para uma relação entre proteção de dados, mas, também, para pensar uma forma de expansão tecnológica. De acordo com Samuelson[53], os EUA objetivam soluções baseadas no mercado econômico, ou seja, na defesa de um modelo que reflete a perspectiva utilitarista. Por outro lado, a União Europeia objetiva um adequado regime regulatório, evidenciado pelo RGPD e pautado na defesa os direitos fundamentais. Sendo assim, as duas posições apresentam não só uma forma de tratamento distinto para a privacidade dos dados pessoais como, também, permitem observar como, no Brasil, a LGPD está em consonância com as disposições dessas leis e apresenta princípios capazes de garantir e expandir o tratamento de dados pessoais sensíveis em termos de diálogo entre as projeções do mercado e do respeito aos direitos fundamentais.

## 4 A PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS E A EXPANSÃO TECNOLÓGICA DA INDÚSTRIA DA SAÚDE.

O Brasil apresenta diretivas especificas para o armazenamento dos dados pessoais sensíveis de pacientes clínicos a partir da utilização de protocolos próprios para a área da saúde[54], assim como para o tratamento dos

53 SAMUELSON, **Privacy As Intellectual Property?.**

54 HL7 FHIR®; HL7 v2®; DICOM®.

dados pessoais sensíveis, a saber: HIPAA[55], HITRUST CSF[56], ISO/IEC 27001[57] e ISO/IEC 27018[58]. Desse modo, a LGPD apresenta possibilidades de ampliação e compreensão desses dados sensíveis de forma a corroborar as especificidades para as áreas de pesquisa e inovação tecnológica nas quais eles podem ser utilizados.

Todavia, a premissa de pensar a possibilidade de um direito de propriedade dos dados pessoais sensíveis não objetiva suscitar os problemas pontuados por Samuelson em sua análise[59], mas ponderar em que medida a perspectiva utilitarista dos EUA, em termos de uma visão econômica voltada à expansão tecnológica e ao desenvolvimento, poderia corroborar a interpretação brasileira no que tange a área da saúde no país. A autora deixa claro os cuidados necessários quando pensamos esses aspectos e aponta o porquê da União Europeia apresentar uma visão mais libertária sobre a proteção de dados pessoais em relação aos Estado Unidos, uma vez que o contexto histórico europeu permite compreender melhor do que o dos EUA o potencial abusivo incutido na utilização desmedida dos dados pessoais.

Contudo, o RGPD também permite ampliações em relação ao tratamento dos dados sensíveis e reconhece o papel das novas tecnologias em termos econômicos, mas, sempre pautados na observação da proteção dos dados pessoais[60]. Portanto, o debate em torno da proteção dos dados sensíveis se inscreve nos termos de articulação dos valores ineren-

---

55 *Health Insurance Portability and Accountability Act* (1996).

56 *Health Information Trust Alliance* (HITRUST) estrutura de segurança comum (CSF).

57 *Information Security Management System* (2005).

58 *Information Security Management System* (2019).

59 i) uma infraestrutura para o funcionamento de um sistema de direitos de propriedade; ii) A alienação de informações pessoais; iii) A concessão de direitos de propriedade não serem aplicáveis aos dados pessoais; iv) a diferença entre os direitos de propriedade propostos com base em informações pessoais e a os direitos de propriedade que regulam o mercado de produtos baseados em informações; v) a concessão de direitos intangíveis em informações intangíveis e uma possível incoerência na lei de propriedade intelectual; vi) a aprovação de uma legislação que cria o direito de propriedade sobre dados pessoais; vii) a privacidade das informações pessoas como um direito civil fundamental. (SAMUELSON).

60 Regulamento (UE) 2016/679. (6).

tes à privacidade das informações as quais devem restringir e estruturar relações sociais, econômicas, tecnológicas e jurídicas (SAMUELSON, p. 4).

Nesses termos é que é preciso ressaltar uma maior intervenção do Estado "para reduzir a assimetria entre as empresas de tecnologia e o usuário, e ao mesmo tempo para limitar a autonomia da vontade dos titulares no que tange à limitação da negociabilidade da própria privacidade" (LANA e D'ALMEIDA, 2019, p.78). A LGPD pode ser interpretada como uma compilação de preceitos fundamentais do direito a proteção dos dados pessoais no decorrer das diversas outras formulações presentes nas legislações brasileiras, tais como o Marco Civil da Internet[61] ou a Lei de Acesso à Informação[62]. Mas, é necessário pensar que, mesmo com a possibilidade de novas perspectivas de proteção para os dados pessoais estarem tramitando na Câmara dos Deputados[63], em que medida a visão de um contexto prático, que compreende a lei-titulares-tecnologia, não permite vislumbrar um equilíbrio entre os titulares dos dados pessoais, a indústria tecnológica e a posição do Estado, no qual todos devem cumprir com as previsões legais, mas, ao mesmo tempo, corroborar a inovação na saúde no país.

A Comissão Nacional de Incorporação de Tecnologias no Sistema Único de Saúde (CONITEC) avalia as diversas tecnologias demandadas em todo o país no setor. Dentre as diretrizes à sua atuação estão a "proteção do cidadão nas ações de assistência, prevenção e promoção à saúde por meio de processo seguro de incorporação de tecnologias pelo SUS"[64]; "a incorporação de tecnologias por critérios racionais e parâmetros de eficácia, eficiência e efetividade adequados às necessidades de saúde"[65]; e "a incorporação de tecnologias que sejam relevantes para o cidadão e para

61 Lei nº 12.965, de 23 de abril de 2014.

62 Lei nº12.527, de 18 de novembro de 2011.

63 PEC 17/2019 - Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

64 Decreto 7.646/2011. Art.3°, II.

65 Decreto 7.646/2011. Art.3°, III.

o sistema de saúde, baseadas na relação custo-efetividade"[66]. Portanto, a CONITEC compreende em seu processo avaliativo de incorporação de novas tecnologias destinadas a área da saúde o cumprimento de um processo seguro, eficiente e pautado nas necessidades do país.

## 5 CONCLUSÃO

Na publicação da LGPD foi disposto uma vedação expressa de comunicação e compartilhamento de dados sensíveis referentes a saúde com objetivo de obter vantagem econômica. Contudo, após a votação da MP nº 869/2018, a Lei foi novamente alterada, com o intuito de permitir o compartilhamento de dados de saúde com objetivo de obter vantagem econômica, nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, recepcionando, inclusive, os serviços auxiliares de diagnose e terapia[67]. Além desta exceção, a lei também abarca os casos de Portabilidade dos dados solicitada pelo titular e; transações financeiras e administrativas resultantes do uso e da prestação dos serviços.

Para Bonafé (2019, p.61) "a alteração legislativa foi extremamente benéfica ao setor, pois, a nova redação elimina possíveis dúvidas na possiblidade de compartilhamento de dados, entre operadoras, prestadores de serviços e gestores do SUS, com fins lucrativos por exemplo".

A impossibilidade de compartilhamento de dados de saúde com fins econômicos caminhava contrariamente a todos os estudos e entendimentos já consolidados no setor da saúde, onde a transferência de informações e o uso de dados é prática necessária e indispensável para os agentes envolvidos na cadeia.

Não obstante, a LGPD foi expressa ao determinar que o compartilhamento de dados pessoais sensíveis referentes à saúde, com objetivo

[66] Decreto 7.646/2011. Art.3°, IV.

[67] Art. 11, § 4º, I e II. Lei Federal nº 13.709/2018.

de obter vantagem econômica, estará sempre atrelado ao interesse do titular. Assim, os agentes de tratamento deverão verificar o objetivo de compartilhamento, com a finalidade de verificar se o titular dos dados será beneficiado de alguma forma.

Foi incluída a impossibilidade de tratamento de dados para a prática de seleção de riscos na contratação de qualquer modalidade[68], a fim de proteger o titular de dados de possível interação entre farmácias, operadoras e seguros privados de assistência à saúde. Para Bonafé (2019, p. 62) a inclusão foi desnecessária "pois a utilização de seleção de risco em qualquer tipo de contratação já era vedada pela Súmula nº 27/2015 da ANS[69]".

Portanto, após a demonstração da indispensabilidade de compartilhamento de dados entre os agentes envolvidos na cadeia da saúde, a alteração legislativa foi assertiva, vez que possibilitou a comunicação e o compartilhamento de dados com fins lucrativos, sem, entretanto, negligenciar os direitos e princípios dos titulares dos dados pessoais sensíveis. Demonstrando, assim, aos moldes de uma integração interpretativa entre a União Europeia[70] e os Estados Unidos[71], como é possível resguardar a proteção dos dados pessoais sensíveis como um direito fundamental, mas, também, projetar possibilidades de desenvolvimento tecnológico para a área da saúde.

## REFERÊNCIAS

***Consumer Data Protection Act.*** Disponível em: https://assets.documentcloud.org/documents/5026543/Wyden-Privacy-Bill.pdf. Acesso em: 05 jul. 2020.

68 Art. 11, § 5º Lei Federal nº 13.709/2018.

69 Súmula Normativa nº 27, de 10 de junho de 2015.

70 In. Seção IV, Capítulo I. MARETTI, Luis Marcello Bessa. MONROE. O dever de transparência no compartilhamento de dados pessoais entre órgãos e entidades de direito público – um comparativo entre o direito europeu e o direito brasileiro.

71 In. Seção II. Capítulo V. TRINDADE, Rangel. CORDOURO, Leonardo. A proteção de dados pessoais do *California Consumer Privacy Act* (CCPA): direcionamento a iniciativas tecnológicas brasileiras no EUA.

BONAFÉ, Lucas Alves da Silva. *et. al*. **LGPD na Saúde**. E-BOOK. 2019. Disponível em: https://lgpdesaude.com.br/. Acesso em: 05 jul. 020.

DALLARI, Analluza Bolivar. **Impactos da LGPD na saúde suplementar e a aprovação de parecer sobre MP 869/2018**. Consultor Jurídico. 07/05/2019. Disponível em: https://www.conjur.com.br/2019-mai-07/analluza-dallariimpactos-lgpd-saude-suplementar. Acesso em: 05 jul. 2020.

**Direito administrativo e interesse público: estudos em homenagem ao Professor Celso Antônio Bandeira de Mello**/ Coordenadores; Romeu Felipe Bacellar Filho; Daniel Wunder Hanchem. Prefácio de Weida Zanconer. Bello Horizonte: Fórum, 2010.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul/dez 2011. Disponível em: http://editora.unoesc.edu.br/index.php/espacojuridico/article/download/1315/658. Acesso em: 01 ago. 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Seminário de Proteção à Privacidade e aos Dados Pessoais – O Arcabouço Legal de Proteção à Privacidade e aos Dados Pessoais no Brasil**. Ministério da Justiça, DPDC, 2014, Color.

FRAZÃO, Ana; TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1. Ed. – São Paulo: Thomson Reuters Brasil, 2019.

GUTIERREZ, Teresa de Souza Dias. et. al. **LGPD na Saúde: o que as empresas precisam saber**. E-BOOK. 2019. Disponível em: https://lgpdesaude.com.br/. Acesso em: 07 set. 2020.

JÚDICE, Lucas Pimenta e NYBO, Erick Fontenele. **Direito das *Startups***. Juruá editora, São Paulo, 2016.

LANA, Alice de Perdigão; D'ALMEIDA, Érica Nogueira Soares. **A efetividade da solução do consentimento na proteção de dados pessoais.** In. WACHOWICZ, Marcos, PEREIRA, Alexandre Libório Dias, LANA, Pedro de Perdigão. NOVOS DIREITOS INTELECTUAIS: ESTUDOS LUSO-BRASILEIROS SOBRE PROPRIEDADE INTELECTUAL, INOVAÇÃO E TECNOLOGIA. Gedai UFPR: Curitiba, 2019.

LGPD: **Lei Geral de Proteção de Dados comentada**/ coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters, 2019.

LGPD: **Lei Geral de Proteção de Dados pessoais: manual de implementação**/ Viviane Nóbrega Maldonado coordenação. – São Paulo: Thomson Reuters Brasil, 2019.

LIMA, Caio César Carvalho. **Objeto. Aplicação material e Aplicação territorial**, in MALDONADO, Viviane Nóbrega BLUM, Renato Ópice (coord.). Comentários ao RGPD: Regulamento Geral de Proteção de Dados da União Européia. São Paulo: Thomson Reuters Brasil, 2018

MACHADO, Nunes. **LGPD na Saúde**. Editora MF, São Paulo, 2019.

MENDES, Laura Schertel Ferreira, **Privacidade, Proteção de Dados e Defesa do Consumidor – Linhas Gerais de Um novo Direito Fundamental**. Saraiva, 2014, Série IDP: linha de pesquisa acadêmica. Não paginado.

MORAES, Maria Celina Bodin de (Org.). Apresentação do autor e da obra. In: RODOTÀ, Stefano. **A vida na sociedade de vigilância: A privacidade hoje**. Rio de Janeiro: Renovar, 2008. p. 1-12. Tradução: Danilo Doneda e Luciana Cabral Doneda.

MULHOLLAND, Caitlin. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18).** Revista de Direitos e Garantias Fundamentais, v. 19, p. 159-180, 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**. A privacidade hoje. Rio de Janeiro: Renovar, 2008. Tradução: Danilo Doneda e Luciana Cabral Doneda.

_____. **Transformações do corpo**. Revista Trimestral de Direito Civil, v. 19, p. 91-107, 2004.

SAMUELSON, Pamela. **Privacy As Intellectual Property?** Professor of Information Management and of Law, University of California at Berkeley.

SCHNEIDE, Giulia. **European intellectual property and data protection in the digital-algorithmic economy: a role reversal (?)** - Journal of Intellectual Property Law & Practice, 2017, Vol. 0, No. 0

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Civilistica.com. Rio de Janeiro, a. 9, n. 1,

2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-l-gpd/. Acesso em: 01 set. 2020.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho**, de 24 de outubro de 1995, (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 24/10/1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31995L0046. Acesso em: 01 set. 2020.

_____. **Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho**, de 23 de abril de 2016, (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&-from=PT. Acesso em: 01 set. 2020.

# Capítulo III

# O CONSENTIMENTO PARA O TRATAMENTO DOS DADOS PESSOAIS DE CRIANÇAS: uma análise de direito comparado

*Marcelo L. F. de Macedo Bürger*[1]

**SUMÁRIO**



**RESUMO**

O texto adota o direito comparado em sua metodologia funcional para evidenciar como a Comunidade Europeia e o Brasil responderam à necessidade de proteção dos dados pessoais de crianças. Para tanto, busca especificamente o desenho normativo dado à exigência de um consentimento especial para o tratamento destes dados, sobretudo quando tal consentimento é exigido, quem é legitimado para manifesta-lo e como pode ser verificado.

**Palavra-chave:** consentimento; criança; dados pessoais.

## 1 INTRODUÇÃO

Setembro de 2020 será por muito tempo lembrado pelo início da vigência da Lei Geral de Proteção de Dados (LGPD) brasileira (Lei 13.709/2018). Seu objeto é a proteção de dados pessoais, considerados o petróleo do século XXI, tamanha a potencialidade de sua exploração e valor econômico.

[1] Advogado. Doutorando e mestre em Direito pela Universidade Federal do Paraná (UFPR). Professor de Direito Civil no Centro Universitário Curitiba – UniCuritiba. Membro do Grupo de Estudos de Direito Autoral e Industrial – GEDAI e do Núcleo de Estudos em Direito Civil Constitucional Virada de Copérnico (PPGD/UFPR). Vice-presidente do Instituto Brasileiro de Direito de Família – Seção Paraná e integrante do IBERC.

Dentre as diversas questões por ela regulamentadas, destaca-se o regime diferenciado para a proteção de dados pessoais de crianças e adolescentes, em especial pelos mecanismos adotados para solver um problema concreto: como conciliar a vulnerabilidade das crianças, ainda em desenvolvimento e mais suscetíveis a escolhas irrefletidas e estímulos manipulativos, com sua inevitável participação no ambiente digital, em que seus dados pessoais podem ser facilmente acessados e captados por terceiros, com inesgotáveis possibilidades de utilização.

A resposta se dá pelo recurso a um regime especial de consentimento exigido para o tratamento[2] de dados pessoais de crianças.

A pesquisa recorre ao Direito Comparado para verificar, pelo método funcional, como a União Europeia conciliou estes fatores, construindo um regime jurídico unitário aplicável a todos os estados membros (Regulamento Geral de Proteção de Dados), e as principais questões debatidas e já testadas naquela espacialidade, sobretudo considerando que o Regulamento foi implementado em 25 de maio de 2018. Em um segundo momento, a pesquisa analisa e problematiza as disposições sobre o consentimento necessário para o tratamento de dados pessoais de crianças contidas na LGPD brasileira, que embora já esteja em vigor ainda não passou pelo crivo do tempo, cotejando-a com a regulamentação europeia e destacando os pontos de aproximação e de distanciamento.

## 2 O RECURSO AO DIREITO COMPARADO

A busca por respostas nem sempre precisa trilhar apenas um caminho. Por vezes, um sobrevoo que permita ao pesquisador um vislumbre das vários vias que podem leva-lo ao seu objetivo possa contribuir não só para se chegar efetivamente ao objetivo perseguido, mas também a

[2] O texto tomará o significante "tratamento" com o significado a ele atribuído pela LGPD: "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

construir um caminho mais seguro e sólido. Não a toa Ícaro, construtor do labirinto do Minotauro, valeu-se de asas para dele escapar, em sobrevoo. Tal como Ícaro, podemos observar os caminhos de cima, em panorama, pelas lentes do direito comparado.

Para o pesquisador ou para Ícaro, o risco será o mesmo: desconhecer as características de seu instrumento pode levar ao fracasso. Para Ícaro, ignorar que as asas eram de cera o levou a cair no mar Egeu e nele se afogar; para o jurista, ignorar o que é o direito comparado ou como funciona pode leva-lo a uma conclusão falaciosa. Daí a necessidade de se prestar contas ao leitor, apresentando antes as premissas de direito comparado que serão adotadas na presente pesquisa.

O primeiro múnus a ser arrostado é o de se afastar desde logo do tentador, posto que fácil, mas descompromissado caminho de tomar a o direito comparado como o simples cotejo entre o direito positivo de diferentes países, importando institutos e figuras de outros países sem as necessárias adaptações. Tal agir acarreta equívocos que posteriormente acabam entregando ao jurista mais dificuldades que esclarecimentos[3].

Para evitar anacronismos quando da leitura do direito estrangeiro, a pesquisa jurídica que pretenda realizar a comparação entre sistemas jurídicos não pode se limitar a cotejar enunciados normativos, seja pela necessidade de sua interpretação sistemática seja por somente revelar uma das faces do direito, notadamente o direito positivo, que nem sempre corresponde àquele efetivamente aplicado (*case law*): o jurista alemão que proceder a leitura do Código Civil brasileiro poderia afirmar,

[3] Tome-se por exemplo a "importação" da guarda compartilhada no Brasil, que embora tenha incorporado ao nosso sistema figura jurídica desenvolvida em outros países, não se atentou das complexidades que decorreriam das peculiaridades de cada sistema jurídico. No específico caso da guarda compartilhada, sua instituição em países como a Inglaterra e a França se justifica pois quando do rompimento do vínculo conjugal, é dado ao juiz atribuir a apenas *um* dos pais, com exclusividade, o exercício da autoridade parental sobre os filhos. Assim, nestes ordenamentos serve a guarda compartilhada para equiparar tal exercício. O direito brasileiro, porém, não admite a cisão nem mesmo do exercício da autoridade familiar (art. 1.634, Código Civil), o que trouxe enormes dificuldades à doutrina para elucidar qual o conteúdo desta figura no direito brasileiro, chegando a receber o rótulo de "instituto vazio, inútil e perigoso" (SIMÃO, 2016, p. 253).

com convicção, que os bens adquiridos onerosamente por pessoas que se casaram após os 70 anos de idade são todos bens particulares, posto que o artigo 1.641 lhes impõem o regime da separação de bens. Ainda que apenas repise o direito positivo, a afirmação estaria equivocada, pois ignora a existência da súmula 377 do Supremo Tribunal Federal[4], amplamente aplicada pela jurisprudência, que torna tais bens comunicáveis entre os cônjuges.

A comparação, portanto, não pode se restringir aos enunciados de direito positivo, pois, como adverte Pierre Legrand, "o passo mais importante que o comparatista deve dar a esse respeito é o de rejeitar o ponto de vista positivista e hipomnésico segundo o qual a ideia de 'Direito' estaria limitada somente aos textos que são normativamente imperativos" (LEGRAND, 2018, p. 64), visão compartilhada por André Luiz Arnt Ramos, para quem "ao contrário do que sugerem os diversos capítulos de trabalhos dedicados ao 'direito comparado', a mirada do estudioso deve buscar não a expressão formal dos textos normativos cotejados, mas a realidade concreta na qual seu conteúdo normativo se faz valer" (RAMOS, 2018, p. 30). Para tanto, cumpre ao comparatista, de acordo com o desiderato por ele perseguido, valer-se também de fontes que revelam o direito enquanto realidade complexa, sobretudo a doutrina, a quem compete "explicar o direito positivado, esclarecendo o significado dos textos" (MARTINS-COSTA, 2014, p. 14), e a jurisprudência, responsável pela concreção do direito positivo por meio da solução de casos concretos.

Ciente de tais perigos, emerge a dúvida de como levar a efeito a pesquisa em direito comparado, pois além dos riscos já destacados, existe ainda uma pluralidade tanto de objetivos quanto de metodologias de direito comparado.

Em breve reconstrução histórica sobre a disciplina, Rodolfo Sacco narra que desde a metade do século XIX e por longo tempo, o objetivo do direito comparado era o de colocar em evidência os pontos comuns

[4] BRASIL. Supremo Tribunal Federal. **Súmula nº 377**: "No regime de separação legal de bens, comunicam-se os adquiridos na constância do casamento".

ou ao menos pontos de contato entre os diferentes ordenamentos jurídicos, buscando assim uma base unitária à "vida jurídica universal". Em que pese essa busca pelo núcleo comum do direito ser ainda hoje legítima (SACCO, 2001, p. 29), eleger os pontos comuns como objeto de estudo do direito comparado não resiste as críticas de Pierre Legrand. Partindo da premissa de que a comparação pressupõe a alteridade no reconhecimento do outro direito, como algo diferente do direito nacional, o jurista "necessariamente inscreve o estudo do Direito estrangeiro numa perspectiva diferencial, isto é, sua pesquisa se articula, inevitavelmente, em torno da diferença entre os direitos" (LEGRAND, 2018, p. 49), de modo que o elemento cerne da comparação invariavelmente será as distinções, não as semelhanças entre os sistemas. Se de um lado tais objetivos não parecem excludentes entre si, de outro pouco contribuem para o objetivo da presente pesquisa, nomeadamente de analisar como se o consentimento para o tratamento de dados pessoais de menores.

A partir do encerramento dos conflitos que dividiram a Europa durante a primeira guerra mundial, o interesse dos comparatistas muda de foco, atraídos pelo recém (re)despertado ideal de unificação do direito[5], objetivo que continua vivo e latente principalmente na espacialidade da Comunidade Europeia, em que foram empreendidos diversos projetos de unificação do direito privado, seja por meio de projetos de *soft law,* como os Princípios do Direito Europeu dos Contratos (PDEC), Princípios UNIDROIT e mais recentemente o DCFR - *Draft Common Frame os Reference* (Projeto de Quadro Comum de Referência), como regulamentos com *status* legislativo e cogente, como o Regulamento Geral sobre Proteção de Dados (RGPD), aprovado em 2016 e em vigor desde 25 de maio de 2018.

Em que pese a vitalidade de tal objetivo, Rodolfo Sacco aponta que a partir da segunda metade do século XX o direito comparado passa a ser

[5] "Em 1924 foi fundada a Academia internacional de direito comparado, que floresceu e que permanece atuante. Em seu estatuto consta como sua finalidade precípua a uniformização do direito. Em 1928 nascia em Roma, o UNIDROIT (*Institut international pour l'unification du droit privé*, integrante há cerca de algumas décadas da ONU), que promove a uniformização do direito privado" (SACCO, Rodolfo. **Introdução ao direito comparado**. Tradução Vera Jacob de Fradera. São Paulo: Revista dos Tribunais, 2001, p. 31).

defendido enquanto ciência, o que justifica nova alteração de seu objetivo, agora centrado no "melhor conhecimento dos modelos jurídicos" e no "estudo comparativo dos sistemas jurídicos" (SACCO, 2001, p. 36-37). Parece esta a compreensão teleológica do direito comparado que melhor serve ao objetivo desta pesquisa, porém, cumpre ainda aclarar a escolha da metodologia de direito comparado eleita para instrumentalizar tal empreitada[6]. A escolha dentre os diversos métodos apresentados pela doutrina não depende de uma classificação hierarquizada que sobreponha qualitativamente uma metodologia sobre a outra, mas perpassa pela compreensão de que podem ser metaforicamente pensadas como instrumentos, ferramentas que devem ser escolhidas de acordo com o a função que desempenham. Noutras palavras, a opção pelo método se dá em razão do objetivo da pesquisa e o que ela pretende responder.

É nesta perspectiva que o método funcional de comparação se apresenta como mais adequado ao objetivo ora buscado, notadamente de analisar como outros sistemas jurídicos respondem a necessidade de consentimento para o tratamento de dados de crianças ou adolescentes. Trata-se de método que admite que regras e conceitos jurídicos podem ser diferentes entre os sistemas, mas que a maior parte deles resolve problemas de um modo similar. A ideia por trás do método funcional portanto é comparar as respostas dadas a um mesmo problema.

Note-se que este método não permite a realização de uma macrocomparação, aqui tomada como aquela empreendida sobre elementos fundamentais ou estruturantes de cada *sistema* jurídico, como "as formas de revelação das normas que compõe o sistema (fontes de direito), a estrutura das próprias normas, os modos de constituição e funcionamento dos órgãos de aplicação do Direito, os métodos por que os juristas operam o 'achamento' do Direito'", etc. Pelo contrário, a metodologia

[6] A escolha e apresentação do método eleito serve, para além de prestar contas ao leitor, para superar a crítica de Mark Van Hoecke, para quem o "Direito Comparado tem sido reiteradamente criticado por não seguir qualquer método para a pesquisa comparativa. De fato, o comparatista frequentemente age como um turista que visita uma cidade estrangeira e vê que as coisas são diferentes, e em alguma medida também semelhantes, comparadas a sua cidade natal" (HOECKE, 2015, p. 1).

funcional é inerente a um grau de microcomparação, em que "o ponto de referência de toda e qualquer comparação há de ser a função desempenhada pelos institutos ou normas a comparar", grau este próprio ao objetivo de "interrogar como é que esse Direito resolve o problema jurídico cuja solução no nosso Direito pretendemos comparar" (DUARTE, 2006, p. 777-780).

A exposição destas premissas se faz salutar tanto para manter os próprios autores distantes do sol quanto para prestar constas ao leitores, sobretudo quanto a construção do próximo capítulo, cujo objetivo é justamente buscar as respostas dada por outros ordenamentos jurídicos, e aqui o recorte se deu especificamente pela escolha da espacialidade europeia, a um problema também brasileiro: o caminho eleito para submeter o tratamento de dados pessoais de crianças e adolescentes ao seu consentimento.

## 3 O CONSENTIMENTO PARA O TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS NA ESPACIALIDADE EUROPEIA

A proteção de dados pessoais é um dos temas que bem ilustra o ainda pulsante objetivo de unificação do direito na espacialidade da Comunidade Europeia (CE), destacado por Rodolfo Sacco e citado no capítulo anterior. O objetivo já era perseguido pelo menos desde 1981, quando o Conselho da Europa aprovou a Convenção 108, cujo objeto era – já no acender das luzes da década de oitenta – a proteção dos dados pessoais face o tratamento automatizado de dados[7], e desde 2016 ganhou especial destaque pela aprovação pelo Parlamento Europeu do Regulamento nº 2016/679 (Regulamento Geral sobre a Proteção de Dados – RGPD), em vigor desde 25 de maio de 2018.

[7] A redação de seu artigo 1º sintetiza seu objeto: "A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»)".

O regulamento se presta à unificação da matéria nos Estados membros, aos quais é diretamente aplicável, sem a necessidade de incorporação para o ordenamento interno de cada país. A unificação da matéria se revela pelo RGPD eleger uma principiologia comum ao tratamento de dados pessoais, norteada sobretudo pela (a) licitude, (b) lealdade, e (c) transparência[8], mas também ao atribuir direitos subjetivos a todos os residentes no território da União Europeia, como, à guisa de exemplo, o direito à informação/confirmação do tratamento de seus dados pessoais (art. 15, 1), à retificação dos dados pessoais (art. 16) e mesmo o controvertido direito ao esquecimento, por meio do apagamento de seus dados pessoais em determinadas situações (art. 17). A unificação, portanto, se revela pela auto aplicabilidade do RGPD aos 28 Estados membros.

A unificação porém não foi totalitária, deixando espaços de regulamentação aos Estados membros para que possam em certa medida adaptar o regramento europeu às peculiaridades locais, a exemplo do artigo 8º, 1, do RGPD que permite a cada Estado membro decidir, dentro do limite imposto pelo RGPD, a partir de qual idade o menor poderá consentir autônoma e validamente com o tratamento de seus dados pessoais.

Importa, ao presente texto, apurar de que forma a Comunidade Europeia, por meio do Regulamento Geral de Proteção de Dados, decidiu normatizar a proteção e o tratamento de dados pessoais de crianças, e mais especificamente, submeter o tratamento de tais dados ao consentimento das crianças ou de seus responsáveis. O ponto de partida dessa análise não pode ser outro que não reconhecer que o RGPD se aplica indistintamente a adultos e a crianças. Noutras palavras, o regramento que lhe dá corpo é, regra geral, igualmente aplicável à proteção de todos, sejam pessoas maiores ou menores de idade, sem distinção, do mesmo modo como já se dava o tratamento pelos diplomas anteriores, como a Diretiva 95/46 da Comunidade.

[8] Todos enunciados no artigo 5º, 1, do Regulamento Geral de Proteção de Dados.

Ao tempo da Diretiva 95/46, porém, a União Europeia ainda não havia promulgado a sua Carta dos Direitos Fundamentais, de 07 de dezembro de 2000, que na linha das constituições nacionais passou a impor em seu artigo 24º que todos os atos praticados por entidades públicas passassem a levar em conta o superior interesse da criança[9].

Para dar concreção a tal dispositivo, o RGPD inovou ao reconhecer a necessidade de um tratamento diferenciado que tenha como critério de discriminação o fator etário, ao menos em relação ao tratamento de algumas matérias, em razão da vulnerabilidade de crianças, que reconhecidamente são sujeitos merecedores de uma tutela jurídica mais protetiva, tal como se extrai do "considerando" nº 38 que compõe o seu preambulo do RGPD:

> "(38) As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança".

Do mesmo modo, o "considerando" nº 75, ao expressar os riscos aos direitos e liberdades individuais decorrentes do tratamento de dados, expressamente segrega a criança dos demais sujeitos ao aponta-las como

[9] **"Artigo 24º**. *Direitos das crianças.*
1. As crianças têm direito à proteção e aos cuidados necessários ao seu bem-estar. Podem exprimir livremente a sua opinião, que será tomada em consideração nos assuntos que lhes digam respeito, em função da sua idade e maturidade. 2. Todos os atos relativos às crianças, quer praticados por entidades públicas, quer por instituições privadas, terão primacialmente em conta o interesse superior da criança. 3. Todas as crianças têm o direito de manter regularmente relações pessoais e contatos diretos com ambos os progenitores, exceto se isso for contrário aos seus interesses".

pessoas vulneráveis, merecedoras, portanto, de grau de consideração reforçado quando seus dados pessoais estiverem em jogo.

Estribado em tais fundamentos, o RGPD optou por manter a aplicabilidade geral de suas regras tanto aos adultos quanto às crianças, agregando, porém, regras especiais destinadas exclusivamente à proteção de dados pessoais titularizados por crianças (MACENAITE e KOSTA, 2017, 148), e em especial quanto ao consentimento de menores de idade para o tratamento de seus dados.

O regramento geral sobre o consentimento é dado pelo artigo 6º do diploma, que traça como preceito geral que o tratamento de dados pessoais só é lícito quando o titular tiver com ele consentido, para uma ou mais finalidades específicas (art. 6º, 1, a). Para além desta cláusula geral, o artigo 6º admite ainda a licitude do tratamento de dados independentemente do consentimento de seu titular em hipóteses restritas, como aquelas em que o tratamento for necessário à execução de contrato ou cumprimento de obrigação do titular dos dados, para a defesa de interesses vitais do titular ou de outra pessoa natural, para o exercício de funções de interesse público ou quando o tratamento for necessário para efeito de interesses legítimos perseguidos pelo responsável pelo tratamento ou por terceiros, exceto quando prevaleçam direitos fundamentais dos titulares. Ainda nesta linha, o artigo 7º atribui ao responsável pelo tratamento dos dados o ônus de provas que teve o consentimento dos titulares dos dados pessoais, e ainda que acaso a cláusula de consentimento esteja inserida em texto sobre outras questões, seja redigida de forma destacada, de modo a permitir a clara distinção entre seu texto e o restante do documento.

Estas disposições aplicam-se indistintamente a todas as pessoas, independentemente de sua idade. Portanto, aplicam-se a adultos e também à crianças ou adolescentes.

O regime jurídico especifico para o tratamento de dados pessoais de crianças encontra-se no artigo 8º do RGPD[10], primeira das regras es-

[10] Art. 8º. Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação.

peciais do Regulamento destinadas especificamente a uma tutela protetiva reforçada para crianças, compreendidas na espacialidade europeia como qualquer pessoa com menos de dezoito anos de idade[11].

O citado dispositivo trata especificamente da necessidade de consentimento[12] da criança para o tratamento de seus dados pessoais. Para sua compreensão, cumpre delimitar seu antecedente normativo, em especial as hipóteses em que tal consentimento é exigido e em que é dispensado, para então perquirir a quem é atribuída a legitimação para consentir: se é atribuída de forma autônoma a própria criança ou aos seus responsáveis.

Ao excepcionar a regra geral sobre o consentimento expressa nos artigos 6º e 7º, é importante compreender que o art. 8º tem um campo de aplicação restrito, ou seja, não tem como campo de incidência todo e qualquer consentimento de menores para o tratamento de dados pessoais, mas apenas uma espacialidade delimitada. Esta moldura restrita é extraída do próprio *caput,* que define seu campo de incidência apenas às

1. Quando for aplicável o artigo 6.º, n.º 1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança; Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos.
2. Nesses casos, o responsável pelo tratamento envida todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível.
3. O disposto no n.º 1 não afeta o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a uma criança.

11 A Convenção das Nações Unidas sobre o Direito das Crianças considera como tal toda pessoa humana com menos de 18 anos de idade, afastando-se, portanto, da distinção usada pelo direito brasileiro entre criança (até 12 anos de idade) e adolescente (entre 12 e 18 anos de idade). O RGPD claramente adotou o critério utilizado pela Convenção das Nações Unidas.

12 O RGPD define consentimento como "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento" (art. 4º, 11).

"condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade de informação".

É esta parte final do *caput*, "em relação aos serviços da sociedade de informação" que evidencia o recorte realizado pelo legislador europeu, de modo que, em não se tratando de "serviços da sociedade de informação" (SSI), crianças e adultos se submetem igualmente às regras do artigo 6º, ao passo que para estes serviços incidirá a regra especial.

Antes de adentrar a especificamente à análise do artigo 8º, emerge a primeira dúvida a ser dirimida. As regras do artigo 6º continuam aplicáveis quando se tratar de SSI prestados à crianças? A resposta não é dada por fonte normativa, sendo necessário recorrer a outras fontes, e aqui a evidência de como o direito comparado não pode se limitar ao mero cotejo de fontes normativas.

A hermenêutica proposta pelo *Center for Information Policy Leadership* (CIPL) é de que o sendo o artigo 6º mais amplo que o artigo 8º, seus dispositivos são aplicáveis de forma subsidiária, sempre que não houver conflito com as regras especiais. Assim, por exemplo, seria possível aplicar a regra de dispensa do consentimento da criança quando o tratamento de dados for necessário para dar efeito aos interesses legítimos do responsável pelo tratamento e não houver violação aos interesses ou direitos fundamentais do titular (art. 6, 1., f), ressalvando, contudo, que o teste de ponderação de interesses deve ser realizado de forma mais cautelosa quando o titular for uma criança (CIPL, 2018, p. 6)[13].

Pragmaticamente, o exemplo trazido pelo CIPL é o da criança faz o download e uso de um *app*, que é sempre acompanhado de mecanismos identificadores do modo de uso daquele aplicativo, e o tratamento dos dados referentes a este modo de uso especificamente para apri-

[13] Em reforço a esta posição, é possível defender que ela decorre do próprio artigo 8º, 1, pois ao eleger como seu suporte fático exatamente aquele do art. 6º, 1, a, ou seja, as hipóteses em que o tratamento de dados pessoais exige o consentimento do titular, a contrário senso, é legítima a conclusão de que as demais hipóteses (alíneas) do art. 6º, 1, não teriam sua aplicabilidade afastada pela regra especial protetiva.

morar as funcionalidades do *app* representaria um interesse legítimo do controlador dos dados que permitiria, pelo teste de balanceamento de interesses do art. 6, 1., f, a dispensa do consentimento do titular dos dados.

Retomando a análise do artigo oitavo, a parte final de seu *caput* delimita o seu campo de incidência aos serviços da sociedade de informação. O significado atribuído aos SSI não é apresentado pelo RGPD, mas foi definido pela Diretiva 2015/1531 do Parlamento Europeu, que em seu artigo 1º, 1, alínea "b" apresenta a definição nos seguintes termos: "«serviço» significa qualquer serviço da sociedade da informação, isto é, qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrônica e mediante pedido individual de um destinatário de serviços"[14].

A redação impõe um desafio interpretativo quanto a exigência de "remuneração". À primeira vista, o interprete é levado a crer que apenas os serviços onerosos estariam submetidos à regra do art. 8º, ou seja, aqueles serviços em que o usuário apenas teria acesso mediante pagamento, o que restringiria enormemente sua aplicação, já que a maior parte dos serviços oferecidos na sociedade de informação (internet) não exigem pagamento, como são exemplos as redes sociais, jogos online, sites provedores de conteúdo, servidores de e-mail ou de mensagens, dentre tantos outros. Mas não é essa a interpretação dada ao dispositivo pela *case law* europeia[15], como deixam claro MACENAITE e KOSTA (2017, 170-171).

---

[14] As definições das expressões "à distância", "por via eletrônica" e "mediante pedido individual de um destinatário de serviços" são também apresentadas pela alínea "b", nos seguintes termos: "i) **«à distância»**: um serviço prestado sem que as partes estejam simultaneamente presentes; ii) **«por via eletrônica»**: um serviço enviado desde a origem e recebido no destino através de instrumentos eletrônicos de processamento (incluindo a compressão digital) e de armazenamento de dados, que é inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos; e iii) **«mediante pedido individual de um destinatário de serviços»**: um serviço fornecido por transmissão de dados mediante pedido individual".

[15] Destaca-se uma vez mais, neste ponto, a importância de não limitar o direito comparado ao texto normativo, que poderia levar o interprete a conclusão falsa, e ainda a especial utilida-

Em diversos casos o Tribunal de Justiça da União Europeia conferiu interpretação extensiva a tal disposição, admitindo sua incidência a serviços que não exigiam pagamento direto. Em Bélgica vs. Humbol[16] a Corte assentou que "a característica essencial da remuneração (...) está no fato de haver qualquer contraprestação pelo serviço", o que permitiu desvincular o caráter remuneratório do pagamento de um valor ou preço, podendo se configurar pela satisfação de qualquer interesse do provedor do serviço. Em Bond van Adverteerders vs. Netherlands[17], a Corte decidiu que "a remuneração não precisa vir do tomador do serviço, sendo suficiente (para o caráter remuneratório) que venha de outra pessoa, como um anunciante". Ou seja, o só fato de o usuário ser submetido à publicidade já transforma a prestação em um serviço remunerado.

Em razão desta interpretação extensiva dada pelo Tribunal de Justiça da União Europeia ao caráter remuneratório do serviço, as autoras apontam que o consentimento exigido pelo art. 8º do RGPD é potencialmente aplicável a uma vasta gama de serviços online, já que a maior parte deles condiciona o uso ao fornecimento dos dados pessoais do usuário ao prestador, e mesmo aqueles serviços que não exigem a cessão dos dados pelo usuário podem obtê-los de forma passiva por meio da impressão digital do navegador ou de cookies (MACENAITE e KOSTA, 2017, 171), satisfazendo assim um interesse do provedor que pode ser considerado como contraprestação. Na mesma linha, para o CIPL a interpretação quanto ao requisito da remuneração "deve ser feita na acepção ampla do termo, na linha da noção aberta de serviço adotada pela legislação europeia, de modo que qualquer serviço que suporte um negócio é considerado por ela abrangido"[18] (CIPL, 2018, p. 8).

---

de do método funcional para buscar a solução adotada por outros ordenamentos para um problema comum, sem restrição de qualquer ordem quanto à fonte do direito.

16 Belgian State v René Humbel and Marie-Thérèse Edel (Belgium v Humbel) [1988] ECR 5365.

17 Bond van Adverteerders v Netherlands State [1988] ECR 2085.

18 Tradução livre do original: "In general, the approach to this requirement has been to take a broad view of the term, in line with the broad notion of services in EU law, so that any service which supports a business is regarded as covered".

Ainda na configuração do antecedente normativo, para além do enquadramento como um serviço da sociedade de informação, o suporte fático do art. 8º, 1, exige ainda que tal serviço seja *oferecido diretamente à crianças*, o que arrosta novo desafio interpretativo, ainda mais complexo. À guisa de exemplo, a proposta interpretativa do *Center for Information Policy Leadership* é de que a expressão "oferecido diretamente à crianças" não significa "disponível para crianças" ou "oferecido indiretamente para crianças" (CIPL, 2018, p. 9), de modo que apenas os serviços que tomem como público alvo especificamente as crianças estariam submetidos à regra do artigo oitavo.

O problema daí derivado é que a estrutura do regulamento não lograria cumprir sua função. Embora a teleologia, a função perseguida pelo artigo oitavo seja claramente a de criar um regime de proteção especial para os dados pessoais de crianças, especificamente por reforçar a necessidade de um consentimento reforçado quando qualquer ISS promova o tratamento de tais dados, ao limitar a aplicabilidade de tais dispositivo apenas aos serviços especificamente dirigidos às crianças, a estrutura da norma infirma sua função ao se constatar que a maior parte dos ISS utilizados por crianças não são especificamente destinados ao público infantil, mas sim a um público amplo, sem restrição de idade ou ao menos não especificamente destinado às crianças.

Conforme MACENAITE e KOSTA (2017, 172), diversos estudos realizados em âmbito europeu e norte americano "reportam que da ampla gama de sites que as crianças usam hoje em dia, os mais populares (como YouTube, Facebook e Google, para citar apenas alguns) não são direcionados especificamente às crianças"[19]. Nesta medida, a norma europeia destinada a proteção dos dados pessoais das crianças não se aplicaria a maior parte dos serviços por elas acessados e utilizados.

[19] Tradução livre do original: "Various studies in Europe and North America report that from a broad range of websites that children use nowadays, the most popular websites (such as YouTube, Facebook and Google search to name just a few) are often not directed specifically to children".

Em que pese o texto comporte interpretações menos restritivas, as Orientações adotadas pela Comissão Europeia, especificamente da WP29, parecem confirmar a tendência restritiva ao enunciar a seguinte diretriz quanto a interpretação do artigo 8º:

> "A inclusão da expressão 'oferecido diretamente à criança' indica que o artigo 8 é aplicável a alguns, e não a todos os serviços da sociedade de informação. Sobre isso, se um prestador de serviço da sociedade de informação deixar claro aos potenciais usuários que está oferecendo o serviço apenas a pessoas com 18 anos ou mais, e isso não for contradito por outras evidências (como o conteúdo do site ou planos de marketing), então o serviço não será considerado "oferecido diretamente à crianças" e o artigo 8 não se aplicará"[20].

Tal orientação pode levar a subtração de grande campo de incidência na norma protetiva, pois ao fim e ao cabo permitiria ao prestador do serviço não se submeter à aplicação das regras protetivas do artigo 8º se incluir em seus termos de uso que sua utilização não se destina a menores de 16 anos.

Ainda não é clara qual será a interpretação dada à expressão "oferecido diretamente à criança", mormente considerando que a única orientação sobre o tema até agora adotada pela Comissão Europeia é a supra transcrita, que não trata dos serviços oferecidos a públicos mistos ou mesmos ao público em geral, como as mídias sociais.

Dissecado o antecedente normativo (suporte fático) do artigo oitavo do RGPD, cumpre analisar seu consequente normativo. Segundo a WP29 (2017, p. 23), "o artigo 8 introduz obrigações adicionais para asse-

[20] Tradução livre do original: "the inclusion of the wording 'offered directly to a child' indicates that Article 8 is intended to apply to some, not all information society services. In this respect, if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply" (WP29, 2017, p. 25). Disponível em https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

gurar um nível reforçado de proteção de dados de crianças em relação aos serviços da sociedade da informação"[21]. No artigo 8º, 1, esta obrigação adicional diz respeito ao consentimento para o tratamento dos dados pessoais.

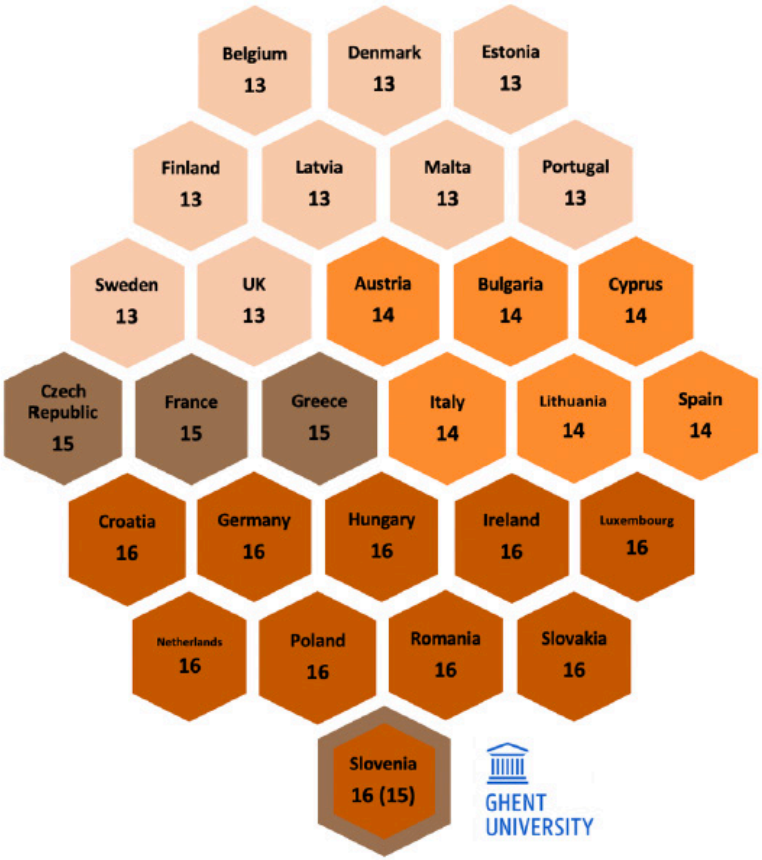
Nas hipóteses em que a regra geral do RGPD exige o consentimento do titular dos dados (art. 6º, 1, a), a licitude do tratamento de dados de crianças dependerá de um critério etário para a eleição do sujeito competente para manifestar o imprescindível consentimento.

A primeira hipótese compreende crianças que tenham 16 anos de idade completos, quando será necessário o seu próprio consentimento para o tratamento dos dados pessoais, prestado de forma autônoma. O Regulamento, porém, permite que os países reduzam esta idade em seu direito interno, desde que ela não seja inferior a 13 anos[22]. Eis, aqui, um espaço de autonomia deixado pelo RGPD aos países membros e que representa importante reconhecimento da autonomia de crianças, mesmo antes de atingirem a capacidade civil.

Ingrida Milkaite e Eva Lievens, pesquisadoras da Universidade de Ghent, realizaram interessante mapeamento da forma como os países membros da União Europeia regulamentaram a questão, apontando o limite etário a partir do qual é a própria criança quem deverá consentir com o tratamento de seus dados (MILKAITE; LIEVENS, 2019, p. 2):

21 Tradução livre do original: "Article 8 introduces additional obligations to ensure an enhanced level of data protection of children in relation to information society services" (WP29, 2017, p. 23).

22 Art. 8º, 1: "(...) Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos".




Conforme se extrai da figura acima, dos 27 países membros que regulamentaram o tema internamente, nove (33,33%) adotaram a idade mínima autorizada pelo RGPD, seis (22,22%) reduziram a idade para 14 anos, apenas três (11,11%) elegeram a idade de 15 anos e nove (33,33%) mantiveram a idade prevista no Regulamento, notadamente de 16 anos. Até a conclusão do estudo, apenas a Eslovênia ainda não havia implementado legislação interna sobre o tema: seu projeto previa a idade de 15 anos, mas como não estava vigente, aplica-se, naquele país, os 16 anos previstos no RGPD.

Se um lado a atribuição de capacidade para consentir à criança que ainda não atingiu a capacidade legal plena é importante instrumento de

seu desenvolvimento e autonomia, de outro exige do responsável pelo tratamento de dados uma maior atenção nas informações prestadas às crianças, utilizando sempre linguagem clara e simples (art. 12, 1). A orientação adotada pela Comissão Europeia é de que "para a obtenção do consentimento informado de crianças, o controlador deve explicar em linguagem clara e simples para elas como pretende processar os dados"[23] (WP29, 2017, p. 24).

A segunda hipótese compreende crianças que não tenham atingido 16 anos ou a idade mínima adotada pelo direito interno, quanto o sujeito competente para consentir com o tratamento de dados será o responsável legal pela criança, definido de acordo com a regra de direito de família de cada país. Nesta hipótese, compete ao responsável pelo tratamento dos dados imprimir esforços para verificar se este consentimento foi efetivamente manifestado pela pessoa responsável (art. 8º, 2), mas o RGDP não especifica o modo pelo qual cumprirá tal mister. Para solver a questão, a WP29 encaminhou a orientação com um método interessante (WP29, 2017, p. 26):

> "O que é razoável, tanto em termos de verificação da suficiência da idade do usuário para dar o próprio consentimento, quando para verificar se a pessoa que está consentindo por uma criança é a responsável por ela, pode depender dos riscos inerentes ao processamento e também da tecnologia disponível. Em casos de baixo risco, a verificação da responsabilidade parental por e-mail pode ser suficiente. Em casos de alto risco, pode ser apropriado solicitar mais provas, de modo que o controlador possa verificar e reter a informação exigida pelo artigo 7, 1, do RGPD"[24].

---

[23] Tradução livre do original: "as mentioned in section 3.1. on informed consent, the information shall be understandable to the audience addressed by the controller, paying particular attention to the position of children. In order to obtain "informed consent" from a child, the controller must explain in language that is clear and plain for children how it intends to process the data it collects".

[24] Tradução livre do original: "what is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases,

A orientação apresenta ainda um exemplo de como se daria essa verificação:

> "Uma plataforma de jogos online quer se certificar que consumidores menores de idade somente subscrevam seus serviços com o consentimento de seus pais ou guardiões. O controlador seguirá os seguintes passos:
>
> Passo 1: peça ao usuário para informar se tem menos ou mais de 16 anos (ou idade alternativa para o consentimento digital). Se o usuário declarar que é menor de idade para obter consentimento digital:
>
> Passo 2: o serviço informa à criança que um pai ou responsável precisa consentir ou autorizar o processamento antes que o serviço seja prestado à criança. O usuário é solicitado a informar o endereço de e-mail de um pai ou responsável.
>
> Etapa 3: o serviço entra em contato com o pai ou responsável e obtém seu consentimento via e-mail para processamento e toma as medidas razoáveis para confirmar que o adulto tem responsabilidade parental.
>
> Etapa 4: em caso de reclamação, a plataforma toma medidas adicionais para verificar a idade do assinante. Se a plataforma atendeu aos outros requisitos de consentimento, ela pode cumprir os critérios adicionais do Artigo 8 do GDPR seguindo estas etapas"[25].

verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR".

[25] Tradução livre do original: "An online gaming platform wants to make sure underage customers only subscribe to its services with the consent of their parents or guardians. The controller follows these steps: Step 1: ask the user to state whether they are under or over the age of 16 (or alternative age of digital consent). If the user states that they are under the age of digital consent: Step 2: service informs the child that a parent or guardian needs to consent or authorize the processing before the service is provided to the child. The user is requested to disclose the email address of a parent or guardian. Step 3: service contacts the parent or guardian and obtains their consent via email for processing and take reasonable steps to confirm that the adult has parental responsibility. Step 4: in case of complaints, the platform takes additional steps to verify the age of the subscriber. If the platform has met the other consent requirements, the platform can comply with the additional criteria of Article 8 GDPR by following these steps".

São estes, à luz da prática europeia, os "esforços razoáveis" que devem ser empreendidos pelo responsável pelo tratamento de dados para a verificação do consentimento em situações que envolvam os dados pessoais de crianças.

## 4 O CONSENTIMENTO PARA O TRATAMENTO DOS DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES NA LGPD BRASILEIRA

Ao tempo da conclusão da presente pesquisa, a Lei Geral de Proteção de Dados (LGPR - Lei 13.709/2018) acabara de entrar em vigor, especificamente em 18/09/2020. Não se trata da primeira legislação voltada a proteção de dados pessoais no Brasil, que já tal matéria havia sido objeto de regulação anterior pelo Marco Civil da Internet (Lei 12.965/2014, art. 3º, III). Ainda que o Marco Civil da Internet faça referência aos direitos de crianças e adolescentes, o faz apenas de forma tímida e apenas em suas disposições legais[26], sem criar efetivamente um regime jurídico diferenciado, de modo que, seguindo o histórico das regulamentações na espacialidade europeia, a LGPD encontra pioneirismo ao compreender regras especiais aplicáveis especificamente para a proteção de dados pessoais de menores de idade em razão de sua vulnerabilidade.

Tal regramento está compreendido no artigo 14 da LGPD[27], que já me seu caput apresenta a submissão e funcionalização do tratamento de

[26] Art. 29. Parágrafo único. "Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no caput, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes".

[27] Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o

dados pessoais de crianças e adolescentes ao "melhor interesse" destas, nos termos do citado artigo e da legislação pertinente[28].

Seguindo o modelo do RGPD europeu, a LGPD diferencia o consentimento exigido para o tratamento de dados pessoais de adultos e de crianças, estabelecendo um regime próprio para estas, mais protetivo. Tal como se fez no capítulo anterior em relação ao modelo europeu, o objetivo deste capítulo é especificamente a análise do regramento sobre este "consentimento específico", delimitando especificamente: (I) seu campo de incidência, ou seja, quando este consentimento especial é exigido; (II) seu sujeito (se a própria criança ou adolescente ou seu responsável legal) e (III) a forma como se dá a verificação deste consentimento.

A hipótese fática, ou o campo de incidência normativo para tal consentimento específico foi estabelecido de forma ampla pelo parágrafo primeiro do artigo 14, segundo o qual "o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal", extraindo-se da expressão "em destaque" um requisito de forma mais robusta, o da forma escrita (ainda que por um click[29]).

---

responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

28 Destaca-se, sobretudo, o art. 227 da Constituição Federal, a Convenção Internacional sobre os Direitos da Criança (Decreto 99.710/90) e o Estatuto da Criança e do Adolescente (Lei 8.069/90).

29 Art. 14 da Lei nº 17.709/2018.

Note-se, aqui, que a regulamentação brasileira não faz qualquer delimitação quanto ao tratamento de dados submetido à norma, ao contrário do RGPD que expressamente limita sua aplicação aos "serviços da sociedade de informação", assim considerados apenas aqueles prestados "mediante remuneração, à distância, por via eletrônica e mediante pedido individual de um destinatário de serviço"[30]. Esta previsão mais ampla afastará, por exemplo, a discussão travada na ambiência europeia sobre a necessidade de remuneração, não exigida pela legislação nacional, e ainda expande seu alcance ao tratamento de dados pessoais que não seja realizado por via eletrônica, mormente considerando que artigo 1º da LGPD é claro ao determinar a aplicação da lei ao "tratamento de dados pessoais, inclusive nos meios digitais", portanto, de forma não exclusiva.

Se este desenho aberto quanto às hipóteses em que se exige um consentimento específico para o tratamento de dados de crianças e adolescentes se revela de um lado hermeneuticamente mais simples por evitar as discussões quanto à natureza do serviço ofertado às crianças, de outro levanta tormentosa dúvida quanto aos sujeitos a quem se destina, sobretudo em razão da redação do texto.

O artigo 14 está inserido no Capítulo II, Seção III, da LGPD, cujo título é "do tratamento de dados pessoais de crianças e adolescentes", deixando claro portanto que se destina aos menores de idade em geral. Na mesma linha, o *caput* do artigo 14 estabelece que "o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse", levando à conclusão de que os sujeitos protegidos por esta regra são tanto às crianças, definidas pelo art. 2º do Estatuto da Criança e do Adolescente como "a pessoa até doze anos de idade incompletos", quanto aos adolescentes, definidos como "aquela entre doze e dezoito anos de idade".

A redação dada ao parágrafo primeiro do art. 14, porém, restringe seu campo de incidência apenas às crianças. Ao contrário do título da

[30] Conforme já citado, tal definição encontra-se na Diretiva 2015/1531 do Parlamento Europeu, artigo 1º, item 1, alínea "b".

Seção III e mesmo do *caput,* não faz referência aos adolescentes, mas apenas às crianças: *"§1º. O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal"*. Esta omissão autoriza dúvida razoável se o consentimento específico para o tratamento de dados pessoais é exigido apenas para os dados de menores de 12 anos de idade (crianças), ou também para os adolescentes entre 12 e 18 anos de idade.

Gustavo Tepedino e Chiara Teffé sustentam que a regra não se aplica aos adolescentes, que estariam, portanto, dotados de capacidade jurídica para consentir de forma autônoma para o tratamento dos próprios dados:

> "Ao não mencionar o adolescente, pessoa entre 12 e 18 anos de idade, o §1º do art. 14 não deixou claro se o consentimento manifestado diretamente pelo mesmo e sem assistência ou representação deveria ser considerado plenamente válido, como hipótese de capacidade especial, ou se simplesmente o legislador teria optado por não tratar do tema, por já existir legislação geral sobre a matéria no Código Civil. Ao que parece, o legislador pretendeu reconhecer a validade do consentimento expresso pelo adolescente. Tomando como base a realidade da utilização da internet e das mídias sociais, que têm entre seus usuários legiões de adolescentes, é possível que tenha optado por considerar jurídica hipótese fática dotada de ampla aceitação social" (TEPEDINO; TEFFÉ, 2020, p. 313).

Esta parece ser a interpretação majoritária, apresentada também por Vinicius Costa e Diego Gualda[31], e mesmo por Ana Carolina Brochado Teixeira e Anna Cristina de Carvalho Rettore, inobstante apresentem interessante crítica à escolha legislativa:

---

[31] "Ao estabelecer uma restrição, no sentido de exigir o consentimento específico, e em destaque, de pelo menos um dos pais ou do responsável legal, o legislador o fez especificamente para crianças, excluindo de tal regra os adolescentes. Não se trata, portanto, de uma lacuna, mas sim de um silêncio eloquente. Desse modo, não parece haver um requisito adicional para além do consentimento do adolescente e/ou da utilização de qualquer uma das bases legais dos artigos 7º ou 11 da LGPD para a hipótese de tratamento de dados" (COSTA; GUALDA, 2020, s/p).

> "Considerada a dificuldade geral de compreensão sobre o possível alcance e resultados do tratamento de dados, não parece correto que, para autorizar o uso de uma projeção tão expressiva da personalidade, como são os dados pessoais, os adolescentes devam poder fazê-lo desde sempre e prescindindo de qualquer acompanhamento" (TEIXEIRA; RETTORE, 2020, p. 525).

A relevância prática desta interpretação é a de que apenas para o tratamento de dados de pessoas menores de 12 anos seria necessário o *consentimento especial* previsto no art. 14, parágrafos primeiro a quinto, de modo que aos adolescentes entre 12 e 18 anos aplica-se o regime comum da LGPD, pelo qual o consentimento para o tratamento de dados pessoais pode se dar inclusive de forma tácita (art. 8º, *caput*).

Esta questão está umbilicalmente ligada também ao sujeito a quem é atribuída legitimação ou capacidade para consentir com o tratamento de dados pessoais. Quando a LGPD opta por exigir um consentimento específico apenas para tratamento de dados de menores de 12 anos, acaba por atribuir uma capacidade extraordinária aos adolescentes para manifestar sua vontade de forma autônoma e válida desde os 12 anos, já que pelo regime geral das incapacidades estabelecido pelo Código Civil, os adolescentes entre doze e dezesseis anos são absolutamente incapazes, e portanto o exercício de seus direitos ocorre por meio de representação de seus pais ou responsáveis, e mesmo entre os dezesseis e os dezoito anos são relativamente incapazes, dependendo assim da assistência de seus pais para a prática de atos jurídicos de forma válida. Neste ponto, a LGPD acaba por conferir maior autonomia aos adolescentes no campo do controle de seus dados pessoais, o que encontra-se harmônico a um reconhecimento de uma liberdade substancial progressiva para o desenvolvimento de sua personalidade, acompanhada de todos os riscos e responsabilidades inerentes.

Daqui já se extraem duas diferenças centrais entre o regime europeu e o brasileiro: aquele se aplica apenas a determinados serviços, qualificados como serviços da sociedade de informação, ao passo que este se

aplica a qualquer serviço; naquele, as regras especiais sobre o consentimento para o tratamento de dados pessoais aplica-se aos dados titularizados por menores de 16 anos de idade[32], ao passo que no Brasil a aplicação é mais restrita, atingindo apenas os menores de 12 anos de idade. Se nestes pontos os regimes se distanciam, em outros se aproximam: de forma muito próxima ao art. 8º, 2, do RGPD europeu, a LGPD impõe ao controlador dos dados a obrigação de "realizar todos os esforços razoáveis" para verificar se o consentimento foi mesmo dado pelo responsável pela criança, "considerando as tecnologias disponíveis" (art. 14, §5º).

Para além da delimitação mais ampla das hipóteses fáticas que atraem a exigência do *consentimento especial* para a coleta de dados pessoais de crianças, o art. 14, §3º o restringe ao permitir a coleta de dados pessoais de crianças sem o consentimento do responsável, desde que sejam usados especificamente para uma destas finalidades: (a) contatar os pais ou o responsável legal, hipótese em que tais dados poderão ser utilizados apenas uma vez e sem armazenamento, ou (b) para a proteção da criança, sendo esta última hipótese de não incidência dotada de tamanha generalidade que certamente dará causa a uma miríade de possíveis interpretações, o que não contribui para a efetividade da regra ou para a segurança jurídica. Em qualquer destas hipóteses, o controlador dos dados fica proibido de repassa-los a terceiros sem o consentimento específico.

Reconhecendo que os usuários em geral, e as crianças em especial estão mais propensas a preferir o benefício imediato obtido com o uso de um serviço online, como um jogo ou mídia social, em detrimento da perda futura do controle sobre suas informações (BUONI, 2019, p. 147), a LGPD adota interessante mecanismo no art. 14, §4º, ao proibir que os controladores de dados condicionem a participação de crianças a "jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade".

[32] Ressalte-se a possibilidade de redução de tal idade pelos países membros, desde que não inferior a 13 anos de idade.

A disposição é de extrema relevância, especialmente por impedir a criação de falsa sensação às crianças de que o acesso àquela utilidade é gratuito, quando em verdade é remunerado por meio de seus dados pessoais, hoje considerados "os principais recursos econômicos de nossa época" (FRAZÃO, 2020, p. 24). Ainda que se reconheça que tal regra pode desestimular a oferta destes serviços às crianças, salutar ter em mente que não lhes retira por completo a atratividade econômica, sobretudo considerando que podem ser remunerados de forma indireta, por exemplo por meio de publicidade, utilizada em alguns aplicativos como moeda de troca para o acesso ou para ganhar certas funcionalidades. Ao invés da criança remunerar o jogo ou a aplicação por meio de seus dados, remunera submetendo-se a um anúncio por determinado tempo. Esta estratégia não é obstada pela LGPD, embora a Resolução 163/2014 do Conselho dos Direitos da Criança e do Adolescente considere a publicidade infantil como prática abusiva.

Por derradeiro, o regime do art. 14 da LGPD também exige que o *consentimento específico* não seja apenas livre, informado e inequívoco, mas também instrumentalizado pelo acesso (público) à informação sobre os tipos de dados que serão coletados, a forma de sua utilização e os procedimentos pelos quais seu titular poderá acessá-los, retificá-los e mesmo excluídos[33].

## 5 CONSIDERAÇÕES FINAIS

A comparação entre o Regulamento Geral de Proteção de Dados da União Europeia e a Lei Geral de Proteção de Dados brasileira não deixa dúvida que esta foi inspirada naquela, em especial quanto ao regime de consentimento especial exigido para o tratamento de dados pessoais de crianças e adolescentes.

[33] "Art. 14. § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei".

Esta inspiração no entanto não implica em identidade de regimes, havendo substanciais distinções entre os regimentos, das quais destaca-se o campo de incidência mais restrito do RGPD, aplicável apenas ao SSI, ao passo que a LGPD tem aplicação mais ampla, atingindo inclusive a relações que não se desenvolvem por meios digitais. O recurso ao método funcional, porém, mostrou que o direito efetivamente aplicado, a *case law,* acaba por aproximar os regimes neste ponto, sobretudo em razão da interpretação extensiva conferida pelo Tribunal de Justiça da União Europeia à expressão serviço remunerado. Destaca-se também a diferença etária adotada por ambos os regimes na seleção dos sujeitos protegidos pela exigência de um consentimento especial. Enquanto o RGPD o aplica aos menores de 16 anos (ainda que permita aos países membros reduzir tal idade para até 13 anos, sendo tal idade limite adotada por um terço dos países), a LGPD, embora dotada de texto dúbio quanto a aplicação apenas para crianças ou para crianças e adolescentes, recebeu interpretação doutrinária majoritária no sentido de que alcança apenas as crianças, portanto, menores de 12 anos de idade, evidenciando novamente a imprescindibilidade do método funcional de direito comparado para se alcançar a solução efetivamente aplicada por cada ordenamento.

A similitude dos regimes fica evidente desde a principiologia seguida, norteada pela proteção da criança, até pela forma legislativa empregada para regulamentar o tema, notadamente pela inserção da temática em um único artigo, cuja regra central é a da submissão do tratamento dos dados pessoais de crianças ao consentimento, exprimido por seus responsáveis até determinada idade, e depois por elas próprias, de forma autônoma. Também se aproximam na dispensa de tal consentimento para a proteção da própria criança, na exigência do uso de linguagem clara e facilitada pelo operador para permitir que o consentimento seja de fato informado, e ainda pela atribuição de um dever ao operador dos dados para que empregue esforços razoáveis para verificar se o consentimento foi dado pela pessoa legitimada.

Resta agora aguardar a efetiva aplicação da LGPD no Brasil para apurar quais serão as dificuldades encontradas pelos juristas e de que

modo o recurso ao RGPD poderá auxiliar em sua superação, bem assim quais soluções serão criadas em solo nacional e que poderão também servir de instrumento hermenêutico para o direito europeu.

## REFERÊNCIAS

AFONSO, Ana Isabel. Apresentação: a relevância do DCFR. In: _____ (coord.) **Um Direito Europeu das Obrigações? A influência do DCFR**. Porto: UC Editora, 2015.

BIONI, Bruno. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019

BROCHADO TEIXEIRA, Ana Carolina; RETTORE, Anna Cristina de Carvalho. A autoridade parental e o tratamento de dados pessoais de crianças e adolescentes. In: FRAZÃO, Ana (et. al.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1ª ed. São Paulo: Revista dos Tribunais, 2019.

COSTA, Vinicius Venancio; GUALDA, Diego. **Tratamento de dados pessoais de menores no ramo da publicidade**. 2020. Disponível em https://www.machadomeyer.com.br/pt/inteligencia-juridica/publicacoes-ij/tecnologia/tr atamento-de-dados-pessoais-de-menores-no-ramo-da-publicidade.

DUARTE, Rui Pinto. **Uma Introdução ao Direito Comparado**. Separata da Revista 'O Direito IV'. Coimbra: Almedina, 2006.

FRAZÃO, Ana. Fundamentos da proteção de dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana (et. al.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** 1ª ed. São Paulo: Revista dos Tribunais, 2019.

HOECKE, Mark Van. Methodology of comparative legal research. **Law And Method**. Boom: Boom Juridische Uitgevers, 2015.

KOSTA, Eleni. MACENAITE, Milda. Consent for processing children's personal data in the EU: following in US footsteps? /**nformation & Communications Technology Law**, 26:2, 146-197, DOI: 10.1080/13600834.2017.1321096.

LEGRAND, Pierre. **Como ler o direito estrangeiro.** Tradução de Daniel Wunder Hachem. São Paulo: Editora Concorrente, 2018.

LIEVENS, Eva; MILKAITE, Ingrida. **Status quo regarding the child's article 8 GDPR age of consent for data processing acres EU.** Better Internet for Kids. Publicado em 20/12/2019.

MARTINS-COSTA, Judith. Autoridade e utilidade da doutrina: construção dos modelos doutrinários. In: _____ (coord.). **Modelos de Direito Privado.** 1ª ed. São Paulo: Marcial Pons, 2014.

RAMOS, André Luiz Arnt. **Responsabilidade por danos e segurança jurídica:** legislação e jurisdição nos contextos alemão e brasileiro. Curitiba: Juruá, 2018.

SACCO, Rodolfo. **Introdução ao direito comparado.** Tradução Vera Jacob de Fradera. São Paulo: Revista dos Tribunais, 2001.

SIMÃO, José Fernando. Guarda exercida pelos pais: um instituto vazio, inútil e perigoso. **Revista da Escola Superior de Advocacia da OAB-PR.** Curitiba, ano 1, número 1, agosto de 2016.

SMAHEL, D., MACHACKOVA, H., MASCHERONI, G., DEDKOVA, L., STAKSRUD, E., ÓLAFSSON, K., LIVINGSTONE, S., and HASEBRINK, U. **EU Kids Online 2020:** Survey results from 19 countries. EU Kids Online. 2020.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: FRAZÃO, Ana (et. al.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1ª ed. São Paulo: Revista dos Tribunais, 2019.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (Regulamento Geral sobre a Proteção de Dados).** 2016. Disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?qid=1559291025147&uri=-CELEX:320 16R0679#d1e1564-1-1.

THE ARTICLE 29 WORKING PARTY. **Guidelines on Consent under Regulation 2016/679**. Brussels, 2017.

VICENTE, Dário Moura. **Direito Comparado. V.2. Obrigações**. Coimbra: Almedina, 2017.

# Capítulo IV

# OS PROCEDIMENTOS INDICADOS PARA OBTENÇÃO DE VERIFICÁVEL CONSENTIMENTO PARENTAL: uma análise de direito comparado

*Bruna Ribeiro dos Santos Titoneli Berco*[1]

**SUMÁRIO**



**RESUMO**

A Lei de Proteção de Dados Pessoais estabelece que o controlador de dados pessoais de criança somente poderá tratar esses dados caso seja concedido o consentimento dos pais ou responsável legal da criança. Todavia, a legislação não estabelece procedimentos para a obtenção deste consentimento, tampouco orienta como fazê-lo. Esta omissão também é verificada no Regulamento Geral de Proteção de Dados da União Europeia, norma na qual a Lei de Proteção de Dados Pessoais se espelhou. Diante disso, faz-se necessária a análise do Chidren's Online Privacy Protection Act (COPPA), a legislação americana e do Age Appropriate Design Code, recente regulamentação do Reino Unido; porque ambas propõem procedimentos com o fim de orientar o controlador dos dados.

**Palavra-chave:** Tratamento de dados pessoais. Criança. Consentimento parental. Procedimentos.

## 1 INTRODUÇÃO

As crianças estão cada vez mais presentes no ambiente virtual. Conforme o levantamento da instituição Better Internet for Kids, portal

[1] Advogada e sócia. Especialista em Direito Público pela UNIBRASIL. Membro do Grupo de Estudos em Direito Autoral e Industrial – GEDAI/UFPR. E-mail: brunasantos@santosberco.com.br

vinculado a Comissão Europeia, as crianças e os jovens já são a maior parte dos usuários que utilizam tecnologias online e móveis na Europa (Better Internet for Kids). No Brasil, a pesquisa realizada pelo Comitê Gestor da Internet no Brasil (TIC Kids Online Brasil) em 2018, constatou que 86% das crianças e adolescentes, entre a faixa etária de 9 a 17 anos, têm acesso à internet, correspondendo a 24,3 milhões de pessoas (CGI.br, 2019).

O acesso à internet é um direito das crianças, neste ambiente a criança também poderá exercer seu direito à liberdade de expressão, opinião e crença, de ter informação, entre outros. Contudo, seu uso indiscriminado tem propiciado experiências negativas às elas, pois têm sido expostas a riscos com os quais não tem maturidade para lidar, uma vez que são pessoas em desenvolvimento, e, possuem vulnerabilidade presumida.

Nos últimos anos, diversos países criaram legislações com o fim de regulamentar o tratamento de dados pessoais, e, em muitas delas, há previsão específica sobre o tratamento de dados pessoais das crianças. No tocante ao RGPD e a LGPD, ambas as legislações não especificam procedimentos para a obtenção do consentimento parental. Diante disso, destacar-se-ão os sistemas do Reino Unido e dos Estados Unidos, que já têm parâmetros para a situação mencionada.

Neste artigo, tratar-se-á distintamente o Reino Unido da União Europeia, tendo em vista a saída daquele país deste bloco econômico, em janeiro de 2020. O Reino Unido, que a época tinha autonomia de um estado-membro, também editou a *Data Protection Act 2018* (DPA).

O Regulamento Geral de Proteção de Dados da União Europeia previu no seu artigo 8 (2) que os dados pessoais das crianças apenas poderão ser tratados mediante o consentimento de um dos pais ou responsável legal. No Brasil, a Lei Geral de Proteção de Dados (LGPD) previu no seu artigo 14, §1º a mesma situação de obrigatoriedade do consentimento parental. A título de esclarecimento, ao mencionar a expressão consentimento parental no presente trabalho, estar-se-á referenciando ao consentimento dado por um dos pais ou pelo representante legal, de acordo com a exigência das legislações suscitadas.

Ante as previsões mencionadas, as instituições estão obrigadas a gerir o risco de tratar dados pessoais de crianças. Por meio de uma conduta ativa, os controladores terão de ter o consentimento dos pais ou responsáveis pela criança, para que seja possível o tratamento dos seus dados. Para tanto, terão de promover os esforços razoáveis e aplicar a tecnologia disponível da época para certificar-se de que o consentimento de fato foi dado por um dos pais ou responsável legal.

Todavia, a execução destes dispositivos ainda resta confusa, uma vez que as legislações da União Europeia e do Brasil não estabelecem padrões para definir como será garantido o consentimento parental; não adotam procedimentos com o fim de orientar o controlador. Muito se tem a esclarecer, como por exemplo, como será possível as empresas que utilizam dados das crianças brasileiras, certificarem-se de que o consentimento será efetivamente dado por um dos pais ou responsável legal? Como o controlador pode garantir que o consentimento não foi fraudado por terceiro ou pela própria criança?

Estas respostas podem ter seu prenuncio de solução em experiências estrangeiras. A Legislação Americana *Chidren's Online Privacy Protection Act (COPPA)* é mais eficiente ao prever instrumentos orientadores para a obtenção do consentimento específico, conforme o § 312.5, b, 2, da lei. Outrossim, a Autoridade Nacional do Reino Unido publicou o código *Age Appropriate Design*, o qual também prevê diversos procedimentos para que o controlador dos dados pessoais da criança possa minimizar o risco de sua atividade econômica e tratar os dados pessoais da criança com mais segurança.

Para a pesquisa foi utilizado o método de pesquisa funcional de Zweigert e Kötz, de Direito Comparado. Para apresentar um resultado analítico, seguiu-se a ordem proposta por Paula Maria Nasser Cury (2014, p. 4):

> (i) Questionamento: como um determinado problema é solucionado? (ii) Escolha dos ordenamentos jurídicos e relatórios sobre as respectivas soluções para o problema pesquisado. (iii) Processo comparati-

> vo *stricto sensu*: em que medida se assemelham as soluções? Em que medida se assemelham as soluções? Em que pontos elas coincidem; através de quais características elas diferem entre si? (iv) Construção de uma sistemática para análise das soluções, esclarecimento de semelhanças e diferenças. (v) Valoração crítica dos resultados, o que eventualmente poderá conduzir à avaliação (discricionária) da melhor solução.

O método de pesquisa citado não tem a pretensão de importar apenas a legislação estrangeira para que, como se fosse o encaixe perfeito, amoldar-se à realidade brasileira. O exercício proposto por este método de pesquisa pretende abordar toda a sistemática jurídica alienígena – legislações, doutrina e jurisprudência – e não apenas um vértice da problemática, para que seja possível perceber as semelhanças e diferenças entre a realidade comparada e a realidade brasileira, e, naquilo que for compatível propor hipóteses de solução.

## 2 DA ECONOMIA INFORMACIONAL AO CRESCENTE USO DA INTERNET PELAS CRIANÇAS

Desde o fim do século XX iniciou-se a Terceira Revolução Industrial, consistente em uma nova economia intimamente vinculada ao novo produto chamado informação. Isto aconteceu em decorrência da evolução tecnológica e do fato de a informação ter se tornado matéria-prima mercantil, deixando de ser considerada como meio de produção econômica, posição esta que ocupava nas Revoluções Industriais anteriores, e, passando a ser considerada como atividade-fim. Diante disso, a economia informacional passou a integrar a realidade da sociedade, que agora se organiza em rede.

Para o sociólogo Manuel Castells (2000, p. 119) a nova economia é informacional, global e com funcionamento em rede, conforme se destaca:

> Uma nova economia surgiu em escala global no último quartel do século XX. Chamo-a de informacional, global e em rede para identificar suas características fundamentais e diferenciadas e enfatizar sua interligação. É *informacional* porque a produtividade e a competividade de unidades ou agentes nessa economia (sejam empresas, regiões ou nações) dependem basicamente de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos. É *global* porque as principais atividades produtivas, o consumo e a circulação, assim como seus componentes (capital, trabalho, matéria-prima, administração, informação, tecnologia e mercados) estão organizados em escala global, diretamente ou mediante uma rede de conexões entre agentes econômicos. É *rede* porque, nas novas condições históricas, a produtividade é gerada, e a concorrência é feita em uma rede global de interação o entre redes empresariais.

O autor ainda menciona que é o primeiro momento histórico em que o intelecto é a força direta de produção. O conhecimento tem se transformado em bens e serviços, seja material ou intelectual e passou a ter valor agregado, nesta relação direta com a economia. Nesse novo modelo, com a evolução da tecnologia, que transmite grande quantidade de informações/comunicações em uma velocidade cada vez maior, a sociedade tem se agrupado em rede em uma comunicação horizontal e agrupada. O emaranhado de computadores ligados entre si formou uma teia mundial direcionada ao usuário (CASTELLS, 2000).

A sociedade em rede tem produzido cada vez mais informações dentro do ambiente virtual, fato que, há muito tempo, tem despertado o interesse financeiro de instituições. Por consequência, as empresas que têm relação com internet têm crescido exponencialmente, as quais, em sua maioria, tem como atividade empresarial o gerenciamento de informações e dados (CASTELLS, 2000).

Essa tendência, que já não é mais nova, transformou o indivíduo que está presente na internet em um produto econômico, porque seus dados são desejados por instituições que pretendem interferir comercialmente no comportamento humano. Infelizmente, a mercantilização

dos dados pessoais do usuário da internet é desprovida de qualquer recato ou ética, porque atinge pessoas de todos os sexos, raças, credos, idades etc. Inclusive, atingem crianças, que estão cada vez mais presentes na internet.

Parece contraditório com o que se acabou de aduzir, mas estar na internet é um direito da criança. A Convenção sobre os Direitos da Criança (ONU) que foi adotada pela ONU e retificada pelo Brasil, em 24/09/1990, destaca alguns direitos pertencentes às crianças como o direito à liberdade de expressão, de crença, opinião, direito de ter informação adequada à sua idade, entre outros[2] (ONU, 1989). Todos estes direitos devem ser assegurados às crianças, inclusive, em âmbito virtual, assim, um meio de garantir esses direitos no ambiente virtual é proporcionar o acesso a internet.

No Reino Unido, o órgão Information Commissioner's Office (ICO), que se assemelha a nossa Autoridade Nacional de Proteção de Dados (ANPD), tem tomado medidas e estratégias com o fim de garantir uma internet melhor para as crianças. Como uma de suas estratégias criou o portal *Better Internet for Kids,* que se dedica às nuances da criança na internet. Em um dos seus estudos, menciona que a Internet proporciona às crianças acesso ao conhecimento, à comunicação, ao desenvolvimento de habilidades e aprimora sua capacitação profissional (Better Internet for Kids).

Importante destacar que fomentar o acesso pela criança à internet não significa desconsiderar sua condição de vulnerabilidade presumida e de indivíduo ainda em formação, permitindo indiscriminadamente a sua

---

[2] Artigo 12, 1: Os Estados Partes devem assegurar à criança que é capaz de formular seus próprios pontos de vista o direito de expressar suas opiniões livremente sobre todos os assuntos relacionados a ela, e tais opiniões devem ser consideradas, em função da idade e da maturidade da criança.

2. Os Estados Partes devem adotar todas as medidas apropriadas para assegurar que a criança seja protegida contra todas as formas de discriminação ou punição em função da condição, das atividades, das opiniões manifestadas ou das crenças de seus pais, representantes legais ou familiares. Disponível em: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca#:~:text=Artigo%2012,e%20da%20maturidade%20da%20crian%C3%A7a.

exposição à uma internet que, até o momento, não foi criada para ela. Em que pese o direito das crianças a este acesso, não se pode desconsiderar suas necessidades e vulnerabilidade que lhes são peculiares (Better Internet for Kids) em virtude de sua tenra idade.

No Brasil, é possível verificar que o ordenamento jurídico reconheceu a vulnerabilidade das crianças e dos adolescentes ao prever, no artigo 227 da Constituição Federal, o dever da família, da sociedade e do Estado em assegurar à criança, ao adolescente e ao jovem, diversos direitos fundamentais.[3] Na sequência, a edição da Lei 8.069/1990 (Estatuto da Criança e do Adolescente) corroborou com a norma constitucional, para dar interpretação sistemática ao diploma legal, principalmente, sob o enfoque do princípio da proteção integral (artigo 1º ECA[4]) (ROSATO; LÉPORE e CUNHA, 2013).

Diante dessa vulnerabilidade que é presumida do indivíduo em desenvolvimento, as crianças são alvos fáceis na internet. Embora a internet ofereça muitas oportunidades de aprendizagem, comunicação, criatividade e entretenimento, também abre espaço para certos riscos para usuários vulneráveis, como crianças[5] (Better Internet for Kids). Um estudo realizado pelo portal *Better Internet for Kids* descreveu os principais riscos aos quais são expostos às crianças que acessam a internet: *fake news; cyberbullying;* preocupação com a privacidade em relação a brinquedos conectados (*privacy concern in connected toys*); a divulgação de conteúdos eróticos e sensuais (*sexting*); exposição a conteúdos e comportamen-

---

3 Artigo 227 da Constituição Federal: É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

4 Art. 1º do **Estatuto da Criança e do Adolescente**: Esta Lei dispõe sobre a proteção integral à criança e ao adolescente. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm

5 Tradução livre, texto original: While the internet offers many opportunities for learning, communication, creativity and entertainment, it also opens up certain risks to vulnerable users such as children. Disponível em: https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids

tos nocivos e perturbadores (*exposure to harmful or disturbing content*) e aliciamento infantil pela internet (*grooming*); pornografia, violência e automutilação.

O documento nº 52012DC0196 (EUR-LEX, 2012) apresentado pela Comissão Europeia ao Parlamento Europeu e demais instituições cita que 4 em cada 10 crianças já foram submetidas aos riscos na internet de conversar com alguém que não conheciam; de publicação de conteúdo criado por eles mesmos com apologia a anorexia, a autoagressão, ao consumo de drogas ou o suicídio; de exposição a imagens de índole sexual on-line; utilização abusiva de dados pessoais; encontros na vida real com pessoas que conheceram apenas através da internet; assédio/intimidação on-line.[6]

Ante o estudo, percebe-se a falta de segurança da criança ao navegar na internet, bem como sua vulnerabilidade e a falta de habilidades emocionais para lidar com os riscos aos quais têm sido expostas. Diante destes riscos, o portal BIK aduziu que medidas eficientes são necessárias para prevenir consequências negativas que a exposição a certos riscos causam desenvolvimento cognitivo, social e emocional da criança (Better Internet for Kids).[7]

O foco do presente trabalho se limitará apenas à problemática atinente a proteção de dados das crianças em detrimento dos demais problemas citados.

## 3 DA PROTEÇÃO DE DADOS PESSOAIS DA CRIANÇA E DO CONSENTIMENTO ESPECÍFICO PARENTAL

6 O'Neill, B., Livingstone, S., & McLaughlin, S: «Final recommendations for policy, methodology and research» (2011), elaboradas no quadro do projeto EUKidsOnline II. Disponível em: http://eprints.lse.ac.uk/39410/1/Final_recommendations_for_policy%2C_methodology_and_research_%28LSERO%29.pdf, citado no documento nº 52012DC0196, disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:52012DC0196

7 Tradução livre, texto original: Online, children can be exposed to harmful content and behaviour such as cyberbullying, sexual harassment, pornography, violence, or self-harm. Efficient responses are needed to prevent negative consequences for their cognitive, social and emotional development.

Diante da economia informacional, na qual a informação é o próprio produto, os métodos capitalistas avançam cada vez mais no sentido de se obter mais informações sobre os usuários na internet. Isto devido ao valor econômico que estas informações têm para empresas e instituições.

Na obra A Galáxia da Internet, Manuel Castells (2001, p. 190) aduz que:

> Em muitos casos, a principal fonte de rendimentos das companhias de comércio eletrônico são a publicidade e o marketing, [...]. Por um lado, elas recebem os lucros das faixas de publicidade que podem exibir para seus usuários. Por outro, vendem os dados de seus usuários para seus clientes para fins de marketing, ou os utilizam elas próprias para melhor mirar seus clientes.

Os negócios, sejam grandes ou pequenos empreendimentos, principalmente os digitais, tem essencialmente como ativo o uso de dados pessoais (OLIVEIRA e COTS, 2020). Para corroborar com o argumento, cita-se o discurso do Senador Ricardo Ferraço, descrito no projeto de lei que originou a LGPD, mencionado na obra de Ricardo Oliveira e Márcio Cots (2020, p. 28):

> Vivemos hoje em uma economia maciçamente baseada em dados (*data driven economy*), em que informações sobre todos os aspectos das relações humanas, inclusive da personalidade dos indivíduos, estão sendo coletados, armazenados e processados como nunca antes fora possível. A todo momento, pessoas, conscientemente ou não, oferecem a um número crescente de empresas – com tecnologia adequada – dados sobre quem são, o que estão fazendo, onde estão, sobre o que falam ou com quem interagem.

No mesmo sentido, o sociólogo Manuel Castells (2001, p. 190) menciona que:

> A transformação da liberdade e da privacidade na Internet é um resultado direto de sua comercialização. A necessidade de assegurar e identificar a comunicação na Internet para ganhar dinheiro com ela, e a necessidade de proteger direitos de propriedade intelectual nela, levaram ao desenvolvimento de novas arquiteturas de software (que Lessig chama de "o código") que permitem o controle da comunicação por computador.

Para ilustrar a comercialização de informações dos usuários, destaca-se dado descrito na obra A Galáxia da Internet de que nos EUA 92% dos websites coletam dados pessoais dos usuários e os transacionam da forma que lhe convêm, comercialmente. (LESSIG, 1999, p. 153 apud CASTELLS, 2001, p. 194). O tratamento de dados pessoais, seja pelo setor público ou privado, tornou-se extremamente importante economicamente, contudo, muitas vezes conflita com o direito fundamental da privacidade. (OLIVEIRA e COTS, 2020).

Na economia informacional, na qual a informação é o produto almejado pelas empresas, há tratamento abusivo e indiscriminado de dados pessoais dos usuários da internet, inclusive, de crianças. Nos Estados Unidos, houve uma situação de suposta violação de dados pessoais praticado pela *The Walt Disney Company*, acusada de coletar ilegalmente dados pessoais de crianças (IRWIN, 2017). A empresa estaria utilizando seus aplicativos para coletar dados de crianças, para compartilhá-lo com anunciantes, sem o consentimento dos pais (CIACCIA, 2017).

Outra situação concreta que elucida a necessidade de proteção de dados da criança foi o fato que ocorreu com o aplicativo *Life360*. Este aplicativo tem como uma de suas atividades compartilhar a localização e deslocamento de crianças e adolescentes com suas famílias, permitindo que seus pais rastreiem em tempo real o paradeiro de seus filhos, em poder destas informações tem criado *profiling* e compartilhado com a empresa Arity, para a venda de seguros de veículo (BREWSTER, 2020).

No Reino Unido, pesquisas realizadas pelo ICO, *Ofcom* e *London School of Economics* constataram que uma das principais preocupações acerca da proteção de dados pessoais é a privacidade e segurança das crianças na internet (ICO, 2020).

Difícil falar de proteção de dados pessoais da criança, quando aquele que tem o devido discernimento para proteger a criança, no caso seus pais ou responsável, negligencia o seu próprio direito à privacidade, para conseguir acessar os benefícios imediatos da Internet. A realidade é de que muitas pessoas renunciam seu direito constitucional à privacidade para ter algum benefício on-line. Ante a necessidade de proteção dos dados pessoais das crianças, nos EUA, durante o governo Clinton, tentou-se emplacar o *Child On-line Protection Act* de 1998, que seria plausível se a real intenção não fosse apenas uma tentativa do governo em censurar a internet (CASTELLS, 2001).

A consideranda 38[8] do RGPD reafirma a necessidade de proteção especial quando do tratamento de dados da criança, em virtude dos riscos a que estão expostos e consequências de toda ordem, que possa trazer prejuízo a essa faixa etária (LIMA, 2019).

A elaboração de uma lei que pretende regular o tratamento de dados pessoais deve considerar a cultura e momento histórico de cada país. Contudo, em virtude da globalização, entende-se que as peculiares enfrentadas se misturam, diante das economias estarem cada vez mais direcionadas ao tratamento de dados, na segmentação do mercado, entre outros (OLIVEIRA e COTS, 2020).

---

[8] (38) As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

Diante disso, salutar ainda trazer à baila o direito comparado para analisar a problemática do presente trabalho. Todos os países abordados neste trabalho, possuem previsão legal acerca do tratamento de dados pessoais das crianças.

Em todas eles, há previsão de que a empresa/instituição que tratarem dados pessoais de crianças, inclusive ao prestar serviços da sociedade da informação (ISS)[9], somente poderá realizar o tratamento, caso haja o consentimento parental ou do responsável legal para que seja possível o mencionado tratamento.

Na União Europeia, foi editado o Regulamento (UE) 2016/679 (RGPD), que entrou em vigor em 25 de maio de 2018. No artigo 8 (1)[10]

---

9 Artigo 1.º
1. Para efeitos da presente diretiva, aplicam-se as seguintes definições:
a) [...];
b) «Serviço» significa qualquer serviço da sociedade da informação, isto é, qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços;
Para efeitos da presente definição, entende-se por:
i) **«à distância»**: um serviço prestado sem que as partes estejam simultaneamente presentes,
ii) **«por via eletrónica»**: um serviço enviado desde a origem e recebido no destino através de instrumentos eletrónicos de processamento (incluindo a compressão digital) e de armazenamento de dados, que é inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos,
iii) **«mediante pedido individual de um destinatário de serviços»**: um serviço fornecido por transmissão de dados mediante pedido individual. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015L1535&from=EN. "Essencialmente, isso significa que a maioria dos serviços online são ISS, mesmo que a "remuneração" ou financiamento do serviço não venha diretamente do usuário final." Tradução livre, texto original: "Essentially this means that most online services are ISS, even if the 'remuneration' or funding of the service doesn't come directly from the end user." Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-are-the-rules-about-an-iss-and-consent/#a3.

10 Artigo 8.º **Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação**
1. Quando for aplicável o artigo 6.º, n.º 1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança.

consta que o controlador, que prestar serviços às crianças abaixo de 16 anos, deverá possuir o consentimento parental ou de responsável legal pela criança, para realizar o tratamento de dados destes usuários. No mesmo artigo 8 (2), também prevê que os Estados-membros pertencentes à União Europeia poderão estabelecer idade inferior a 16 anos, caso assim desejem, todavia, o limite mínimo será de 13 anos.

A *Data Protection Act 2018* (DPA 2018) promulgada pelo Reino Unido, que dispõe sobre o tratamento de dados pessoais, ratificou a maior parte do RGPD, com as devidas complementações e adaptações à realidade britânica. Nesta legislação, houve a adaptação da previsão geral contida no RGPD no tocante a obrigatoriedade da obtenção do consentimento específico para menores de 16 anos, passando a vigorar a idade máxima de 13 anos para a obrigatoriedade do consentimento.[11]

Importante destacar um caso concreto que o RGPD foi utilizado para pacificar a lide. Nos países baixos ocorreu um caso concreto de uma mãe contra a avó, que não queria tirar fotos dos seus netos de suas redes sociais do *facebook* e *pinterest*. Em que pese o RGPD não servir a solução de casos de familiares, o artigo 8º da Legislação foi utilizado para solucionar o conflito e determinar a exclusão das fotos postadas (PEQUENINO, 2020). A decisão mencionada utilizou o RGPD para regular caso familiarista, mesmo sendo uma legislação voltada a solucionar a proteção de da-

Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos.
2. Nesses casos, o responsável pelo tratamento envida todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível.
3. O disposto no n.º1 não afeta o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a uma criança. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=-CELEX:32016R0679&from=PT

[11] **9 Child's consent in relation to information society services**
In Article 8(1) of the GDPR (conditions applicable to child's consent in relation to information society services)—
(a)references to "16 years" are to be read as references to "13 years", and
(b)the reference to "information society services" does not include preventive or counselling services. Disponível em: https://www.legislation.gov.uk/ukpga/2018/12/section/9/enacted

dos entre empresas particulares e entidades públicas quando utilizados os dados de indivíduos.[12]

A proteção de dados das crianças nos Estados Unidos, é regulamentada pela *Chidren's Online Privacy Protection Act (COPPA).* No seu § 312.5, a, 1 e b,1, prevê que o operador de site ou serviço on-line direcionado a crianças, deverá obter o consentimento verificável dos pais antes de qualquer coleta ou divulgação das informações.[13] Além disso, a legislação fixa como criança o indivíduo abaixo de 13 anos e menciona que o operador deverá promover todos os esforços razoáveis para garantir o consentimento e utilizar a tecnologia disponível, como o RGPD.[14]

No Brasil, a Constituição Federal protegeu, expressamente, a intimidade e a vida privada das pessoas, nos termos do artigo 5º, inciso X[15]. Assim, a proteção de dados pessoais tem como fio condutor o princípio fundamental da privacidade. Não diferentemente das Legis-

---

12 Para consulta da decisão proferida segue o link: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBGEL:2020:2521&showbutton=true&keyword=AVG

13 §312.5 Parental consent.
(a) *General requirements.* (1) An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.
(2) [...].
(b) *Methods for verifiable parental consent.* (1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. Disponível em: https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5#se16.1.312_14

14 §312.2 Definitions.
*Child* means an individual under the age of 13. Disponível em: https://www.ecfr.gov/cgi-bin/text=-idx?SID4939=77e77c1a1a08a1ccb905ff4c409b&node16=3%1A0.1.3.36.&rgn-div5#se16.1.312_14

15 Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
[...]
X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

lações acima citadas, no Brasil, também há a Lei Geral de Proteção de Dados sob nº Lei nº 13.709/2018 (LGPD), nela consta previsão legal acerca da proteção de dados quando do tratamento de dados pessoais de crianças.

O tratamento de dados deste grupo da sociedade deve sempre observar os princípios previstos no ECA, quais sejam: o melhor interesse da criança e a proteção integral (LIMA, 2019).

O artigo 14, §1º da Lei consta que o tratamento de dados das crianças deverá ser feito, apenas, diante de consentimento específico de um dos pais ou responsável.[16]

Caio César Carvalho Lima (2019, p. 209-210), na obra que pretende comentar a LGPD, explica o que seria o consentimento específico:

> [...] importante observar que o consentimento será entendido como "específico quando, antes da coleta dos dados, no contrato, na política

[16] Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

> de privacidade ou em outro documento relacionado, houver detalhamento sobre o ciclo de vida do tratamento dos dados pessoais, com referência objetiva e clara sobre todos os limites e as finalidades em relação aos quais os dados serão tratados, inclusive sendo granular, cabendo ao usuário a seleção sobre o tratamento que deseja efetivamente autorizar.

No tocante a idade máxima prevista para obrigatoriedade da obtenção do consentimento, a LGPD não fixa idade para a exigência do consentimento específico, apenas fazendo constar que ele será necessário quando houver tratamento de dados de crianças. Neste sentido, o Estatuto da Criança e do Adolescente define que criança é o indivíduo que possui doze anos incompletos, conforme o artigo 2º.[17]

Sobre como o consentimento que deverá ser obtido, o §5º do artigo 14 da LGPD menciona que o controlador deverá realizar todos os esforços razoáveis para garantir o consentimento específico, utilizando a tecnologia disponível.

Resta evidente a dificuldade de assegurar com toda certeza de que o consentimento foi dado pelo próprio pai/mãe ou responsável legal pela criança. Como se pode observar, tanto a Legislação europeia quanto a brasileira, dispõem de conceitos semelhantes no tocante a proteção dos dados da criança, contudo, não especificam e nem orientam os procedimentos que servirão à obtenção do consentimento específico de um dos pais ou responsável legal pela criança, pelo controlador dos dados (YANDRA; SILVA e SANTOS, 2020).

Não há orientação ao controlador de como ele deverá proceder para requerer o consentimento específico. Assim, é essencial visualizar as legislações e/ou Regulamentos que desta forma dispõem, na tentativa de trazer, mesmo que minimamente, luz à realidade brasileira.

---

[17] Artigo 2º do **ECA**: Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade.

## 4 OS PROCEDIMENTOS INDICADOS PARA A OBTENÇÃO DE VERIFICÁVEL CONSENTIMENTO PARENTAL

O acesso da criança à internet condicionado ao controle parental já é discutido há algum tempo. O presente trabalho não abordará a temática acerca do controle parental excessivo e a privacidade das crianças, mas o que não se pode desconsiderar é o fato de que na medida adequada, ele promove segurança virtual a elas. Na União Europeia, o documento nº 52012DC0196, enviado pela Comissão Europeia ao Parlamento Europeu, já mencionava o controle parental como ferramenta de de proteção à criança, quando da utilização da internet. Todavia, a implanação dessas tecnologias é considerada pelas empresas como custo adicional, que apenas estariam dispostas a investir quando o mercado justificar o investimento, não sendo o público infantil merecedora de investimento (EUR-LEX, 2012).

Na época, constatou-se que havia uma incapacidade do mercado em fornecer medidas de proteção e de conteúdo de qualidade às crianças, em toda a Europa. Isto porque, as ferramentas analisadas capazes de realizar o controle parental eram eficazes, em sua maioria, no idioma inglês. Além disso, constatou-se que não existia, na ocasião, muitas ferramentas para realizar o controle parental nos aparelhos de *video game*, *tablets* e *celulares*, os quais são mais utilizados pelas crianças ao acessar o mundo on-line. Ademais, para os dois últimos aparelhos não havia solução quando eram acessadas aplicações ao invés de buscadores (EUR-LEX, 2012).

Neste momento, em que o tratamento de dados pessoais tem sido cada vez mais regulamentado em diversos lugares do mundo, é imperioso que as instituições controladoras de dados estejam em conformidade com as normativas, não podendo mais se valer de pretextos que não condizem com a atividade empresarial, o regramento da proteção de dados é inerente ao próprio risco da atividade.

A realidade não é diferente quando se pretende proteger os dados pessoais da criança. O controlador não deve poupar esforços para mini-

mizar o risco de sua atividade ao tratar dados destas pessoas, praticando todos os esforços razoáveis e utilizando a tecnologia disponível.

Para elucidar como o controlador poderá colocar em prática as determinações legais, com o fim de assegurar que o consentimento foi dado efetivamente por um dos pais ou responsável, destacam-se as sugestões/indicações de ferramentas descritas no *Children's Online Privacy Act* (COPPA), legislação americana já citada anteriormente, a qual é uma referência internacional de extensa regulamentação sobre o tratamento de dados de crianças. Nela consta procedimentos que devem ser adotados pelo controlador dos dados quando da obtenção do consentimento (LIMA, 2019).

A legislação busca estruturar métodos de obtenção do que chama de "consentimento verificável", definido como: o controlador fazer qualquer esforço (levando em consideração a tecnológica disponível) para garantir que, antes do processamento de dados pessoais da criança, um dos pais seja notificado sobre as práticas de tratamento, bem como seja por ele autorizada (E-CFR, 1998). A menção à prática de esforços razoáveis e utilização de tecnologia disponível também ocorreu no artigo 8 (2) do RGPD e no artigo 14, §5º, da LGPD.

No § 312.5, b, 2, há previsões de métodos para obter o consentimento verificável dos pais, como formas legítimas de o controlador utilizar e verificar a identidade dos pais. Os métodos indicados são os seguintes:[18]

[18] Tradução livre, texto original: §312.5 Parental consent.
(b) *Methods for verifiable parental consent.* (1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.
(2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:
(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;
(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
(iii) Having a parent call a toll-free telephone number staffed by trained personnel;
(iv) Having a parent connect to trained personnel via video-conference;

(i) Fornecer um formulário de consentimento a ser assinado pelos pais e devolvido à operadora por correio postal, fax ou digitalização eletrônica;

(ii) Exigir dos pais, em conexão com uma transação monetária, use um cartão de crédito, cartão de débito ou outro sistema de pagamento online que forneça notificação de cada transação, ao titular da conta principal;

(iii) Ter acesso a um dos pais para ligar para um número de telefone gratuito com uma equipe treinada;

(iv) Fazer com que um dos pais ligue para um número de telefone gratuito ou faça uma videoconferência com a equipe ou se conecte por videoconferência a uma equipe treinada;

(v) Verificar a identidade de um dos pais comparando uma forma de identificação emitida pelo governo em bancos de dados de tais informações, onde a identificação dos pais é excluída pelo operador de seus registros imediatamente após a verificação ser concluída; ou

(vi) Desde que, um operador que não "divulgue" (conforme definido por §312.2) informações pessoais de crianças, pode usar um e-mail juntamente com etapas adicionais para fornecer garantias de que a pessoa que fornece o consentimento é o pai. Essas etapas adicionais incluem: Enviar um

(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or
(vi) *Provided that,* an operator that does not "disclose" (as defined by §312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email. Disponível em: https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5#se16.1.312_14

> e-mail de confirmação para os pais após o recebimento do consentimento, ou obter um endereço postal ou número de telefone dos pais e confirmar o consentimento dos pais por carta ou telefonema. Um operador que usa esse método deve avisar que os pais podem revogar qualquer consentimento dado em resposta ao e-mail anterior.

Estas são algumas ferramentas disponibilizadas pelo COPPA. Percebe-se que as hipóteses apresentadas para obter o verificável consentimento parental são autoexplicativas na própria legislação, fato que não se vislumbra, nem de longe, no RGPD e na LGPD, que provavelmente, foi deixado a cargo da Autoridade Reguladora.

No mesmo sentido, só que no Reino Unido, o *Data Protection Act 2018*, na seção 123 (1) previu que o Comissário Oficial (ICO) deveria elaborar um código de prática que contivesse orientações sobre as normas de consentimento adequado à idade dos serviços relevantes da sociedade da informação que possam ser acessados por crianças. (Legislation.gov.uk, 2018).[19] Desta forma, a respectiva Autoridade Nacional (ICO) publicou o código *Age Appropriate Design*, no dia 02 de setembro de 2020, ainda em período de transição de 12 meses. A regulamentação conta com a previsão de 15 padrões flexíveis que o controlador deverá adotar para promover segurança e adequação às crianças on-line.

O Código *Age Appropriate Design* tem como objetivo assegurar que os serviços online que são acessados por crianças sejam apropriados para seu uso e atendam às suas necessidades de desenvolvimento. O Código se desenvolveu para orientar o controlador a compreender a faixa etária das crianças que são usuários do seu serviço online e a probabilidade

[19] Tradução livre, texto original: 123 Age-appropriate design code
Age-appropriate design code
(1)The Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children. Disponível em: https://www.legislation.gov.uk/ukpga/2018/12/part/5/crossheading/codes-of-practice/enacted

de acessar ao serviço, atendendo as diferentes necessidades das crianças em diferentes idades e estágios de desenvolvimento, é fundamental para todo o conceito de "design adequado à idade".

Resumidamente, dentre os 15 padrões estabelecidos que se destinam à regulamentar, também, o acesso da criança aos serviços on-line, estão: agir de acordo com o melhor interesse da criança; realizar avaliação de impacto da proteção de dados; verificar a aplicação apropriada para a idade; agir com transparência; não utilizar os dados de forma prejudicial à criança; cumprimento das próprias políticas, condições e termos; oferecer às crianças configurações de privacidade padrão; minimizar a coleta de dados da criança àquilo estritamente necessário; agir com cautela ao compartilhar dados; cuidados com os dados de geolocalização da criança; disponibilizar ferramentas para o controle dos pais; cautela na utilização de *profiling*; cuidado ao utilizar *nudge techniques*; agir com clareza quando do uso de brinquedos e dispositivos conectados por crianças; produzir ferramentas on-line para que a criança possa conhecer e exercer seus direitos.

Um dos padrões que é interessante destacar é aquele que orienta o controlador a realizar a verificação de idade consoante ao consentimento parental verificável, este padrão tem o condão de diminuir o risco da atividade do controlador. A verificação adequada da idade possibilita gerenciar os riscos e manter conformidade com as normas regulatórias, isto diminui a pontencialidade de se obter um consentimento falso, que ao invés de ser dado por um dos pais ou responsável, foi dado pela própria criança e também de criminosos tentando fraudar identidades.

Assim, o código estabeleceu os seguintes métodos para a verificação de idade: 1. Autodeclaração; 2. intelegência artificial; 3. serviço de verificação de idade e de verificação de terceiros; 4. Confirmação do titular da conta; 5. Medidas técnicas; 6. Identificadores físicos (ICO, 2020).

Abaixo remetará as explicações dada pelo Código referente a cada conduta[20]:

[20] Texto original em inglês Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-

(i) Autodeclaração: é quando um usuário simplesmente informa sua idade, mas não fornece nenhuma evidência para confirmá-la. Pode ser adequado para processamento de baixo risco ou quando usado em conjunto com outras técnicas;

(ii) Inteligência artificial: pode ser possível fazer uma estimativa da idade de um usuário usando inteligência artificial para analisar a maneira como o usuário interage com seu serviço. Da mesma forma, poderá usar esse tipo de perfil para verificar se a maneira como um usuário interage com seu serviço é consistente com sua idade autodeclarada. Se esta for a opção do controlador, ele precisará dizer aos usuários que ele fará isso antecipadamente; recolhe apenas a quantidade mínima de dados pessoais de que necessita para este efeito; e não usar quaisquer dados pessoais coletados para esta finalidade para outros fins;

(iii) Serviços de verificação de idade de terceiros: poderá escolher usar um serviço de terceiros para o fornecimento de uma garantia da idade de seus usuários. Esses serviços normalmente funcionam em um sistema de "atributo", em que se solicita a confirmação de um atributo de usuário específico (neste caso, idade ou faixa etária) e o serviço fornece uma resposta "sim" ou "não". Este método reduz a quantidade de dados pessoais que precisa coletar e pode permitir que se aproveite a experiência tecnológica e os desenvolvimentos mais recentes na área;

(iv) Confirmação do titular da conta: é possível contar com a confirmação da idade do usuário de um titular da conta existente que se sabe ser um adulto. Por exemplo, se fornecer um serviço conectado ou baseado em assinatura, poderá permitir que o titular da conta principal (adulto confirmado) configure perfis de criança, restrinja o acesso posterior com uma senha ou PIN ou simplesmente confirme a faixa etária de usuários de contas adicionais;

-for-online-services/3-age-appropriate-application/

(v) Medidas técnicas: As medidas técnicas que desencorajam as falsas declarações de idade, ou identificam e encerram contas de menores, podem ser úteis para apoiar ou fortalecer os mecanismos de autodeclaração. Os exemplos incluem a apresentação neutra de telas de declaração de idade (em vez de cutucar a seleção de certas idades) ou impedir que os usuários reenviem imediatamente uma nova idade se não tiverem acesso ao seu serviço quando declararem a idade pela primeira vez;

(vi) Identificadores físicos: é possível confirmar a idade usando soluções que apontam para documentos de identificação formal ou "identificadores rígidos", como um passaporte. No entanto, recomenda-se que se evite dar aos usuários nenhuma escolha a não ser fornecer identificadores rígidos, a menos que os riscos inerentes ao seu processamento realmente justifiquem tal abordagem. Isso ocorre porque algumas crianças não têm acesso a documentos de identidade formais e podem ter apoio parental limitado, dificultando o acesso aos serviços de verificação de idade, mesmo que sejam adequados para a idade. A exigência de identificadores físicos também pode ter um impacto desproporcional na privacidade dos adultos.

Os métodos de averiguação de idade acima elencados dependerá do serviço que é usado por usuários autenticados ou não autenticados, podendo os riscos também variar conforme o contexto. Sobre a utilização de verificação de idade, a Comissão Europeia (CE) respondeu uma questão sobre a aplicação do consentimento específico e aduziu que as empresas devem fazer todos os esforços razoáveis, levando em consideração a tecnologia disponível, para verificar se o consentimento dado está realmente em conformidade com a lei. Isso pode envolver a implementação de medidas de verificação de idade, como fazer uma pergunta que uma criança comum não seria capaz de responder ou solicitar que o menor forneça o e-mail de seus pais para permitir o consentimento por

escrito.[21] Observa-se que o entendimento converge com os direcionamentos dados pelo ICO.

Internalizando a análise, constata-se que a LGPD não faz qualquer menção quanto a procedimentos para assegurar o consentimento parental verificável, podendo-se utilizar de outros diplomas como inspiração. Espera-se que a Autoridade Nacional de Proteção de Dados (ANPD) promova a regulamentação detalhada, para sanar a omissão apontada.

## 5 CONSIDERAÇÕES FINAIS

A proteção de dados pessoais é um assunto ainda recente para a sociedade, pouco se fala e se educa quanto a questão, quiçá sobre a proteção de dados pessoais da criança, a qual está on-line em uma internet que sequer foi projetada para ela. Além das medidas legislativas sobre a preservação dos dados, é importante desenvolver e difundir a educação midiática, pois somente a educação será capaz de conter todos os infortúnios proporcionados pelo processamento de dados pessoais.

Neste sentido, a Comissão Europeia elaborou um jogo chamado de "Cyber Chronix" para explicar o GDPR às pessoas mais novas, o objetivo do jogo é ajudar seu personagem a chegar a uma festa, enquanto eles encontram vários obstáculos relacionados à proteção de dados ao longo do caminho (EUROPEAN COMMISSION, 2018). No Brasil nenhuma medida semelhante foi vislumbrada até o momento, iniciada pelos poderes ou instituições estatuais, todavia, pode-se citar como um indício de tentativa de alfabetização digital o artigo 14, §6º da LGPD que prevê a necessidade de clareza, acessibilidade e simplicidade nas informações fornecidas às crianças e os pais, referente ao tratamento de dados.

[21] Tradução livre, texto original: Companies have to make reasonable efforts, taking into consideration available technology, to check that the consent given is truly in line with the law. This may involve implementing age-verification measures such as asking a question that an average child would not be able to answer or requesting that the minor provides his parents' email to enable written consent. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en

É importante que para além de previsões legais a sociedade assuma o seu papel e sua responsabilidade em relação aos seus dados pessoais, não os renunciando em troca de qualquer benefício on-line. Para isso, a conscientização do conceito de privacidade deve ser disseminada de forma imediata. No tocante a economia informacional baseada na informação, o artigo contido neste livro, na parte II, seção II, capítulo I, aduz que é possível se afirmar que o emprego de dados pessoais é essencial para o progresso da maioria das atividades econômicas, todavia, a utilização indiscriminada de dados pessoais dos usuários da internet não proporciona a segurança e a privacidade adequadas.

Como medida repressora, a LGPD pretende combater os abusos no tratamento dos dados pessoais, mas ainda o diploma legal não se apresentada como medida estanque a resolver a questão, entendendo-se que ainda resta pendente de regulamentação alguns de seus artigos, como por exemplo, a falta de orientação quanto aos procedimentos para se obter o verificável consentimento parental no tratamento de dados da criança.

O COPPA e o código *Age Appropriate Design* apresentam alguns direcionamentos quanto à situação. A experiência americana está a frente daquelas ventiladas no presente trabalho, isto porque, a proteção de dados já é assegurada há mais tempo, uma vez que o COPPA foi publicada em 1998, bem como o sistema americano esteleceu meio de fiscalização mais eficaz quanto ao descumprimento das normas de proteção de dados. De acordo com o artigo contido nesta obra, na parte II, seção II, capítulo II, cita outra legislação estadunense que também trata da proteção de dados: a *Consumer Data Protection* (2018), que fixa quesitos e responsabilidades para aqueles que realizam o tratamento dos dados, cuja denúncia de qualquer violação poderá ser feita a *Federal Trade Comission* (FTC), agência que protege os consumidores e fiscaliza situações atinentes a privacidade dos dados pessoais.

No Brasil, além de não ser de conhecimento geral a educação digital, também se vislumbram algumas omissões na LGPD. Para tanto, a esperança está na estruturação da ANPD, a qual terá atribuição de editar normativas regulamentadoras e orientadoras acerca da lei principal. O

cidadão brasileiro e as instituições destinatários desta legislação necessitam urgentemente de parâmetros para que seja possível o seu devido cumprimento com toda segurança. Enquanto não se concretiza o efetivo funcionamento da ANPD, contemplam-se as experiências internacionais sobre o tratamento de dados pessoais da criança e a obtenção do consentimento parental pelo controlador.

## REFERÊNCIAS

BETTER INTERNET FOR KIDS. **Better internet for kids.** Disponível em: https://www.betterinternetforkids.eu/web/portal/policy/better-internet. Acesso em: 14 set. 2020.

BETTER INTERNET FOR KIDS. **Creating a Better Internet for Kids.** Disponível em: https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids. Acesso em: 14 set. 2020.

BETTER INTERNET FOR KIDS. From safer internet programme to better internet for kids: a policy roadmap. Disponível em: https://www.betterinternetforkids.eu/web/portal/policy/better-internet/policy-roadmap. Acesso em: 14 set. 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Portal da Legislação, Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 set. 2020.

BRASIL. **Lei nº 8.069 de 13 de julho de 1990.** Estatuto da Criança e do Adolescente (ECA). Portal da Legislação, Brasília, DF, 13 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 20 set. 2020.

BREWSTER, Thomas. FORBES. Life360 comes at you fast – cops convince arson suspect's kid to give up dad's location on Family tracking app. Disponível em: https://www.forbes.com/sites/thomasbrewster/2020/02/12/life360-comes-at-you-fast--cops-use-family-surveillance-app-to-trace-arson-suspect/#518eb306380a. Acesso em: 25 set. 2020.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução Maria Luiza X. de A. Borges. Editora: Zahar.

CASTELLS, Manuel. **A sociedade em rede**. Tradução: Roneide Venancio Majer. vol. 1. 8. ed. rev. e ampl. Editora: Paz e Arte.

CIACCIA, Chris. FOX NEWS. Disney app spying on childre, lawsuit claims. Disponível em: https://www.foxnews.com/tech/disney-apps-spying-on-children-lawsuit-claims. Acesso em: 23 set. 2020.

COMITÊ GESTOR DE INTERNET NO BRASIL. **Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil.** Disponível em: https://cetic.br/media/docs/publicacoes/216370220191105/tic_kids_online_2018_livro_eletronico.pdf. Acesso em: 22 set. 2020.

CURY, Paula Maria Nasser. Métodos de direito comparado: desenvolvimento ao longo do século XX e perspectivas contemporâneas. **Revista de estudos constitucionais, hermenêutica e teoria do direito (RECHTD)**, julho-setembro 2014, p. 176-185. Disponível em: http://www.revistas.unisinos.br/index.php/RECHTD/article/viewFile/rechtd.2014.62.06/4303. Acesso em: 01 set. 2020.

EUROPEAN COMMISSION. **Can personal data about children be collected?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en. Acesso em: 25 set. 2020.

EUROPEAN COMMISSION. **Understanding GDPR:** new game from the JRC. Disponível em: https://ec.europa.eu/jrc/en/news/understanding-gdpr-new-game-jrc. Acesso em: 30 set. 2020.

EUR-LEX. DIRETIVA (UE) 2015/1535. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015L1535&from=EN. Acesso em: 20 set. 2020.

EUR-LEX. Documento 52012DC0196 – Comunicação da comissão ao parlamento europeu, ao conselho, ao comitê das regiões. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:52012DC0196. Acesso em: 15 set. 2020.

INFORMATION COMMISSIONER'S OFFICE (ICO). **Age appropriate design**: a code of practice for online services. . Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/. Acesso em: 23 set. 2020.

_____. **Children's Online Privacy Protection Act of 1998**. Disponível em: https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905f-

c4b409&node =16%3A1.0.1.3.36&rgn=div5#se16.1.312_14. Acesso em: 25 set. 2020.

_____. Data Protection Act 2018. Legislation.gov.uk. Disponível em: https://www.legislation.gov.uk/ukpga/2018/12/part/5/crossheading/codes-of-practice/enacted. Acesso em: set. 2020.

LIMA, Caio César Carvalho. **LGPD:** Lei geral de proteção de dados comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. 2. ed. rev., atual e ampl. São Paulo: Thomson Reuters Brasil, 2019.

OLIVEIRA, Ricardo, COTS Márcio. **O legítimo interesse e a LGPD:** Lei geral de proteção de dados pessoais. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

PEQUENINO, Karla. **Avó obrigada a apagar fotografias dos netos das redes por tribunal nos Países Baixos.** PUBLICO. Disponível em: https://www.publico.pt/2020/05/22/tecnologia/noticia/avo-obrigada-apagar-fotografias-netos-redes-tribunal-paises-baixos-1917728. Acesso em: set. 2020.

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS. **Regulamento (EU) 2016/679.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT . Acesso em: 20 set. 2020.

ROSSATO, Luciano Alves; LÉPORE, Paulo Eduardo; CUNHA, Rogério Sanches. **Estatuto da criança e do adolescente comentado**: lei 8.069/1990 – artigo por artigo. 5. ed. rev, atual e ampl. São Paulo: Editora Revista dos Tribunais, 2013.

UNICEF. **Convenção sobre os Direitos da Criança**. Disponível em: https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca. Acesso em: 26 set. 2020.

YANDRA, Barbara Fernanda Ferreira; SILVA, Amanda Cristina Alves; SANTOS, Jéssica Guedes. **Lei geral de proteção de dados e a tutela dos dados pessoais de crianças e adolescentes:** a efetividade do consentimento dos pais ou responsáveis legais. Internet&sociedade, n. 1, v. 1, fevereiro de 2020, páginas 230-249. Disponível em: https://revista.internetlab.org.br/wp-content/uploads/2020/02/Lei-Geral-De-Protec%CC%A7a%CC%83o-De-Dados.pdf. Acesso em: 23 set. 2020.

# Capítulo V

# A PROTEÇÃO DE DADOS PESSOAIS DO CALIFORNIA CONSUMER PRIVACY ACT (CCPA): direcionamento à iniciativas tecnológicas brasileiras nos EUA

*Rangel Oliveira Trindade*[1]

*Leonardo Cordouro*[2]

## SUMÁRIO



**RESUMO**

O estudo da Lei de Privacidade do Consumidor da Califórnia (California Consumer Privacy Act – CCPA) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) tem como objetivo indicar semelhanças e diferenças entre os dois instrumentos jurídicos, apontando em quais temas os dois se aproximam e em quais temas os dois se afastam. Através de análise legislativa, bibliográfica e jurisprudencial, se demonstra quem são os sujeitos que são obrigados a seguir as previsões dos dois instrumentos, assim como quem são os que estão protegidos pelos ordenamentos, passando a descrever quais são as informações protegidas e suas formas de proteção. O estudo pretende direcionar o agente tecnológico que atua em inovação para que observe os aspectos técnicos das citadas leis. Como hipóteses, tem-se que existe um desconhecimento em relação ao teor do CCPA, e isto inviabiliza negócios, uma vez que um produto ou serviço tecnológico quase sempre utiliza dados pessoais; ainda, é realizada uma análise sobre a possibilidade que o CCPA tem para inspirar a redação de futura norma geral nos Estados Unidos no âmbito federal voltada à proteção de dados pessoais.

**Palavras-chave:** Dados Pessoais. Proteção de Dados. LGPD. CCPA.

[1] Doutorando em Direito - UFPR. Mestre em Direito e Relações Internacionais - UFSC. Pesquisador do GEDAI/UFPR. Professor universitário, advogado e consultor, atuando nos temas Direito, Tecnologia, Propriedade Intelectual e Inovação.

[2] Mestre em Ciências Jurídicas Internacionais - Universidade Clássica de Lisboa. Pesquisador do GEDAI/UFPR. Advogado e membro da Associação Portuguesa de Direito Intelectual e da Comissão de Inovação e Gestão da OAB/PR.

## INTRODUÇÃO

Em uma sociedade onde tecnologia e conhecimento caminham juntos, sendo que a tecnologia tem a capacidade de mudar tendências de toda a sociedade, e o conhecimento figura como uma das forças motrizes da mesma, há um volume expressivo de informações sendo coletadas e grande parte dessas informações são relacionadas aos indivíduos. Aí ocorre um fenômeno transfronteiriço onde agentes tecnológicos tornam seus negócios itinerantes, e migram em busca de um aprimoramento, seja este técnico, comercial, financeiro ou até mesmo regulatório, e um dos exemplos mais marcantes deste fenômeno é o deslocamento para a Califórnia, atual residência de grande parte das companhias que ditam tendências e criam inovações no mundo.

Um produto desenvolvido, validado e/ou aceito na Califórnia tem um grande potencial para ser recepcionado de maneira exitosa em grande parte do mundo; entretanto, a Califórnia atualmente possui uma legislação que trata justamente da intersecção entre o que as empresas que coletam dados pessoais podem fazer com eles e quais são os direitos dos sujeitos que têm estes dados coletados.

O tema ganha maior relevância porque não são somente as empresas que têm o tratamento de dados como atividade principal que se sujeitam às regras deste ordenamento, e sim qualquer empresa de qualquer segmento, desde que se enquadre nos parâmetros definidos pela lei.

O artigo apresenta uma análise comparativa elaborada por operadores do direito brasileiro, sendo este o viés do trabalho desenvolvido. Por fim, colhe impressões e tece observações acerca da CCPA como base de uma futura lei geral norte-americana.

## 1 INOVAÇÃO TECNOLÓGICA POR MEIO DE STARTUPS E DADOS PESSOAIS

Sociedade, informação e tecnologia são elementos indissociáveis da realidade contemporânea. Uma nova forma de organização das so-

ciedades com base tecnológica - mas principalmente pautada em dados - surge tão veloz quanto o avançar do hardware.

Os novos modelos de negócios, além de proverem espaço à liberdade individual, fazem das futuras corporações locais de cooperação entre equipes e empresas que em tempos atrás seriam concorrentes. Agora não se tem mais o foco na elaboração de coisas de valor que antes era limitada pela extensão dos requerimentos de capital produtivo. Importante é a observação de Nonaka, que identifica o resquício entre gerações:

> Em uma economia onde a única certeza é a incerteza, apenas o conhecimento é fonte segura de vantagem competitiva. Quando os mercados mudam, as tecnologias proliferam, os concorrentes se multiplicam e os produtos se tornam obsoletos quase da noite para o dia, as empresas de sucesso são aquelas que, de forma consistente, criam novos conhecimentos, disseminam-nos profusamente em toda a organização e rapidamente os incorporam em novas tecnologias e produtos. Essas atividades caracterizam a empresa criadora de conhecimento, cujo negócio exclusivo é a inovação contínua". (NONAKA, 2000)

As novas iniciativas em tecnologia reúnem um grupo de pessoas à procura de um modelo de negócios repetível e escalável, por meio de uma *startup*, trabalhando em condições de extrema incerteza, e que contempla conceitos que desafiam a inovação: tem-se um cenário de incertezas que dá à ideia e ao projeto de empresa "a chance de não darem certo". O modelo de negócios é como essa startup gera valor, transformando seu trabalho em dinheiro (SEBRAE, 2020). [3]

A viabilidade de um negócio nesta monta deve ser repetível e escalável, ou seja, amplia-se o público-alvo com um mesmo produto que é direcionado a lugares diferentes, e até mesmo países distintos. Havendo receita para começar a crescer, a startup passa a ganhar um grau de cres-

[3] SEBRAE: Extraído de https://www.sebrae.com.br/sites/PortalSebrae/artigos/o-que-e-uma-startup,6979b2a178c83410VgnVCM1000003b74010aRCRD. Acesso em: 19 set. 2020.

cimento por meio de investimentos e parcerias estratégicas para tornar o produto eficiente e muito rentável.

Existem estágios de crescimento, e o que importa abordarmos ao estudo é o estágio que estaria em um momento posterior à chamada "Série A" para o modelo de startups: o chamado estágio de crescimento ("Growth") ou estágio de expansão, momento em que existe a testagem de um produto tecnológico (se este for o escopo de negócio) a um público massivo quase definitivo, e até mesmo além fronteiras. O destino de empresas inovadoras de tecnologia tem sido o Vale do Silício, no estado norte-americano da Califórnia.

O Vale, por meio de empresas maiores já estabelecidas, oferece oportunidade para um startup testar seu produto ou serviço tendo o suporte logístico e tecnológico de um *player* de mercado, e, acima de tudo, trocar conhecimentos.

É necessário mencionar que os modelos de negócio, seja pelo formato startup ou empresa tradicional, precisam decidir como irão lidar com os dados que coletam e possuem, baseados em legislação vigente.

## 2 A ORIGEM DA LGPD E DA CCPA

O Capítulo Segundo da LGPD brasileira, que cuida do tratamento de dados pessoais, justifica a sua existência nos direitos do titular elencados no artigo 17, que ressalta o caráter fundamental de assegurarmos à pessoa a titularidade de seus dados pessoais e garantir os direitos fundamentais de liberdade, de intimidade e de privacidade.

Interessante acrescentar que o referido tratamento sensível ressalta o fato de que a LGPD em sua concepção compreende tanto o tratamento de dados digitais como também os não digitais; tanto aquele que ocorre dentro da internet, como aqueles que ocorrem fora dela (SALMEN; BELLÉ, nesta obra).

Nesta linha, a Lei nº 12.965/2014 conhecida como Marco Civil da Internet (MCI), em seu artigo 7º, ainda destaca os direitos do usuário de

internet, tudo para que possamos compreender a lógica sistemática brasileira. Ao assegurar, no inciso X, a exclusão definitiva dos dados pessoais que (o usuário) tiver fornecido a determinada aplicação da internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstos nesta lei (MCI), temos a consonância da mencionada tutela de direito embasadora do Capítulo Segundo da LGPD.

Apesar de alguns apontarem a origem da LGPD residindo única e exclusivamente no Ordenamento Europeu de Proteção de Dados (RGPD), a trajetória da sua promulgação é anterior a isso. Em 2010 o Ministério da Justiça realizou uma Consulta Pública sobre o tema "proteção de dados pessoais" e recebeu mais de 2.500 contribuições[4]. No dia 13 de junho de 2012 o Deputado Federal Milton Monti apresentou o Projeto de Lei 4.060/2012 que dispõe sobre o tratamento de dados pessoais e no dia 13 de agosto de 2013 o então Senador Antônio Carlos Valadares apresentou o Projeto de Lei do Senado (PLS 330/2013) que dispõe sobre a proteção, o tratamento e o uso dos dados pessoais.

No dia 15 de outubro de 2015 é apresentado pelo Relator do Projeto, o Senador Aloysio Nunes, um substitutivo ao Projeto de Lei do Senado 330/2013 que foi aprovado pela Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT). Já no dia 13 de maio de 2016, fruto da consulta pública do Ministério da Justiça iniciado em 2010, é apresentado pelo Poder Executivo o Projeto de Lei 5.276/16 que é apensado ao PL 4.060/12.

No dia 17 de março de 2018 é revelado o caso Cambridge Analytica[5] que, assim como nos Estados Unidos e na Europa, força a necessidade de debater a regulamentação do tratamento de dados pessoais; em sequência, no dia 25 de maio de 2018 o Regulamento Geral sobre a Prote-

[4] Disponível em https://www.conjur.com.br/2011-jan-25/consulta-publica-traca-diretrizes-lei-protecao-dados-pessoais e. Acesso em: 17 set. 2020.

[5] Disponível em https://tecnoblog.net/236612/facebook-cambridge-analytica-dados/ e. Acesso em: 17 set. 2020.

ção de Dados (RGPD) passa a ter eficácia plena na Europa e no mesmo dia o Relator do PLS 330/13 apresenta seu relatório e voto para submeter o Projeto ao Plenário. Entretanto, tanto o trâmite legislativo do PL 5.276/16 quanto do PL 4.060/2012 restam prejudicados em razão da apresentação do Projeto de Lei da Câmara 53/2018 que foi aprovado na Câmara. Ainda, nesta sequência o Projeto de Lei da Câmara 53/2018 também foi aprovado no Senado - que prejudicou o PLS 330/13 – assim, o PLC 53/2018 em 14 de agosto de 2018 é sancionado parcialmente e transformando-se na Norma Jurídica 13.709 de 2018 que ainda teve veto parcial.

Em relação à legislação norte-americana específica do Estado da Califórnia, Alastair Mactaggart[6] em novembro de 2017 propõe a mudança da lei de privacidade da Califórnia sob o título de CCPA (Lei de Privacidade do Consumidor da Califórnia (*California Consumer Privacy Act*), sendo que, em um primeiro momento o projeto é duramente criticado pela comunidade envolvida com tecnologia, mas eventos que aconteceram naqueles meses fazem a opinião popular mudar. Em abril de 2018 o Facebook retira sua oposição ao CCPA[7] logo após Mark Zuckerberg prestar testemunho em audiência no Senado sobre o escândalo envolvendo a Cambridge Analytica[8].

No mês de maio de 2018 a proposta legislativa de Mactaggart conseguiu a quantidade suficiente de assinaturas para ser levada a votação, sendo que no dia 28 de junho após alguns ajustes legislativos, o primeiro texto do CCPA é aprovado por unanimidade no Senado e na Assembleia. Logo após sua aprovação - em setembro do mesmo ano - o CCPA foi emendado para estar em conformidade com leis federais de privacidade e para fortalecer subsídios aos consumidores para exigir seus direitos, e este é o texto que se encontra vigente.

---

6 Disponível em https://iapp.org/about/person/0011a00000rimlxAAI/ e. Acesso em: 15 set. 2020.

7 Disponível em https://yubanet.com/california/facebook-withdraws-opposition-to-california-consumer-privacy-act/ e. Acesso em: 15 set. 2020.

8 Disponível em https://g1.globo.com/economia/tecnologia/noticia/mark-zuckerberg-depoe-ao-senado-sobre-uso-de-dados-pelo-facebook.ghtml e. Acesso em: 15 set. 2020.

A Califórnia, assim, se tornou o primeiro estado norte-americano a promulgar uma legislação abrangente sobre proteção de dados[9], e a nova lei de privacidade impôs obrigações e restrições significativas a muitas empresas que lidam com informações pessoais de residentes no Estado.

## 3 SEMELHANÇAS E DIFERENÇAS ENTRE OS SISTEMAS BRASILEIRO E NORTE-AMERICANO DE PROTEÇÃO DE DADOS

Comparar os sistemas brasileiro e da Califórnia de Proteção de Dados passa pela análise entre a Lei de Privacidade do Consumidor da Califórnia (*California Consumer Privacy Act* – CCPA) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD). Tem-se como objetivo indicar semelhanças e diferenças entre os dois instrumentos jurídicos, apontando em quais temas os dois se aproximam e em quais temas os dois se afastam. Possibilita-se assim uma compreensão pelo sujeito que já está em conformidade com a LGPD, para que tenha ciência dos procedimentos que devem ser adotados para atender às previsões legais do CCPA.

É fundamental demonstrar quem são os sujeitos que estão obrigados a seguir as previsões dos dois instrumentos, assim como quem são os sujeitos que estão protegidos pelos ordenamentos, passando a descrever quais são as informações protegidas, as formas de proteção das informações.

### 3.1 A quem se aplica:

O CCPA só será aplicado se a empresa tiver operações na Califórnia e se enquadrar em uma ou mais das seguintes opções[10]:

---

9 CALIFORNIA CONSUMER PRIVACY ACT, 2018 Cal. Legis. Serv. Ch. 55 (AB 375) (WEST)

10 Cal. Civ. Code § 1798.140(c)*: (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or*

(1) tenha uma receita anual bruta de mais de $25.000.000,00 (vinte e cinco milhões de dólares);

(2) anualmente compre, venda ou compartilhe as informações pessoais de mais de 50.000 clientes da Califórnia; ou

(3) se mais de 50% de seu rendimento anual for derivado da venda das informações pessoais dos clientes residentes na Califórnia.

E, ainda, à qualquer entidade que controle ou seja controlada por uma empresa que se enquadre em uma das três opções acima[11].

O escopo e o alcance territorial da LGPD neste ponto são muito mais amplos[12], além da diferença natural entre a legislação brasileira ter abrangência nacional e a legislação da Califórnia ter abrangência estadual; a LGPD abrange qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independen-

*financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:*
(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
*(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.*

11 Cal. Civ. Code § 1798.140(c): (2) *Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.*

12 Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

temente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional; ou a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou, ainda, os dados pessoais objeto do tratamento tenham sido coletados no território nacional. (LGPD, 2020)

## 3.2 Quem Protege

O CCPA em seu texto indica a proteção ao "consumidor" que trata como sendo uma pessoa física residente na Califórnia, conforme definido no "*Section 17014 of Title 18 of the California Code of Regulations*"[13], desde que esta pessoa seja identificada, inclusive por qualquer número e ou cadastro de identificação exclusivo (*Unique Identifier*)[14].

---

[13] Section 17014 of Title 18 of the California Code of Regulations: "*The term "resident," as defined in the law, includes (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents.*
*Under this definition, an individual may be a resident although not domiciled in this State, and, conversely, may be domiciled in this State without being a resident. The purpose of this definition is to include in the category of individuals who are taxable upon their entire net income, regardless of whether derived from sources within or without the State, all individuals who are physically present in this State enjoying the benefit and protection of its laws and government, except individuals who are here temporarily, and to exclude from this category all individuals who, although domiciled in this State, are outside this State for other than temporary or transitory purposes, and, hence, do not obtain the benefits accorded by the laws and Government of this State.*
*If an individual acquires the status of a resident by virtue of being physically present in the State for other than temporary or transitory purposes, he remains a resident even though temporarily absent from the State. If, however, he leaves the State for other than temporary or transitory purposes, he thereupon ceases to be a resident.*
*If an individual is domiciled in this State, he remains a resident unless he is outside of this State for other than temporary or transitory purposes."*

[14] *Cal. Civ. Code § 1798.140(x): "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.*

A LGPD aponta como Titular[15], ou seja, a pessoa protegida pela lei, a pessoa natural a quem se referem os dados pessoais que foram objeto de tratamento.

Apesar de realizarem abordagens diferentes, o CCPA indicando o consumidor e a LGPD indicando o titular dos dados pessoais, os dois instrumentos normativos se assemelham no efeito, ou seja, ambos se concentram em dados relacionados a uma pessoa física, mudando somente a forma de tratamento.

Deve ser destacada neste ponto a extraterritorialidade apresentada pelo CCPA, para qualquer pessoa física que tenha seu domicílio na Califórnia, mas que esteja fora por motivo temporário ou transitório.

## 3.3 Quais informações são protegidas?

As informações pessoais que identificam, se relacionam com algo ou descrevem alguém são capazes de ser associadas ou podem estar razoavelmente vinculadas, direta ou indiretamente, a um determinado consumidor ou família.

A definição legal inclui:

i. identificadores como nome real, pseudônimo, endereço postal, identificador pessoal único, identificador online, endereço de protocolo de internet, endereço de e-mail, nome da conta, número do seguro social, número da carteira de motorista, número do passaporte ou outros identificadores semelhantes;

ii. quaisquer categorias de informações pessoais descritas na subdivisão (e) da Seção 1798.80[16];

---

[15] Art 5º, V: Para os fins desta Lei, considera-se titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

[16] Seção 1798.80 (e) "*Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification*

iii. características individuais classificadas como protegidas pela lei da Califórnia ou federal[17];

iv. informações comerciais, incluindo registros de bens pessoais, produtos ou serviços adquiridos, obtidos ou considerados, ou outras compras ou consumir histórias ou tendências;

v. informações biométricas;

vi. informações sobre atividades na Internet ou em rede, incluindo, mas não se limitando a, histórico de navegação, histórico de pesquisa e informações sobre a interação de um consumidor com um site, aplicativo ou anúncio da Internet;

vii. dados de geolocalização;

viii. informações sonoras, eletrônicas, visuais, térmicas, olfativas ou semelhantes;

ix. informações profissionais ou relacionadas com o emprego;

x. informações sobre educação e que não estão publicamente disponíveis como informações de identificação pessoal, conforme definido na Lei dos Direitos Educacionais e Privacidade da Família (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99)[18];

xi. resultados extraídos de qualquer uma das informações previstas acima para criar um perfil sobre um consumidor refletindo as preferências, características, tendências psicológicas, predisposições, comportamento, atitudes, inteligência, habilidades e aptidões do consumidor.

---

*card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records*.

17 Raça, cor, nacionalidade, religião, gênero, deficiência, idade e status de cidadania.

18 20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99(4)(A): *For the purposes of this section, the term "education records" means, except as may be provided otherwise in subparagraph (B), those records, files, documents, and other materials which— (i)contain information directly related to a student; and (ii)are maintained by an educational agency or institution or by a person acting for such agency or institution*.

O CCPA não considera como "informações pessoais" as informações que estão publicamente disponíveis e indica como "publicamente disponível" as informações que são legalmente disponibilizadas em registros do governo federal, estadual ou local.

Entretanto, afirma categoricamente que "publicamente disponível" não são as informações biométricas coletadas por uma empresa sem o seu conhecimento do consumidor.

Outro aspecto relevante é a indicação de que as informações de consumidores que foram "anonimizadas" ou as chamadas informações agregadas de consumidores não podem ser consideradas como informações pessoais; entretanto, dados pessoais pseudonimizados podem ser qualificados como informações pessoais de acordo com o CCPA porque continuam sendo capazes de ser associados a um determinado consumidor ou família.

"Anonimizada" é a forma genérica que o CCPA apresenta para desidentificado ou ainda as informações agregadas de consumidores.

O CCPA não estabelece limites sobre o quanto uma empresa pode coletar, usar, reter, vender ou divulgar informações do consumidor, desde que sejam desidentificadas ou agregadas. No entanto, o CCPA estabelece um alto padrão para determinar em que estado os dados passam a ser considerados desidentificados, pseudonimizados ou agregados.

"Desidentificado" para o CCPA correspondem às informações que não podem identificar, relacionar, descrever, ser capaz de ser associado ou estar vinculado direta ou indiretamente, a um determinado consumidor, desde que a empresa que usa a informação desidentificada tenha adotado as seguintes rotinas:

I. tenha implementado salvaguardas técnicas que impedem a reidentificação do consumidor a quem as informações podem pertencer;

II. tenha implementado protocolos de negócios que proíbem especificamente a reidentificação das informações;

III. tenha implementado protocolos para evitar a liberação inadvertida de informações não identificadas; e

IV. não faça nenhuma tentativa de reidentificar as informações.

"Informações agregadas do consumidor" são as informações trazidas pela lei relacionadas a um grupo ou categoria de consumidores, das quais as identidades individuais dos consumidores foram removidas, ou que não estão vinculadas ou razoavelmente vinculáveis a qualquer consumidor ou família.

Por "pseudonimização" entende-se o processamento de informações pessoais de uma maneira que torne as informações pessoais não mais atribuíveis a um consumidor específico sem o uso de informações adicionais; desde que as informações adicionais sejam mantidas separadamente e estejam sujeitas a procedimentos técnicos e organizacionais para garantir que os dados pessoais não sejam atribuídos a um consumidor identificado ou identificável. Entretanto, as informações pseudonimizadas se diferem das informações desidentificadas, pois estas podem ser associadas a determinado consumidor ou família e não tem rotinas pré-definidas em lei para que um dado pessoal seja considerado pseudonimizado.

## 3.4 Formas de Proteção

A referida lei da Califórnia trás as seguintes formas de proteção:

> I. "Notificação aos titulares dos dados": o CCPA prevê que as empresas que estão sujeitas a sua regulamentação forneçam informações específicas aos consumidores assim como os, terceiros que obtenham estes dados também devem fornecer aos consumidores uma notificação e disponibilizar uma oportunidade de cancelar a revenda de informações pessoais adquiridas de outra empresa.

Este procedimento é realizado através do "*Privacy Notice*", que é um aviso de privacidade e é o documento que deve ser fornecido pela

empresa que utiliza os dados aos titulares. Este documento deve incluir, entre outras coisas, uma descrição de quais tipos de dados pessoais a empresa coleta, como a empresa usa esses dados, com quem compartilha os dados e como a empresa protege os dados.

O CCPA prevê, ainda, que a empresa que utiliza os dados do titular deve apresentar aos titulares dos dados, juntamente com o aviso de privacidade, os protocolos de privacidade adotados pela da empresa.

Este é um ponto que distancia muito o CCPA da LGPD, pois como no CCPA existe a possibilidade expressa da venda de dados pessoais, surgem regras específicas para quem compra estes dados, regras estas que não são encontradas de forma explícita na LGPD, entretanto não existe uma vedação expressa na LGPD para tal atividade, bastando que a empresa atenda a todos os requisitos previstos em seu texto para o exercício da atividade almejada.

> II. "Direito de acesso aos dados": o direito de acesso aos dados se refere à capacidade do titular de dados solicitar que uma empresa confirme se possui informações pessoais sobre ele, o tipo de informação pessoal que a empresa mantém sobre ele e, ainda, solicitar cópia das informações específicas que a empresa possui em arquivo[19].

Na CPPA as solicitações de acesso do titular dos dados à suas informações são chamadas de "*Data Subject Access Requests*" (*DSARs*) ou ainda "*Subject Access Requests*" (*SARs*).

A LGPD em seu Art. 18, I e II[20], apresenta previsões muito semelhantes, trazendo a possibilidade, mediante requisição do titular dos dados de confirmação da existência de tratamento por parte da empresa e de obter acesso aos seus dados.

---

19 Cal. Civ. Code § 1798.100(a): A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

20 Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados.

Neste tópico, a diferença entre as normativas é que o CCPA vai além de somente buscar a "confirmação da existência de dados" e o "acesso aos dados": através de uma solicitação à suas informações, o consumidor californiano pode indagar qual é a base legal utilizada pela empresa para a realização da operação, quais os prazos adotados pela empresa para guarda dos dados pessoais, como os dados foram obtidos, a existência de informações obtidas pela análise dos dados pessoais e, ainda, como terceiros podem ter acesso aos dados pessoais.

Outro ponto interessante é o entendimento do CCPA que, caso as solicitações sejam entendidas como abusivas, existe a possibilidade de realização de cobrança por parte da empresa para o fornecimento destes dados.

> III. "Direito de ser esquecido": o direito de ser esquecido refere-se à capacidade do titular dos dados solicitar que a empresa que detenha dados pessoais seus exclua as informações que detém. É importante destacar que o CCPA só se aplica a um número limitado de situações. Existem várias previsões legais[21] que desobrigam as empresas a ex-

[21] Cal. Civ. Code § 1798.105:*(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:*
*(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.(3) Debug to identify and repair errors that impair existing intended functionality.(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.(6) Engage in public or peer-re-*

> cluir as informações pessoais do titular dos dados, por exemplo: cumprir a Lei de Privacidade de Comunicações eletrônicas da Califórnia[22] ou detectar incidentes de segurança.

A LGPD a seu turno prevê em seu Art.18, VI[23], a possibilidade de realizar a eliminação de dados pessoais, mesmo que tratados com o consentimento do seu titular, indicando como excludente somente o previsto em seu art. 16[24].

> IV. "Direito de excluir informações pessoais para venda": Este é o tópico mais polêmico relacionado o CCPA e que causou várias críticas em relação às suas previsões, inclusive indicando que o CCPA seria apenas um normativo que regulamenta a venda de dados pessoais.

---

*viewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.(8) Comply with a legal obligation.(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.*

22 *California's Electronic Communications Privacy Act (CalECPa),* Disponível em https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178 e. Acesso em: 20/09/2020.

23 Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

24 Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

De plano deve-se saber que a premissa imputada de maneira tácita pelo CCPA é a possibilidade de venda dos dados pessoais[25] e neste diapasão são indicados procedimentos que devem ser seguidos para a realização da operação.

O primeiro procedimento trazido é a possibilidade do consumidor, a qualquer momento, comunicar a empresa que opera a venda de dados pessoais para não vender seus dados, este direito do consumidor é chamado de "*Opt-Out Right*". Além disso, a empresa que realizar a venda de informações pessoais deverá notificar o consumidor[26].

---

[25] Cal. Civ. Code § 1798.120: *(a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.*
*(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.*
*(c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."(d) A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.*

[26] Cal. Civ. Code § 1798.120: *(a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers: (1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.*
*(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:(A) Its online privacy policy or policies if the business has an online privacy policy or policies.(B) Any California-specific description of consumers' privacy rights.(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.(4) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling*

Existem, ainda, regras que estabelecem que em cada site de empresas que trabalham com a negociação de dados pessoais devem existir links de fácil acesso para que o consumidor possa optar pela não venda dos seus dados pessoas e se o consumidor optar pela não venda dos dados pessoais a empresa só deve fazer novamente este pedido depois de transcorridos 12 meses.

Exatamente como tratado no tópico sobre a notificação aos titulares de dados, considerando que a LGPD não trata efetivamente da negociação de dados pessoais, inexistem regras específicas para estes casos, sendo aplicadas somente as previsões gerais.

V. "Direito de receber serviços em termos iguais": O direito de receber serviços em termos iguais refere-se à proibição imposta pelo CCPA[27]

*personal information collected by the business about the consumer.(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.*

27 Cal. Civ. Code § 1798.125: *(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:*
*(A) Denying goods or services to the consumer.(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.(C) Providing a different level or quality of goods or services to the consumer.(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data.(2) A business that offers any financial incentives pursuant to this subdivision shall notify consumers of the financial incentives pursuant to Section 1798.130.*

> de discriminar consumidores que venham a exercer seus direitos conforme previsto no CCPA, ou seja, quando o consumidor exerce esse direito, a empresa que está sendo demandada é proibida de negar bens ou serviços a este consumidor, ou de cobrar um preço diferente ou ainda de impor penalidades.

Entretanto é importante destacar a previsão já indicada ao apresentar o "*Opt-Out Right*". Se a solicitação feita pelo titular dos dados pessoais for considerada abusiva, existe a possibilidade de a empresa realizar cobrança por essa atividade.

A LGPD também neste tema não é explícita e não apresenta nenhuma regra que objetiva se deva ser aplicada somente a essas situações de abuso por parte das empresas em relação a titulares que buscam ativamente valer os seus direitos.

## 4 CCPA e produto a ser testado com proteção de dados

É necessário mencionar que nos modelos de negócio, seja pelo formato startup ou empresa tradicional, precisa-se decidir como os agentes irão lidar com os dados que coletam e possuem. Segundo informações do CDPInstitute[28], as principais áreas de preocupação para tomadores de decisão são:

Acesso - quem no setor de marketing e em outras áreas terá acesso a dados específicos do cliente;

Armazenamento - por quanto tempo a empresa manterá as Informações de Identificação Pessoal (IIP); e

---

*(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.*

28 CDPInstitute: https://blog.cdpinstitute.org/Blog/Blog1038/Getting-ahead-of-privacy-legislation-is-crucial-for-data-driven-companies

Transparência - como a empresa garantirá que os clientes sejam mantidos informados sobre como e quais dados seus são usados.

O posicionamento dos setores de marketing direto, que levam o produto a ser testado ao consumidor, estabelece, primeiramente, políticas de *compliance*, e o momento posterior passa a ser uma política de privacidade que contemple as legislações operantes. O CDPInstitute cita a observação de Caitlin Fennessy, Diretora de Pesquisa do IAPP *(The International Association of Privacy Professionals*), que afirma que

> o pessoal de marketing direto está entre as principais pessoas que deveriam estar olhando para isso hoje. Os profissionais de marketing devem ser proativos ao garantir que haja uma conversa bidirecional entre eles e os especialistas em privacidade de sua empresa para garantir: 1) que tenham uma visão completa do trabalho com o marketing de dados; 2) que tenham uma compreensão clara do que são e não são dados pessoais; 3) que seja determinado quais proteções especiais devem ser implementadas em relação aos dados pessoais; e 4) que haja uma imagem clara dentro da empresa de quem precisa ser informado sobre como essas informações são tratadas e que um cronograma regular é estabelecido para o check-in." (CDPInstitute, 2020)

O CCPA demonstra a importância de permitir que os consumidores tenham acesso aos seus dados, dando-lhes a chance de cancelar seu envio, e certificando que os processos estão claramente definidos nas políticas de privacidade.

## 5.5 CCPA e Estados Unidos: futura lei geral?

O atual cenário jurídico que rege a proteção de dados nos Estados Unidos é complexo, e em regra o "direito à privacidade" desenvolvido na lei comum e na doutrina constitucional fornece poucas salvaguardas para o usuário comum da Internet. Propostas de criação de uma política federal unificada de proteção de dados por meio de uma lei geral inspirada no CCPA ganham força.

Embora o Congresso norte-americano tenha decretado uma série de leis projetadas para aumentar a segurança individual e os direitos de proteção de dados, a atual colcha de retalhos da lei federal geralmente se limita a participantes específicos do setor, tipos específicos de dados ou práticas de dados injustas ou enganosas. (MULLIGAN *et al,* 2019).

O Congresso, nesta perspectiva, deveria considerar a criação do CCPA que viesse a inspirar uma lei federal, e chegou a manifestar esta possibilidade. Como não houve a edição desta antecipando-se à iniciativa californiana, a manutenção da lei estatal existente sem alterações e o alcance que tem recebido por meio da indústria e do consumidor pelos Estados Unidos cada vez mais ressaltam a potencialidade de uma base segura para lei geral.

No entanto, a legislação sobre proteção de dados assume abordagens que buscam regular a coleta, o uso e a disseminação de informações pessoais on-line; nesta linha, tem sido dito que existem limitações impostas pela Primeira Emenda da Constituição dos Estados Unidos, uma vez que garante a liberdade de expressão como direito imutável. A limitação é incidente ao considerarmos os dados como sendo expressão pessoal / discurso, e esta linha de pensamento torna ainda mais complexa a adoção de uma legislação abrangente naquele país, diferentemente de nossa essência jurídico-constitucional que concebeu a LGPD.

## CONSIDERAÇÕES FINAIS

O trabalho buscou, através de análise legislativa, bibliográfica e jurisprudencial, direcionar o agente tecnológico que atua em inovação tecnológica - e que pretende operar em parcerias no Vale do Silício (Califórnia/EUA) - para que observe os ditames e aspectos legais, tudo sob a perspectiva de direito comparado funcional-moderado. Como opera no país adequando-se à LGPD brasileira, ao lançar-se ao mercado externo para teste e consolidação de um produto tecnológico, revela desconhecimento em relação ao teor do CCPA.

Partindo da análise ponto a ponto da LGPD comparada ao CCPA, este estudo indicou semelhanças e diferenças entre os dois instrumentos jurídicos. Em linhas finais, repisamos de tratarem de abordagens diferentes: o CCPA volta-se ao consumidor, e a LGPD indica o titular dos dados pessoais. Ambos os instrumentos normativos se assemelham no efeito, uma vez que se concentram em dados relacionados a uma pessoa física, mudando somente a forma de tratamento.

Pode-se ainda salientar que o referido "California Act" não estabelece limites às empresas ao que elas podem coletar, usar, reter, vender, ou ao que será divulgado em relação a informações do consumidor, mas estabelece um alto *standard* para o estágio de desidentificação e pseudonimização dos dados, ponto não especificado na LGPD.

Chama a atenção, ainda, a disposição no CCPA que vai além da busca de "confirmação da existência de dados" e do "acesso aos dados". Um consumidor californiano pode requerer a uma empresa a base legal utilizada pela empresa para a realização de sua operação, bem como outras informações sensíveis em relação ao acesso ocorrido a seus dados pessoais.

Ressaltamos ainda os pontos que não são objeto da lei brasileira e que estão presentes no Vale do Silício: lá existe a possibilidade expressa da venda de dados pessoais, e existem regras específicas para quem compra estes dados, regras estas que não são encontradas de forma explícita na LGPD.

A perspectiva de direito comparado nos dá, por fim, algo que poderia ter sido incorporado pela LGPD e que é constante no CCPA, por medida de inteiro direito: se uma solicitação feita pelo titular dos dados pessoais for considerada abusiva, existe a possibilidade da empresa realizar cobrança por essa atividade.

Pode-se afirmar que a existência nos Estados Unidos de uma base legal para criação de uma lei geral protetiva de dados pessoais espelha o fluxo informacional mundial que merece ser acompanhado de ponta a ponta. Em um cenário de existência do RGPD europeu, e muito antes,

proclamado na Declaração Universal dos Direitos Humanos de 1948 por meio de seu artigo 12 - que deu azo à proteção jurídica dos dados pessoais fundada no direito ao respeito pela vida privada (DIAS PEREIRA, nesta obra) - inspira algumas nações a criarem suas legislações, o passo a ser dado na direção da sociedade 4.0 primeiramente passa por enfrentar juridicamente os novos desafios regulatórios que se impõem.

Os novos modelos de negócios voltados ao consumidor, moderno *hub* de dados, motivam a inovação para que considere paradigmas que pertencem a este novo momento da sociedade informacional e que refletem a interdependência dos direitos individuais em relação a proteção e circulação de dados pessoais.

## REFERÊNCIAS

ALMEIDA SANTOS, Fabíola Meira de. TALIBA, Rita. **Lei geral de proteção de dados no brasil e os possíveis impactos**. Revista dos Tribunais, vol. 998/2018, p. 225 – 239, dez. 2018, DTR\2018\22545.

BARBIERI, Carlos. **Governança de Dados**. Rio de Janeiro: Alta Books Editora, 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOYNE, Shawn Marie. **Data Protection in the United States**. Downloaded from https://academic.oup.com/ajcl/article-abstract/66/suppl_1/299/5048964 by guest on 20 August 2018.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 6 set. 2020.

_____. **Lei 12.965 de 23 de Abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 set. 2020.

BUKATY, Preston. **The California Consumer Privacy Act (Ccpa): An Implementation Guide**. Paperback, 2019.

CALIFORNIA'S CONSUMER PRIVACY ACT **(CCPA)**, 2018 Cal. Legis. Serv. Ch. 55 (AB 375) (WEST). Disponível em https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375. Acesso em: 20 ago 2020.

CALIFORNIA'S ELECTRONIC COMMUNICATIONS PRIVACY ACT **(CalECPa)**, Disponível em https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178. Acesso em: 20 set. 2020.

CAVE, Bryan & PAISNER, Leighton. **California Consumer Privacy Act (Ccpa) – Pratical Guide**. Disponível em https://ccpa-info.com/wp-content/uploads/2019/09/bclp-practical-guide-to-the-ccpa.pdf, CBPL, fevereiro, 2020.

CDPInstitute. **Getting ahead of privacy legislation is crucial for data driven companies**, 2020. Disponível em https://blog.cdpinstitute.org/Blog/Blog1038/Getting-ahead-of-privacy-legislation-is-crucial-for-data-driven-companies. Acesso em: 14 set. 2020.

CUEVA, Ricardo Villas Bôas. **Proteção de dados pessoais no Judiciário**. Revista do Advogado (AASP) nº 144, pp 134-140, novembro de 2019.5.

DETERMANN, Lothar. **California Privacy Law – Practical Guide And Commentary** U.S. Federal and California Law 3rd Edition, IAPP, 2018.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei geral de proteção de dados. 2 ed. – São Paulo: Thompson Reuters Brasil, 2019.

MALDONADO, Viviane Nóbrega. GUTIERREZ, Andriei. **A estratégia brasileira para a transformação digital e as questões que dela emergem no que se refere à proteção de dados pessoais**. Revista dos Tribunais, vol. 993/2018, p. 293 – 304, jul. 2018, DTR\2018\15758.

MALDONADO, Viviane Nóbrega. BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Thompson Reuters Brasil.

MULLIGAN, Stephen P; FREEMAN. Wilson C; LINEBAUGH, Chris D. **Data Protection Law:** An Overview - March 25, 2019 - Congressional Research Service. Disponível em https://crsreports.congress.gov R45631. Acesso em: 09 set. 2020.

NONAKA, Ikujiro. A empresa criadora de conhecimento. In: **HARVARD BUSINESS REVIEW. Gestão do Conhecimento.** Tradução: Afonso Celso da Cunha Serra. Rio de Janeiro: Campus, 2000.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei nº 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

PIURCOSKY, Fabrício Pelloso, COSTA, Marcelo Aparecido, FROGERI, Rodrigo Franklin e CALEGARIO, Cristina Lelis Leal. **A lei geral de proteção de dados pessoais em empresas brasileiras:** uma análise de múltiplos casos. Suma de Negocios Vol. 10 Num. 23 (Julio - Diciembre) 2019 - Tipo: Artículo de Investigación. Disponível em: http://dx.doi.org/10.14349/sumneg/2019.V10.N23.A2. Acesso em: 30 jul 2020.

SANTIN, Altair Olivo. **Os desafios e impactos da lei geral de proteção de dados**. Migalhas de Peso. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/312847/os-desafios-e-impactos-da-lei-geral-de-protecao-de-dados. Acesso em: 30 jul 2020.

# Seção III

## Da autodeterminação à discriminação: a proteção subjetiva de dados pessoais

# Capítulo I

# DIREITO À AUTODETERMINAÇÃO INFORMATIVA E O EXERCÍCIO DEMOCRÁTICO: reflexões sobre as experiências alemã e brasileira

*Alice de Perdigão Lana*[1]

*Marcelle Cortiano*[2]

**SUMÁRIO:**



**RESUMO**

A pesquisa propõe a leitura crítica das relações entre o direito à autodeterminação informativa, fundada nas prerrogativas subjetivas de controle sobre os próprios dados pessoais, e a efetiva participação democrática, atribuindo a adequação do exercício à imprescindibilidade de sólida autonomia individual. A partir do método funcional de direito comparado, busca-se revisitar os históricos socioculturais alemão e brasileiro no tratamento de dados pessoais, a fim de identificar convergências e rupturas entre os dois ordenamentos, com destaque às abordagens impulsionadoras das competências democráticas como forma de cumprimento de demandas sociais. A conclusão estrutura-se no sentido da necessidade de fortalecimento e constante aperfeiçoamento das regulações vigentes em diálogo com a sociedade, sobretudo na consolidação da proteção dos dados pessoais como garantia fundamental, vez que representa a via ponderada para assegurar a autonomia individual e o exercício democrático, tanto na experiência teutônica quanto na brasileira.

**Palavras-chave:** Autodeterminação informativa. Democracia. Alemanha. Direito comparado. Intervenção regulatória.

[1] Mestranda em Direito das Relações Sociais na Universidade Federal do Paraná/UFPR. Bolsista CAPES. Pesquisadora do Grupo de Estudos em Direito Autoral e Industrial - GEDAI/UFPR e do Grupo Direito, Biotecnologia e Sociedade - BIOTEC/UFPR. E-mail: aliceplana@gmail.com

[2] Mestranda em Direitos Humanos e Democracia (UFPR). Pesquisadora do Grupo de Estudos em Direito Autoral e Industrial - GEDAI/UFPR. Membro da Clínica de Direito e Arte da UFPR. Advogada e publicitária. E-mail: marcellecortiano@gmail.com.

## 1 INTRODUÇÃO

A despeito das previsões elencadas pelas constituições contemporâneas, uma democracia não se origina exclusivamente a partir do texto constitucional. O efetivo exercício das práticas democráticas é fruto, dentre outras circunstâncias, de aspectos educacionais, socioculturais e políticos, que envolvem as relações intersubjetivas e o desenvolvimento funcional de determinada coletividade. Por outro lado, as condições para que as competências democráticas sejam desenvolvidas e exercidas têm origem constitucional e legal. No Estado Democrático de Direito, é papel do ordenamento jurídico oportunizar e garantir este desenvolvimento, a partir de dispositivos que promovam a participação efetiva, a igualdade e universalidade do voto, o entendimento esclarecido e a autonomia cidadã.

O desempenho de todas estas competências está interrelacionado. Assim, para além de instituições sólidas e procedimentos eficazes, uma democracia funcional exige como condição central a presença de efetiva consciência democrática – expresso pelo voto unitário, que representa, em última análise, a vontade popular. O componente subjetivo, em sua autonomia, é o responsável por agregar tal elemento na base das demais competências demandadas pela proposta da democracia.

A autonomia cidadã, a seu turno, sujeita-se à necessária proteção da privacidade individual e, especialmente, da realização do direito à autodeterminação informativa. Em síntese, esse aspecto refere-se à capacidade de determinada pessoa de controlar a circulação de informações a seu respeito, configurando-se imprescindível para o desenvolvimento da personalidade individual. Nesse sentido, a relação de cada cidadã e cidadão com seus dados pessoais é peça fundamental para compor o arranjo de uma sociedade democrática, à medida em que esses dados substancializam a identificação particularizada dos membros sociais. A liberdade de manifestar-se, a possibilidade de acessar serviços de assistência social e a autonomia do exercício do voto são apenas alguns exemplos de atividades consumadas pela existência da identidade singular de cada indivíduo.

Na internet, o manuseio desses dados – pelos procedimentos de coleta, tratamento, utilização e armazenamento – têm consolidado o protagonismo da discussão sobre a circulação de informações pessoais na sociedade em rede, permeada por processos informatizados e automatizados. A individualização e a identificação oportunizadas por esses dados faz com que sejam essenciais para o desempenho das atividades de governo eletrônico, sobretudo aquelas ligadas à cidadania digital e à realização de procedimentos institucionais online.

Contudo, a excessiva quantidade de informação que circula na rede e as incalculáveis formas de tratamento e aplicação de elementos na identificação pessoal, em muitas ocasiões por procedimentos opacos e pouco inteligíveis, faz com que a segurança dos dados pessoais seja uma questão premente e delicada. A exposição a riscos – desde coleta sem consentimento até utilização para fins desviantes ou ilícitos – exige a adoção de medidas compatíveis dos agentes envolvidos. Busca-se, desse modo, a neutralização dos efeitos potencialmente nocivos e a salvaguarda dos direitos dos indivíduos cujos dados estão circulando, sem, contudo, causar interferências descabidas na aplicação das tecnologias de informação e comunicação.

Não se trata, evidentemente, de uma consequência exclusivamente atribuída a particularidades locais. A ubiquidade das interações tecnológicas e a desterritorialização da internet exigem que todas as comunidades que sustentam um discurso democrático elaborem maneiras de enfrentar a temática, a fim de preservar as garantias de seus componentes sociais e a própria continuidade do sistema político. Nesse sentido, a observação da experiência de ordenamentos jurídicos que tratam formalmente o tema e suas implicações sociais há um período mais longo mostra-se uma ferramenta profícua no estabelecimento de diálogos pela identificação de padrões convergentes. Adicionalmente, opera também como mecanismo de elaboração de questionamentos e modulação de propostas, a serem suscitadas e eventualmente aplicadas à realidade e às peculiaridades socioculturais locais, na medida de suas demandas.

Os itens a seguir estruturam-se a partir da projeção de um olhar analítico da abordagem da proteção de dados pessoais e suas interlocuções com o exercício democrático presentes nas práticas alemã e brasileira. No desenvolvimento da pesquisa, busca-se traçar correspondências jurídicas e especificidades sociais e culturais, além da identificação de possíveis aprendizados que a regulamentação nacional pode depreender da experiência teutônica.

A necessidade da tutela da privacidade, e mais especificamente da proteção de dados pessoais, tem como pressuposto a busca pela compensação da assimetria que se revela na detenção de poder informacional. A proposta do texto pretende, assim, evidenciar como a inevitável relação entre o controle sobre os próprios dados e o exercício democrático deve ser alcançada por adequadas práticas regulatórias dialogadas entre o Estado e o corpo social, que neutralizem, ou ao menos atenuem, as desigualdades informacional e tecnológica e a eventual inobservância às garantias fundamentais.

## 2 A ABORDAGEM COMPARATIVA FUNCIONAL: UMA LEITURA CONVENIENTE

A busca por possibilidades para dirimir conflitos regulatórios e preencher lacunas diversas – ou puramente a satisfação do interesse do pesquisador – contempla um caminho promissor na comparação entre ordenamentos jurídicos distintos. Especialmente na virada do século XIX para o século XX, recorreu-se imensamente à viabilidade dos métodos de direito comparado, que passavam a ser valorizados em uma perspectiva propriamente científica, para além de seu mero caráter jurídico-político (CURY, 2014, p. 177).

Em vista de severas críticas atribuídas à técnica, o decorrer do século XX presenciou um enfraquecimento do modelo comparativo de obtenção de resultados científicos e solução de problemas jurídicos. As discordâncias pautavam-se, acima de tudo, no argumento da alegada superficialidade do procedimento, que consistiria em mera aproximação de

enunciados normativos de realidades por vezes incompatíveis, reduzindo a análise a um cotejo positivista de afinidades ou contrastes deslocados.

O desenvolvimento do método funcional aplicado ao direito comparado buscou contestar tais julgamentos, ao propor uma sistemática orientada pela identificação de funções conciliáveis e seus efeitos na resolução de conflitos que afligem dado ordenamento. Nesse sentido, a leitura comparativa funcionalista supera o mero exame do texto positivado para abordar também entendimentos doutrinários e jurisprudenciais (CURY, 2014, p. 178), oportunizando um processo comparativo analítico e viável.

O foco do comparatista passa a ser, portanto, a função jurídica efetiva da adoção de determinada alternativa no saneamento de adversidades jurídico-normativas. Isso permite o exame paralelo de dilemas locais – semelhantes aos do ordenamento estrangeiro em questão – encaminhados por maneiras diversas, mas cujos remédios em realidade preenchem a mesma função da medida adotada internacionalmente. Conforme sintetiza Paula Maria Nasser CURY, o emprego deste protocolo metodológico permite reconhecer "normas jurídicas ou sociais que desempenhem o mesmo papel (função)" que normativas identificadas em outros sistemas regulatórios (2014, p. 179).

Após críticas ao método, em especial em função da problemática presunção de similitudes (DE CONINCK, 2010, p. 332) e da ausência de análise diferencial das "jurisculturas" (LEGRAND, 2018), passou-se a adotar uma versão ajustada do método funcional, que absorveu parte das críticas de modo a se moldar em um funcionalismo moderado.

Diferentemente de sua versão tradicional, a corrente moderada do funcionalismo aplicado ao direito comparado não teria a pretensão de monopolizar os métodos voltados a esta aproximação. Este aspecto é especialmente notável, vez que destaca a possibilidade de aplicação da abordagem apenas para determinados casos e reconhece eventuais limitações da proposta funcional.

Conclusivamente, Paula Maria Nasser CURY (2014, p. 184) é categórica: o comparatista não dispõe de um método impecável e absoluto

e sua opção deve ser pautada a partir das alternativas apresentadas de modo a alcançar com a maior adequação possível sua finalidade científica.

Nas áreas de aplicação que cercam a análise do objeto proposto na pesquisa – qual seja, a relação entre o direito à autodeterminação informativa e o exercício democrático – reconhece-se a possibilidade de uma oportuna leitura a partir da abordagem comparativa funcional, extraindo-se critérios cabíveis de ambas as correntes, tradicional e moderada. Além disso, vale-se da noção de juriscultura para investigar os vestígios interdisciplinares que revelam fundamentos e circunstâncias da elaboração dos direitos alemão e brasileiro em relação à proteção de dados.

## 3 A PROTEÇÃO DE DADOS PESSOAIS NA ALEMANHA

A Alemanha é frequentemente apontada como pioneira mundial na discussão jurídica sobre proteção de dados pessoais. A consolidação da efetiva existência de um direito à autodeterminação informativa (*informationelle Selbstbestimmung*) remonta, indubitavelmente, à consagrada decisão do Tribunal Constitucional Federal alemão de 15 de dezembro de 1983. Na ocasião, pacificou-se o entendimento de que o indivíduo teria direito a controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos à sua pessoa (DONEDA, 2011, p. 95), resultando na determinação da inconstitucionalidade de trechos do censo populacional proposto no ano anterior.

### 3.1 A decisão paradigmática de 1983: antecedentes e repercussões

O posicionamento da corte constitucional alemã foi a responsável por pavimentar caminhos fundamentais no tratamento de dados pessoais e em sua validação como direito subjetivo básico. Os reflexos da decisão de 1983 permanecem ainda nítidos no ordenamento do país;

compreender seus critérios e o direito à autodeterminação informativa é, portanto, a peça chave para assimilar a perspectiva alemã sobre a proteção de dados (HORNUNG; SCHNABEL, 2009).

A fim de revisitar o pano de fundo que culminou neste julgamento, há de se regressar algumas décadas ainda, para possibilitar uma leitura ampliada de como a necessidade de garantia da privacidade – e, consequentemente, de proteção de dados pessoais – fundou suas estruturas no território europeu e espraiou-se para os demais ordenamentos.

No contexto global, a Declaração Universal de Direitos Humanos de 1948 consolidou a necessidade de observância ao direito à privacidade, em seu artigo 12, na esteira do entendimento consagrado pelos juízes estadunidenses Samuel D. WARREN e Louis D. BRANDEIS (1890, p. 193) na publicação em que desenvolvem o "*right to be let alone*". No texto em questão, a definição da garantia da privacidade assentava-se em bases individuais, vinculadas especialmente à inviolabilidade da intimidade do sujeito frente a invasões de tablóides da época – facilitadas pela nova tecnologia da fotografia "instantânea".

Especificamente na Alemanha, a crescente automatização de variados processos econômicos e sociais durante a década de 60 – incluindo o processamento de dados – descortinou uma tendência à valorização das conveniências trazidas pelo aparato tecnológico em detrimento de eventuais efeitos prejudiciais à privacidade individual. Iniciativas ainda esparsas indicavam os potenciais riscos às garantias subjetivas, tendo os esforços sido convertidos em regramentos apenas em instâncias locais.

J. Lee RICCARDI (1983) relata que, embora o Parlamento alemão sinalizasse preferências no sentido de uma regulação geral para se dirigir ao tema do processamento de dados, a primeira proposta com este fim, datada de 1973, foi ratificada apenas quatro anos mais tarde, após numerosas manifestações divergentes e ajustes por parte dos envolvidos no procedimento legislativo.

Assim, a *Bundesdatenschutzgesetz* (BDSG), ou Lei Federal Alemã de Proteção de Dados, de 27 de janeiro de 1977, representou a tentativa de

estabilizar, a nível nacional, a proteção subjetiva contra o uso indevido de dados pessoais no processamento de dados. Como registrado, anteriormente a este marco regulatório pelo menos 130 outros diplomas legais já abordavam, de alguma maneira, o manuseio de dados pessoais no país (RICCARDI, 1983, p. 245), denotando o pioneirismo alemão no enfoque do assunto, ainda que em âmbito regional. Conquanto encerrasse variadas lacunas e imprecisões, a BDSG representou um passo fundamental para o fortalecimento do debate acerca da garantia de proteção de dados pessoais no país.

No ano de 1982, o Parlamento determinou, por unanimidade de votos, a condução de um censo populacional que ocorreria no ano seguinte. A comoção popular foi intensa, motivada pelo caráter invasivo da coleta de informações – mais de 160 questões a serem respondidas por cada habitante – e ainda pela falta de transparência e inteligibilidade dos mecanismos de processamento de dados (HORNUNG; SCHNABEL, 2009).

O *Bundesverfassungsgericht* (Tribunal Constitucional Federal) embasou seu entendimento nos artigos 1.1 e 2.1 da *Grundgesetz*, a Lei Fundamental da República,[3] para declarar a existência de um "direito à autodeterminação informativa", destacando ainda que o censo, nos moldes em que foi concebido, configuraria uma interferência injustificada, em especial a esta garantia (BUNDESVERFASSUNGSGERICHT, 1983, p. 1). Os trechos da proposta que previam a comparação e a transmissão dos dados pessoais a repartições públicas seriam, portanto, incompatíveis com os dispositivos da Constituição Alemã.

A coleta de dados foi reformulada, em observância à declaração de inconstitucionalidade, e ocorreu no ano de 1987 – não sem alguma resistência da esfera social, que permanecia contrária à invasividade da consulta. Não obstante a realização do censo, o pronunciamento do *Bundesverfassungsgericht* em 1983 é considerado o marco decisivo no esta-

[3] O artigo 1.1 da Constituição Alemã refere-se à inviolabilidade da dignidade humana, enquanto o 2.1 refere-se ao direito ao desenvolvimento da personalidade. Fonte: DEUTSCHER BUNDESTAG. **Grundgesetz für die Bundesrepublik Deutschland**. 23 maio 1949. Disponível em: https://www.bundestag.de/gg. Acesso em: 05 set. 2020.

belecimento das disposições constitucionais e infraconstitucionais direcionadas ao tratamento e proteção de dados pessoais que surgiriam nos anos seguintes.

## 3.2 A consolidação da autodeterminação informativa e o trajeto até o Regulamento Geral de Proteção de Dados (RGPD)

É perfeitamente possível reconhecer traços e influências do extenso histórico alemão que tangencia o tema ao se observar a atual regulamentação europeia de proteção de dados. Formalmente, porém, pode-se considerar que a etapa basilar em nível continental para a consolidação efetiva do Regulamento Geral de Proteção de Dados (RGPD) deu-se com o estabelecimento, em 1995, da Diretiva Europeia de Proteção de Dados (Diretiva 95/46/EC).[4]

Essa diretiva buscava assegurar aos indivíduos o controle de seus dados pessoais (BIONI, 2019, p. 205; BIONI, 2015, p. 43) e adotava concepções da Convenção 108, de Strasbourg, do Conselho da Europa – que foi influenciada pelas diretrizes da Organização para Cooperação e Desenvolvimento Econômico (OCDE) para Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais. A diretiva não estabelecia somente o direito de controle dos dados pessoais pelo titular, mas determinava também deveres aos responsáveis pelo tratamento destes dados, expandindo o espectro do controle para todos os sujeitos inseridos na cadeia do fluxo informacional (BIONI, 2019, p. 205). Além disso, proibia a transferência de dados pessoais a países cujos mecanismos voltados a essa proteção não atingissem níveis adequados.

[4] Nesse sentido, Hornung e Schnabel (2009, p. 87) relatam que a própria Diretiva 95/46/EC normatizou princípios contidos na decisão do Tribunal Constitucional Federal Alemão de 1983. Ainda que tais princípios não tenham sido "criados" pelo *Bundesverfassungsgericht*, foram por ele formalizados e posteriormente fixados em âmbito continental, destacando novamente o protagonismo alemão na regulamentação do tema e os efeitos da declaração, décadas mais tarde.

Embora não gerasse efeitos diretos em termos formais, tendo sua implementação condicionada à adaptação dos ordenamentos jurídicos nacionais, uma característica polêmica da Diretiva 95/46/EC foi justamente seu vasto alcance, ao atingir não apenas empresas europeias, mas "qualquer companhia que faça uso de equipamentos ou meios de processamento de dados na Europa, salvo para mero trânsito, bem como para qualquer empresa que colete informações de cidadãos europeus" (LEONARDI, 2011, pp. 331-332).

Para os alemães, a necessidade de adaptação ao regramento continental veio na esteira de alterações que já eram operadas na BDSG desde a célebre decisão do Tribunal Constitucional. Em 1990, a Lei Federal Alemã de Proteção de Dados de 1977 sofreu sua primeira grande reforma, em larga medida com a finalidade de incorporar os reflexos do direito à autodeterminação informativa que se consolidava. Seis anos após a entrada em vigor da Diretiva 95/46/EC, foi enfim promulgada a nova *Bundesdatenschutzgesetz,* com a ressalva feita pela Comissão Europeia de que os parlamentares alemães não teriam feito a completa transposição dos dispositivos da normativa continental para a BDSG que entrava em vigor (HORNUNG; SCHNABEL, 2009, p. 86).

Paralelamente às diretrizes continentais, mantiveram-se atuantes as operações legiferante e jurisprudencial alemãs em relação à proteção de dados. As décadas de 2000 e 2010 presenciaram decisões notórias do Tribunal Constitucional Federal alemão no tocante à circulação de informações pessoais no ambiente digital, bem como relevantes ajustes no regramento sobre retenção de dados por serviços de telecomunicações, reafirmando o protagonismo do direito à autodeterminação informativa como critério majoritariamente aplicável.

No território europeu, a implementação da Diretiva 95/46/EC em variados ordenamentos jurídicos locais cimentou o caminho para as discussões a respeito de um regime geral, cuja proposta foi enfim formalizada em 2012, apresentada como uma reforma da diretiva vigente. Quatro anos de intensas deliberações culminaram na aprovação, em 2016, do Regulamento UE 2016/679 – o RGPD –, e sua entrada em vigor se deu

em 2018. Já no primeiro Considerando, a regra geral europeia declara que a proteção relativa ao tratamento de dados pessoais é um direito fundamental do indivíduo, enquanto o Considerando 7 reforça que cada pessoa singular deve ter o direito de controlar o uso que é feito de seus dados pessoais.

Ainda em relação ao titular de dados, o RGPD dispõe no capítulo III (artigos 12 a 23) normas especificamente direcionadas à proteção das pessoas singulares. Na mesma esteira da diretiva anterior, as previsões abrangem a exigência de procedimentos transparentes e acessíveis, de notificações sobre a origem da coleta, de possibilidades de acesso, retificação e eliminação e de restrições ao processamento, e ainda de oposição e de não sujeição a decisões individuais automatizadas. Na Alemanha, a recepção do diploma resultou em um novo pacote de reformas à *Bundesdatenschutzgesetz*, operacionalizado durante o ano de 2017. A nova BDSG – agora designada *Datenschutz-Grundverordnung* (DSGVO), para se referir ao regulamento geral – substituiu a anterior em 25 de maio de 2018, quando o RGPD entrou em vigor em todo o continente.

A implementação do RGPD teve notável influência na elaboração do texto da Lei Geral de Proteção de Dados (LGPD) brasileira. Contudo, vale destacar que a discussão em território nacional a respeito da necessidade da proteção de dados pessoais não surgiu apenas após a edição do diploma geral europeu.

## 4 A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A garantia de oferta de serviços públicos eficientes e a tutela do interesse e segurança públicos são argumentos que dialogam diretamente com o inevitável manuseio de dados pessoais (LUZ; LOUREIRO, 2018). A exemplo da experiência internacional, o avanço vertiginoso do aparato tecnológico naturalmente impulsionou a discussão sobre a necessidade de proteção das informações individuais no ordenamento jurídico brasileiro.

Não obstante sua urgência, as providências brasileiras avançaram durante décadas em marcha relativamente moderada, enfim excedendo a abordagem constitucional estruturante e a legislação esparsa apenas recentemente, com a efetiva consolidação de um instrumento regulador específico.

## 4.1 As disposições sobre a proteção de dados e a necessidade de um regramento geral

O direito à privacidade figura no rol de garantias fundamentais da Constituição da República Federativa do Brasil de 1988, que determina, no inciso X, a necessidade de proteção da intimidade e da vida privada. No que tange à proteção informativa, o inciso XII dispõe sobre a inviolabilidade das correspondências e das comunicações telegráficas, de dados e telefônicas, dirigindo-se de maneira genérica ao sigilo das informações pessoais.

Ainda dentre os direitos fundamentais elencados no artigo 5º, três incisos referem-se ao direito de acesso à informação (SALGADO, 2015, p. 5) – uma das facetas da proteção de dados e da autodeterminação informativa. Inicialmente, o inciso XIV estabelece que "é assegurado a todos o acesso à informação [...]". Já o inciso XXXIII prevê que "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo e geral [...]".

O inciso LXXII dispõe sobre o *habeas data*, ação constitucional que objetiva "assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público" ou retificar dados. Esse remédio jurídico oponível ao Estado é uma das formas de concretização do direito de proteção aos dados pessoais para a população brasileira, pois permite que pessoas físicas e jurídicas conheçam e retifiquem informações pessoais.

Alguns anos depois, foi promulgado o Código de Defesa do Consumidor - CDC (Lei nº 8.078/1990), que também contém disposições espar-

sas a respeito da proteção dos dados pessoais dos consumidores, especialmente no artigo 43. Em seu § 2º, há a previsão de dever de notificação prévia do consumidor sobre a abertura de um banco de dados por ele não solicitado. Já o § 3º prevê direitos de acesso, retificação e cancelamento de informações errôneas.

A Lei de Acesso à Informação (Lei nº 12.527/2011) é outro marco importante na discussão sobre proteção de dados face ao poder público, pois estabelece procedimentos que devem ser respeitados pelos entes estatais para assegurar o direito fundamental de acesso à informação. A Lei do Cadastro Positivo (Lei nº 12.414/2011) também regula questões relacionadas a dados pessoais, em especial nos artigos 4º e 5º, que versam sobre os direitos do cadastrado e as autorizações do gestor do banco de dados.

O Marco Civil da Internet (Lei nº 12.965/2014), que regula os direitos e garantias do cidadão nas relações travadas na internet, buscou efetivar o direito do usuário de controlar seus próprios dados, adotando uma adjetivação do consentimento, que deve ser livre, expresso e informado (BIONI e LIMA, 2015, p. 270). No artigo 7º do mesmo diploma legal, há disposições acerca das obrigações do responsável pelo tratamento de dados pessoais, que deverá prestar informações claras e completas (inciso VI), com cláusulas contratuais destacadas para o consentimento (inciso IX), dando publicidade às políticas de uso (inciso XI).

Conquanto sintética, a catalogação das disposições recentes remissivas a privacidade e dados no ordenamento brasileiro sinaliza a pertinência de sua discussão em termos regulatórios. Mais do que isso, denota a acentuada necessidade de uniformização das previsões esparsas em um regramento geral e vinculante, especialmente em face da crescente automatização dos procedimentos na sociedade da informação.

## 4.2 A Lei Geral de Proteção de Dados (LGPD) e a autodeterminação informativa nos direitos do titular

Ao discutir a consolidação da ideia de autodeterminação informativa, vê-se que, no processo de intensificação de coleta e fluxo de dados pessoais através das tecnologias da informação, o direito à proteção de dados pessoais, fundado na ideia da autodeterminação informativa, começa a se autonomizar. Segundo KISS e SZŐKE (2015, p. 315), a noção de autodeterminação informativa fez com que o controle e o consentimento do titular de dados pessoais se tornassem as principais bases legais para o processamento de dados.

A aposta na solução do consentimento do indivíduo vai sendo atualizada – mas não abandonada – com o passar do tempo. Considerando que, atualmente, o compartilhamento de dados pessoais, na prática, é pressuposto de participação de interações sociais fundamentais, buscou-se formular um direito que incluísse o poder de determinar como participar na sociedade (MAYER-SCHÖNBERGER, 1998, p. 228-229).

A autodeterminação informativa manifesta-se no texto da normativa brasileira acerca da proteção de dados pessoais, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) – ainda que leis anteriores já tratassem, esparsamente, de proteção de dados e consentimento no Brasil. Como indicado anteriormente, leis setoriais como o Código de Defesa do Consumidor - CDC (Lei nº 8.078/1990), a Lei do Cadastro Positivo (Lei nº 12.414/2011), a Lei de Acesso à Informação (Lei nº 12.527/2011) e o Marco Civil da Internet (Lei nº 12.965/2014) já buscavam garantir a autodeterminação informacional dos titulares de dados pessoais.

O direito à autodeterminação informativa é entendido no direito brasileiro como um feixe de prerrogativas, "que permite que cada cidadão decida até onde vai a sombra que deseja que paire sobre as informações que lhe respeitam" (CASTRO, 2005, p. 27). Assume-se como um direito de personalidade, que permite que o titular controle a utilização

das informações a seu respeito e não se refere apenas à garantia do direito à intimidade da vida privada.

Essa solução jurídica busca interditar e limitar a renúncia individual em relação a alguns pontos especialmente sensíveis, para proteção da autodeterminação da própria pessoa (MAYER-SCHÖNBERGER, 1998, p. 233; DONEDA, 2011, p. 98). De um lado, busca-se fortalecer a posição do indivíduo face às instituições que acumulam dados, na tentativa de igualar os poderes de barganha. De outro, pretende-se limitar parte da liberdade individual que havia sido garantida nas duas gerações anteriores, devido à crença de que "algumas áreas da privacidade informacional devem ser absolutamente protegidas, e não podem ser negociadas individualmente" (MAYER-SCHÖNBERGER, 1998, p. 233).

A tendência que se observa hoje é a adjetivação do consentimento – que deve ser informado, livre, inequívoco, com finalidades determinadas, específico e expresso. Novamente, o enfoque está no indivíduo e no exercício de sua autodeterminação informativa. A adjetivação é uma tentativa de evitar o problema de um possível consentimento ilusório mas, ao mesmo tempo, demonstra a manutenção de sua opção como melhor resposta (BIONI, 2019, p. 255).

A Lei Geral de Proteção de Dados Pessoais (LGPD), na linha do direito europeu e da valorização da autodeterminação informativa, estabelece uma adjetivação extensa do consentimento, novamente apostando no papel do indivíduo no controle do fluxo de seus dados pessoais. Este é definido como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (artigo 5º, XII). É necessário o consentimento específico do titular para que o controlador comunique ou compartilhe dados pessoais obtidos com seu consentimento a outros controladores (artigo 7º, § 5º). O consentimento específico também é adotado no caso de tratamento de dados pessoais de crianças e de adolescentes (artigo 14º, § 1º), e é uma das hipóteses que autoriza a transferência internacional de dados pessoais (artigo 33, VIII).

Bruno BIONI (2019, p. 206) ressalta que grande parte dos princípios adotados pela LGPD giram em torno da ideia dos direitos do titular e, como consequência, da autodeterminação informativa. Isso ocorre tanto nos princípios clássicos (como transparência, a especificação de propósitos, de acesso e qualidade de dados) quanto nos princípios mais modernos (como adequação e necessidade, pelos quais o tratamento deve corresponder às legítimas expectativas do indivíduo, no caso o titular dos dados).

Além disso, a LGPD contém uma série de disposições voltadas a concretizar, orientar e reforçar o controle dos dados pessoais com enfoque na autodeterminação informacional e no consentimento individual do titular dos dados. Alguns exemplos são: a exigência de que o consentimento seja feito por meio de cláusulas destacadas; a nulidade das autorizações genéricas (artigo 8º, §4º); a previsão de que a eventual dispensa de consentimento não desobriga os agentes de tratamento das demais obrigações da LGPD (artigo 7º, § 6º); e ainda que, nesses casos, o titular pode opor-se a tratamento caso seja feito em descumprimento ao disposto na lei (artigo 18, § 2º).

No âmbito jurisprudencial, mesmo antes de entrar em vigor a Lei Geral de Proteção de Dados já demonstrou que a temática tem ocupado papel central nas discussões a respeito da circulação de informações. Nos dias 6 e 7 de maio de 2020, foi referendada pelo Supremo Tribunal Federal a Medida Cautelar nas ADINs ns. 6387, 6388, 6389, 6393, 6390, suspendendo a aplicação da Medida Provisória n. 954/2018. A decisão foi relatada pela Min. Rosa Weber e seu voto foi acompanhado por outros nove ministros. O caso em pauta aproximava-se do tema de fundo da paradigmática decisão alemã de 1983: a Medida Provisória n. 954/2018, que foi suspensa, obrigava as operadoras de telefonia a repassarem ao Instituto Brasileiro de Geografia e Estatística (IBGE) dados identificados de seus consumidores de telefonia móvel, número de telefone celular e endereço.

No corpo da decisão, a Min. Rosa Weber cita a LGPD diversas vezes, direta e indiretamente, invocando seus princípios e seus dispositivos. A ministra afirma que "o respeito à privacidade e à autodeterminação in-

formativa foram positivados, no artigo 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais"[5]. Destaca também o agravamento da situação pelo fato de a LGPD ainda não estar em vigor na ocasião. Em adição, a decisão pronuncia explicitamente o princípio de autodeterminação informacional.

## 5 ASPECTOS FUNCIONAIS DOS INSTRUMENTOS REGULATÓRIOS DE PROTEÇÃO DE DADOS

Nos itens prévios, descreveu-se instrumentos e proposições resolutivas para demandas sociais de proteção de dados pessoais adotados nos ordenamentos jurídicos alemão e brasileiro. A partir do referencial funcional desempenhado pelas normas e institutos propostos, e de posse do histórico circunstancial, social e regulatório das duas localidades, pretende-se evidenciar brevemente as convergências sistemáticas passíveis de identificação, mas especialmente examinar sua eficácia no cumprimento da função para a qual foram designadas.

Preliminarmente, cumpre notar que o direito à privacidade não se confunde com o direito à proteção de dados, vez que o primeiro se destina a resguardar-se da intromissão de terceiros, enquanto o segundo refere-se à possibilidade de controlar como os dados do titular são manuseados. Porém, ainda que a proteção de dados seja uma das numerosas maneiras de viabilizar a garantia de privacidade (BOEHME-NESSLER, 2016, p. 4), no contexto da digitalização das relações sociais o controle sobre os próprios dados adquire uma projeção maior e extrapola a discussão a respeito do direito a ser deixado só.

Conforme esclarece Danilo DONEDA (2011, p. 95), a disciplina do tratamento de dados pessoais faz com que garantias anteriormente vin-

[5] SUPREMO TRIBUNAL FEDERAL. Voto da Min. Rosa Weber, Medida Cautelar na ADI 6.387, Rel. Min Rosa Weber, julgamento em 07-05-2020, Plenário. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 19 set. 2020.

culadas ao direito à privacidade passem "[...] a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais". Isso porque a ideia da regulação da proteção de dados não surge no sentido de impedir seu tratamento – nesse ponto, diferenciando-se da prestação negativa necessária para garantir a privacidade – mas sim com a finalidade de moderar esse procedimento, com diretrizes que envolvem controle e transparência.

Além disso, a ubiquidade tecnológica e os mecanismos de vigilância digital e processamento de informações dela decorrentes evidenciam a dependência cada vez mais marcante dos dados pessoais nos processos automatizados, seja para fins de identificação e individualização, ou mesmo para possibilitar o desempenho de tarefas básicas da vida civil. Assim, é inevitável que em algum momento a necessidade de tratamento de dados pessoais perpasse as relações sociais e institucionais, o que reforça a premência da abordagem do tema em âmbito regulatório, inclusive a fim de viabilizar a cidadania digital.

O crescente leque de possibilidades para o uso das informações de caráter pessoal – pelo poder público, pelo mercado, pelo próprio titular – exige a consolidação de um marco legal que preveja contornos adequados para as dinâmicas de coleta, tratamento, uso e transmissão desse conteúdo, vinculado a uma autoridade independente e forte para implementar suas previsões legais. Ainda, não se deve afastar o protagonismo das tecnologias de informação e comunicação, cujo desenvolvimento contínuo gera reflexos que demandam regularmente respostas da sociedade e principalmente das autoridades reguladoras.

Na Alemanha, o amadurecimento da noção de autodeterminação informativa e da necessidade de proteção dos dados pessoais verificou-se durante um prolongado período de tempo, além de contar com iniciativas de diversos setores da sociedade. Isso permitiu o aperfeiçoamento no tratamento da matéria, orientado pela necessidade de compatibilização de interesses que se manifestavam.

Em relação à experiência brasileira, a ausência de um marco regulatório específico para as informações pessoais no decorrer de décadas, especialmente com a crescente automatização de procedimentos de tratamento de dados, resultou no surgimento de disposições esparsas para atender a demandas específicas. Embora esta estratégia regulatória padeça de problemas, essas iniciativas possibilitaram a constante discussão e referência ao tema, tornando cada vez mais acentuada a pressão por um regramento geral.

Tanto na Alemanha quanto no Brasil, nota-se que as leis de proteção de dados visam a suprir demandas sociais subjetivas de empoderamento e controle frente às crescentes possibilidades de tratamento e uso de dados pessoais.[6] Em ambas as experiências, ainda que em momentos bastantes distintos, o forte apelo social resultou na apreciação da temática também pelo judiciário, intensificando pressão por medidas céleres e efetivas do Poder Legislativo de cada país.

É essencial frisar que em nenhum dos casos os regramentos destinam-se, numa visão geral, a impedir ou proibir a circulação de informações dos indivíduos – salvo, evidentemente, aqueles dispositivos especificamente destinados a este fim –, mas sim de regular a atividade, de forma a garantir a efetividade dos direitos fundamentais vinculados à proteção de dados pessoais.

O intenso fluxo transfronteiriço de dados exige que as regulações voltadas à normatizar a circulação de informações pessoais encerrem traços harmônicos entre si. Nessa percepção, é indispensável que haja possibilidade de que os diplomas de diferentes países dialoguem em algum grau, para que não se impeça a transferência de dados entre localidades distintas. Isso faz com que todos esses regimes compreendam elementos comuns, sobretudo no que tange aos princípios dirigentes, que notadamente já compõem o núcleo estrutural do ordenamento relativo à proteção de dados.

---

[6] Uma comparação mais ampla, para além dos direitos do titular e da autodeterminação informativa, pode ser encontrada no artigo "A nova lei brasileira de proteção de dados - uma visão crítica", de Thomas Hoeren e Stefan Pinelli, na primeira parte desta obra.

Alguns desses elementos evidenciam-se reiteradamente, como é o caso do direito de acesso, que garante ao cidadão o direito de controlar suas próprias informações independentemente de onde estão armazenadas – e que oportuniza, em última análise, todas as outras atividades relacionadas à cidadania eletrônica –, além dos princípios já habituais que informam o tratamento de dados: finalidade, transparência, adequação, não discriminação, entre outros.

As leis gerais de proteção de dados cumprem, portanto, a função de estabelecer formas de controlar, acessar e inclusive permitir o tratamento dos próprios dados, em observância à necessidade de segurança subjetiva que este tipo de prática demanda. A tutela é geral, vez que independe de qual agente ou setor da sociedade está conduzindo o tratamento; os dados individuais requerem ampla salvaguarda indiferentemente deste aspecto.

Ainda, por serem regramentos voltados à proteção do indivíduo, não se pode dizer que os diplomas aqui tratados têm a pretensão de neutralidade. Em verdade, o RGPD e a LGPD, além das normas e decisões adjacentes que se dedicam à proteção de dados, encerram mecanismos protecionistas e favorecedores dos direitos subjetivos, especialmente da autonomia individual, ao mesmo tempo que também protegem interesses das empresas, ao regular (e, portanto, justificar) o fluxo de dados pessoais.

## 6 OS REFLEXOS DA REGULAÇÃO DA PROTEÇÃO DE DADOS NA AUTONOMIA INDIVIDUAL E NA DEMOCRACIA

A necessidade de mecanismos de proteção de dados tem como um de seus fundamentos o pressuposto da assimetria informacional. O sujeito, enquanto componente individual do tecido social, ainda que inserido e partícipe em quaisquer coletividades, demanda instrumentos que o permitam reequilibrar uma equação estruturalmente desbalanceada.

É fato notório que a sociedade informacional encerra uma multiplicidade de atores operantes, sendo que diversos deles – tanto da inicia-

tiva privada, quanto do setor público – dispõem de capacidades de coleta, tratamento, armazenamento e transmissão de dados imensamente maiores que as aptidões individuais.

## 6.1 Os componentes do tratamento de dados: uma equação desequilibrada

Há, em especial por parte do mercado, um firme posicionamento de que a coleta e tratamento massivo de dados é essencial para o desenvolvimento da economia. O CEO do Facebook, Mark Zuckerberg, em 2010, afirmou que a "privacidade já não é mais uma norma social",[7] e boa parte das grandes companhias de tecnologia tratava as movimentações a respeito da proteção de dados pessoais como um novo ludismo, protagonizado por pessoas que se colocavam no caminho do progresso e do desenvolvimento da humanidade. Com o tempo, esse posicionamento "anti-privacidade" passou a ser criticado pelo campo social e foi sendo reformulado em alguma medida.

A efetiva proteção dos dados pessoais não pode ser vista como inibidora ou oponente ao progresso e à consolidação da democracia; pelo contrário, é justamente pela inserção e proteção das cidadãs e cidadãos que se pode realmente falar de uma democracia adequadamente estruturada e fortalecida. A coleta e tratamento de dados pessoais à revelia das cidadãs e cidadãos é, em essência, anti-democrática. Para BOBBIO, a própria democracia seria o governo do poder visível (1986, p. 87), ou seja, onde o ato de governar não ocorre de maneira oculta. Ela se fundamentaria, nas palavras do mesmo autor, no governo do poder público em público. Isso porque a visibilidade e a publicidade do poder são mecanismos necessários para que o povo possa controlar a conduta dos governantes (LAFER, 1988, p. 244).

[7] Trecho extraído da declaração proferida por Mark Zuckerberg em 11 de janeiro de 2010, na ocasião do evento "Crunchie Awards" em San Francisco, Califórnia. Disponível em: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy. Acesso em: 01 set. 2020.

Segundo Wallace Paiva MARTINS, para uma verdadeira democracia é preciso o reconhecimento da "existência de um direito subjetivo público ao conhecimento da atuação administrativa em todos os seus níveis" (2012, p. 234). Assim, é possível afirmar que a transparência e publicidade do que é feito pelo Estado é um princípio estrutural da própria democracia, que o diferencia de um governo ditatorial ou absolutista.

Além disso, conforme afirma Eneida Desiree SALGADO (2015, p. 2), é intrínseca à noção de República a busca pela identidade da ação dos poderes institucionais com o interesse público. Consequência direta disso é a necessidade de transparência e ampla publicidade dos poderes públicos, pois é preciso que seja possível a visualização e controle dos atos praticados por agentes públicos em nome de toda a sociedade. Dessa forma, a transparência pode ser colocada como "uma condição de possibilidade do Estado plural, republicano e aberto às exigências do controle racional das decisões" (CLÉVE; FRANZONI, 2013, p. 2).

Aqui também cabe destacar que o que subsidia a necessidade da proteção de dados pessoais perante os entes públicos é igualmente válido para a proteção de dados pessoais perante entes privados. Um dos motivos disso é a facilidade com que ocorre o fluxo de dados entre entes privados e públicos – seja através de parcerias, ordens judiciais ou privatizações de órgãos inicialmente estatais.

Além disso, frequentemente dados coletados e tratados por empresas privadas têm fortes efeitos no âmbito público – como bem demonstra o escândalo do Cambridge Analytica e, mais recentemente, as revelações da *whistleblower* Sophie Zhang, ex-cientista de dados do Facebook.[8] Até mesmo os relatórios oficiais de algumas plataformas dão conta da gigante influência do conteúdo que ali circulava no destino político de nações.[9]

---

[8] O editorial pode ser conferido na íntegra em: BUZZFEED NEWS. Whistleblower Says Facebook Ignored Global Political Manipulation. 14 set. 2020. Disponível em: https://www.buzzfeednews.com/article/craigsilverman/facebook-ignore-political-manipulation-whistleblower-memo. Acesso em: 16 set. 2020.

[9] Um exemplo é o relatório do próprio Facebook a respeito da remoção de contas com comportamento inautêntico na Tailândia. Fonte: ABOUT FACEBOOK. Removing Coordinated

Na contemporaneidade, não há por que falar de proteção de dados apenas frente ao Estado ou apenas frente às empresas; é preciso lutar pela proteção de dados pessoais como um todo. Nesse sentido, as regras voltadas a esta finalidade têm a função de paramentar o indivíduo com reais instrumentos de controle sobre seus dados, reafirmando sua autonomia frente aos agentes de tratamento de dados, de forma a balancear essa relação.

## 6.2 A primazia da autonomia no desenvolvimento da personalidade individual e das competências democráticas

Compreender o direito à autodeterminação informativa como uma garantia fundamental é a decorrência lógica das noções democráticas, segundo as quais a formação da personalidade individual deve ser respeitada com fundamento na dignidade e na autonomia.

A Corte Constitucional alemã entende que este direito ao livre desenvolvimento da personalidade encerra o mais alto valor constitucional (RICCARDI, 1983, p. 245), sendo a diretriz que orienta o desenvolvimento de todas as demais competências necessárias para que as cidadãs e cidadãos possam estar no centro da agência da democracia.

Na esteira desse raciocínio, HORNUNG e SCHNABEL (2009, p. 88) atentam para o elevado nível de percepção da população alemã na década de 80, ao se preocupar com os efeitos negativos da vigilância excessiva na democracia como um todo e protestar contra a invasividade das medidas propostas na época. Curiosamente, este interesse social enfraqueceu durante a década de 90, apesar de a vigilância e o processamento de dados ficarem cada vez mais intensos com a crescente ubiquidade da tecnologia.

---

Inauthentic Behavior in Thailand, Russia, Ukraine and Honduras. 25 jul. 2019. Disponível em: https://about.fb.com/news/2019/07/removing-cib-thailand-russia-ukraine-honduras/. Acesso em: 15 set. 2020.

Ainda que em movimentos alternados, a experiência alemã revela significativas dinâmicas socioculturais. Conforme leciona LEGRAND (2018), a leitura prolífica do direito estrangeiro parte do pressuposto de que o ordenamento jurídico é um elemento integrante da cultura, e sua materialização é fruto de sujeitos institucionalizados naquela sociedade e naquele ordenamento. Analisar como países e coletividades distintas lidam com um problema semelhante – a coleta e tratamento excessivo de dados – pode nos trazer interessantes reflexões.

Desta forma, a estratégia que parece mais acertada, levando em consideração o desenvolvimento histórico do conceito de autodeterminação informativa e seu par, a assimetria informacional, é a aposta em instrumentos regulatórios estatais – desenvolvidos de forma transparente, sujeitos à *accountability*, e com participação ativa de múltiplos setores da sociedade. Uma adequada proteção de dados pessoais vai ao encontro dos interesses de toda a sociedade, para além do indivíduo em sua esfera autônoma.

É necessária a intervenção de instrumentos externos de regulação para que seja mitigado o desequilíbrio informacional e tecnológico. Nesse sentido, considerar a proteção de dados como direito fundamental é benéfico para uma proteção mais sólida em âmbito individual. Há uma negociabilidade limitada no que tange ao controle dos próprios dados pessoais – justamente para assegurar o livre desenvolvimento da personalidade do indivíduo e evitar influências escusas no cenário político-econômico de países (BIONI, 2019, p. 310).

Vale ressaltar que não se defende um protecionismo estatal excessivo – cujos desdobramentos seriam, inclusive, prejudiciais para o titular de dados. O que se reconhece é que, considerando a assimetria informacional e a ausência de uma cultura coletiva a respeito da importância e impacto da proteção de dados, o indivíduo deve ser entendido como um hipossuficiente nesta relação.

Outro argumento nesse sentido é que, hodiernamente, o cidadão precisa disponibilizar seus dados para o Estado e para empresas para

participar efetivamente da sociedade. No ambiente digital, por exemplo, as vulnerabilidades do sujeito intensificam-se à medida em que ele fornece seus dados pessoais e suas preferências de navegação e consumo em troca da possibilidade de participação em uma esfera cujo discurso é monista, autocrático e excludente. A justificativa subjetiva individual revolve em torno do desejo de integração neste meio, a fim de não restar excluído ou desatualizado frente a seus pares (GEDIEL; CORRÊA, 2008). Nesse contexto, é falso falar em real espaço de escolha, que resta relativizado pelas ameaças à privacidade e às informações pessoais.

Nesse sentido, a noção de heterorregulação, apresentada por Ana FRAZÃO (2019, p. 128), pode ser útil: a regulação seria o fio condutor que orienta e conforma as demais formas de regulação, evitando também que regras de mercado, impostas unilateralmente por agentes mais poderosos dominem todas as formas de regulação dos dados e descaracterizem a proteção de dados implementada pela lei.

Outra abordagem interessante é a de corregulação, apresentada no texto "*A cláusula aberta dos interesses legítimos e as autoridades nacionais: análise comparativa entre LGPD e RGPD*" (seção II, capítulo I). Para os autores, é profícuo que se abandone a lógica simplória e maniqueísta, que apenas rivaliza modelos da desregulamentação, heterorregulação e autorregulação, em prol da construção de um modelo que aproveite o que há de melhor dentre todos os modelos. Neste sentido, seria melhor para a proteção de dados pessoais a adoção de uma perspectiva que busque a "interação e harmonização entre os modelos da heterorregulação estatal e da autorregulação pelo mercado, além de alternativas apresentadas pela via da própria tecnologia" – como as PETs, *privacy enhancing technologies*.

O contorno dessa intervenção regulatória é justamente a autodeterminação sobre as próprias informações. Elas fortalecem-se e limitam-se mutuamente. A autodeterminação informacional deve balizar a intervenção por parte do Estado, evitando que ela se estenda para além do necessário, mas também garantindo a proteção do titular de dados num contexto de assimetria informacional.

Porém, é incontestável que apostar apenas na autodeterminação informativa é insuficiente. O caminho de intervenções regulatórias bem desenvolvidas e bem aplicadas relaciona-se com a ideia do dirigismo informacional, que não deixa sob responsabilidade do indivíduo toda a carga de proteção de dados pessoais (BIONI, 2019, p. 310). Garantir uma intervenção estatal cuidadosa, portanto, significa apostar na redução do desequilíbrio entre as empresas de tecnologia e os usuários, ao mesmo tempo que se limita a autonomia da vontade dos titulares em relação à negociabilidade da própria privacidade.

Evidentemente, o aperfeiçoamento das competências democráticas depende substancialmente da autonomia cidadã, assegurada pela possibilidade de desenvolvimento da personalidade individual. Conforme asseverado nos itens anteriores, na sociedade informacional o fortalecimento da autonomia do cidadão decorre da garantia de controle moderado sobre suas próprias informações, balanceado por diretrizes ponderadas que levam em conta a hipossuficiência individual nas relações de tratamento de dados.

## 7 CONSIDERAÇÕES FINAIS

A relação entre a autodeterminação informativa e os valores democráticos mostra-se cada vez mais evidente em ponderações multidisciplinares, especialmente com a emergência de debates sobre o processamento de dados e as numerosas formas de vigilância. Apesar disso, a posição ocupada pelo direito à proteção de dados pessoais como uma garantia fundamental deve ser constantemente reiterada e fortalecida, para que não se perca de vista a severidade desta discussão central.

No âmbito individual, as regulações voltadas à proteção de dados encerram uma clara finalidade: fornecer mecanismos para que as cidadãs e cidadãos possam se empoderar frente às possibilidades de tratamento de dados pessoais, vez que tais processos ocorrem frequentemente à margem da compreensão da sociedade em geral. Com fundamentos na premissa do direito à autodeterminação informativa, os instrumentos

regulatórios promovem essa capacitação ao promover o controle sobre os próprios dados e o desenvolvimento individual na sociedade digital da informação.

A coleta e tratamento de dados pessoais pode, de fato, ser útil para o desenvolvimento de políticas públicas mais eficazes e para a otimização de gastos públicos, por exemplo. O que se deve buscar, portanto, não é a proibição absoluta do processamento de dados pessoais ou a inibição de sua circulação. Afinal, reconhece-se que a inferência de conclusões a partir de informações pessoais, quando adequadamente utilizadas, oferece mecanismos de aprimoramento das relações sociais nos regimes democráticos.

Precisamente, o que se deve combater é a coleta sem motivos ou com motivos torpes, que invadem e violam os direitos fundamentais à privacidade e à autodeterminação dos indivíduos. Nota-se, progressivamente, como o tratamento inadequado das informações pessoais pode conduzir a resultados discriminatórios, prejudiciais e irreversíveis, como abordam variados capítulos desta seção.

Hoje, o recolhimento de dados demonstra ter efeitos muito mais severos do que anteriormente, influenciando sub-repticiamente a formação da personalidade (em caráter pessoal, político, dentre outros) de um expressivo número de indivíduos. Assim, o controle sobre os próprios dados, materializado no direito à autodeterminação informativa, representa um requisito condicionante para a autonomia individual, que por sua vez é a premissa exordial para o exercício da plena cidadania, inclusive em seu desdobramento eletrônico.

É necessária a insistente conscientização da sociedade civil sobre os efeitos do tratamento de dados pessoais, bem como do municiamento de estratégias e ferramentas disponíveis para se opor a isso, caso os indivíduos assim desejem – mas isso não é tudo. Naturalmente, o Estado precisa agir para regular de forma clara e factível a circulação de dados pessoais, justamente para balancear a clara assimetria informacional existente na relação entre particulares e agentes de tratamento.

Essas estratégias regulatórias estatais devem ser informadas por estudos conduzidos em outros campos técnicos, sendo indispensável a interação multidisciplinar na atenção às demandas sociais. Um exemplo de iniciativa que visa tornar o futuro mais democrático e inclusivo é projeto alemão "*AlgoRules - Rules for the Design of Algorithmic Systems*" (em tradução livre, regras para o design de sistemas algorítmicos).[10] Trata-se de um catálogo de critérios formais e éticos que permitem uma concepção e supervisão mais benéfica, em termos sociais, de sistemas algorítmicos.

Não há dúvidas de que as estratégias regulatórias estatais têm muito a ganhar em termos de aperfeiçoamento e responsividade com o diálogo orientado por estudos estratégicos nesses moldes. E novamente, este constitui mais um aspecto em que a proposta democrática brasileira tem muito a aprender com a experiência alemã.

## REFERÊNCIAS

BIONI, Bruno Ricardo. **Xeque-Mate**: O tripé da proteção de dados pessoais no jogo de xadrez. São Paulo: GPoPAI/USP, 2015.

_____. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. Ebook.

BOBBIO, Norberto. **Futuro da democracia**: uma defesa das regras do jogo. Trad.: Marco Aurélio Nogueira. Rio de Janeiro: Paz e Terra, 1986.

BOEHME-NESSLER, Volker. Privacy: a matter of democracy. Why democracy needs privacy and data protection. **International Data Privacy Law**, 2016, Vol. 00, No. 0 - International Data Privacy Law Advance Access published July 25, 2016.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Portal da Legislação, Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 03 ago. 2020.

[10] Para acessar mais informações sobre a iniciativa: ALGORULES. Rules for the Design of Algorithmic Systems. Disponível em: https://algorules.org/en/home/. Acesso em: 15 set. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Portal da Legislação, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 26 ago. 2020.

_____. STF. **Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387**, Distrito Federal. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 29/4/2020

BUNDESVERFASSUNGSGERICHT. Decisions. Decision on the constitutionality of the 1983 Census Act. 15 dez. 1983. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html.. Acesso em: 05 set. 2020.

CASTRO, C. S. E. **Direito da informática, privacidade e dados pessoais:** a propósito da legalização de tratamentos de dados pessoais (incluindo videovigilância, telecomunicações e Internet) por entidades públicas e por entidades privadas, e da sua comunicação e acesso. Coimbra: Almedina, 2005.

CLÈVE, Clèmerson Merlin; FRANZONI, Júlia Ávila. Administração Pública e a nova Lei de Acesso à Informação. **Interesse Público**. Belo Horizonte, ano 15, n. 79, maio/jun. 2013.

CURY, Paula Maria Nasser. Métodos de Direito Comparado: desenvolvimento ao longo do século XX e perspectivas contemporâneas. **Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD).** São Leopoldo, v. 6, n. 2, p. 176-185, jul./set. 2014.

DE CONINCK, Julie. The Functional Method of Comparative Law: Quo vadis? **Rabels Zeitschrift für ausländisches und internationales Privatrecht** / The Rabel Journal of Comparative and International Private Law, v. 74, n. 2, p. 318–350, 2010. Disponível em: www.jstor.org/stable/27878873. Acesso em: 13. set. 2020.

DEUTSCHER BUNDESTAG. **Grundgesetz für die Bundesrepublik Deutschland**. 23 maio 1949. Disponível em: https://www.bundestag.de/gg. Acesso em: 05 set. 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

EUROPEAN COMMISSION. Data protection in the EU. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en#legislation. Acesso em: 12 set. 2020.

EUROPEAN DATA PROTECTION SUPERVISOR. The history of the General Data Protection Regulation. Disponível em: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Acesso em: 29 ago. 2020.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA). **Handbook on European data protection law**. Luxemburgo: Publications Office of the European Union, 2018.

FRAZÃO, Ana. Objetivos e alcances da Lei Geral de Proteção de Dados. p. 99-129. In: FRAZÃO, Ana; TEPEDINO, Gustavo. OLIVA, Milena Donato. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o mercado. **Revista da Faculdade de Direito - UFPR**, Curitiba, n. 47, p. 141-153, 2008.

HOFFMANN-RIEM, Wolfgang. Inteligência artificial como oportunidade para a regulação jurídica. **RDU**, Porto Alegre, Volume 16, n. 90, 2019, p. 11-38, nov-dez 2019.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data protection in Germany I: The population census decision and the right to informational self-determination. **Computer Law & Security Report**, Volume 25, Issue 1, 2009, p. 84-88. Disponível em: https://doi.org/10.1016/j.clsr.2008.11.002. Acesso em: 29 ago. 2020.

INTERNATIONAL NETWORK OF PRIVACY LAW PROFESSIONALS (INPLP). A brief history of data protection: how did it all start? Disponível em: https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/. Acesso em: 29 ago. 2020.

KISS, A.; SZŐKE, G. L. Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation. In: GUTWIRTH, S.; LEENES, R.; DE HERT, P. **Reforming European Data Protection Law**. Dordrecht: Springer, v. 20, 2015.

LAFER, Celso. **A reconstrução dos direitos humanos**: um diálogo com o pensamento de Hannah Arendt. São Paulo: Cia. das Letras, 1988.

LEGRAND, Pierre. **Como ler o direito estrangeiro**. Trad.: Daniel Wunder Hachem. São Paulo: Contracorrente, 2018.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Editora Saraiva, 2011.

LESSIG, Lawrence. **Code**: Version 2.0. New York: Basic Books, 2006.

LUZ, Pedro Henrique Machado da; LOUREIRO, Maria Fernanda Battaglin. Privacidade e proteção de dados pessoais: os novos desafios na Sociedade em Rede. **Meritum**. Belo Horizonte, v. 13, n. 1, p. 69-86, jan./jun. 2018.

MARTINS JUNIOR, Wallace Paiva. Princípio da publicidade. In: MARRARA, Thiago (Org.). **Princípios de direito administrativo**. São Paulo: Atlas, 2012, p. 234.

MAYER-SCHÖNBERGER, V. Generational development of data protection in Europe. In: AGRE, P. E.; ROTEMBERG, M. **Technology and privacy:** The new landscape. Cambridge: MIT Press, 1998.

MICHAELS, Ralf. Explanation and Interpretation in Functionalist Comparative Law – A Response to Julie de Coninck. **Rabels Zeitschrift für ausländisches und internationales Privatrecht** / The Rabel Journal of Comparative and International Private Law, v. 74, n. 2, 2010, p. 351-359.

MOROZOV, Evgeny. **Big Tech:** a ascensão dos dados e a morte da política. Trad. Claudio Marcondes. São Paulo: Ubu Editora, 2018.

RICCARDI, J. Lee. The German Federal Data Protection Act of 1977: Protecting the Right to Privacy? **Boston College International & Comparative Law Review**. Volume 6, n. 1, p. 243-271, dez. 1983. Disponível em: http://lawdigitalcommons.bc.edu/iclr/vol6/iss1/8. Acesso em: 02 set. 2020.

RODOTÀ, Stefano. Democracia y protección de datos. **Cuadernos de Derecho Público**, ns. 19-20, maio/dez. 2003.

SALGADO, Eneida Desiree. **Lei de Acesso à Informação (LAI)**: comentários à Lei nº 12.527/2011 e ao Decreto nº 7.724/2012. São Paulo: Atlas, 2015.

SUPREMO TRIBUNAL FEDERAL. Voto da Min. Rosa Weber, Medida Cautelar na ADI 6.387, Rel. Min Rosa Weber, julgamento em 07-05-2020, Plenário. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 19 set. 2020.

TAVARES NETO, José Querino; FREITAS, Cinthia Obladen de Almendra; COSTA, Andréa Abrahão (Org.). **Métodos de pesquisa aplicados ao direito**: um pressuposto epistemológico necessário. Curitiba: CRV, 2017.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, 1890, p. 193-220, dez. 1890.

# Capítulo II

# ÉTICA NAS DECISÕES AUTOMATIZADAS: direito à explicação no RGPD e o direito de revisão na LGPD

*Gisele Pereira Mendes*[1]

*Antônio Carlos Gonçalves Filho*[2]

## SUMÁRIO



## RESUMO

No contexto de evolução digital os dados pessoais são os artigos de maior valor no mercado, existe a necessidade de regulamentação da proteção à privacidade da pessoa humana de uma forma mais específica, visando proteger o indivíduo objetivamente da velocidade em que seus dados fluem dentro do sistema e também, da forma como serão manipulados por uma inteligência artificial. Mais do que "bens" os dados pessoais são indicadores de individualidade, únicos e intransponíveis. Neste artigo, analisando a LGPD e o RGPD se faz uma relação entre o funcionamento da inteligência humana e da inteligência artificial, provendo uma noção de como as máquinas aprendem, a fim de nortear a discussão acerca da automatização de decisões que anteriormente eram proferidas exclusivamente por humanos, enfatizando os vieses dos programadores de algoritmos de máquinas, e os direitos à explicação e à revisão como ferramentas para a defesa dos direitos dos titulares dos dados que foram tratados para alcançar determinada decisão automatizada.

**Palavras-chave:** proteção de dados, processamento, ética, decisão automatizada.

[1] Mestranda em Direito, Tecnologia e Desenvolvimento pela Universidade Positivo (UP); Especialista em Negócios Internacionais pela FAE Business School (FAE); Especialista em Direito do Trabalho e Processual do Trabalho pela Pontifícia Universidade Católica do Paraná (PUC-PR). Advogada, internacionalista e escritora no site www.direitodemigrar.com. Contato: gimendes01@hotmail.com

[2] Doutorando na área de Direitos Humanos e Democracia pela Universidade Federal do Paraná e Mestre na mesma área pelo Centro Universitário Autônomo do Brasil (UniBrasil). Foi pesquisador do Núcleo de Pesquisa em Direito Civil e Constituição da Unibrasil. Especialista em Teoria Crítica dos Direitos Humanos pela Universidad Pablo de Olavide de Sevilha/Espanha. Advogado. Contato: antonio.carlosfilho@hotmail.com.

Ambos são Membros do Grupo de Estudos em Direito Autoral e Industrial – GEDAI/UFPR.

## 1 INTRODUÇÃO

O mundo a nossa volta está passando por uma revolução digital, vemos uma interação cada vez maior das aplicações de computador com os seres humanos. Sistemas de recomendação de produtos e serviços com base no perfil pessoal, assistentes pessoais ativados por voz, smartphones com reconhecimento facial, sistemas automatizados para processos de seleção, entre outros (DSA, 2020, C. 1). No âmbito destas interações, nas quais as máquinas, que são compostas de inúmeras camadas de processamento, o que as faz capaz de aprender representações de dados com diversos níveis de abstração (CHAGAS, 2019, p. 01), cabe à sociedade procurar entender quais as possíveis consequências advindas do ponto de convergência onde a inteligência artificial, criada pela inteligência humana sob a limitação da programação algorítmica, encontrará, ou confrontará, as habilidades da própria inteligência humana.

Para uma análise preliminar, é importante entender substancialmente como a inteligência artificial (IA) está se desenvolvendo e o que ela representa para o humano hoje. Considerando que o próprio humano desenvolveu uma estrutura eletrônica com o objetivo de construir sistemas que apresentem comportamento inteligente e desempenhem tarefas com um grau de competência equivalente ou superior ao grau com que um especialista de sua espécie desempenharia, e que continua trabalhando para aprimorá-la, presume-se que o grau de importância que a IA representa ao humano, é muito elevado, que continuará sendo aprimorada e cada vez mais será introduzida no cotidiano comum.

A inteligência eletrônica criada pelo humano alcançou um patamar no qual é capaz de armazenar uma quantidade gigantesca de dados, inclusive de caráter pessoal, e processá-los em alta velocidade, os quais, quando combinados, resultam em um produto com alto valor de mercado (Big Data). Utilizando-se desta base de dados, heterogênea, e da capacidade de analisar múltiplas bases ao mesmo tempo para agir, a máquina ganhou a capacidade de aprendizado, o que ficou conhecido como Aprendizagem de Máquina (Machine Learning), que é conceito central da IA.

No Aprendizado de Máquina, os modelos conceituais são treinados com base em dados armazenados, por humanos, possibilitando prever resultados para novos conjuntos de dados. Dependendo do contexto, os sistemas de IA podem até mudar seus comportamentos e resultados para uma maior eficiência, se adequando às decisões e ações que o cérebro humano tomaria. Para esta evolução dá-se o nome de Aprendizagem por Reforço (RL).

Do Aprendizado de Máquina, desenvolveu-se uma sub-área denominada Aprendizagem Profunda (Deep Learning), que funciona basicamente, com o processamento de dados para literalmente imitar, ou tentar imitar, o processamento feito pelo cérebro humano.

> A unidade fundamental de uma rede neural artificial é um nó (ou neurônio matemático), que por sua vez é baseado no neurônio biológico. As conexões entre esses neurônios matemáticos também foram inspiradas em cérebros biológicos, especialmente na forma como essas conexões se desenvolvem ao longo do tempo com "treinamento" (DSA, 2020, C. 1)

Dentro desta perspectiva de volume, velocidade, variedade e valor empregada ao processamento de dados, estipulou-se que quando os dados a serem processados são de titularidade de uma pessoa humana, existem algumas regras no âmbito legal que devem ser observadas, a fim de garantir a proteção de direitos fundamentais de liberdade e de privacidade do indivíduo, além de garantir o livre desenvolvimento de sua personalidade ("direito de não ser manipulado")[3]. Adiante serão analisadas comparativamente as recentes evoluções históricas correspondentes às legislações da União Europeia, até chegar ao atual Regulamento Geral da Proteção de Dados (RGPD), em vigor desde maio de 2018, e do Brasil, até a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), em setembro de 2020 (exceto penalidades), formulado com base na redação do RGPD.

[3] O cientista de dados Jaron Lanier, entre outros executivos do ramo da tecnologia, no documentário O DILEMA DAS REDES, alertam para o poder manipulador das redes sociais e sobre como a tecnologia transformou o ser humano em produto, de modo a moldar vontades pessoais e tendências sociais, mediante o tratamento de dados pessoais.

A proteção de dados pessoais engloba todos os dados da pessoa. Tanto os dados que identificam a pessoa objetivamente, quanto os dados que tornam a pessoa identificável, ainda que não seja possível estabelecer um vínculo imediato com determinada pessoa, mas que possa ser determinante para uma identificação indireta ou mediata[4]. A LGPD enfatiza cinco direitos principais do titular dos dados: (i) direito de confirmação da existência de tratamento[5], bem como o de acesso aos dados pessoais coletados[6]; (ii) o direito à correção dos dados[7], pelo qual o titular pode solicitar a alteração deles; (iii) o direito de eliminação, pelo qual o titular pode solicitar que os dados sejam deletados; (iv) o direito de portabilidade[8], pelo qual deve ser possível que o titular transfira seus dados de um sistema para outro; e, por fim, o (v) direito à revisão[9], pelo qual o titular pode solicitar informações sobre todos os algoritmos que interagem com seus dados, para entender, por exemplo, o resultado de uma decisão automatizada e, se for o caso, solicitar a sua revisão (LGPD, 2020).

> A lei também proíbe, entre outras coisas, o **tratamento dos dados pessoais para a prática de discriminação ilícita ou abusiva**. Esse tratamento é o cruzamento de informações de uma pessoa específica ou de um grupo para subsidiar decisões comerciais (perfil de consumo para divulgação de ofertas de bens ou serviços, por exemplo), políticas públicas ou atuação de órgão público (AGÊNCIA SENADO, 2020, grifo nosso).

4 Conceito expansionista de dados pessoais.

5 Art. 19, LGPD. "A confirmação de existência ou acesso a dados pessoais serão providenciados, mediante requisição do titular (...)".

6 Art. 18, LGPD. "Declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento."

7 Art. 18, III, LGPD. "Direito de solicitar a correção de dados incompletos, inexatos ou desatualizados."

8 Art. 18, V, LGPD.

9 Art. 20, LGPD. Art. 20, § 1°, descrição de explicação sobre critérios e procedimentos utilizados para a decisão automatizada. A LGPD deu um passo à frente ao RGPD e trouxe um elemento a mais para o direito à explicação, acrescentando ao direito à explicação a oportunidade para o titular dos dados tratados de solicitar a revisão de uma decisão, caso quede-se claro que houve carência de ética no tratamento dos dados fornecidos, de modo consciente ou inconsciente.

Por sua vez, analisar a utilização da IA em processos de tomada de decisões, conhecidas como "decisões automatizadas", que acarretarão consequências fáticas a humanos, e tentar responder às perguntas insurgentes: elas são de fato neutras, não há influência evidente de vieses humanos? São mais justas? A máquina não erra? Qual é o risco em potencial que elas representam para a sociedade, dentro de uma lógica de tratamento de dados pessoais, selecionados, inseridos e configurados por inteligência humana dentro de um sistema de inteligência artificial? Até que seja possível responder às questões colocadas, com assertividade, de forma favorável ao humano, valer-se dos direitos de explicação e de revisão, previstos no RGPD e LGPD, podem ser as melhores ferramentas para garantir os direitos dos titulares dos dados tratados, quando atingidos por decisões exclusivamente automatizadas.

A LGPD, na forma como foi aprovada, prevê o direito à explicação no caso de decisões totalmente automatizadas que possam ter um impacto na vida do titular dos dados, principalmente no contexto de formação e uso de perfis comportamentais. A explicação deve incluir não somente informações sobre os dados pessoais que serviram de substrato para o algoritmo, mas também sobre a lógica por trás de tais decisões. O direito à explicação também é possível quando houver o tratamento de dados anonimizados, quando esse tipo de dado for utilizado na formação de perfis comportamentais de pessoas identificadas.

Para a conclusão destes estudos, estes mecanismos legais de defesa serão analisados comparativamente para que sejam esclarecidas as suas diferenças substanciais.

## 2 DA NÃO INTERVENÇÃO NA VIDA PRIVADA DO INDIVÍDUO À PROTEÇÃO DE DADOS PESSOAIS

Enfrentando muitas incertezas, o Regulamento Geral de Proteção dos Dados Pessoais da União Europeia (RGPD)[10], ou Regulamento nº

[10] A sigla em inglês que se destaca nos quadros internacionais é GDPR, correspondente à "General Data Protection Regulation". Em português, a sigla corresponde é RGDP, e por

679/2016, entrou em vigor em 25 de maio de 2018. Com ele, instaurou-se um novo paradigma de proteção de dados pessoais, capaz de influenciar condutas nas esferas pública e privada e, especialmente, nos ambientes informacional e digital.

No Brasil, ocorreu o mesmo com a Lei Geral de Proteção de Dados Pessoais (LGPD), ou Lei 13.709/2018, que entrou em vigor em setembro de 2020 (AGÊNCIA SENADO, 2020)[11], com exceção dos dispositivos referentes às penalidades. Assim como o RGPD, a lei brasileira visa a proteção da universalidade de bens intangíveis da pessoa humana, os denominados "dados pessoais", com o objetivo de resguardar a sua privacidade, da forma mais ampla possível, uma vez que os dados, quando analisados de forma combinada, resultam em informação de caráter estritamente pessoal. As leis e normas que foram evoluindo até alcançarem as versões amplas consolidadas supracitadas, procuraram fortalecer a posição da pessoa humana em relação às entidades que coletam e processam seus dados, reconhecendo gradualmente o desequilíbrio nessa relação que não era resolvido por medidas que simplesmente reconheciam o direito à autodeterminação informativa (DONEDA, 2011).

Internacionalmente, a discussão sobre a proteção de dados pessoais se inicia, mesmo que de forma discreta, em 1948, com a previsão do direito à não intervenção ou ataque à vida privada da pessoa humana, expresso na Declaração Universal dos Direitos Humanos. Em 1950, com mais ênfase, a Convenção Europeia dos Direitos do Homem prevê a proteção à vida privada e familiar dos indivíduos, de modo a reforçar o direito à privacidade como um direito humano universal e inviolável.

---

esta razão, é a sigla predominantemente adotada ao longo deste livro. UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). POLIDO, F. et al. Título: GDPR e suas repercussões no direito brasileiro. Subtítulo: Primeiras impressões de análise comparativa. IRIS, 2018.

11 A Lei Geral de Proteção de Dados entrou em vigor 18 de setembro de 2020. É um marco legal que regulamenta o uso, a proteção e a transferência de dados pessoais no Brasil. Fonte: Agência Senado

A comunidade europeia, entretanto, a fim de consolidar a proteção à vida privada dos indivíduos, no início da década de 1980 instituiu o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados: a Convenção n° 108/81 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao tratamento Automatizado de Dados Pessoais. Esta Convenção inovou ao prever especificamente, pela primeira vez, a proibição do tratamento de dados sensíveis da pessoa humana quando há intenção de torná-la identificável. (PARLAMENTO EUROPEU, 2020). Os dados sensíveis, para relembrar, são aqueles capazes de tornar uma pessoa identificável indiretamente ou de forma mediata, como informações sobre a raça, opinião política, a saúde, as convicções religiosas, a vida sexual ou o registo criminal de uma pessoa (SERPRO, 2020).

Nesta década, em 1988 no Brasil, em período de redemocratização, foi promulgada a atual Constituição Federal, incluindo o direito à privacidade como um direito fundamental, correspondente ao inciso X, do art. 5°, indicando que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação".

Em 1995, buscando aperfeiçoar as normas anteriores, a União Europeia promulgou a Diretiva 95/46/CE, que objetivava estabelecer, harmonizar e promover igualdade no tratamento de dados pessoais pelos estados-membros. Esta Diretiva foi substituída pelo atual RGPD. Atualmente, na Europa, além do RGPD, estão em vigor a Diretiva (UE) 2016/680, que garante a proteção de dados pessoais de vítimas, testemunhas e suspeitos de crimes, além de facilitar a cooperação transfronteiriça no combate à criminalidade e ao terrorismo, quando os dados forem utilizados pelas autoridades responsáveis pela aplicação da lei penal; a Diretiva 2002/58/CE sobre a proteção da privacidade no setor das comunicações eletrônicas; Regulamento (UE) n° 2018/1725 sobre a proteção no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, além de outras normativas setorias, mais voltadas ao combate ao terrorismo. (PARLAMENTO EUROPEU, 2020)

No Brasil, até a consolidação da importância da matéria e unificação das normas setoriais que regulam de forma direta ou indireta a proteção de dados, diversos dispositivos sobre o tema estavam espalhados em mais de quarenta normas. O Código de Defesa do Consumidor (CDC), de 1990, por exemplo, prevê em seu artigo 43 que o consumidor deve ter acesso às suas informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como suas respectiva fontes (MONTEIRO, 2018, p. 7). Vale ressaltar que o mercado de consumo é um dos maiores responsáveis pela crescente problematização relacionada aos dados pessoais. É para os fornecedores de produtos e serviços que os dados pessoais têm mais valor monetário direto, justamente para que eles possam localizar potenciais consumidores ou para que possam manipulá-los até chegarem às suas ofertas.

> Um dos setores da economia e do mercado que mais se vale do uso e tratamento de dados pessoais, principalmente para viabilizar decisões automatizadas para ofertar seus serviços, é o de consumo. Este setor é caracterizado pela necessidade de se entender o consumidor e, inclusive, influenciar seus hábitos (MONTEIRO, 2018, P. 6).

O uso intenso de informações pessoais pelo mercado de consumo leva a práticas indesejáveis, prejudiciais e abusivas e, portanto, a proteção ao consumidor, que é a parte mais vulnerável nesta relação, não pode falhar.

A diferença substancial entre a LGPD e o CDC entretanto, é que este último institui que o desrespeito às suas prerrogativas de defesa do consumidor caracteriza infração penal, punível com pena de detenção ou multa. A LGPD, por sua vez, prevê sanções de caráter administrativo e financeiro aos seus infratores.

Posteriormente, ainda no Brasil, em 1996, a Lei da Escuta Telefônica e em 2011, a Lei do Cadastro Positivo, também incluíram dispositivos de proteção aos dados pessoais, ambas seguindo a lógica da transparência sendo que, nesta última, é trazido pela primeira vez ao Brasil o direito à

explicação, juntamente com o direito à revisão de decisão realizada exclusivamente por meios automatizados, no âmbito da concessão de crédito e cálculo de risco de inadimplência.

Em 2013 ocorreu no Brasil o avanço mais significativo para que os cidadãos e o governo pudessem entender o que de fato acontece na internet. O Marco Civil da Internet foi fundamental.

Historicamente, é nítido que o RGPD foi construído a partir do reconhecimento da estatura jurídica fundamental do direito à privacidade e à proteção dos dados pessoais como garantidores de liberdades e direitos da pessoa natural, e, consequentemente, com base nestas premissas, no Brasil foi editada a LGPD. Em decorrência da rapidez do trânsito de informações na era digital, o RGPD foi elaborado em diversos níveis, positivando garantias fundamentais amplas, a fim de abranger, inclusive, hipóteses de violações futuras. Ou seja, o RGPD tem como base princípios e garantias que são tecnologicamente neutros (POLIDO, F. B. P. et al., 2018, p. 8).

A era da autodeterminação informativa exclusivista, portanto, parece ter dado um salto enorme para o seu fim. Até a entrada em vigor das legislações em comento, somente quem disponibilizava de poderes econômico, informativo e sociais e, inclusive, de tempo, eram capazes de reivindicar seu direito à privacidade relacionado à utilização indevida de seus dados pessoais, e modo geral. A partir de agora, espera-se que o cumprimento da proteção aos dados pessoais seja cumprido de forma natural

## 3 COMO AS INTELIGÊNCIAS HUMANA E ARTIFICIAL DECIDEM

O cérebro humano é a máquina mais fantástica da atualidade. Ele evoluiu por milhares de anos até seu estado atual. Como resultado da evolução contínua, somos capazes de entender os processos inerentes da natureza e entender as relações de causa e efeito. Com base nestas

percepções, somos capazes de aprender com a natureza e desenvolver máquinas e mecanismos semelhantes para evoluir e melhorar constantemente nossas vidas.

Fundamentalmente, a inteligência humana trabalha com o paradigma da reunião de informações sensoriais (visão, audição, toque, paladar, olfato), que são armazenadas de forma consciente ou inconsciente e processadas para tomar decisões em uma fração de milissegundo para agir em um contexto e estímulo situacionais (DESHPANDE; KUMAR, 2018, p.1). Tudo isto ocorre de forma natural. O cérebro humano, aproveitando-se da sua rede composta por bilhões de neurônios e suas interconexões, age sem esforço, utilizando-se de pouca energia.

Ocorre que a raça humana evoluiu de tal forma, que encontrou uma maneira de armazenar informações também em formato eletrônico. Isto, somado à expansão da internet, resultou na criação, ou divulgação, de mais dados nos últimos dois anos do que em toda a história da raça humana (O DILEMA DAS REDES, 2020).

A inteligência artificial (IA), termo cunhado pela primeira vez em 1956, ou o cérebro eletrônico, é capaz de armazenar volumes enormes de informações em alta velocidade, permitindo criar modelos e atingir altos níveis de precisão. Isto é o que chamamos de Big Data. O interessante nisto é a percepção de que a velocidade de armazenamento de informações é consistente em todas máquinas, quando compatíveis tecnologicamente. Entretanto, no caso do cérebro humano, as capacidades de armazenamento e processamento variam de acordo com os indivíduos, mesmo considerando aqueles em situação similar, de modo geral (DESHPANDE; KUMAR, 2018, p.4). Isto, consequentemente, gera resultados diferentes para situações similares.

Basicamente, a Inteligência Artificial é o núcleo da discussão acerca da tecnologia. O Aprendizado de Máquina, que é subcategoria da IA, corresponde ao modo no qual os computadores têm a capacidade de melhorar progressivamente o desempenho de uma tarefa específica com dados, sem serem diretamente programados. O que não era possível du-

rante muitas décadas. Por sua vez, o Aprendizado Profundo, é uma subcategoria do Aprendizado de Máquina que corresponde ao que se tem de mais inovador hoje, no sentido de autonomia de decisão das máquinas (ou computadores). É ele o responsável pelas tomadas de decisões exclusivamente automatizadas.

As duas categorias de Aprendizado Profundo mais relevantes são (i) a aprendizagem supervisionada e (ii) a aprendizagem não supervisionada. Como é fácil de se deduzir, a aprendizagem supervisionada é aquela que ocorre quando são apresentados ao algoritmo dados de entrada e as respectivas saídas (soluções), estas últimas não são apresentadas na aprendizagem não supervisionada, na qual o algoritmo descobre as saídas sozinho, buscando informações na sua base de dados.

Ademais, existe ainda uma terceira categoria de Aprendizado Profundo, é o Aprendizado por Reforço (RL). Este aprendizado se dá por meio de repetidas tentativas e erros, até que a máquina encontre uma solução para o problema no contexto em que se encontra, por um processo de captação de recompensas e penalidades, programado pelo cientista de dados. A partir deste processo, o modelo de IA deve descobrir como exEcutar a tarefa para maximizar a recompensa, começando com testes completamente aleatórios e terminando com soluções sofisticadas, desenvolvidas pela própria IA.

Inicialmente, por muitas décadas, os computadores somente seguiam instruções predefinidas. Esta limitação dos computadores tradicionais para responder a situações desconhecidas ou não programadas leva à pergunta: Uma máquina pode ser desenvolvida para pensar e evoluir como os humanos? Para se entender o ponto de divergência atual entre as inteligências humana e artificial, é possível traçar o seguinte paralelo: quando o humano dirige um carro, basta que o faça em uma pequena quantidade de situações e em determinadas ruas e estradas para que a inteligência humana possa aprender a reagir a novas situações e desencadear várias ações (aplicar pausas, virar, acelerar e assim por diante). Utilizando o exemplo de um carro autônomo, para que esta máquina seja programa de forma apropriada neste formato, a IA utilizará o modo

de Aprendizagem Profundo no modo RL, ou seja, muitas situações terão que ser simuladas para que a máquina conheça todos os tipos de situações possíveis a fim de evitar que cometa um grave erro quando uma nova situação, não prevista e calculada, não ocasione um grave acidente (DSA, 2020, C. 62).

## 4 A SOMA DOS VIESES ÍNTIMOS E (IN)CONSCIENTES DOS PROGRAMADORES DE MÁQUINAS (INSERÇÃO DE DADOS) E DOS JUÍZES DE DIREITO (FONTE DOS DADOS). QUAL É O RESULTADO?

Quando partimos do pressuposto que o processo de automação é uma inevitabilidade e reconhecemos a necessidade das decisões automatizadas, a questão se torna, então, como lidar com essa nova realidade e com as perguntas que esse cenário levanta. Em outros termos, *quais as implicações que são levantadas com a presença de decisões automatizadas em nossa realidade*? Para os fins deste tópico, iremos nos focar em alguns dos questionamentos éticos levantados pelo uso da inteligência artificial para o fim de realizar decisões judiciais.

Um ponto inicial dessa discussão é esclarecer que, apesar de ser superficialmente o caso, máquinas não são agentes neutros, especialmente quando usadas com o fim de determinar decisões judiciais. Esse fato já se torna claro quando temos em mente que a base pela qual essas decisões serão tomadas, a origem das informações, parte, da inteligência humana. Como bem pontuado por Daniel Henrique Arruda Boeing, decisões humanas estão sempre sujeitas a heurísticas e vieses, fato que foi explorado a fundo pela psicologia cognitiva, que trouxe à tona a possibilidade de erro na cognição humana (BOEING, 2019).

Existem vários exemplos que podem ser usados para reforçar esse argumento, mostrando como o processo de tomada de decisões pode ser afetada por aspectos subjetivos, implícitos e não completamente conscientes. Um exemplo desse processo pode ser observado em aprovação de currículos de emprego. Um estudo conduzido pelo instituto

estado-unidense *National Bureau of Economic Research* (NBER), indicam que currículos enviados a empregadores, nas regiões de Chicago e Boston, que contenham nomes que sugiram uma descendência afro-americana teriam menores chances de serem aprovados do que aqueles que contenham nomes que são normalmente associados a cidadãos caucasianos (NBER). Nessa mesma linha, podemos pontuar uma pesquisa similar, em que uma pesquisa feita pela *Harvard Business School*, que demonstrou que indivíduos afro-americanos ou hispânicos passaram a ocultar suas descendências étnicas de seus currículos para assim obter maiores chances de serem contratados, e que essa estratégia, de fato, funcionou (HBSWK).

Essas pesquisas implicam a existência de um *bias*, uma tendência, não necessariamente intencional, que afeta o processo humano de tomada de decisões. É bastante lógico, seguindo essa linha de raciocínio, que essa subjetividade estaria presente, também, na tomada de decisões judiciais. Um dos cenários em que é possível perceber, de forma mais clara, como esse viés afeta diretamente decisões judiciais é no meio penal. É por meio do direito penal que se escancara não apenas a presença desse viés, como também suas consequências diretas. É um fato que foi percebido por autores como o professor Eugenio Raúl Zaffaroni, que analisou o direito penal enquanto o reflexo de um processo social de exclusão, na qual determinadas classes, membros da sociedade, são caracterizados como inimigos. O professor Zaffaroni entende que esse processo de escolha do inimigo, é diretamente consequente de um projeto de poder, de forma similar há como Carl Schmitt compreende o inimigo externo, o estrangeiro, ou seja, *todos aqueles que incomodam o poder*, os indesejáveis (ZAFFARONI, 2007, p. 22 - 23).

Teorizar quanto a *quem* seriam esses indesejáveis no Brasil é algo que pode ser, estatisticamente, sugerido de forma bastante convincente. Por exemplo, quando temos em mente que, segundo dados recentes, cerca de 64% da população carcerária, no Brasil, é negra, sendo também a maioria da população morta em ações policiais, cerca de 74%, se tem uma ideia quanto a que grupo de cidadão o *viés de inimigo* estaria focado

no Brasil neste caso. Há quem diga que o encarceramento tem cor (AGÊNCIA SENADO).

Esses dados revelam a presença ativa de um *viés* em decisões judiciais, corroborando com a perspectiva de Zaffaroni quanto ao tema. Um fato que deve ser reiterado, e explorado com maior profundidade, é que, no geral, não é um processo completamente consciente, mas sim o reflexo de um processo imparcial de tomada de decisões, realizado por juízes com seus próprios *bias*. Em sua tese de doutorado, o autor Eduardo José da Fonseca Costa chama a atenção para a pesquisa dos psicólogos israelenses Daniel Kahneman e Amos Tversky, que pontuavam a existência de *ilusões cognitivas* (COSTA, 2016, p.46). Nas palavras do autor:

> No estudo, desafiando modelos racionais até então dominantes, eles relacionaram e sistematizaram as regras heurísticas, definindo-as como as **regras cognitivas que todo o ser humano aplica inconscientemente ao processar uma informação que recebe do exterior** e que permitem reduzir as tarefas complexas de atribuir probabilidade e predizer valores a operações de juízo mais simples. Enfim, trata-se de formas disfuncionais de processar a informação, que afetam o raciocínio lógico-abstrato e que acontecem de forma possível em circunstâncias particulares em todos os países e culturas (COSTA, p. 46).

Costa reforça que não se trata de desvirtuamentos de pensamento, como aqueles gerados por emoções, como ódio ou medo, mas sim de erros sistemáticos de opinião, resultantes do projeto mecanismo cognitivo, ou seja, são erros gerados por vieses e predisposições automáticas que todos os indivíduos estariam sujeitos, independentemente de sua inteligência ou racionalidade (COSTA, p. 47). Ainda, o autor esclarece que o reconhecimento desses erros não significa um abandono de modelos de escolha racional, pois esses modelos podem ser usados em situações "transparentes", mas tais premissas são violadas em contextos "não-transparentes", onde existe um risco de incerteza (COSTA, p. 59).

A questão central, em nossa atual discussão, é a seguinte: podem essas ilusões cognitivas estarem presentes em decisões realizadas por

juízes, humanos, que deveriam ser imparciais? A resposta automática que poderia se chegar, com o que foi exposto até o momento, seria um provável "sim". No entanto, Eduardo Fonseca é extremamente cuidadoso ao analisar a presença de ilusões cognitivas nas decisões judiciais. Ele pontua que o ramo de conhecimento científico de *Behavioral Law and Economics*, ainda se encontra em fase de infância, se resumindo a uma coleção de vieses e heurísticas que necessita ainda ser unificada dentro de uma análise teórica, prosseguindo de forma modesta suas análises e experimentos (COSTA, 88). *Ainda assim*, o autor pontua com que os trabalhos de campo que já foram realizados indicam que juízes provavelmente também estão sujeitos a ilusões cognitivas (COSTA, 88).

> [...] a judicatura se deve cercar de *cuidados institucionalizados*, que propiciem a mitigação, a neutralização ou a eliminação mesma dessas ilusões, garantindo uma margem segura de atuação funcionalmente imparcial. Noutras palavras: embora a ideia de *boundedly rational judge* seja um modelo pendente de testes de falseabilidade, o simples risco de que esse modelo seja verídico justifica a reforma cautelar dos sistemas brasileiros positivos de direito processual a fim de que prevejam procedimentos técnicos de isolamento e desenviesamento até então ignorados (COSTA, 88).

Achamos importante reforçar aqui o ponto central da citação acima. O autor entende que a suspeita da presença de ilusões cognitivas já basta para justificar uma reforma cautelar dos sistemas positivos do direito processual. Ou seja, o *risco* de que essas ilusões cognitivas estejam presentes é, por si mesmo, grande demais para ser permitido. A ideia de que o aplicador da lei possa ter sua perspectiva de realidade influenciada por ilusões cognitivas, seria um argumento a favor de repensar os sistemas positivos do direito processual. Esse é um ponto fundamental que é aprofundado pelo autor logo em seguida em seu texto. Ele entende que **a imparcialidade judicial é o núcleo duro do devido processo legal, não podendo ser tolerados riscos de potenciais quebras inconscientes de imparcialidade** (COSTA, 89). Conforme bem pontua Eduardo Cos-

ta: *um sistema processual não pode consentir em quebras desse jaez, pois isso equivaleria a consentir em inconstitucionalidade* (COSTA, 89).

Essa perspectiva se casa muito bem com o que foi visto anteriormente na obra de Zaffaroni. O autor se preocupa especificamente com a influência das narrativas construídas em torno de certos cidadãos como "inimigos", como uma ameaça real às garantias constitucionais. O autor defende que o direito penal deve caminhar enquanto um apêndice do direito constitucional de um estado de direito, reduzindo e contendo o poder punitivo dentro dos limites menos irracionais possíveis (ZAFFARONI. p. 172). Nesse sentido, ele aponta que, no caso de o direito penal não conseguir que o poder jurídico assuma essa função, tanto ele, quanto o próprio Estado de Direito iria perecer, dando lugar apenas a um Estado de polícia, focado em procurar e exterminar os "inimigos" dentro das relações de poder daquele Estado (ZAFFARONI. p. 172).

O direito penal, se tratando de uma das faces mais opressivas do poder jurídico, com sua capacidade de limitar a liberdade dos cidadãos diretamente, seria uma das frentes onde os riscos da parcialidade, conscientes ou não, de juízes, se refletiria de maneira mais direta, no entanto, se trata de um risco presente em *todas* as áreas do direito. Juízes, especialmente em situações de excesso de demanda, não teriam condições, ou mesmo incentivo, de analisar detalhadamente as demandas que chegam até eles em todas as suas particularidades e complexidades, o que os leva a criar "atalhos mentais" para decidir (BOEING, p. 60). Tais atalhos servem como um meio de configurar "decisões pré-prontas", não apenas reduzindo a carga de trabalho mental, mas também criando uma sensação de coerência e conforto cognitivo (BOEING, p. 60).

Todas essas considerações são essenciais quando chegamos ao ponto-chave desse tópico, algo que foi perfeitamente resumido por Daniel Boeing:

> Uma inteligência artificial será tão boa quanto for o material por meio do qual ela é treinada, de forma que dados tendenciosos farão com que ela chegue a resultados igualmente ruins. Mais que isso, a depen-

> der da forma como são implementados, algoritmos não apenas irão reproduzir o comportamento decisório humano, mas desenvolver seus próprios vieses e, inclusive, acentuar certas distorções (BOEING, p. 60).

Uma inteligência artificial baseada em decisões judiciais corre o risco de reproduzir os mesmos preconceitos, vieses e tendências, conscientes e inconscientes dos juízes que formularam tais decisões. Uma inteligência artificial, ao contrário do que se poderia pensar a priori, não é neutra, ela depende de um modelo simplificado de realidade que pode ser facilmente compreendida e por onde se pode inferir diversas ações e pensamentos (O'NEIL, 2016, p. 26). O resultado é que essa inteligência artificial teria de praticar apenas uma única atividade, com enormes pontos cegos, onde podem ser refletidos os julgamentos e prioridades de seus criadores (O'NEIL, p. 26). Valores e desejos são reproduzidos sem que exista uma ação consciente nesse sentido pelos seus desenvolvedores, eles influenciam os dados que são coletados e as perguntas que são feitas, nesse sentido, modelos nada mais seriam do que opiniões traduzidas em matemática (O'NEIL, p. 27). O resultado é um cenário em que um modelo poderia estar funcionando perfeitamente aos olhos de seus programadores, mas não para aqueles que são diretamente afetadas por ele (BOEING, p. 62). Ou seja, para os titulares dos dados que estariam sendo sujeitos às decisões automatizadas.

Algoritmos, nesse sentido, podem ser armadilhas, opiniões disfarçadas com a suposta imparcialidade de uma máquina. Por isso, algoritmos podem se tornar perigosos.

> Acontece que, quando embutidas em um algoritmo, além de se revestirem de autoridade científica, tais opiniões passam geralmente despercebidas, pois não são inteligíveis para a maior parte das pessoas. Todavia, elas continuam (e sempre continuarão) a ser, simplesmente, opiniões, mas que agora estão perpetuadas e disfarçadas (BOEING, p. 62).

Essa prerrogativa se torna especialmente assustadora no meio jurídico, especialmente tendo em mente as considerações feitas no decorrer desse capítulo. Levando em conta os vieses e ilusões cognitivas que estão presentes nas decisões judiciais, os riscos pontuados por Zaffaroni e Costa são bastante reais, sendo necessário se levar seriamente em consideração, podendo ser reproduzidos de maneira a tornar injustiças sociais ainda mais toleradas e sistematizadas. Esse processo representa um risco genuíno a diversos grupos vulneráveis, e a própria segurança jurídica que deve ser prezada e defendida dentro de uma democracia constitucional. Nesse contexto, um direito a questionar decisões automatizadas se torna *essencial* para a aplicação desse sistema. Eis que entra em cena o direito a explicação.

## 5 DIREITO À EXPLICAÇÃO

Diante do que foi exposto até o momento, é seguro dizer que a presença de decisões automáticas acompanha consigo a inevitabilidade de seus riscos. Mecanismos para impedir, ou ao menos, coibir, a sistematização de decisões que possam gerar consequências nocivas e desiguais para aqueles que serão afetados diretamente pela inteligência artificial, são fundamentais. Neste contexto, a necessidade de garantir aos titulares de dados, a transparência e a possibilidade de acessar os dados que estão sendo tratados pelos agentes de tratamento, e que resultarão em decisões automáticas, passa a ser fundamental. O direito à explicação, previsto pelo RGPD, inicialmente, é a complementação essencial que permitirá vislumbrar com clareza o trajeto dos dados e os potenciais erros e acertos presentes no processo de tomada de decisão por inteligência artificial, de modo a possibilitar o treinamento da IA para que se aproxime cada vez mais de se tornar um modelo seguro de tomada de decisões imparciais e justas, que é o ideal que se busca por meio da utilização do aprendizado da máquina para esta finalidade.

Em primeiro lugar, a princípio, não seria necessário que decisões tomadas por juízes-robôs sejam transparentes, visto que esse seria um

papel cumprido por um juiz revisor humano (BOEING, p. 70). Entretanto, quanto mais bem "explicadas" sejam as decisões tomadas por robôs, mais convincente seria argumentar a legitimidade delas, sendo possível obter algo similar à transparência caso os algoritmos sejam capazes de expor termos e frases que teriam maior peso na qualificação do caso, bem como quais leis e precedentes foram aplicados para decidir quanto a sua resolução (BOEING, p. 70 - 71). O objetivo não é, claro, esperar uma transparência a nível de minúcias de funcionamento, mas apenas no sentido de tornar suas decisões inteligíveis em um nível humano (BOEING, p. 71).

Juízes humanos, a princípio, não serão substituídos completamente por máquinas em um futuro próximo. O motivo desse fato não tem a ver necessariamente com a complexidade intelectual das tarefas processadas pela inteligência artificial, mas sim por conta das diversas frentes que são necessárias para o trabalho de um juiz, incluindo linguagem, pesquisa, habilidades sociais e solução criativa de problemas. Máquinas teriam a função de decidir, um aspecto específico da função de um juiz, talvez a mais mecânica de suas funções: o ato de analisar como resolver determinado caso concreto. Ironicamente, as ações que poderiam tornar as decisões mais seguras, aquelas que naturalmente cobraríamos de um juiz de carne e osso, como fundamentação e embasamento legal, são exatamente aquelas que prejudicariam a eficiência de sua performance enquanto máquinas (BUOCZ, p. 48 - 49). É uma exigência diferente daquela feita a um juiz humano, não se trata de saber a linha de pensamento da máquina, apenas a explicação específica de como chegou a uma determinada decisão (BUOCZ, p. 49). Na hipótese de juízes-robôs decidirem individualmente um processo, o fato de terem suas metodologias expostas dessa maneira terá um efeito direto no ato de posterior análise judicial feita por um juiz humano.

O processo de fundamentação seria menos comum em ações simples (*plain cases*), onde os termos gerais do caso necessitariam de pouca ou nenhuma interpretação e onde o reconhecimento de instâncias parecem não muito problemáticas, ou, apropriadamente, automáticas, existindo um acordo geral em julgamentos quanto as aplicabilidades dos

termos classificadores (BUOCZ, p. 56). Casos difíceis (*hard cases*) surgem quando as respostas demandadas não são tão claras pela lei, desconhecidas ou profundamente desconcertantes (BUOCZ, p. 56). Se tratam de situações onde as circunstâncias do caso são colocadas na direção oposta das regras relevantes ou o caso é o primeiro de seu gênero (BUOCZ, p. 56).

Em contextos como esse, seria uma estratégia interessante, para salvar custos legais, trazer apenas casos difíceis para revisão, frente a um juiz humano, pois evidências sugerem que decisões de casos simples tomadas por uma inteligência artificial são raríssimas vezes questionadas ou revogadas, esse é um cenário lógico, quando levamos em conta o fato de que decisões por inteligência artificial são feitas para apresentar uma performance superior a humana diante da aplicação de regras *claras* (BUOCZ, p. 56). Ainda, juízes humanos podem agir no sentido de corrigir máquinas na decisão de casos simples quando elas cometem erros óbvios, impedindo o risco de uma rejeição pública de inteligências artificiais no poder judiciário (BUOCZ, p. 57).

Quanto aos casos difíceis, esse parece oferecer o limite para a superioridade da inteligência artificial, não por um limite na tecnologia, mas sim pelo limite humano, afinal, nesses cenários, o quão "correta" seria uma decisão, é um fator em segundo plano se comparado ao quão compreensível é sua fundamentação (BUOCZ, p. 56). Por se tratar de um caso sem solução clara e precisa, tanto o humano quanto a máquina teriam chances de tomar uma decisão errada, apesar da maior chance estatística de erro ser por parte do humano, saindo da realidade de casos simples, em que seria claro que a máquina estaria decidindo corretamente ou se teria cometido um erro (BUOCZ, p. 56).

Feitas as considerações quanto a decisões automáticas, resta ainda analisar como que tais mecanismos seriam entendidos dentro do território brasileiro. Nesse contexto, é relevante entendermos como a legislação brasileira tem lidado com essa necessidade intrínseca do sistema de inteligência artificial, especialmente em relação a legislação ao qual o Brasil usa como base. O entendimento legal brasileiro quanto ao tema de proteção de dados é bastante próximo do modelo europeu, já

que reconhece seu status de direito fundamental como um desdobramento da tutela de privacidade (POLIDO, p. 25). No entanto, existem ainda diversas ineficiências na legislação brasileira, há lei, geral ou especial, que regule de maneira abrangente a atividade de tratamento de dados pessoais feita por entidades públicas ou privadas, seja dentro de um ambiente interconectado em redes digitais ou não (POLIDO, p. 25). As peculiaridades da lei brasileira dentro do tema de proteção de dados podem ser entendidas pela sua própria estrutura constitucional. Nesse sentido,

> Por sua vez, na Constituição da República de 1988, apesar de o direito à privacidade ter sido consagrado no artigo 5º, incisos X e XI, foi no inciso LXXII que o constituinte cuidou diretamente das informações pessoais e de seu estatuto jurídico, positivando a garantia do habeas data. Esta, entretanto, possui função jurídica muito restrita se confrontada com o homônimo instituto argentino (POLIDO, p. 25).

No entanto, a comparação com a legislação europeia ganhou um aspecto mais preocupante diante de alterações que foram realizadas pelo presidente da república na aprovação da sua Lei Geral de Proteção de Dados (Lei 13.709/2018). O presidente vetou no projeto de lei os artigos que defendiam pela possibilidade de revisão humana em decisões tomadas por robôs (CONSUMIDOR MODERNO). Posteriormente, o veto presidencial foi mantido pelo senado federal pois, apesar da maior parte dos senadores ter opinado contra o veto (40 a 15 votos), o necessário para derrubar o veto na casa legislativa é de 41 votos. Na Câmara dos Deputados, o veto foi rejeitado por 261 votos a 163, nessa hipótese, o número mínimo de votos para derrubar um veto presidencial é de maioria absoluta, ou seja, 257 votos de derrubados – o que ocorreu (CONSUMIDOR MODERNO). Em comparação, a GDPR, em seu art. 22, reconhece a importância da revisão humana das decisões automatizadas. De fato, a lei europeia é tão certa quanto a necessidade da revisão judicial, que os casos que dispensam essa possibilidade são a *exceção*, não a regra, conforme se observa a seguir,

1- The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2- Paragraph 1 shall not apply if the decision:

a) is necessary for entering into, or performance of, a contract between the data b) subject and a data controller;

is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c) is based on the data subject's explicit consent.

3- n the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4- Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

O texto da LGPD constava equivalente similar em sua redação, antes do veto presidencial. Agora, essa revisão é apenas possível em duas hipóteses: *(i) a natureza e o porte da entidade ou (ii) o volume de operações de tratamento de dados* (MARRAFON, 2019). Essa decisão não veio sem resistência, de fato, no (extenso) parecer apresentado pelo relator da Câmara de legisladores, diversos argumentos foram levantados em defesa da reforma dessa decisão. Destaca-se, aqui,

> Com a popularização do uso da Inteligência Artificial e outros mecanismos automatizados para a prestação de serviços e a consequente retirada da pessoa humana, o exercício dos direitos humanos, de cidadania e do consumidor (previstos no art. 2, VI e VII) são dificultados e, por consequência, enfraquecidos. Ademais, a inexistência de humanos dificulta em sobremaneira a interação com controladores por parte de pessoas que possuam deficiência de julgamento ou experiência, o que poderia levar a práticas abusivas (SENADO).

Ainda, o relatório pontua que a retirada dessa previsão enfraqueceria a aplicação de garantias previstas na própria LGPD, especificamente o exercício dos direitos humanos, de cidadania e do consumidor previstos em seu art. 2º, VI e VII (SENADO). O relatório também argumenta que os algoritmos que processam os dados são baseados em cálculos probabilísticos e estatísticas e que, por não englobarem o universo dos titulares e seus comportamentos, geram o risco de levar a erros e desvios padrões, uma vez que se baseiam apenas em amostras e intervalos de confiança, além de estarem sujeitos a incorreções próprias do desenvolvimento tecnológico (SENADO). Por fim, o relatório argumenta que a retirada entra em conflito com a previsão da GDPR, que poderia resultar em dificuldades na integração comercial e a geração de oportunidades e investimentos (SENADO).

Apesar de tais argumentos, a posição do presidente se manteve. Seu argumento foi definido da seguinte maneira:

> A propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária (PLANALTO).

O argumento falha em confrontar de maneira satisfatória as críticas apresentadas ao veto. O relatório tinha seu foco nos riscos humanos e nas inseguranças que a ausência dessa revisão traria para cidadãos. Mas não ignora que o fato dessa determinação legal ser incoerente com outras previsões similares, mais obviamente, a GDPR europeia, ao qual nossa LGPD tem como *base*, poderia gerar dificuldades em investimentos e integração comercial com a Europa, bem como outros países que prevêem tais garantias. Ou seja, se trata de uma análise que falha em entender os interesses econômicos e *humanos* que justificam a possibilidade de revisão.

## 6 CONSIDERAÇÕES FINAIS

O desenvolvimento tecnológico que vivemos torna as decisões automáticas inevitáveis. Inteligências artificiais se tornam mais desenvolvidas e complexas a cada dia, prometendo um futuro onde processos judiciais poderiam ser solucionados com pouca ou nenhuma interferência humana. Nesse cenário, se torna fácil esquecer que a base para esses programas, para esses juízes robôs, ainda é humana, estando sujeitos a reproduzir acriticamente vieses e preconceitos de juízes de carne e osso. Diante de tal cenário, a possibilidade dessas decisões serem questionadas, de maneira a apontar tais imparcialidades, é um aspecto *fundamental* dessa nova realidade.

É por conta desse fato que omitir a possibilidade de revisão de uma decisão judicial eletrônica é tão grave, pois garante não apenas a perpetuação de injustiças e desigualdades sociais, mas sua *sistematização* em níveis ainda mais profundos do que já se encontram. É relevante relembrar que esses vieses não são sequer conscientes necessariamente, podendo estar presentes nas decisões que servem de base para decisões eletrônicas sem uma intenção por parte do juiz. Ainda, a impossibilidade de rever decisões de inteligências artificiais também gera o risco de sistematizar erros cognitivos de outras naturezas. São riscos grandes demais para serem banalizados, pois afetam negativamente os objetivos pelos

quais essas tecnologias foram desenvolvidas e, em uma maior escala, a própria sociedade democrática que deveriam garantir.

## REFERÊNCIAS

AGÊNCIA SENADO. **Lei Geral de Proteção de Dados entra em vigor.** Senado Federal, 2020. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor. Acesso em: 21 set. 2020.

CHAGAS, Edgar Thiago De Oliveira. Deep Learning e suas aplicações na atualidade. **Revista Científica Multidisciplinar Núcleo do Conhecimento**. Ano 04, ed. 05, vol. 04, pp. 05-26, 2019.

DATA SCIENCE ACADEMY. Título: Deep Learning Book. Data Science Academy, 2020. eBook Disponível em: http://deeplearningbook.com.br/deep-learning-a-tempestade-perfeita/.

DESHPANDE, Anand. KUMAR, Manish. **Inteligência Artificial para Big Data**. eBook Packt, 2018.

DONEDA, Danilo. **A proteção de dados pessoais como um direito fundamental.** Joaçaba: Espaço Jurídico, 2011.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de dados Pessoais. Diário Oficial da União, Brasília, DF, n. 157, publicado em 15/08/2018. Seção 1, página 59.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?** eBook: Instituto Igarapé, 2018.

O DILEMA DAS REDES. Direção: Jeff Orlowski. Produção: Larissa Rhodes. Estados Unidos: Netflix, 2020.

Parlamento Europeu. Título: **Proteção dos Dados Pessoais.** Parlamento Europeu, 2020. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em: 20 set. 2020.

POLIDO, F. B. P. et al. **GDPR e suas repercussões no direito brasileiro. Primeiras impressões de análise comparativa**. Belo Horizonte: Instituto de Referência em INternet e Sociedade (IRIS), 2018.

SERPRO. Título: **Proteção de Dados**, subtítulo: Dados Sensíveis. SERPRO, 2020. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd. Acesso em: 20 set. 2020.

# Capítulo III

# O DIREITO DE EXPLICAÇÃO DAS DECISÕES TOTALMENTE AUTOMATIZADAS NO RGPD EUROPEU E NA LGPD BRASILEIRA

*Letícia Canut*[1]

*Heloísa Gomes Medeiros*[2]



**RESUMO**

A obscuridade ou falta de transparência dos algoritmos, em decorrência dos efeitos discriminatórios ou vieses que apresentam, é tema de constante pesquisa no âmbito das ciências sociais. No presente artigo, examina-se este assunto no contexto do Regulamento Geral de Proteção de Dados da União Européia (RGPD) e da Lei Geral de Proteção de Dados brasileira (LGPD), em especial, o comumente denominado "direito de explicação das decisões totalmente automatizadas". O objetivo da pesquisa consiste em demonstrar que o direito de explicação não se limita a uma dimensão subjetiva e que pode assumir uma abordagem mais ampla, sob uma dimensão objetiva. Identificou-se que algumas características e elementos permitem apurar uma dimensão objetiva do direito em pauta, conectada às políticas e ferramentas apropriadas à essa dimensão como, por exemplo, os relatórios de impacto à proteção de dados. Demonstrou-se, por meio da análise comparativa, que o âmbito internacional é terreno fértil para o debate, enquanto no território nacional os debates ainda são tímidos ou não conectados diretamente ao direito de explicação.

**Palavras-chave:** Decisões automatizadas; Direito de explicação; Lei Geral de Proteção de Dados Brasileira; Regulamento Geral de Proteção de Dados da União Européia.

1 Pós-doutora em Direito pela Universidade Federal do Paraná (UFPR), com auxilio do CNPq. Doutora e mestra em Direito pela Universidade Federal de Santa Catarina (UFSC). Graduada em Direito pela Universidade Federal de Uberlândia (UFU). Pesquisadora do Grupo de Estudo em Direito Autoral e Industrial (GEDAI/UFPR).Professora do curso de direito do Centro Universitário Estácio de Santa Catarina. Advogada. E-mail: leticiacanut@gmail.com

2 Doutora e mestra em Direito pela Universidade Federal de Santa Catarina (UFSC). Graduada em Direito pela Faculdade São Luís/MA. Pesquisadora do Grupo de Estudo em Direito Autoral e Industrial da Universidade Federal do Paraná (GEDAI/UFPR). Professora Universitária. Advogada. E-mail: medeiroshg@gmail.com

## INTRODUÇÃO

Os software e algoritmos, que viabilizam as decisões automatizadas, têm sido fonte motivadora de pesquisas das autoras deste trabalho desde o ano de 2017. Os temas foram examinados sob diferentes abordagens para observar, por exemplo, como afetam o direito de informação do consumidor, os princípios da publicidade e da fundamentação das decisões judiciais e implicações do direito do autor sobre o software para a governança dos algoritmos. No contexto destas abordagens a obscuridade/falta de transparência dos algoritmos foi uma constante.

Apesar da grande conexão dessas temáticas com a proteção de dados pessoais, os interesses levantados naqueles momentos, em conjunto com a necessidade de delimitação do objeto de pesquisa, fizeram com que a proteção de dados não fosse uma variável analisada.

Com essa bagagem e diante da oportunidade de desenvolver uma pesquisa comparativa acerca da proteção de dados pessoais no Regulamento Geral de Proteção de Dados da União Européia (RGPD) e na Lei Geral de Proteção de Dados brasileira (LGPD), a seleção do tema de estudo não poderia ser diferente: optou-se por examinar aquele que vem sendo denominado de "direito de explicação". A delimitação do tema foi um desafio tendo em vista, especialmente, os posicionamentos divergentes e os diversos pontos polêmicos levantados a partir das previsões do RGPD no âmbito internacional.

A partir disso definiu-se o problema que irá nortear a pesquisa: analisar se e em que medida é possível identificar, a partir do RGPD e seus reflexos sobre a LGPD, uma abordagem que ultrapassa a dimensão individual do direito de explicação. Parte-se da hipótese de que, apesar de a dimensão individual ter sido o centro dos debates, novas discussões sinalizam para uma dimensão que tira o foco do titular de dados. O objetivo é demonstrar que o direito de explicação pode assumir uma abordagem mais ampla, sob uma dimensão objetiva.

Para tanto, o trabalho é dividido em três tópicos. O primeiro explica o tratamento totalmente automatizado de dados no RGPD e na LGPD, o

segundo apresenta o debate originário sobre o direito de explicação a partir do RGPD e o direito de explicação na LGPD, e o terceiro expõe sobre os diferentes tipos de transparência das decisões automatizadas e uma perspectiva objetiva do direito de explicação.

O artigo utiliza o método dedutivo, por meio de pesquisa descritiva, abordagem qualitativa, procedimentos de pesquisa bibliográfica e documental e método auxiliar comparativo.

Destacam-se ainda alguns aspectos apontados pela doutrina e que se consideram preliminares à análise proposta neste artigo:

(i) O reconhecimento da inegável influência do RGPD na LGPD mas, também, das particularidades entre tais normas, como a técnica legislativa utilizada, que influenciam no estudos comparativos das legislações. O RGPD apresenta orientações interpretativas que não se repete na LGPD (BIONI, MENDES, 2019). Essa diferença é essencial para a análise proposta neste artigo, tendo em vista que grande parte das discussões acerca do direito de explicação gravitam em torno do disposto no considerando 71 do RGPD, sendo este o único momento em que a a palavra explicação aparece de forma expressa;

(ii) Tendo em vista que a pesquisa também baseia suas análises nas "diretrizes interpretativas emitidas por um grupo anteriormente conhecido como Grupo de Trabalho do Artigo 29[3] e agora denominado Comitê Europeu de Proteção de Dados" , cabe destacar que tais diretrizes, apesar de não terem "força direta de lei", consistem em "indicativos de como os aplicadores interpretarão a lei", tendo um papel significativo na prática (MARGOT, 2019, p. 194). Tais orientações serão denominadas, no presente trabalho apenas como diretrizes/orientações do Grupo de trabalho do artigo 29 ou apenas como Diretrizes; e

[3] Orientações/Diretrizes do Grupo de trabalho do artigo 29 sobre as decisões individuais automatizadas e a definição de perfis para efeitos do RGPD. (GRUPO DE TRABALHO DO ARTIGO 29, 2018)

(iii) O fato de que o RGPD, diferentemente da LGPD, é consequência de uma trajetória da sociedade europeia que ocorreu ao longo do tempo sobre o tema da proteção de dados pessoais (BIONI, MENDES, 2019).

## 1 O TRATAMENTO TOTALMENTE AUTOMATIZADO DE DADOS NO RGPD E NA LGPD

O RGPD refere-se ao tratamento automatizado de dados em diferentes oportunidades, deixando esse tipo de tratamento em evidência, por exemplo: No artigo 4.º(2), ao definir *tratamento;* no artigo 2º (1), ao dispor sobre o âmbito de aplicação material do RGPD; no artigo 4.º(4), quando da "definição de perfis[4]". (PARLAMENTO EUROPEU, 2016)

Mesma preocupação não é observada na LGPD ao conceituar *tratamento*, no artigo 5º, inciso X, e ao estabelecer seu âmbito de aplicação no artigo 3º. Nessas oportunidades não se ocupa em qualificar o tratamento como "automatizado". Além disso, o termo "perfil"[5] sequer foi objeto de conceituação, constando apenas no § 2º[6] do artigo 12 ,sobre dados anonimizados. Isso, no entanto, não significa exclusão de tal tipo de tratamento vez que a forma de redação aberta do texto abrange qualquer tipo de tratamento. (PARLAMENTO EUROPEU, 2016)

---

4 Importante ressaltar que os perfis não envolvem, necessariamente, uma decisão automatizada. Nesse sentido: "As decisões automatizadas podem ser realizadas com ou sem definição de perfis; a definição de perfis pode ocorrer sem serem realizadas decisões automatizadas. Contudo, a definição de perfis e as decisões automatizadas não constituem necessariamente atividades levadas a cabo separadamente. […] (GRUPO DE TRABALHO DO ARTIGO 29, 2018, 2018, p. 8).

5 Considerando as grandes influências do texto europeu para a elaboração da Lei brasileira, nota-se que o tema "perfilização", não teve recepção integral do texto europeu. Dentre outros fatores, a LGPD "[…] é menos restritiva com relação à perfilização do ponto de vista de (i) ausência de um conceito jurídico expresso e (ii) ausência de uma norma geral proibitiva ao profiling, como ocorre na União Europeia."(ZANATTA, 2019, p. 20).

6 "Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada."

Tanto a norma européia quanto a brasileira apresentam previsões expressas acerca de um tipo específico de tratamento automatizado de dados: aquele exclusivamente ou unicamente automatizado. Ainda que se considere apenas o texto vinculativo do RGPD, o tema envolve um conjunto de artigos e incisos: artigos 22 (1), 22 (2), 22(3) e 22(4)e sua conexão com os direitos de ser informado constantes nos artigos 13 (2) alínea f), e artigo 14 (2), alínea g) e o dever de acesso constante no artigo 15 (1), alínea h). Já na lei brasileira o tema envolve número menor de dispositivos, sendo marcante o artigo 20 e seus parágrafos, oportunidade em que os "perfis" são tratados juntamente com as decisões tomadas unicamente com base em tratamento automatizado, apresentando, ainda, relação com o §2 do artigo 12.(PARLAMENTO EUROPEU, 2016)

O artigo 22 (1) do RGPD garante ao titular dos dados "o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, *que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar*". Apesar de todas as discussões geradas no âmbito acadêmico acerca de esta previsão significar uma proibição geral ou um direito de se opor a tal tipo de decisão, de acordo com as diretrizes do Grupo de trabalho do artigo 29 trata-se de proibição geral, que se aplica independentemente de o titular dos dados adotar uma medida relativa ao tratamento dos seus dados pessoais", e que "as pessoas estão automaticamente protegidas dos possíveis efeitos deste tipo de tratamento" (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 21,22).

O significado do termo *unicamente automatizadas,* outro tema muito debatido no âmbito acadêmico, também foi esclarecido nas diretrizes do Grupo: são compreendidas como aquelas em que não há nenhum tipo de intervenção humana. "Se um ser humano examinar e ponderar outros fatores ao tomar a decisão final, esta não será 'tomada exclusivamente com base' no tratamento automatizado. O responsável pelo tratamento não pode eximir-se do disposto no artigo 22.o fabricando uma intervenção humana. […]".. Além disso, consta que no âmbito da sua avaliação de impacto sobre a proteção de dados (AIPD),

" compete ao responsável pelo tratamento identificar e registar o grau de intervenção humana no processo decisório e a fase em que essa intervenção ocorre". (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 23)

A proibição geral do 22(1) é afastada diante de três exceções - 22(2) alíneas *a, b* e *c* - ou seja, é permita a decisão tomada exclusivamente com base no tratamento automatizado, quando*:*

> *a)* For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados. (PARLAMENTO EUROPEU, 2016)

O fato de o consentimento afastar tal proibição e de ser fator constante no dia-a-dia dos titulares de dados, acaba possibilitando um cenário marcado por tais decisões, ainda que a regra seja a proibição geral. Não por acaso, o artigo 22(3), prevê que tanto no caso de consentimento (c) quanto de necessidade para celebração ou execução de contrato (a), são exigidas dos responsáveis pelo tratamento de dados que recorrem a tais tipo de decisões *medidas adequadas para salvaguardar* "os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, *obter intervenção humana* por parte do responsável, *manifestar o seu ponto de vista* e *contestar a decisão*" (grifo nosso). (PARLAMENTO EUROPEU, 2016)

Ao resumir o artigo 22, as Diretrizes do grupo de trabalho do artigo 29 reforça, dentre outros pontos, a necessidade de medidas para tais salvaguardas e esclarecem que

> incluem o direito de ser informado (contemplado nos artigos 13.o e 14.o – concretamente, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas para o titular

> dos dados) e as garantias, a saber, o direito de obter intervenção humana e o direito de contestar a decisão (contemplados nos artigo 22.o, n.o 3) (GRUPO DE TRABALHO DO ARTIGO 29, 2018,, p. 22)

Mencionam, ainda, que tais medidas "devem incluir, no mínimo, um meio através do qual o titular dos dados *possa obter intervenção humana, m*anifestar o seu ponto de vista e contestar a decisão.[…]. O texto é expresso ao reconhecer que "a intervenção humana é um elemento essencial.[…]". O considerando 71[7] é mencionado no sentido de que "as garantias adequadas também deverão incluir: '[…] a informação específica ao titular dos dados e o direito [...] de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão.'" (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 30).

Além disso, as orientações destacam que esse quadro "[…] realça a necessidade de transparência quanto ao tratamento. O titular dos dados apenas poderá contestar uma decisão ou manifestar o seu ponto de vista se compreender plenamente como foi tomada e com que fundamento […]". (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 30).

Ainda discorrendo sobre as salvaguardas, as diretrizes referem-se á possibilidade de erros e enviesamento nos dados ou nos processos de decisão automatizados de forma a afetar negativamente as pessoas e destacam que 1) nesses casos, devem aos responsáveis pelo tratamento efetuarem avaliações frequentes nos conjuntos de dados para verificar tais situações e até mesmo de desenvolver formas de responder a eventuais elementos prejudiciais; 2) os "sistemas de controlo de algoritmos e as revisões periódicas da exatidão e relevância das decisões automatizadas, incluindo a definição de perfis" são outras medidas úteis. (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 31).Enfatizam, ainda, que

[7] Em outra passagem o texto faz, mais uma vez, conexão direta entre as salvaguardas do artigo 22(3) e o considerando 71 ao citá-lo em nota de rodapé e ao mencionar que a redação do artigo é apoiada nele. ((GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 21,22).

> Os responsáveis pelo tratamento devem introduzir medidas e procedimentos adequados para prevenir a ocorrência de erros, imprecisões[43] ou a discriminação com base nos dados de categorias especiais. Estas medidas deverão ser utilizadas de modo cíclico, ou seja, não apenas na fase de conceção, mas também permanentemente enquanto for aplicada uma definição de perfis às pessoas. O resultado destas análises deverá ser refletido na conceção do sistema. (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 31).

O artigo 22(4) também se refere ás exceções do inciso(2), prevendo que quando estas previsões "não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.º, n.º 1, a não ser que o n.º 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular". (PARLAMENTO EUROPEU, 2016)

Outro ponto que as Diretrizes procura clarear, até mesmo em razão dos intensos debates em torno da questão, consiste na - relembrando das exceções já citadas que permitem a realização desse tratamento - restrição da proibição do artigo 22(1) *apenas* para circunstâncias em que "[…] o tratamento automatizado, incluindo a definição de perfis, *produz efeitos jurídicos ou afeta alguém significativamente de forma similar,* […]" (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p.22), ou seja, a "efeitos com impactos graves".

Para elucidar estas duas expressões, o Grupo de trabalho do artigo 29 recorre a exemplos sobre situações que "afete significativamente de forma similar" mencionados no considerando 71. Mesmo que reconheça a dificuldade de indicar com precisão tal significado, menciona que tal decisão "deve ser suscetível de: afetar significativamente as circunstâncias, o comportamento ou as escolhas das pessoas em causa; ter um impacto prolongado ou permanente no titular dos dados; ou nos casos mais extremos, dar *origem a uma exclusão ou discriminação das pessoas.*" (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 24)

Importante ressaltar que há previsão nas Diretrizes no sentido de que "qualquer tratamento suscetível de implicar um elevado risco para os

titulares dos dados exige que o responsável pelo tratamento efetue uma avaliação de impacto sobre a proteção de dados (AIPD). […]. (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p.22)

Os artigos 13(2)f, 14(2)g e 15(1)h se conectam ás decisões totalmente automatizadas em razão de todos eles estabelecerem idêntica previsão no sentido de que se houver "decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.os 1 e 4, e, pelo menos nesses casos, *informações úteis relativas à lógica subjacente,* bem como a *importância e as consequências previstas de tal tratamento para o titular dos dados*." (grifo nosso). (PARLAMENTO EUROPEU, 2016)

Apesar de o texto ser idêntico em tais dispositivos, o contexto em que são mencionados é marcadamente diferente. Os artigos 13(2)f e 14(2) g referem-se aos *direitos do titular de ser informado,* que estabelecem informações "*necessárias para garantir um tratamento equitativo e transparente*", em duas ocasiões diferentes: 13(2)f quando os dados forem recolhidos junto ao titular e 14(2) quando os dados não forem recolhidos junto ao titular. Além disso, o artigo 15(1)h faz aquela previsão no contexto dos direitos de acesso do titular de dados.(grifo nosso) (PARLAMENTO EUROPEU, 2016)

No que diz respeito a esses direitos de ser informado, relacionados ás decisões unicamente automatizadas, as diretrizes enfatizam que eles cobram dos responsáveis pelo tratamento, muita atenção para suas obrigações de transparência. Além de enfatizar que devem prestar informações específicas e de fácil acesso sobre tais decisões e que tem , nesses casos, que : "comunicar ao titular dos dados que está a levar a cabo esse tipo de atividade; fornecer informações úteis relativas à lógica subjacente; e *explicar a importância e as consequências previstas do tratamento*." *(*grifo nosso) (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 27)

Ao requerer que sejam específicas e de fácil acesso, verifica-se , apesar de não citado nas Diretrizes, a conexão com a previsão do artigo com o artigo 12 - sobre "Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados"- segundo o qual ,

> O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios. (PARLAMENTO EUROPEU, 2016)

As Diretrizes informam que o cumprimento daquelas prestações de informação - do art. 13 e 14 acima citadas - contribui para os próprios responsáveis pelo tratamento ao "assegurar que cumprem algumas das garantias necessárias a que se referem o artigo 22.o, n.o 3, e o considerando 71." Donde se verifica-se, mais uma vez, a referência ao considerando 71 (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 27).

A Diretrizes ainda dedicam um tópico ás "Informações úteis relativas à «lógica subjacente» no qual, após considerar que "o crescimento e a complexidade da aprendizagem automática poderão tornar difícil perceber o funcionamento do processo de decisão automatizada ou da definição de perfis", destacam que "o responsável pelo tratamento deverá encontrar formas simples de comunicar ao titular dos dados a lógica subjacente, ou os critérios aplicados para tomar a decisão". Um exemplo é dado para ilustrar tais informações e ainda é enfatizado que

> O RGPD obriga o responsável pelo tratamento a fornecer informações úteis relativas à lógica subjacente, e *não necessariamente uma explicação complexa sobre os algoritmos utilizados ou a divulgação do algoritmo na íntegra*. As informações prestadas devem, no entanto, ser suficientemente completas para permitir ao titular dos dados compreender os motivos da decisão.(GRUPO DE TRABALHO DO ARTIGO 29, 2018, p.28). (grifo nosso)

Complementam, em nota de rodapé, que a complexidade não pode ser utilizada como argumento para a não oferta de tais informações. Além disso, nessa oportunidade é citado o considerando 58 em razão de ele indicar a relevância do princípio da transparência, especialmente, em "situações em que a proliferação de operadores e a complexidade tecnológica das práticas tornam difícil que o titular dos dados saiba e compreenda se, por quem e para que fins os seus dados pessoais estão a ser recolhidos, como no caso da publicidade por via eletrónica". (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 28).

No que se refere aos textos «Importância» e «consequências previstas» ,constantes daqueles três dispositivos normativos, as Diretrizes esclarecem que "este termo sugere que tenham de ser fornecidas informações sobre os tratamentos previstos ou futuros" (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 28).

No que diz respeito ao direito de acesso, constante do artigo 15(1) h, importa destacar que as Diretrizes mencionam que o responsável pelo tratamento deveria já ter facultado ao titular dos dados as referidas informações, tendo em vista suas obrigações informacionais e ressalta que "o responsável pelo tratamento deve prestar ao titular dos dados informações acerca das *consequências previstas* do tratamento, em vez de uma explicação sobre uma decisão *específica*."Além de destacar tais expressões, verifica-se a menção ao considerando 63 no sentido de que ele estaria "indicando que cada titular de dados deverá ter um direito de acesso, para «ser informado» do tratamento automático de dados, incluindo a lógica subjacente, e, *pelo menos* quando tiver por base a definição de perfis, das suas consequências (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p.28).

Em conformidade com as Diretrizes, deve o responsável pelo tratamento "facultar ao titular dos dados informações genéricas (nomeadamente, sobre os fatores tidos em conta no processo decisório e a «relevância» dos mesmos em termos globais) que também lhe sejam úteis para contestar a decisão". O texto conecta esse dever ao exercício do direto do artigo 15, ao mencionar que nesta situação, pode o titular de

dados "[…] tomar conhecimento de uma decisão que lhe diga respeito, incluindo se for baseada na definição de perfis"(GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 28).

Ao examinar o *caput do* artigo 20 da LGPD, acima mencionado, verifica-se que o texto não oportunizou interpretações no sentido de uma proibição geral[8], tendo estabelecido que, nos casos de decisões tomadas unicamente com base no tratamento automatizado de dados pessoais "*que afetem seus interesses incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade* o titular de dados tem o direito de solicitar a revisão de tais decisões. (BRASIL, 2018).

O § 1o prevê que no caso de utilização desse tipo de decisão, "o controlador, *sempre que solicitadas*, *deverá fornecer* informações claras e adequadas a respeito dos critérios *e dos procedimentos utilizados para tal decisão,* observados os segredos comercial e industrial". Além disso, em caso de tais informações não serem fornecidas, o § 2o estabelece que, "baseado na observância de segredo comercial e industrial, a autoridade nacional poderá *realizar auditoria para verificação de aspectos discriminatórios* em tratamento automatizado de dados pessoais". (BRASIL, 2018).

O § 3º, que aos moldes do RGPD previa a possibilidade de intervenção/revisão humana das decisões totalmente automatizadas[9], foi vetado[10],

---

8 Segue nesse sentido a análise de Rafael Zanatta ao considerar os perfis: "A GPDR afirma que o titular dos dados (data subject) possui um direito de não se submeter à decisão exclusivamente automática incluindo o profiling (GDPR, Artigo 22, 1). Já a legislação brasileira adota uma postura diversa. A LGPD não predispõe que o titular dos pessoais possui o direito de não ser submetido à decisão automatizada incluindo a perfilização.Ela dispõe que, se a perfilização acontecer, o titular dos dados pessoais passa a dispor de um conjunto de direitos". (2019, p.20)

9 Que foi alterado pelo art. 2º do projeto de lei de conversão. § 3º A revisão de que trata o caput deste artigo deverá ser realizada por pessoa natural, conforme previsto em regulamentação da autoridade nacional, que levará em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados." (BRASIL, 2019)

10 Nas razões do veto, esse tipo de revisão foi considerado contrário ao interesse público em razão dos obstáculos que poderia criar para os novos modelos de negócios, como as startups assim como pelo impacto na" análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos

levantando diversas críticas no âmbito acadêmico[11] o que se justifica tendo em vista a importância dada a esse elemento no contexto do RGPD, como referenciado linhas acima. (BRASIL, 2019)

Não identificaram-se, no âmbito da LGPD, muitos debates voltados para definição e limites dos termos presentes no artigo 20 e seus §s. Apesar disso, o debate pôde ser verificado no contexto do projeto de Lei PLS 4496/2019, em tramitação no Senado. O PL analisa a incorporação da definição de "decisão automatizada"[12] no texto da LGPD. Diferentemente das Diretrizes do grupo de trabalho do artigo 29 acima citadas, o texto não se ocupa com as decisões *unicamente* automatizadas, mencionadas no *caput do artigo 20*. Além disso há críticas no sentido de que "a definição de 'decisão automatizada' tampouco parece muito precisa, uma vez que não diferencia a decisão em si com o processo decisório"[…] (SILVA, MEDEIROS, 2019).

## 2 O DEBATE ORIGINÁRIO SOBRE O DIREITO DE EXPLICAÇÃO A PARTIR DO RGPD E O DIREITO DE EXPLICAÇÃO NA LGPD

O direito de explicação não consta do rol dos direitos dos titulares de dados nem no RGPD nem na LGPD. No entanto, a partir do RGPD emergiram muitos debates acerca da existência do que vem sendo de-

consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária." (BRASIL, 2019)

11 Por fim, como visto, a nova lei silencia-se novamente quanto à possibilidade de revisões humana, atribuindo o direito de revisão tão só a outro sistema automatizado, não oferecendo concretamente as formas pelas quais a revisão poderá ser oferecida, o que ensejaria um correto exercício do direito de revisão.(SILVA, MEDEIROS, 2019).

12 Segundo o artigo Art. 1o do PL, O art. 5o da Lei no 13.709, de 14 de agosto de 2018, passa a vigorar acrescido do seguinte inciso: "XX – decisão automatizada: processo de escolha, de classificação, de aprovação ou rejeição, de atribuição de nota, medida, pontuação ou escore, de cálculo de risco ou de probabilidade, ou outro semelhante, realizado pelo tratamento de dados pessoais utilizando regras, cálculos, instruções, algoritmos, análises estatísticas, inteligência artificial, aprendizado de máquina, ou outra técnica computacional." (NR) (BRASIL, 2019 a).

nominado *direito de explicação das decisões totalmente automatizadas,* ainda que a expressão "direito à explicação" apareça apenas uma vez de forma expressa, no Considerando 71, que não tem caráter vinculativo. […]"(WACHTER *et al,* 2017, p. 80). Enquanto na LGPD ela sequer é mencionada.

Esse direito passou a ser pensado a partir, especialmente, dos artigos 13 (2) f, 14 (2)g, 15 (1) h e 22 (1) e (3)[13] e dos Considerandos 71 e 63. Desse cenário mencionam-se três possíveis bases jurídicas possíveis do RGPD para fundamentar esse direito: 1)[…] salvaguardas contra o processo automático de tomada de decisões, conforme exigido pelo artigo 22.º, n.º 3, e comentado pelo considerando 71; 2) deveres de notificação previstos nos artigos 13.º a 14.º, comentados nos considerandos 60 a 62; ou 3) o direito de acesso nos termos do artigo 15.º, e comentado pelo considerando 63. (WACHTER *et al,* 2017, p. 4). Ainda que possa haver alguma variação entre as diferentes abordagens, essa é uma boa ilustração do cenário.

Há posicionamentos "[…] contra a mera possibilidade de tal direito existir" (BURT,2017) e considerando que "existem várias razões para duvidar da existência, escopo e viabilidade de um "direito à explicação" de decisões automatizadas". enquanto outros, parecem achar que o direito é claramente evidente[14], sendo o "direito à explicação" de decisões tomadas por sistemas algorítmicos automatizados e artificialmente inteligentes legalmente exigido pelo GDPR. (WACHTER *et al,* 2017, p. 1,2). Para além dos debates acerca da existência ou inexistência de tal direitos, é objeto de estudos o exame acerca da sua abrangência e formas para seu exercício. (POLIDO *et al,* [s/d], p. 12).

Alguns trabalhos se destacaram na abordagem do tema, tanto por sua abordagem pioneira quanto pela importância que tomaram ao

[13] Para além desses artigos BURT cita ainda, o artigo 21, destacando que tanto este quanto o artigo 22 se enquadram na Seção 4 (lidando especificamente com o direito do sujeito à objeção da tomada de decisão automatizada) (BURT, 2017). No entanto, o artigo 21 não será objeto de análise do presente trabalho.

[14] Tradução livre de BURT (2017).

se tornarem referência e fundamento para outras pesquisas sobre a temática. Neste cenário referenciam-se os artigos de Goodman e Flaxman; Wachter et al e de Selbst e Powles[15] que são anteriores ás orientações do Grupo de trabalho do artigo 29 para a proteção de dados, "sobre as decisões individuais automatizadas e definição de perfis para efeitos do Regulamento (UE) 2016/679", que foram adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018. (GRUPO DE TRABALHO DO ARTIGO 29, 2018).

Várias questões levantadas nestes três artigos foram objeto de análise das Diretrizes. No entanto, elas não foram suficientes para pôr um ponto final nos debates sobre o tema. Ainda que tenham contribuído para compreensão de algumas questões e tenham finalizado alguns questionamentos, em outros casos conduziu para (re)direcioná-los[16] e, até mesmo, para gerar novas discussões. Assim, "apesar dos esforços combinados do RGPD para detalhar as proteções consagradas nos termos dos artigos 13, 14, 15 e 22, muitas incertezas continuam a envolver o regulamento quanto ao que é chamado de "direito à explicação"[…]." (CASEY, FARHANGI, VOGL, 2019, p.158)

Goodman e Flaxman, em um trabalho partindo da análise dos artigos 13-15, ressaltaram a importância de diferenciar entre direitos de notificação dos direitos de acesso e das salvaguardas exigidas a partir do artigo 22 ao definir o perfil, ainda que estas não estejam bem definidas além do "direito de obter intervenção". Com foco na formação de perfis - e seu potencial de gerar discriminação- os autores destacaram que a partir da previsão dos artigos 13 e 14 acerca do direito de informação do titular de dados sobre a lógica envolvida quando da criação de perfis surge o questionamento: "o que significa e o que é necessário para explicar a decisão de um algoritmo (2017, p.6).

A abordagem evidenciou a preocupação em relação á transparência na tomada de decisões algorítmicas sem desconsiderar que transpa-

[15] Tais trabalho serão examinados seguindo a ordem cronológica de suas publicações já que os artigos posteriores foram elaborados em resposta aos antecedentes.

[16] Os trabalhos de Michael Veale e Lilian Edwards ilustram esse quadro ( 2018; 2018 a)

rência consiste em um requisito nem sempre claro. Associaram as três barreiras á transparência algorítmica apresentadas por Burrel ao direito de explicação (GOODMAN, FLAXMAN, 2017, p. 6)

Neste quadro, consideraram que: as informações a serem disponibilizadas ou fornecidas ao titular dos dados do artigo 13 sinalizam, de alguma forma, uma resposta a primeira barreira, a "ocultação intencional por parte de empresas ou outras instituições, onde os procedimentos de tomada de decisão são mantidos fora do escrutínio público"; a exigência de comunicação "concisa, inteligível e facilmente acessível" para o titular de dados seria uma forma de lidar com a segunda barreira que consiste em "lacunas na alfabetização técnica, o que significa que, para a maioria das pessoas, simplesmente ter acesso ao código subjacente é insuficiente" (GOODMAN, FLAXMAN, 2017, p. 6,7).

Para a terceira barreira consideram que os desafios são maiores e envolvem questões relativas ao design e seleção de algoritmos já que essa barreira consiste e "incompatibilidade entre a otimização matemática na característica de alta dimensionalidade do aprendizado de máquina e as demandas de raciocínio em escala humana e estilos de interpretação", sendo que a explicação do algoritmo envolve compreensão humana sobre : o modelo de treinamento; no mínimo, explicação de "como os recursos de entrada se relacionam com as previsões", o que se torna mais difícil diante de algoritmos complexos que usam modelos avançados de Inteligência Artificial-IA. Aqui destacam, com base em Datta et al, que "um caminho promissor de pesquisa diz respeito ao desenvolvimento de algoritmos quantificar o grau de influência das variáveis de entrada nas saídas, dado o acesso de caixa preta a uma previsão treinada algoritmo"[17] (GOODMAN, FLAXMAN, 2017, p. 6).

Sob o título *Por que um direito à explicação da tomada de decisão automatizada não existe no Regulamento Geral de Proteção de Dados,* a pesquisa de Watcher et al ganhou destaque. A análise foi estruturada de forma a refutar, uma a uma daquelas três bases jurídicas usadas para fundamentar

[17] Tradução livre das autoras de GOODMAN, FLAXMAN ( 2017, p. 6).

o direito de explicação e teve como base a classificação do direito de explicação, em cada caso analisado, nos seguintes tipos : em razão do que se tem em foco, 1) se a funcionalidade do sistema ou 2) uma decisão específica; em razão do tempo em relação ao processo de tomada de decisão, como 1) *ex ante* ou 2) *ex post.*[18] (WACHTER *et al,* 2017, p. *3)*. Nesse sentido,

> funcionalidade do sistema, ou seja, a lógica, a importância, consequências previstas e funcionalidade geral de um sistema automatizado de tomada de decisão, […] ; ou para decisões específicas, ou seja, o fundamento lógico, razões e circunstâncias individuais de uma decisão automatizada específica, por exemplo, a ponderação de recursos, definidos por máquina regras de decisão específicas do caso, informações sobre grupos de referência ou de perfil.11
>
> […] : uma explicação ex ante ocorre antes de uma tomada de decisão. Observe que uma explicação ex ante pode logicamente abordar apenas a funcionalidade do sistema, uma vez que a justificativa de uma decisão específica não pode ser conhecido antes que a decisão seja tomada; uma explicação ex post ocorre após um tomada de decisão. Observe que uma explicação ex post pode abordar a funcionalidade do sistema e o fundamentação de uma decisão específica[19] (WACHTER *et al,* 2017, p. *3)*.

Observaram que a próprio entendimento e abrangência do que é ou virá a ser o direito de explicação depende da definição de diversos termos presentes naquelas três bases legais - que estavam, da forma apresentada no momento em que fizeram sua pesquisa, potencializando maior número de interpretações. Sem pretensão de resumir toda a análise elaborada por esses pesquisadores de Oxford, mencionam-se algumas análises que fizeram.

Ao refutarem a base jurídica das salvaguardas 22(3), dando ênfase ao caráter não vinculativo do considerando 71, concluíram que o RGPD

[18] O texto em resposta a este artigo faz críticas a esta distinção e menciona não acreditarem que tal organização corresponda com os propósitos dos redatores do RGPD ( SELBST; POWLES, 2017, P. 238)

[19] Tradução livre das autoras.

não "concedeu um direito ex post legalmente vinculativo de explicação de decisões automatizadas específicas com base nas garantias jurídicas do artigo 22.º (WACHTER *et al,* 2017, p. 4,5)

Ao afastarem um direito à explicação derivado de deveres de notificação - artigos 13 e14 combinados com as salvaguardar do art.22(3), afirmaram que tais dispositivos não concedem um direito ex post de explicação da " 'existência ... lógica envolvida ... significado... e as consequências previstas da tomada de decisão automatizada' seja porque a funcionalidade do sistema 13 (2) f e 14 (2)g só pode ser explicada ex ante , seja porque ao RGPD não vincula tais artigos ás salvaguardas do 22 (3) e ainda, estas não se referem a uma explicação ex post, que só está previsto no Considerando 71, de onde resultaria incabível pensar em uma explicação ex post e de uma decisão já tomada (p.7).

Em relação ao direito de explicação derivado do direito de acesso, consideraram que apesar de o Artigo 15 (1) h ser idêntico aos Artigos 13 (2) f e 14 (2) h: , trata-se de direito que precisa ser inovado pelo titular de dados. No entanto, enfatizam que esses três dispositivos são orientados para o futuro, e que "consequências possíveis" devem ser interpretado como "possíveis consequências do tomada de decisão automatizada antes de tal processamento ocorrer", o que só permite explicações ex ante e a respeito da funcionalidade do sistema e não de decisões específicas. (p.8,9).Fazem, ainda uma análise da Diretiva de 1995 para respaldar essa análise.

Apesar de todas essas objeções, concluem que "o direito de acesso do GDPR fornece o direito de explicação sobre a funcionalidade do sistema, o que chamamos de "direito de ser informado", restrito pelo interesses dos controladores de dados e interpretações futuras do Artigo 15.(p. 21)".

Estranha-se essa conclusão diante do título do trabalho.Tudo indica, no entanto, que a negação relativa ao direito de explicação no RGPD está relacionada a um tipo específico de explicação, que eles classificam com ex post e decisão específica.[20] O exame de Selbst e Powles segue

[20] Burt segue a mesma linha de análise: Destacando que a explicação exata de como uma decisão individual automatizada (prevista no considerando 71) foi tomada é extremamente

nesse sentido, ao concluírem que a proposta de "direito de ser informado", consiste em "um direito limitado à explicação da funcionalidade dos sistemas automatizados de tomada de decisão" (ênfase adicionada) […]" (SELBST; POWLES, 2017, p. 239).

Watcher et al destacaram, ainda, que apesar de o direito de explicação não ter sido previsto no RGPD, as contribuições que ele traz para "a responsabilidade e transparência da tomada de decisão automatizada pode fornecer razões convincentes para os legisladores ou controladores de dados introduzirem um no futuro."(WACHTER *et al,* 2017, p. 15,16).

Apesar de reconhecerem a desavença[21] acerca da existência do "direito de explicação" no GDPR, para Selbst e Powles ele é visível diante de uma leitura clara dos artigos 13 (2) (f), 14 (2) (g), 15 (1) (h) e 22. Eles fazem uma inversão de abordagem para observar que o artigo 22 e o considerando 71 apoiam a leitura dos artigos 13–15 como uma fonte independente do direito. Isso sugere que embora um direito à explicação não possa ser derivado do próprio artigo 22, este artigo, no entanto, sustenta a existência desse direito derivado de Artigos 13–15[22] (2017).

Eles consideram que faz sentido chamar o direito a "informações significativas sobre a lógica envolvida 'em decisões automatizadas de tais

difícil em sistemas de aprendizado de máquinas, BURT considera que essa previsão consiste em uma sugestão dos redatores do Regulamento mas não uma determinação. E, por isso, para ele, a relação do *direito à explicação* a uma decisão específica "se tornou um assunto polêmico"(BURT, 2017) Análise anterior ás Diretrizes do grupo de trabalho do artigo 29.

21 o Artigo é feito como uma resposta ao dois artigos citados acima neste trabalho: "As contribuições mais proeminentes são dois artigos explosivos de Oxford, que moldaram imediatamente o debate público.8 O primeiro artigo, por Bryce Goodman e Seth Flaxman, afirmam que o O GDPR cria um "direito à explicação", mas não se estende muito além desse ponto.9 O segundo artigo, de Sandra Wachter, Brent Mittelstadt e Luciano Floridi, afirma que tal direito não existe atualmente. 10 Ele o faz por restringir desnecessariamente a ideia do "direito à explicação", ao mesmo tempo que concebe um diferente "direito a ser informado" que equivale a um direito a um tipo particular de explicação."Além disso, considera que"Acreditamos que a resposta de Wachter e outros é uma reação exagerada a Goodman e Flaxman que distorce o debate, e nenhum dos dois artigos de forma significativa aborda as disposições mais relevantes que apoiam tal direito, especificamente aqueles que criam direitos para " informações sobre a lógica envolvida 'na tomada de decisão automatizada. (p. 234, 237-241)

22 Tradução livre das autoras.

artigos de direito à explicação e que este direito deve ser interpretado funcionalmente, de forma flexível, e deve, no mínimo, permitir que um titular de dados exerça seu ou seus direitos sob o GDPR e as leis de direitos humanos[23]".( SELBST, POWLES, 2017, p. 242)

A partir da análise acerca de quando as informações específicas podem ou não ser "significativas" eles seguiram no sentido de que o direito de explicação abrange decisões específicas, tecendo críticas severas ás análises de Watcher et al. (p. 235) de um lado e, de outro, reconhecendo como estreita a versão de Goodman e Flaxman acerca explicações de uma decisão específica sobre um pessoa e sem argumentos suficientes para embasá-la e para definir o alcance de tal direito. (SELBST, POWLES, 2017, p.238).

Com foco na definição de perfis, que são vistos "como um subconjunto da questão mais ampla da tomada de decisão automatizada", e tendo em vista a melhoria da capacidade dos titulares de dados de lidar com tais atividades, esses pesquisadores mencionaram que "melhorias aos artigos 5 e 12 reforçam a ênfase do GDPR em transparência e responsabilidade significativas, de certa forma que seja útil, inteligível e acionável para o titular dos dados.[…]" (SELBST, POWLES, 2017, p. 234p. 242)'

Desse debate pioneiro extrai-se que o foco da preocupação desses estudiosos consistiu em definir que tipo explicações e quando elas serão direcionadas para o titular de dados, sinalizando trabalhos que seguem uma abordagem e perspectiva centrada na dimensão subjetiva de tal direito a partir do RGPD. Toma-se por base a doutrina dos direitos fundamentais para compreender esta dimensão como a possibilidade do titular de dados de exigir e impor sua concretização perante responsáveis pelo tratamento dos dados e/ou autoridades de proteção de dados.[24]

---

23 Tradução livre das autoras.

24 No presente trabalho elaborou-se uma adaptação dos ensinamentos de Sarlet acerca da dimensão subjetiva dos direitos fundamentais que, segundo este doutrinados, traduz a possibilidade de o titular – pessoa individual ou ente coletivo – de direito fundamental exigir e impor judicialmente a sua defesa, proteção e concretização, podendo, assim, exi-

Os argumentos acerca do direito de explicação na LGPD, a partir do artigo 20 e seus parágrafos, sinalizam sua "importação" para o cenário brasileiro sem grandes referências aos debates internacionais em torno do mesmo. (SILVA, MEDEIROS, 2019; FRAZÃO, 2019, 2019 a; VERONESE, 2019). Além disso, há análises que ultrapassam o artigo 20, para reconhecer que o direito a explicação alcança, também "tratamento de dados anonimizados, quando esse tipo de dado for utilizado na formação de perfis comportamentais de pessoas identificadas"(MONTEIRO, 2018, p.13), hipótese mencionado no tópico 1.

Nota-se que até mesmo o projeto de Lei PLS 4496/2019, mencionado no tópico anterior, toma por existente o direito em pauta. Na justificação do projeto, considera-se que as decisões automatizadas do artigo 20 podem ser levadas a cabo por diferentes tipos de decisões automatizadas e, especialmente, aquelas "mais sofisticadas e geralmente menos explícitas"que recorrem a "técnicas de aprendizado de máquina (machine learning) ou de inteligência artificial". E que a "inclusão dessas técnicas avançadas no conceito de "decisão automatizada" é essencial, em particular, para garantir o chamado "direito à explicação", previsto no § 1o do citado art. 20. […]" (BRASIL, 2018) Nenhum dos trabalhos nacionais ora citados ou mesmo consultados até o momento final desta pesquisa levantou efetivamente a discussão ora apresentada a partir do RGPD para chegar á conclusão de que o direito de explicação existe na LGPD. Não analisam a fundo a discussão sobre a existência ou não de tal direito e, especialmente, para fins desse trabalho, não destacam ou não mencionam de forma expressa a preocupação em verificar, de um lado, se tal direito abrange explicações 1) de decisões específicas, 2) se apenas sobre da lógica do sistema 3) de ambas e, de outro, a quem são dirigidas tais explicações. Isso não significa que tais pesquisadores não tenham tido acesso ou mesmo referenciado os trabalhos aqui analisados[25] , ou outros

gir ações estatais positivas ou negativas para tutelar o seu direito fundamental404 (SARLET, 2003, p. 157; SARLET, 2010, p. 154)

[25] Apenas a título ilustrativo, verifica-se que um dos trabalhos que ganhou destaque no âmbito nacional, o artigo de Monteiro, há referência ao artigo de Selbst e Powles como fundamento para argumentar sobre a existência do direito á explicação. (2018)

similares. Nem nem exclui suas análises acerca de um possível conceito ou abrangência do direito de explicação. Sinaliza que seguiram outra delimitação para seus trabalhos.

## 3 A DIMENSÃO OBJETIVA DO DIREITO DE EXPLICAÇÃO

A abordagem sobre Decisões automatizadas não é inovação nem no RGPD nem na LGPD. O RGPD é mencionado como uma atualização das previsões da Diretiva de Proteção de Dados da União Européia (DPD de 1995 acerca das decisões automatizadas. (GOODMAN, FLAXMAN, 2017, p. 2; VOGL, FARHANGI, CASEY, 2018)[26] e, no Brasil, a Lei do Cadastro positivo costuma ser uma referência[27].

Reforçando esta previsão, Michael Veale e Lilian Edwards, esclarecem que a proibição do artigo 22 foi migrada da Diretiva de Proteção de Dados de 1995 e da antiga lei francesa de Proteção de dados para o RGPD e afirmam que o que há de novo é a atenção que tal previsão passou a receber. Se antes era pouco utilizada e conhecida, diante do RGPD tomou nova dimensão e importância tendo em vista dois fatores: 1) "uso mais frequente de algoritmos de aprendizado de máquina complexos, opacos e invisíveis para tomada de decisões ou como apoio para tomada de decisões muito importantes em diferentes âmbitos da vida das pessoas, podendo gerar resultados discriminatórios, tendenciosos ou injustos" e 2) *o potencial do artigo ora em estudo restringir o poder de tais algoritmos*" (2018 a, p. 398,399)[28] (grifo nosso).

---

[26] Goodman e Flaxman mencionam que o RGPD vem reafirmar o direito da DPD à explicação e restrições na tomada de decisões automatizadas. (GOODMAN, FLAXMAN, 2017, p. 2). Em sentido similar, há afirmações de que o regulamento atualiza os direitos da DPD sobre a tomada de decisões automatizadas sendo esta atualização um marco para o que se passou a denominar de *direito à explicação* (VOGL, FARHANGI, CASEY, 2018).

[27] Conforme Citado por Zanatta (2019, p. 15-19) Frente a tais considerações, ressaltam-se, especialmente, os direitos garantidos nos incisos IV, VI e VII da Lei 12.414/2011: IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; eVII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.

[28] Esse cenário acentua-se quando as decisões envolvem a definição de perfis já que "é suscetível de perpetuar os estereótipos existentes e a segregação social. Pode igualmente

Este primeiro fator tem levantado debates nas mais diversas áreas do conhecimento, especialmente no âmbito jurídico, tendo em vista os efeitos que podem ter, de diferentes formas, sobre variados direitos dos indivíduos. O Grupo de trabalho do artigo 29 evidencia que decisões automatizadas e definição de perfis envolvem processos que podem ser pouco transparentes e "suscetíveis de gerar riscos significativos para os direitos e as liberdades das pessoas", exigindo garantias adequadas."(-GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 5,6)

Ao considerar que os algoritmos[29] passam a controlar a vida de todos, Renato Monteiro explica que se trata "de sequências pré-definidas de comandos automatizados que, com base em dados pessoais e não pessoais,[2] chegam a conclusões que podem sujeitar alguém a uma determinada ação, a qual pode ou não ter impacto significativo na sua vida. […]"(MONTEIRO, 2018, p. 2)

A questão é que algoritmos operam com dados e ,"usando esses dados como entrada, eles produzem uma saída; especificamente, uma classificação (ou seja, se você deve conceder um empréstimo a um candidato ou se deve marcar um email como spam)". A respeito desse resultado, os algoritmos são opacos no sentido de que, se alguém recebe a saída do algoritmo (a decisão de classificação), raramente tem um senso concreto de como ou por que uma classificação específica foi obtida a partir das entradas. Além disso, as próprias entradas podem ser totalmente desconhecidas ou conhecidas apenas parcialmente (BURREL, 2016). Na realidade o cenário pode ser ainda mais intenso se for levado em conta que algoritmos inteligentes fazem parte do dia-a-dia das pessoas e elas nem percebem. (TAURION, 2016)

amarrar as pessoas a uma categoria específica e limitá-las às respetivas preferências sugeridas, pondo assim em causa a sua liberdade para escolher, por exemplo, determinados produtos ou serviços, tais como livros, música ou fluxos de notícias. Em certos casos, a definição de perfis é suscetível de resultar em previsões imprecisas. Noutros casos, poderá dar origem a uma negação de serviços e bens e a uma discriminação injustificada. (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 6)

29 Os algoritmos, são a parte técnica essencial do software que diz respeito ao processo – com a sequência de etapas a serem cumpridas- para solução de um problema identificado. (CANUT, MEDEIROS, 2017, p.1042).

A opacidade dos algoritmos de IA, qualquer que seja a sua causa[30] tem sido um dos grandes problemas apontados no contexto das decisões automatizadas. Dentre as potencialidades negativas[31] decorrentes da sua opacidade, uma das que tem ganhado mais relevo, seja no âmbito internacional como nacional, é a relativa aos resultados carregados de preconceitos, também denominado de vieses. Esse tem sido um debate desafiador tanto para operadores do direito quanto para cientistas da computação e áreas correlatas. Mendes e Mattiuzzo evidenciam que "a falta de transparência é uma séria preocupação no que se refere às consequências legais da discriminação algorítmica", segundo elas

> Isso ocorre, em primeiro lugar, porque, se o algoritmo é obscuro, é difícil afirmar que algum tipo de discriminação ocorreu; em segundo lugar, pois pode ser difícil prevenir que discriminações ocorram; terceiro, porque os algoritmos, se utilizados de maneira descuidada, podem acabar por reforçar resultados discriminatórios ao invés de combatê-los. (2019, p. 47).

O debate acerca da opacidade/falta de transparência das decisões automatizadas envolve questões complexas e conhecimentos de diversas áreas científicas. Sem pretensão de se debruçar sobre as variáreis que envolvem o assunto, destaca-se nesse trabalho um ponto fundamental para se examinar o tema: o reconhecimento de que opacidade/falta de transparência pode derivar de diferentes fatores, podendo ter diversas justificativas, técnicas e não técnicas Diega(2018, p. 9-10) e que, a consequente transparência esperada pode variar conforme o contexto - e assim o tipo de opacidade - e os sujeitos diretamente envolvidos.

Guido Noto La Diega(2018, p. 9-10) relaciona essa falta de transparência a três "caixas-pretas": (i) a organizacional, relacionada ao fato de, na maior parte das vezes os algoritmos serem implementados por entidades privadas que maximizam o lucro e operam sob obrigações mínimas de

[30] Há vários tipos de opacidade, como se verá adiante.

[31] Várias potencialidades negativas foram referenciadas por CANUT e MEDEIROS ( 2018)

transparência; (ii) a técnica, que diz respeito ao uso da inteligência artificial que torna difícil de acessar a lógica das decisões algorítmicas; e (iii) a legal, que está associada à propriedade intelectual. Jenna Burrel elaborou uma trilogia da opacidade dos algoritmos - que foi utilizada por Goodman e Flaxman, como visto no tópico anterior - e ressaltou que cada forma "[…] de opacidade pode ser abordada por diferentes ferramentas e abordagens que variam do legislativo, ao organizacional ou programático, ao técnico[…]"(2016, p.3). Considera-se que a opacidade relacionada aos dados utilizados como *input* dos algoritmos e/ou aos dados utilizados para treiná-los faz parte da caixa-preta técnica.

Esse quadro, apenas ilustrativo, demonstra a necessidade de maiores delimitações dos debates acerca direito de explicação para que propostas para lidar com suas potencialidades negativas possam ser produtivamente concebidas e direcionadas. Isso quer dizer que, tomando a opacidade/falta de transparência enquanto dificuldade/ impossibilidade de compreender uma saída/output, ou seja, uma resposta ou decisão algorítmica, deve-se considerar que haverá diferentes tipos e níveis de opacidade a depender de qual é o tipo de opacidade constatada no caso concreto e, quem são os interessados ou envolvidos diretamente.

Percebe-se, como já assinalado no tópico anterior, que os trabalhos pioneiros sobre o direito de explicação, analisaram problemas e possíveis soluções decorrentes da opacidade/ falta de transparência dos algoritmos tendo em vista o titular de dados, sua esfera individual. A partir dessa contextualização propuseram, cada um ao seu modo, abordagens subjetivas de tal direito, que envolvem debates em torno do tipo de explicação a ser fornecida/requerida a este sujeito e o tempo em que ela deverá ocorrer, tendo tido destaque a diferença proposta por Watcher et al. entre explicação de uma decisão específica ex post e explicação da funcionalidade do sistema, ex ante ou ex post.

Observa-se que mesmo após as Diretrizes do grupo de trabalho do artigo 29, muitos trabalhos, de diferentes nacionalidades, continuam a manter o foco na perspectiva individual do direito de

explicação[32]. No entanto, observa-se, também, que tais orientações têm conduzido a entendimentos que seguem uma outra perspectiva, que está relacionada ao segundo fator citado por Michael Veale e Lilian Edwards linhas acima: o potencial do artigo ora em estudo restringir o poder de tais algoritmos.

Optou-se por denominar esta perspectiva, neste trabalho, de dimensão objetiva do direito de explicação[33]. Recorrendo a ideias e classificações da doutrina dos direitos fundamentais para pensar tal direito, entende-se que sua dimensão objetiva[34] está ligada questões normativas, valorativas, institucionais e funcionais, cobrando "elementos objetivos e institucionais para a garantia dos novos direitos e de suas funções". (BONAVIDES, 2009, p. 72) [35].

[32] Nesse sentido Cassey, Farhangi e Vogl, em publicação posterior a tais orientações, mencionam que "apesar dos esforços combinados do GDPR para detalhar as proteções consagradas nos termos dos artigos 13, 14, 15 e 22, muitas incertezas continuam a envolver o regulamento quanto ao que é chamado de "direito à explicação". Considerando o mandato do RGPD confuso, tais autores consideram que ele parece prever, no mínimo, "um direito limitado para os titulares dos dados compreenderem e verificar a funcionalidade básica de certas tomadas de decisão. Mas, além desse limite mínimo, os contornos precisos do "Direito à explicação" tem sido objeto de muita especulação - dando origem a um debate público "explosivo". (CASEY, FARHANGI, VOGL, 2019, p. 158) (grifo nosso). Tradução livre das autoras.

[33] Ressalta-se que há trabalhos recentes que após tecer comentários acerca da dificuldade de implementar tal direito, em razão de desafios técnicos, afirmam que o direito à explicação - tomando-o como direito de buscar uma explicação de uma decisão específica e apenas ex post - pode não ser necessário e às vezes pode até ser prejudicial. Em vez disso, propõem uma avaliação externa de modelos de classificação com relação a seus correção e justiça. (GRYZ, Jarek; SHAHBAZI, 2020)

[34] Ressalta-se que apesar do empréstimo de tais considerações das doutrinas dos direitos fundamentais, trata-se de um debate que, se levado mais a fundo, cobrará o enquadramento do direito de proteção de dados em alguma das categorias de direitos sociais fundamentais: sociais, econômicos ou culturais ou ,ainda, alguma nova classificação que surja no âmbito de suas análises.

[35] Faz-se tal adaptação a partir dos ensinamentos de Bonavides que seguem no sentido de que: Com o crescimento dos fins estatais (BONAVIDES, 2009, p. 72), ou seja, com a transformação de sua unifuncionalidade em multifuncio- nalidade, tornaram-se necessários elementos objetivos e institucionais para a garantia dos novos direitos e de suas funções. Emergiu, ao lado da dimensão subjetiva, dimensão objetiva dos direitos fundamentais, ligada a questões normativas, valorativas, institucionais e funcionais91 (BONAVIDES, 1995, p. 366-367). Com esta dimensão pretendeu-se superar a visão estritamente subjetiva de

A dimensão objetiva dos direitos fundamentais abarca vários aspectos: a) feição axiológica (LUÑO, 1995, p. 21) e seus desdobramentos – eficácia dirigente e parâmetro para o controle de constitucionalidade –; b) feição de força jurídica autônoma – na qualidade de efeitos que não estão necessariamente atrelados aos direitos fundamentais que consagram direitos subjetivos – a qual se desdobra na denominada eficácia irradiante, que está ligada à eficácia horizontal e nos deveres de prote-ção do Estado, o qual consiste no encargo de agir positivamente para proteger o exercício dos direitos fundamentais contra atos do Estado, de particulares e até mesmo de outros Estados; c) fundamento para "criação e constituição de organizações (ou instituições) estatais e para o procedimento" (SARLET, 2003, p. 150; 152-155, grifo nosso).

Destes vários aspectos são abarcados por essa dimensão, destaca-se, neste momento, sua conexão com as políticas políticas públicas[36], que envolve diferentes momentos, num ciclo de agenda, formulação, implementação e avaliação.

Apesar de o trabalho de Margot não utilizar essa classificação e terminologia -nem de forma aproximada - considera-se que ele abrange estas duas perspectivas ou dimensões mencionadas ao longo do trabalho, a subjetiva e a coletiva. A subjetiva pode ser verificada a partir de duas considerações sobre as Diretrizes: a primeira, de que elas reconhecem que o indivíduo "tem o direito de explicação de uma decisão individual porque essa explicação é necessária para que ela invoque os outros direitos[37] - por exemplo, para contestar uma decisão, para expressar sua

tais direitos (BONAVIDES, 2003, p. 616; 622), que foi realçada no modelo de Estado de direito liberal.

36 Canotilho (2003, p. 408-409) questiona se a dimensão objetiva das normas de direitos fundamentais obriga os poderes públicos a implementarem políticas sociais que conduzam à criação de instituições (como hospitais, escolas), serviços (segurança social) e fornecimento de prestações (rendimento mínimo, habitação, econômica etc.). E fornece uma resposta ao afirmar, com base na Constituição Portuguesa de 1976, que "é líquido que as normas consagradoras de direitos sociais, econômicos e culturais [...] individualizam e impõem políticas públicas socialmente activas".

37 O GDPR estabelece - contestação, correção e eliminação - e o tipo de transparência individualizada que ele exige. Isso sugere algo interessante sobre a transparência: a substância

opinião - que são enumerados explicitamente no texto do RGPD". (grifo nosso) (2019, p. 204). Um sentido que retoma e reforça alguns posicionamentos presentes nos estudos pioneiros sobre o direito á explicação.

Apesar de não haver pretensão em aprofundar exames acerca de nenhuma dessas perspectivas, as autoras do presente artigo não conseguem visualizar essa mesma clareza. Isso porque, a partir dos exames feitos no tópico 1, considera-se que as Diretrizes do grupo de trabalho do artigo 29 ora sinalizam um direito á uma decisão específica ex post , como quando comentam sobre a salvaguarda da intervenção humana e, ao mesmo tempo, enfatizam não se relacionar a uma decisão específica, quando do exame dos termos "importância"e consequências" presentes no art. 15(h)[38].

A segunda consideração de Margot que remete á dimensão subjetiva inova frente àqueles trabalhos pioneiros, apresentados no tópico anterior, ao examinar que as Diretrizes estabelecem uma versão do devido processo algorítmico individual, criando uma oportunidade de ser ouvido"(2019,p. 204, 205).Apesar de receber outra denominação, a proposta de Zanatta, no âmbito nacional, parece envolver argumentos similares. Ao tratar o tema a partir do contexto da perfilização, aborda um novo tipo de obrigação de natureza dialógica, contribuindo para os debates daquela dimensão aqui denominada de subjetiva:

> a ação de 'encaixar uma pessoa', a partir de seus dados pessoais e dados anonimizados, em um perfil social e inferir algo sobre ela implica em obrigações de três naturezas: (i) informacional, relacionada à obrigação de dar ciência da existência do perfil e garantir sua máxima transparência, (ii) anti- discriminatória, relacionada à obrigação de não utilizar parâmetros de raça, gênero e orientação religiosa como

de outros direitos legais subjacentes frequentemente determina a substância da transparência.137 Se alguém tem o direito de correção, precisa ver os erros. Se alguém tem o direito contra a discriminação, precisa ver quais fatores são usados em uma decisão. Caso contrário, as assimetrias de informação invalidam os direitos subjacentes. (MARGOT, 2019,p. 213) Tradução livre das autoras.

38 No trabalho de Veale e Edwards, verifica-se uma análise mais detida sobre o tema. (2018 a).

> determinantes na construção do perfil, e (iii) dialógica, relacionada à obrigação de se engajar em um 'processo dialógico' com as pessoas afetadas, garantindo a explicação de como a perfilização funciona, sua importância para determinados fins e de como decisões são tomadas. (ZANATTA, 2019, p.22,23)

Ainda sobre tal perspectiva, é importante observar as críticas tecidas a respeito do pesado ônus deixado aos usuários para desafiar decisões automatizadas com resultados ruins, tanto numa possível tutela individual quanto naquelas coletivas (tradicionais). Seja por falta de acesso á justiça - em especial para as últimas - ou ainda pelas dificuldades de seu exercício em termos administrativos já que no que diz respeito ás autoridades de dados estaduais na Europa, pode faltar apoio em termos de falta de recursos humanos e expertise desses órgãos (VEALE, EDWARDS, 2018, p. 49)

Estas são apenas algumas breves e resumidas observações acerca das novas interpretações do direito de explicação em sua dimensão individual/subjetiva. Não havendo pretensão nem oportunidade, nesse trabalho, de aprofundar o tema ou de se posicionar a favor de alguma teoria.

No que diz respeito á dimensão objetiva do direito de explicação, foi possível observá-la diante da crítica de Margot sobre os recentes debates do direito de explicação, no sentido de que eles perderam a centralidade da transparência e, nesse contexto, não deram importância "ao significativo regime de responsabilidade algorítmica estabelecido pelo RGPD". Com base nessas argumentações e nas Diretrizes do grupo de trabalho do artigo 29 Margot propõe "o direito de explicação revisitado",(2019, p. 206; 209) por meio do qual interpreta "salvaguardas adequadas" de modo a incluir, também , medidas de responsabilidade sistêmica, como auditoria e conselhos de revisão ética". As avaliações/relatórios de impacto algorítmicas e as propostas de proteção de denunciantes. (2019, p. 208;210;215). Algumas já mencionadas no tópico 1 no contexto das Diretrizes do referido grupo de trabalho.

Segundo Margot:

> Essas medidas de responsabilidade sistêmica têm duplo significado: Elas podem ser entendidas como reforçando os direitos individuais, garantindo que alguém imparcial está fornecendo supervisão em nome de indivíduos, ou fornecendo a responsabilidade necessária sobre o comportamento da empresa em um regime de governança colaborativa (parceria privada / pública), à medida que as empresas criam e implementam sistemas para prevenir erros, preconceitos e discriminação. (2019, p. 205) (grifo nosso) ( tradução livre das autoras).

O que corrobora com os entendimentos acerca da dimensão objetiva dos direitos fundamentais e, assim, do direito de explicação.

Margot reconhece - fazendo menção á Frank Pasquale - que o RGPD estabelece um sistema de "transparência qualificada" sobre a tomada de decisão algorítmica, segundo a qual relaciona um tipo de informação aos titulares de dados e outro tipo aos especialistas e reguladores. Um tipo de transparência em camadas no sentido de que "o quem" e o "porquê" da transparência ditam "o quê", quando e 'como" (2019, p. 210, 211). Donde se verifica que sua proposta se interconecta com os diferentes tipos e níveis de opacidade acima relacionados, que apresenta variações, de um lado em razão do tipo de opacidade/falta de transparência e, de outro, do sujeito que está diretamente interessado/envolvido.

Os estudos de Veale e Edwards no seu artigo Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"? também foram fundamentais para trazer o debate acerca dessa dimensão objetiva do direito de explicação. Não só pelas críticas acerca da dimensão individual, como o exemplo citado acima, mas, especialmente, ao considerarem que "um direito legal a uma explicação pode ser um bom lugar para começar, mas de forma alguma é o fim da história" e que a 'falácia da transparência' é algo contra o qual devemos nos proteger e que deve nos estimular, […], a olhar para maneiras alternativas e complementares de construir sistemas melhores (2018, p. 50) propondo

> ferramentas de governança que têm impactos a montante, enquanto sistemas estão sendo projetados ou pelo menos antes de serem implantados. Privacidade por Design, Proteção de Dados por Design, e avaliações de impacto. O RGPD introduz uma série de novas disposições que, radicalmente, não conferem direitos individuais, mas sim tenta criar um ambiente no qual sistemas automatizados menos "tóxicos" serão construídos no futuro. (VEALE, EDWARDS, 2018, p. 50)

Com base nessas análises e tendo vista as Diretrizes do grupo de trabalho do artigo 29, explicitadas no tópico 1, acredita-se ser possível identificar em diversos trabalhos nacionais - alguns com conexão mais direta e detalhada com o direito de explicação- argumentos que encaminham/ aproximam estudos sobre os algoritmos dessa dimensão objetiva.

Há estudos voltados para a análise da explicabilidade dos algoritmos que alertam para a necessidade de "desbordar do campo exclusivamente jurídico e atentar a questões relativas aos desenhos de políticas públicas, além de observar possibilidades e ferramentas que a ciência da computação provê" e mencionam que a preocupação com accountability deve estar presente desde o desenvolvimento dos algoritmos. (FERRARI, [s/data], p. 13; )

Diversos trabalhos referem-se á importância da accountability no contexto de discriminação algorítmica. Alguns com referência ao direito de explicação e analisando a LGPD (FRAZÃO,2019, 2019 a) outros, de forma mais geral, levantando "debates obre a necessidade de governança algorítmica, transparência e fiscalização" (MENDES, MATTIUZZO, 2019). Doneda et al chegam a mencionar expressamente que "[…] a obscuridade dos processo s algorítmicos é um problema posto não só para os indivíduos, mas também as autoridades reguladoras e supervisoras (DONEDA et al, 2018, p. 5).

Há, ainda, estudos que buscando retirar a autodeterminação informacional do centro dos debates, consideram "o princípio da accountability e os relatórios de impacto à proteção de dados pessoais, elementos centrais das Leis de proteção de dados." E que eles se revelam- "como

possíveis feixes de entrada para a aplicação do princípio da precaução à IA, ainda mais quando se tem em vista que boa parte do emprego dessa tecnologia envolverá o processamento de dados pessoais" (BIONI, LUCIANO, [s/data] p. 8; 9-10)

No trabalho de Wtacher et al, já havia uma sinalização para uma perspectiva objetiva do direito de explicação. Isso porque eles compreendem o direito de explicação como"[…] um mecanismo promissor no busca mais ampla por parte do governo e da indústria para responsabilidade e transparência em algoritmos, artificiais inteligência, robótica e outros sistemas automatizados […][39]"( WACHTER *et al,* 2017, p. 77), conforme já mencionado no tópico anterior.

## CONSIDERAÇÕES FINAIS

Conforme elucidado na introdução, a presente pesquisa foi desenvolvida com base no método auxiliar comparativo. Quando da elaboração do projeto de pesquisa acreditava-se que tanto o desenvolvimento do trabalho quanto suas considerações finais seriam formatadas de maneira a apresentar um efetivo quadro comparativo, diante de um paralelo feito ponto a ponto entre o contexto do direito de explicação no RGPD e na LGPD.

O primeiro tópico, voltado para o exame das previsões normativas do RGPD - incluindo seus considerandos e as Diretrizes do Grupo de Trabalho do artigo 29 - e da LGPD acerca das decisões totalmente automatizadas, forneceu um ótimo resultado enquanto quadro comparativo ponto a ponto. No entanto, não foi possível alcançar desfecho similar nos tópicos seguintes, nos quais o centro do debate foi o RGPD e as discussões em torno dessa normativa o que, consequentemente, conduziu á formatação de exames com poucas referências diretas á LGPD.

Primeiramente, verificou-se que a LGPD apresenta disposições sobre as decisões totalmente automatizadas - especialmente artigo 20 e

[39] O que reflete o tema da presente pesquisa ser uma complementação e continuidade de temas já abordados pelas autoras em outros artigos científicos.

seus parágrafos - que se aproximam daquelas estabelecidas no texto vinculativo do RGPD sobre o tema - artigos 22 (1) a (4), artigo 13 (2) f, 14 (2) g, 15(1) h. Tendo sido verificadas, também, diferenças quanto aos textos utilizados, à organização e à distribuição de tais previsões.

No segundo tópico, apresentaram-se os debates pioneiros sobre o direito de explicação que surgiram no contexto internacional tendo em vista, principalmente, os artigos ora citados do RGPD e, ainda, alguns de seus considerandos. Três trabalhos, que são referência sobre o tema, foram objeto de exame. Observou-se que nos três, as explicações voltavam-se para o titular de dados, considerados individualmente, sendo o indivíduo o centro do debate. Diante disso, e recorrendo a lições dos direitos fundamentais, identificou-se que estas análises pioneiras tiveram como objeto uma dimensão subjetiva do direito de explicação.

O terceiro tópico levantou, de forma resumida, desafios da opacidade/falta de transparência das decisões automatizadas e ressaltou que o tipo e nível de opacidade e, consequentemente, o de transparência apresentam variações tendo em vista o interessado ou envolvido diretamente na proteção de dados. Diante desse contexto, e tendo em vista, também, as Diretrizes do grupo de trabalho do artigo 29 sobre decisões totalmente automatizadas, traçadas no primeiro tópico, puderam ser observados novos debates sobre o direito de explicação. Alguns inovaram quanto á dimensão subjetiva desse direito, mencionando, por exemplo, um processo dialógico, enquanto outros trouxeram argumentos que, para as autoras desta pesquisa, se enquadram em uma nova perspectiva de análise do direito de explicação que se optou por denominar, a partir de lições das classificações dos direitos fundamentais, de dimensão objetiva do direito de explicação.

Enfatiza-se que o formato final deste trabalho, no sentido de o RGPD e suas interpretações terem tido centralidade em detrimento da LGPD e suas análises, reforça o método comparativo e põe em evidência que o direito de explicação tem sido abordado a partir da LGPD como uma simples incorporação das previsões internacionais acerca do RGPD para a realidade nacional. Disso resulta um importante alerta: a

necessidade de tal direito - receba ou não a denominação de direito de explicação - ser objeto de análises mais profundas que consigam explorar o debate que já foi feito e aquele que tem sido conduzido no âmbito internacional para que sirvam de contribuição para os debates nacionais sobre o tema.

Nesse sentido, o presente trabalho demonstra a importância de considerar que tal direito envolve duas dimensões - subjetiva e objetiva -, que são complementares entre si, e evidencia a relação da dimensão objetiva e com as políticas públicas de proteção de dados pessoais, que têm o potencial de estabelecer e regular instrumentos e ferramentas que, de um lado orientam os responsáveis pelo tratamento de dados e, por outro, viabilizam a fiscalização/auditoria e até mesmo responsabilização, envolvendo um contexto de governança dos algoritmos. Os relatórios de impacto foram mencionados tanto no contexto do RGPD, nos tópicos 1 e 3, quanto no contexto da LGPD, no tópico 3, como possíveis ferramentas dessa dimensão. Resta claro que sob esta dimensão, a transparência volta-se para outros interessados que não do titular de dados e, por isso, exige outros instrumentos para que seja viabilizada. O que envolve a "transparência qualificada" mencionada no tópico 3.

Trata-se de um contexto que cobrará, diante de cada caso, examinar e identificar: num primeiro momento qual é o tipo de opacidade/falta de transparência - se organizacional, técnica ou legal; e na sequência, quem é o interessado diretamente, se o titular de dados, o Estado e seus órgãos ou, ainda, organizações não governamentais, sendo que cada tipo de opacidade e de interessado conduzirá a propostas diferentes para viabilizar o direito de explicação.

Diante desse panorama considera-se que, orientado pela problemática apresentada na introdução, o presente trabalho pôde confirmar a hipótese de pesquisa proposta. Apesar de não terem sido encontrados trabalhos que mencionassem o reconhecimento de uma dimensão objetiva para o direito de explicação, que ultrapassa e complementa a sua perspectiva/dimensão subjetiva, as novas abordagens sobre este direito, especialmente as posteriores às Diretrizes do grupo de trabalho do artigo

29, forneceram elementos suficientes para que as autoras as enquadrassem como estudos que orientam para uma nova dimensão do direito de explicação: a dimensão objetiva. Nesse contexto o objetivo do trabalho também foi alcançado,.

O estudo não pretendeu nem conseguiria esgotar o tema. Ele foi elaborado com intuito de provocar novas reflexões sobre a temática, enfatizando, inclusive, que pensar numa dimensão objetiva para o direito de explicação significa, de um lado liberar o pesado ônus que tem sido colocado á encargo dos titulares de dados, e, de outro, colocar em evidência o papel das políticas públicas na área de proteção de dados.

Importante notar que um debate a partir dessa perspectiva - complementar daquela subjetiva - conduzirá, também, á expansão/revisão daquelas três bases jurídicas identificadas no segundo tópico para analisar o direito de explicação. Cobrará mais estudos sobre o princípio da transparência, do tratamento justo e equitativo e da não-discriminação, tanto no RGPD quanto na LGPD.

Por fim, deve-se ter em vista que o debate apresentado neste artigo, ao tomar como ponto de partida o RGPD e a LGPD, limita-se a um contexto específico das decisões *unicamente/*totalmente automatizadas, excluindo de seu âmbito outros tipo de decisão automatizada que, apesar de não serem unicamente automatizadas, tem o potencial de causar diferentes prejuízos para os titulares de dados.

## REFERÊNCIAS

BRASIL. Lei 13.709, de 14 de agosto de 2018. **Lei Geral de proteção de dados pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: ago. 2020.

BRASIL. Presidência da República. Secretaria -geral. Subchefia para assuntos jurídicos. Mensagem n. 288, de 8 de julho de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm. Acesso em: ago. 2020.

BRASIL. **Projeto de Lei de 2019**. Altera a Lei no 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), para definir a expressão "decisão automatizada ". 2019 a. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7990341&ts=1594035945675&disposition=inline. Acesso em: ago. 2020.

BIONI, R.Bruno; LUCIANO, Maria. **O princípio da precaução na regulação da inteligência artificial**: seriam as leis de proteção de dados o seu portal de entrada? [s/data]. Disponível em: https://brunobioni.com.br/wp-content/uploads/2019/09/Bioni-Luciano_O-PRINCI%CC%81PIO-DA-PRECAUC%CC%A7A%CC%83O-PARA-REGULAC%CC%A7A%CC%83O-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf. Acesso em: ago. 2020.

BIONI, R.Bruno. MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalênciaIn:FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato, (coord.) **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. edição [2019] THOMSON REUTERS BRASIL CONTEÚDO E TECNOLOGIA LTDA Edição do Kindle.

BONAVIDES, Paulo. **Curso de Direito Constitucional.** 13. ed., rev. e atual. São Paulo:Malheiros, 2003.

BONAVIDES, Paulo. **Do Estado Liberal ao Estado Social.** 9. ed. São Paulo: Malheiros, 2009.

BONAVIDES, Paulo. **Teoria do Estado**. 3. ed., rev. e ampl. São Paulo: Malheiros, 1995.

BURRELL, jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society January–June 2016: 1–12 https://doi.org/10.1177/2053951715622512. Disponível em: http://journals.sagepub.com/doi/pdf/10.1177/2053951715622512. Acesso em: jul. 2020.

BURT, Andrew. **Is there a 'right to explanation' for machine learning in the GDPR?** https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/.2017. Acesso em: jul. 2018.

CANOTILHO, J. J. Gomes. **Direito Constitucional e teoria da Constituição**. 7. ed., 6. reimp. Coimbra: Almedina, 2003.

CANUT, Letícia; MEDEIROS, Heloísa Gomes. Os algoritmos nas relações de consumo eletrônicas: análise do direito do consumidor à informação. GEDAI Grupo de Estudos de Direito Autoral e Industrial Prof. Dr. Marcos Wachowicz (organizador). **Anais do XI CODAIP. XI Congresso de Direito de autor e interesse Público Estudos de Direito de Autor e Interesse Público**. Curitiba: Universidade Federal do Paraná, 2017. Disponível em: http://www.gedai.com.br/sites/default/files/publicacoes/anais_xi_codaip-2017-gedai.pdf. Acesso em: jul. 2018.

CANUT, Letícia; MEDEIROS, H.G. Direito de autor sobre o software e suas implicações sobre a governança dos algoritmos. In: Anais XII CODAIP - Anais do XII CODAIP. XII Congresso de Direito de Autor e Interesse PúblicoCuritiba: GEDAI/UFPR,2018. **Anais do XII Congresso de Direito de Autor e Interesse Público** (2018: Curitiba, PR). Coordenadores: Marcos Wachowicz, Marcia Carla Pereira Ribeiro, Sérgio Staut Jr e José Augusto Fontoura Costa. p. 475-504. ISSN: 2178-745X. Disponível em:<http://www.gedai.com.br/wp-content/uploads/2019/05/021-O-DIREITO-DE-AUTOR-SOBRE-O-SOFTWARE-E.pdf

DIEGA, Guido Noto La Against the Dehumanisation of Decision-Making Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information. Disponível em: file:///Users/leticia/Downloads/against-thedehumanisationofdecision-makingJIPITEC_9_1_2018_3-34.pdf. Acesso em: jun. 2020.

Doneda, Danilo Cesar Maganhoto Doneda et al. * Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. In: **Pensar**, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018. DOI: 10.5020/2317-2150.2018.8257. Disponível em: https://periodicos.unifor.br/rpen/article/view/8257/pdf. Acesso em: jul. 2020.

FERRARI, Isabela. **Accountability de Algoritmos:** a falácia do acesso ao código e caminhos para uma explicabilidade efetiva. [s/data]. Disponível em: https://itsrio.org/wp-content/uploads/2019/03/Isabela-Ferrari.pdf. Acesso em: ago. de 2020.

FRAZÃO, Ana. Importância da Lei Geral de Proteção de Dados. In:FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato, (coord.) **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. edição [2019] THOMSON REUTERS BRASIL CONTEÚDO E TECNOLOGIA LTDA Edição do Kindle.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In:FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato, (coord.) **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. edição [2019 a] THOMSON REUTERS BRASIL CONTEÚDO E TECNOLOGIA LTDA Edição do Kindle.

GOODMAN, Bryce; FLAXMAN, Seth. European Union regulations on algorithmic decision-making and a "right to explanation". **AI Magazine**, Vol 38, No 3, 2017. DOI: 10.1609/aimag.v38i3.2741. Disponível em: https://arxiv.org/pdf/1606.08813.pdf. Acesso em: jul. 2018.

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS. Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679. 2018. Disponível em: https://www.cnpd.pt/home/rgpd/docs/wp251rev01_pt.pdf. Acesso em: maio 2020.

SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, Volume 7, Issue 4, 1 November 2017, Pages 233–242, https://doi.org/10.1093/idpl/ipx022. p. 233- 242. Disponível em: https://academic.oup.com/idpl/article/7/4/233/4762325. Acesso em: jul. 2018.

TAURION, Cezar. **Onde os algoritmos e a inteligência artificial vão nos levar?** 29 de junho de 2016. Disponível em: http://computerworld.com.br/onde-os-algoritmos-e-inteligencia-artificial-vao-nos-levar. Acesso em: ago. 2017.

CASEY, Bryan; FARHANGI, Ashkon; vogl, Roland. Rethinking Explainable Machines: The GDPR'S "right to explanation"debate and the rise algorithmic audits in enterprise.2019. DOI: https://doi.org/10.15779/Z38M32N986. Disponível em: https://btlj.org/data/articles2019/34_1/04_Casey_Web.pdf . Aceso em: jul. 2020.

LUÑO, Antonio Enrique Pérez. **Los derechos fundamentales**. 6. ed. Madrid: Tecnos, 1995.

MARGOT E. Kaminski, The Right to Explanation, Explained, 34 BERKELEY TECH. L.J. 189 (2019), available at https://scholar.law.colorado.edu/articles/1227. Disponível em: https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=2335&context=articles. Acesso em: jul. 2020.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. In: **RDU**, Porto Alegre, Volume 16, n. 90, 2019, 39-64, nov-dez 2019. Disponível em: file:///Users/leticia/Downloads/Discrimina%C3%A7%C3%A3o%20Algor%C3%ADtmica%20Conceito,%20Fundamento%20Legal%20e%20Tipologia%20(Laura%20Schertel%20Mendes,%20Marcela%20Mattiuzzo).pdf. Acesso em: set. 2020.

MONTEIRO, RENATO LEITE. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? INSTITUTO IGARAPÉ | ARTIGO ESTRATÉGICO 39 | DEZEM-

BRO 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf, Acesso em: jul. 2020.

POLIDO, Fabrício B. Pasquot, et al. Instituto de Referência em Internet e Sociedade. GDPR e suas repercussões no direito brasileiro. Primeiras impressões de análise comparativa. [s/d]. Disponível em: http://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%C3%B5es-no-direito-brasileiro-Primeiras-impress%C3%B5es-de-an%C3%A1lise-comparativa-PT.pdf. Acesso em: jul. 2018.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 3. ed., rev., atual e ampl. Porto Alegre: Livraria do Advogado, 2003.

_____. **A eficácia dos direitos fundamentais. Uma teoria geral dos direitos fundamentais na perspectiva constitucional.** 10. ed., rev., atual. e ampl. Porto Alegre: Livraria do Advogado, 2010.

SILVA, Priscilla; MEDEIROS, Juliana. A polêmica da revisão (humana) sobre decisões automatizadas. **ITS Rio**. Dezembro de 2019. Disponível em: https://feed.itsrio.org/a-pol%C3%AAmica-da-revis%C3%A3o-humana-sobre-decis%C3%B5es-automatizadas-a81592886345. Acesso em: maio 2020.

PARLAMENTO EUROPEU. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: maio 2020.

VEALE, Michael; EDWARDS, Lilian. Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"? University College London May/June 2018 Copublished by the IEEE Computer and Reliability Societies 1540-7993/18/$33.00 © 2018 IEEE. Disponível em: https://michae.lv/static/papers/2018enslavingthealgorithm.pdf. Acesso em: ago. 2020.

VEALE, Michael; EDWARDS, Lilian. Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. Computer law & security review 34 (2018 a) 398–404. Disponível em: https://reader.elsevier.

com/reader/sd/pii/S026736491730376X?token=6555E87B844229771999065F-98453F7A5D7C98A85F29005217E078267D5015AF1279FB21F9E308DBA2C1E-58B1587C9AD. Acesso em: ago. 2020.

VERONESE, Alexandre.Os direitos de explicação e de oposição frente às decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato, (coord.) **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** edição [2019 a] THOMSON REUTERS BRASIL CONTEÚDO E TECNOLOGIA LTDA Edição do Kindle.

VOGL, Roland ; FARHANGI, Ashkon; CASEY, Bryan. Rethinking Explainable Machines: The Next Chapter in the GDPR's 'Right to Explanation' Debate. 15 May 2018. Disponível em: https://www.law.ox.ac.uk/business-law-blog/blog/2018/05/rethinking-explainable-machines-next-chapter-gdprs-right-explanation. Acesso em: jul. 2017.

GRYZ, Jarek; SHAHBAZI, Nina. Futility of a Right to Explanation Jarek Gryz, 2020 Copyright held by the owner/author(s). Published in Workshop Proceedings of the EDBT/ICDT 2020 Joint Conference, March 30-April 2, 2020 on CEUR-WS.org Distribution of this paper is permitted under the terms of the Creative Commons license CC BY 4.0 Disponível em: nima@mindle.ai http://ceur-ws.org/Vol-2578/PIE1.pdf. Acesso em: set. 2020

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, Volume 7, Issue 2, 1 May 2017, Pages 76–99,https://doi.org/10.1093/idpl/ipx005. Disponível em: https://academic.oup.com/idpl/article/7/2/76/3860948. Acesso em: jul. 2018.

ZANATTA, Rafael, A. F. Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. Fevereiro de 2019. DOI: 10.13140/RG.2.2.33647.28328. Project: Risk regulation and data protection. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais. Acesso em: jan. 2020.

# Capítulo IV

# A RESPONSABILIDADE CIVIL NO TRATAMENTO DE DADOS PESSOAIS PELAS APLICAÇÕES DE IA

*Bruna Werlang Paim*[1]

*Lukas Ruthes Gonçalves*[2]

## INTRODUÇÃO;



## RESUMO

As operações de tratamento de dados já podem ser realizadas por aplicações de IA (Inteligência Artificial). Atualmente, já se considera o fenômeno de "chefes robóticos", ou seja, aplicações de IA que são as efetivamente responsáveis por gerir os dados de clientes e decidir o melhor curso de ação de determinada empresa ou associação. Com a edição de normas de proteção de dados como a LGPD e o RGPD esse tipo de operação já se enquadra nas funções de controladores e operadores, que podem ser responsabilizados juridicamente pelos seus atos. Nesse sentido, o presente artigo objetiva verificar em primeiro lugar o que seriam essas aplicações de IA e quais as atribuições do controlador e do operador de dados de acordo com a LGPD e o RGPD. Logo em seguida, verificar-se-á como se dá o regime de Responsabilidade Civil na Europa e no Brasil no que tange ao regime de proteção de dados para, por fim, abordar qual seria a responsabilidade civil de um agente de tratamento de dados não-humano. Como conclusão percebe-se que uma aplicação de IA não passa de uma ferramenta e que a responsabilidade recairia no operador ou controlador pessoa física, em especial no segundo.

**Palavras-chave:** Aplicações de IA; LGPD; RGPD; Controlador e operador de dados; Responsabilidade Civil.

[1] É advogada, pós-graduanda em Direito, Logística e Negócios Internacionais e graduada pela Pontifícia Universidade Católica do Paraná (PUCPR). Pesquisadora junto ao Núcleo de Estudos Avançados em Direito Internacional (NEADI).

[2] É advogado, mestre em Direito pela Universidade Federal do Paraná. Pesquisador junto ao Grupo de Estudos de Direito Autoral e Industrial (GEDAI), cadastrado no CNPq.

## INTRODUÇÃO

Ao prever sanções administrativas significativas, como por exemplo multas que podem chegar até cinquenta milhões de reais por infração no caso da LGPD, a responsabilidade civil dos agentes de tratamento de dados torna-se objeto de relevante debate.

Independentemente do ramo de atuação, o uso de aplicações de inteligência artificial cresce consideravelmente. No entanto, quando utilizada para o tratamento de dados pessoais, a aplicação da IA traz consigo não apenas as facilidades da inovação mas também as incertezas jurídicas do que ainda é considerado novidade.

Assim, uma vez que o direito necessita do diálogo com as demais áreas da ciência, é imperioso compreender o que compõe e como funciona a inteligência artificial, a essa temática, dedicar-se-á o primeiro capítulo. Em seguida, abordar-se-ão os agentes de tratamento de dados de acordo com a LGPD (Lei Geral de Proteção de Dados) e o RGPD (Regulamento Geral de Proteção de Dados) da União Europeia, explorando-se, assim, os papéis e responsabilidades do controlador e operador de dados pessoais. No terceiro capítulo, em análise comparada, buscar-se-á verificar como se dá a responsabilidade civil no Brasil e na legislação europeia, tomando como referência a lei alemã, considerando-se a falta de um direito civil europeu. Para então, com o anteriormente exposto, apresentar as reflexões acerca da responsabilidade civil nos casos em que a inteligência artificial figure como agente de tratamento dos dados pessoais.

## 1 OS TRÊS ELEMENTOS ESSENCIAIS QUE COMPÕEM UMA APLICAÇÃO DE IA: SOFTWARE, HARDWARE E DADOS

Para se explorar como uma aplicação de IA poderia ser utilizada em operações de tratamento de dados pessoais, é necessário entender em primeiro lugar como se dá a operação de um programa do tipo e quais são os elementos que possibilitam seu funcionamento. O entendimento

preciso do que se trata a tecnologia da Inteligência Artificial é de fundamental importância para se compreender alguns dos desafios que sua regulamentação apresenta.

Russell e Norvig (2016) trazem Inteligência Artificial como sendo "o estudo e concepção de agentes inteligentes, onde um agente inteligente é um sistema que percebe seu ambiente e realiza ações que maximizam suas chances de sucesso". Seguindo essa mesma linha de pensamento, Kurzweil (1990) aborda essa tecnologia como sendo "a arte de criar máquinas que desempenhem funções que requeiram inteligência quando realizadas por pessoas".

Essas são apenas duas de uma série de definições que esse conceito possui e que vem ganhando ainda mais fama nos últimos tempos. Porém, o conceito de Inteligência Artificial a ser adotado para fins deste trabalho provém de Gonçalves (2019, p. 33) que fala que a IA:

> Se trata de uma área de estudo focada em resolver problemas (ou criar máquinas que desempenhem essa função) que anteriormente somente a mente humana saberia responder. Desse modo, não se pode falar que exista "uma" ou "a" Inteligência Artificial. O que existem são uma série de diferentes aplicações que se utilizam de tecnologia avançada com o fim de suprir a capacidade de raciocínio humano em um uso ou outro.

Ou seja, uma aplicação de Inteligência Artificial se trata de um programa que é executado em algum tipo de computador e que emula o raciocínio humano com base nas informações que recebe. Ver-se-á mais acerca dos elementos que compõem esse tipo de aplicação nos itens abaixo.

Dentro dessa área de estudo, encontra-se ainda uma discussão importante sobre a distinção entre as modalidades de aplicações de IA existentes. Na literatura existente sobre o tema se encontram popularmente quatro tipos: a *narrow* em contraposição à *general AI* e a *weak* em contraposição à *strong AI* (também chamada de AGI: *Artificial General Intelligence*).

Diz Teemu Roos (2018) que *Narrow* diz respeito à aplicação de IA capaz de executar uma única tarefa. *General,* por outro lado, seria uma máquina capaz de lidar com qualquer atividade do intelecto. Todos os métodos de Inteligência Artificial utilizados atualmente são caracterizados como *Narrow*. Ou seja, tratam-se de aplicações programadas com um único propósito e que só conseguem executar esse único propósito. A *General AI*, aquela capaz de executar qualquer tarefa independentemente de ela ter sido programada ou não, se encontra no âmbito da ficção científica.

Já a dicotomia entre *weak* e *strong* se resume à distinção filosófica entre parecer inteligente por meio de suas ações e efetivamente ser inteligente, conforme problematizado pelo Teste de Turing[3]. De acordo com Teemu Roos (2018), uma *strong AI* equivaleria a uma mente genuinamente inteligente e autoconsciente. Já a *weak AI* seria o que efetivamente existe, nomeadamente sistemas que exibam comportamentos inteligentes apesar de serem apenas aplicações de computador.

Diz Gonçalves (2019, p. 35) que "ainda que a humanidade não esteja próxima de desenvolver uma AGI que tenha sua própria consciência, sua aplicação de maneira restrita já está bastante difundida na sociedade, mesmo que de um modo não tão evidente". Assim, esse tipo de aplicação *narrow* não impede que os programas existentes já tenham a capacidade de tomar decisões com base nas informações que recebam, conforme será abordado ao longo deste trabalho.

Exemplos de usos de aplicações de IA na atualidade, que já surtem efeitos na sociedade e no ambiente empresarial contemporâneo, incluem seleção e recrutamento de candidatos por meio da análise de currículos dos atuais funcionários; treinamento de colaboradores a partir da utilização de aplicações de IA em conjunto com dispositivos de realida-

[3] De acordo com o teste de Turing (TURING, 1950), um interrogador deveria inquirir dois jogadores, uma pessoa e um computador, sem saber sua identidade, com o fim de determinar se o computador poderia fazer o interrogador pensar que ela é humana com sucesso. Tendo sucesso, isso seria uma prova de que uma máquina poderia ser sim dotada de inteligência.

de aumentada; gerenciamento de atividades repetitivas para aumentar a produtividade dos trabalhadores e; monitoramento da quantidade e qualidade do trabalho executado por funcionários através de aplicações de IA e dispositivos de IoT (MARR, 2019).

Assim, abordou-se a definição de IA como sendo a área de estudo dedicada a criar dispositivos que emulem com sucesso o raciocínio humano, tais como aqueles que influenciam no processo de contratação de funcionários, auxiliando uma empresa a tomar decisões. Agora se falará sobre os principais elementos que viabilizam o adequado funcionamento de uma aplicação do tipo, que são três: software, hardware e dados.

## 1.1 O Software

Para falar sobre o software colaciona-se em primeiro lugar mais uma definição de IA, que para McCarthy (1955) seria a "teoria e o desenvolvimento de sistemas de computador capazes de realizar tarefas que normalmente requereriam inteligência humana, como percepção visual, reconhecimento de fala, tomada de decisões e tradução entre línguas". Os termos-chave desta definição são "sistemas de computador", que nada mais são do que programas, ou softwares da tradução para o inglês, os quais são por sua vez compostos por algoritmos.

O algoritmo "é um conjunto de instruções matemáticas, uma sequência de tarefas para alcançar um resultado esperado em um tempo limitado" (KAUFMAN, 2018). Ou seja, de acordo com Gonçalves (2019, p. 44):

> Sua existência não é necessariamente vinculada a um computador ou outro dispositivo eletrônico, de modo que uma receita de bolo, por exemplo, pode ser considerada um algoritmo para o mundo físico, por ser uma série de instruções para se atingir determinado fim.

De acordo com Solomon Gandz (1926) o termo seria inclusive a latinização do nome de um matemático persa do século IX de nome Al-Khwãrizmi, que ensinava em suas obras técnicas matemáticas a serem resol-

vidas manualmente, sendo ele o responsável por apresentar a primeira solução das equações lineares e quadráticas.

Voltando para o ramo da computação, de acordo com Cormen et al. (2002, p. 3), algoritmo seria definido como "qualquer procedimento computacional bem definido que toma algum valor ou conjunto de valores como entrada e produz algum valor ou conjunto de valores como saída".

Sobre esse tema discorre Gonçalves (2019, p. 45):

> Tal conjunto de instruções que transforma determinado valor de entrada em um resultado de saída pode ser realizado por meio de linhas de código que quando aplicadas em determinada máquina executam ações específicas. Tais linhas de código constituem, fundamentalmente, um programa de computador...

Quando utilizados em aplicações de IA que se valham de Machine Learning, buscam-se "algoritmos que podem aprender e fazer previsões sobre dados – esses algoritmos seguem instruções estritamente estáticas ao fazer previsões ou decisões baseadas em dados, através da construção de um modelo a partir de entradas de amostra" (KAUFMAN, 2018).

Ou seja, aplicações de IA que se valham da técnica de Machine Learning se tratam de programas de computador que produzem um determinado valor de saída que emula o raciocínio humano com base nas informações que lhe são fornecidas como valor de entrada. Isso significa que o modo como uma aplicação do tipo recebe e gere esses dados que servem como *input* é extremamente importante, como se verá a seguir.

Da aplicação da técnica de Machine Learning se desenvolveu uma nova modalidade de programação mais complexa denominada *Deep Learning*. Ela utiliza redes neurais artificiais, simulações simplificadas de como neurônios biológicos se comportam, para extrair regras e padrões de determinados conjuntos de dados (ECONOMIST, 2015).

Essa tecnologia consiste em uma série de unidades similares a neurônios que combinam uma série de valores de entrada para produzir

um valor de saída. Esse output, por sua vez, também é passado para outras unidades neurais, seguindo uma corrente (OSTP, 2016, p. 09). Desse modo, de acordo com Gonçalves (2019, p. 46) "uma aplicação que utilize *Deep Learning* vai, em uma primeira etapa, analisar uma sequência de dados para chegar em determinado padrão; em seguida vai passar esse padrão por uma segunda camada de análise para chegar em um padrão mais refinado e daí em diante".

Temu Roos (2018) afirma que é justamente essa profundidade de camadas que permite a rede aprender estruturas mais complexas sem necessitar de quantidades irrealmente excessivas de dados. Além disso, destaca o autor que outra grande razão para se construir redes neurais artificiais seria para utilizar os sistemas biológicos presentes nos humanos como inspiração para programar melhores programas de IA. De acordo com ele (ROOS, 2018):

> O caso das redes neurais em geral, como uma abordagem da IA, baseia-se em um argumento semelhante ao das abordagens baseadas em lógica. Neste último caso, pensava-se que, para alcançar a inteligência em nível humano, precisamos simular processos de pensamento de nível superior e, em particular, a manipulação de símbolos que representam certos conceitos concretos ou abstratos usando regras lógicas.

Viu-se, então, que uma aplicação de Inteligência Artificial é constituída por um software, cujo algoritmo é feito por meio de técnicas que melhor permitem emular o pensamento humano (*Machine Learning* e *Deep Learning*). É necessário verificar agora onde esse tipo de programa é executado para fazer surtir efeitos no mundo físico.

## 1.2 O Hardware

Hans Moravec (1976), faz uma analogia de que uma aplicação de IA necessitaria de poder de computação do mesmo modo que aviões necessitam de cavalos de potência. Abaixo de certo limite a tecnologia não

funcionaria, mas à medida que o poder aumenta a tarefa se torna mais fácil. Nesse sentido, a área do Hardware é uma que, felizmente, vem apresentando constante melhora.

De acordo Gonçalves (2019, p. 49) "empresas como a Microsoft vêm desenvolvendo os chamados Computadores Quânticos, os quais prometem melhorar consideravelmente a capacidade de análise que as máquinas atuais permitem". Para efeito de comparação "em 1997, o Deep Blue da IBM analisava 200 milhões de movimentos por segundo para superar o campeão de xadrez Garry Kasparov. Uma máquina quântica, por outro lado, seria capaz de analisar 1 trilhão de movimentos a cada segundo" (GARRETT, 2018).

Isso porque, continua Gonçalves (2019, pp. 49-50), a diferença estaria no modo como um computador quântico funciona. Uma análise feita pelo time de computação quântica da Microsoft discorre que o processamento em um computador tradicional ocorre de maneira binária, com a informação sendo transmitida a partir de *bits* os quais só podem ter um valor binário de 0 ou 1, o que limita a capacidade de processamento. Já na computação quântica, um *quantum bit* pode segurar os dois valores ao mesmo tempo, o que é chamado de estado de superposição, e isso permite com que a velocidade de processamento seja vastamente superior se comparado a computadores tradicionais (MICROSOFT, 2018).

Um Hardware mais rápido também possibilitaria a solução de outra barreira tecnológica explicada pelo que é chamado de Paradoxo de Moravec. De acordo com Gonçalves (2019, p. 48) esse se trata da constatação "de que problemas mentais complexos requerem uma capacidade computacional baixa para serem replicados e que atividades motoras de baixo grau de complexidade (como segurar um copo) necessitariam, inversamente, de enormes recursos". De acordo com Moravec (1988, p. 15):

> É comparativamente fácil fazer com que os computadores exibam desempenho de nível adulto em testes de inteligência ou jogando damas, e difícil ou impossível lhes dar as habilidades de uma criança de um ano de idade quando se trata de percepção e mobilidade.

Gonçalves completa (2019, p. 49) que se justifica "essa dificuldade pelo fato dessas atividades aparentemente mais simples exigirem uma quantidade grande de dados para serem realizadas, mas que não são percebidas pelo consciente humano". Porém, para as atividades consideradas complexas, como análise e classificação de informações, felizmente a quantidade e o tipo de dados necessários se torna mais fácil de ser avaliado, o que torna operações de gestão de dados pessoais, por exemplo, mais fáceis de serem executadas por aplicações de IA.

## 1.3 Os Dados e as Informações

Isso porque, além dos avanços na tecnologia dos computadores faz-se necessário a aplicação de IA ter as informações necessárias para produzir determinado resultado. Quanto maior a quantidade e a qualidade dos dados, melhor será o resultado em informações obtido por um programa de *Machine Learning*. Relatou Pamela McCorduck (2004, p. 299) que pesquisadores de IA começaram a suspeitar que a inteligência poderia muito bem ser baseada na habilidade de se utilizar grandes quantidades de diferentes conhecimentos de diferentes maneiras.

Relatam Russell e Norvig (2016, p. 27) que durante o período de 60 anos de história da ciência da computação, de 1950 até aproximadamente 2010, os esforços tinham sido muito mais focados no algoritmo como objeto de estudo. Contudo, ainda de acordo com eles, estudos recentes no campo da IA revelam que para muitos problemas seria melhor se preocupar mais com os dados coletados do que sobre os critérios acerca de qual algoritmo se aplicar. Isso se daria por conta da grande disponibilidade de bases de dados presentes na Internet.

Esses mesmos autores (RUSSELL e NORVIG, 2016, p. 27) citam um trabalho de David Yarowsky do ano de 1995 sobre a importância de uma maior disponibilidade de dados para as aplicações de Inteligência Artificial. O problema abordado por Yarowski, relatam os autores, era: dado o uso da palavra 'planta' em uma frase, ela se referiria à flora ou à fábrica? Abordagens prévias a esse questionamento se valiam de exemplos rotulados

por pessoas combinados com algoritmos de *machine learning*. Yarowsky demonstrou que a tarefa poderia ser executada, com uma precisão superior a 96%, sem qualquer dado selecionado e classificado por humanos. Dizem Russell e Norvig que dando-se à uma aplicação de IA uma grande quantidade de texto não editado e somente as definições de dicionário de ambos os sentidos da palavra 'planta' ('trabalhos, planta industrial' e 'flora, vida vegetal'), já se tornava possível rotular os exemplos dados e a partir desse ponto somente modificar o algoritmo para aprender novos padrões que ajudariam a identificar novos exemplos.

Banko e Brill têm um texto seu de 2001 também citado por Russell e Norvig (2016, p. 28) ao afirmarem que técnicas como a demonstrada acima têm um desempenho ainda melhor à medida que a quantidade disponível de textos vai de um milhão a um bilhão de palavras. Além disso, eles enfatizam que esse aumento na performance da utilização de mais dados excederia qualquer diferença na escolha do algoritmo. Ainda, atestam Banko e Brill que um algoritmo de baixa complexidade que tem acesso a um banco de dados de treinamento não rotulados com 100 milhões de palavras consegue um resultado melhor que um algoritmo mais avançado com apenas 1 milhão de palavras como *input*.

O modo como uma aplicação de IA faz uso de bancos de dados é uma questão muito importante, pois com leis como a LGPD e o RGPD os controladores e os operadores dos dados são os legalmente responsáveis pelo seu uso. Prerna Sindwani menciona um estudo da Infosys e Gaertner que prevê no futuro vários escritórios eliminando a função de gerência de várias empresas (SINDWANI, 2020). O relatório de Prerna menciona que uma quantidade menor de gerentes será necessária, pois muitas de suas tarefas incluem coleta de dados, supervisão e ações de *compliance*, as quais poderão ser completadas por aplicações de IA.

A partir disso já é possível de se perceber o quão fundamental é, assim, a compreensão de exatamente quais as funções do controlador e do operador de acordo com a LGPD e o RGPD. Isso permitirá uma melhor investigação da responsabilidade civil de operadores do tipo que se tratem de aplicações de IA.

## 2 OS AGENTES DE TRATAMENTO DE DADOS DE ACORDO COM A LGPD/RGPD

Não há uma definição única para o que se entende por tratamento de dados, uma vez que ambas as legislações, LGPD e RGPD, preveem, em rol exemplificativo, diversas ações[4] para a sua definição, que pode ser resumida como toda operação realizada com dados pessoais.

Assim, é também definido a quem são previstas tais funções de tratamento. No caso do Brasil e da União Europeia, trata-se do papel de controlador e operador, cuja legislação brasileira, fortemente inspirada na europeia, define respectivamente como: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; e pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Para elucidar, pode-se, muito resumidamente, dizer que o controlador dos dados é quem determina se e como o tratamento dos dados será realizado. Já o operador é quem literalmente fará a ação referente ao tratamento.

Assim, tem-se a estreita vinculação dos dois agentes de tratamento de dados, precipuamente no que tange a atuação do operador em nome do controlador. Ainda, aponta-se a possibilidade de confusão de papéis entre os agentes, podendo uma mesma pessoa ser responsável por tomar a decisão e executá-la. Em decorrência disso, far-se-á a análise de ambos os agentes ao mesmo tempo, tanto na legislação europeia quanto na brasileira.

### 2.1 Controlador e Operador no RGPD

Considerando-se os mais de 25 anos de experiência em proteção legal dos dados pessoais, a União Europeia evolui seu sistema proteti-

[4] LGPD. Art. 5º Para os fins desta Lei, considera-se: X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

vo, bem como alguns conceitos já anteriormente previstos. No entanto, as definições de *controller*/responsável pelo tratamento e *processor*/subcontratante - figuras importadas pelo ordenamento jurídico brasileiro como controlador e operador - trazidas pela Diretiva 95/46/CE foram substancialmente mantidas pelo RGPD[5]. Para fins de melhor acepção do conteúdo neste trabalho, optar-se-á por tratar de tais figuras conforme a lei brasileira, ou seja, controlador e operador.

Dessa forma, a legislação europeia define controlador como a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro. Na mesma linha, define operador como uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes. Adaptando-se a versão do regulamento em português europeu e a versão em inglês, compreende-se que tanto controlador quanto operador podem ser pessoa natural ou pessoa jurídica.

Antes mesmo de definir quem pode ser e as atribuições do controlador e operador, o RGPD traz diversos considerandos que não apenas observam as peculiaridades que embasam o relacionamento da União Europeia com seus Estados-Membros, mas já imputam responsabilidades ao controlador. Apontam-se três exemplos, o Considerando n° 39 que prevê o dever de fixação de prazos pelo controlador para o apagamento ou a revisão periódica de conservação dos dados, a fim de que ocorra apenas enquanto necessário; o Considerando n° 42, o qual prevê que para que o consentimento do titular dos dados seja dado

[5] Para uma análise detalhada sobre o responsável pelo tratamento de dados segundo o RGPD fazer referência ao artigo da Parte I "O responsável pelo tratamento de dados segundo o regulamento europeu", de Alexandre Libório Dias Pereira.

com conhecimento de causa, este deverá conhecer, pelo menos, a identidade do controlador e as finalidades a que o tratamento se destina e o Considerando n° 59, pelo qual o controlador deverá ser obrigado a responder aos pedidos do titular dos dados sem demora injustificada e o mais tardar no prazo de um mês e expor as suas razões quando tiver intenção de recusar o pedido.

Ainda, ao longo de todo o regulamento são atribuídos esparsamente direitos e deveres do controlador, como condições aplicáveis ao consentimento, informações a facultar quando os dados pessoais são ou não recolhidos junto do titular, disposições concernentes ao legítimo interesse do controlador, dever de retificar dados inexatos, dentre outros. No entanto, ao destinar o Capítulo 4 às funções de controlador e operador, o regulamento dispõe separadamente quais as responsabilidades de cada um.

Conforme consta no artigo 24, tendo em vista o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas naturais, cuja probabilidade e gravidade podem ser variáveis, o controlador aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o RGPD. Tais medidas devem ser revistas e atualizadas conforme necessidade e caso sejam proporcionadas em relação às atividades de tratamento, estas incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo controlador. Ainda, pode o controlador comprovar o cumprimeneto de suas obrigações por meio do cumprimento de códigos de conduta aprovados, nos termos do artigo 40, ou de procedimentos de certificação aprovados, artigo 42.

Há, ainda, a previsão da chamada proteção dos dados *by design* e *by default*. Trata-se, em grandes linhas, do momento em que encontra a aplicação das medidas técnicas e organizativas adequadas, como a pseudonimização, para o tratamento dos dados pelo controlador, podendo ser no momento de definição (*by design*) ou durante o tratamento propriamente dito (*by default*).

O controlador pode optar por determinar os fundamentos e meios de tratamento dos dados pessoais de forma unilateral ou ainda conjuntamente com outros controladores. Quando de forma conjunta, os controladores podem acordar suas respectivas responsabilidades a fim de realizarem o tratamento dos dados nos termos do RGPD, o que não obsta o titular dos dados de exercer seu direito em face de qualquer dos controladores.

Ainda, o controlador atua com a figura do operador. Este deve apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma que o tratamento dos dados satisfaça os requisitos do RGPD e assegure a defesa dos direitos do titular dos dados. Em grandes linhas, o operador é aquele que, como pessoa física ou jurídica, age em nome e subordinação do controlador. A título de exemplo, pode-se imaginar uma academia que aciona uma gráfica local para a produção de convites para um evento a ser realizado pela academia, a qual fornece à gráfica os nomes e endereços para os convites e envelopes para que então os envie. Neste caso, a academia é a controladora dos dados pessoais processados junto aos convites, é ela quem determina os objetivos para o tratamento dos dados pessoais, qual seja enviar individualmente os convites a cada endereço, bem como determina também o meio pelo qual o tratamento ocorre, unindo os dados pessoais ao endereço detalhado de cada indivíduo membro da academia. Assim, a gráfica é a operadora tratando os dados pessoais apenas sob instrução da academia como controladora (ICO, 2020).

Pelo regulamento europeu, o operador pode, sob autorização expressa do controlador, contratar outro operador. Assim, tem-se que tanto a relação operador-operador, como a relação controlador-operador estão condicionadas à formalização contratual ou outro instrumento jurídico vinculativo e por escrito. No que se refere ao conteúdo do contrato controlador-operador, o instrumento deve prever que, a menos que seja legalmente obrigado a fazer diferente, o operador trata os dados pessoais apenas mediante instruções documentadas do controlador, incluindo no que diz respeito às transferências de dados para

países terceiros ou organizações internacionais. Deve ainda contribuir para auditorias e prestar assistência ao controlador a fim de que suas obrigações sejam cumpridas, além de apagar ou devolver-lhe todos os dados pessoais depois da finalização do serviço prestado. Por fim, com o RGPD, o ordenamento jurídico europeu reforça importância e responsabilidades do controlador e do operador, figuras fundamentais para identificação e notificação dos casos de violação de dados pessoais.

## 2.2 CONTROLADOR E OPERADOR NA LGPD

A LGPD prevê taxativamente as hipóteses de tratamento dos dados, no que tange ao controlador, destaca-se a possibilidade quando necessária para o cumprimento de sua obrigação legal ou regulatória, bem como quando necessária para atender aos seus interesses legítimos ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Assim, nenhuma dessas hipóteses, inclusive e principalmente o legítimo interesse do controlador, podem ser entendidas como uma autorização sem consequências para o tratamento dos dados. A eventual dispensa da exigência do consentimento, não desobriga os agentes de tratamento das demais obrigações legalmente previstas, especialmente da observância dos princípios gerais, como necessidade, e da garantia dos direitos do titular.

Destina-se, exclusivamente o Capítulo VI às previsões concernentes aos agentes de tratamento de dados pessoais, que, ao estilo da regulação europeia, trata-se das figuras de controlador e operador. No entanto, apesar da forte inspiração da LGDP no RGPD, pode-se dizer que aquela fora muito mais sucinta ao abordar a temática, dispondo de apenas 4 artigos excluída a seção sobre o encarregado pelo tratamento dos dados e a seção de responsabilidade e ressarcimento de danos.

Em linhas gerais, a lei dispõe que os agentes devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse, sendo de responsabilida-

de do controlador, quando determinado pela autoridade nacional, a elaboração do relatório de impacto à proteção de dados pessoais quando tratados (contendo, no mínimo a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados).

Por fim, no tocante à relação controlador-operador, a LGPD prevê a subordinação do operador ao controlador, devendo aquele realizar o tratamento segundo as instruções fornecidas por este, que verificará a observância das próprias instruções e das normas sobre a matéria. Em seguida, a legislação já versa sobre a figura do encarregado pelo tratamento de dados e sobre a responsabilidade e ressarcimento de danos, dando fim ao capítulo destinado aos agentes de tratamento de dados pessoais.

Dessa forma, a confusão apresentada no início do capítulo deste estudo pode acabar acentuada quando da realização do tratamento com base na LGPD, uma vez que, ao contrário do RGPD, o capítulo da lei destinado aos agentes de tratamento de dados pessoais não apresenta com clareza as distinções, bem como não apresenta de fato as responsabilidades de cada agente.

Aponta-se como possível solução para a falta de clareza legal concernente às atribuições e vinculação do operador ao controlador, a formalização contratual, ou outro meio jurídico, que assim determine expressa e objetivamente.

## 3 RESPONSABILIDADE CIVIL DO CONTROLADOR E OPERADOR IA NO TRATAMENTO DE DADOS

A evolução tecnológica é fruto da busca humana por meios de simplificar sua vida para que possa mudar o foco de sua atenção, sendo um dos maiores exemplos disso a autonomização dos veículos. Ao não se preocupar com a direção do veículo, o motorista pode passar ao papel de quase mero passageiro, a depender do nível de autonomização do veículo,

e pode, por exemplo, voltar sua atenção às leituras ou até mesmo dormir. Fato é que o objetivo de se desenvolver a inteligência artificial está intimamente ligado ao seu uso como ferramenta de majoração da qualidade de vida do ser humano.

Assim, o tratamento dos dados pessoais realizado sob auxílio da inteligência artificial pode desafiar a identificação do sujeito a ser responsabilizado nos casos de violação à legislação de proteção de dados pessoais.

Uma vez que não há previsão legal no ordenamento jurídico brasileiro que imputa a responsabilidade civil à inteligência artificial, o estudo comparado serve de elucidação e quiçá orientação. Quando se trata de proteção de dados pessoais, o natural é que se compare a legislação brasileira à europeia. Ocorre que, no que tange ao direito civil, a Europa não possui unificação legislativa. Dessa forma, uma vez que "a classificação dos ramos de Direito Civil é realizada com base na chamada classificação germânica" (ASCENSÃO, 2010, p. 16), ter-se-á como base comparativa o Código Civil Alemão.

## 3.1 Responsabilidade objetiva na Europa e no Brasil

Quanto à responsabilidade objetiva na Europa, Ascensão comenta que "não podemos falar em um Direito Civil Europeu e muito menos na pretensão de se criar um Código Civil europeu. A existência da União Europeia não significa que há um Direito europeu" (CJF, 2011). Por esse motivo, como enfatizado por Ascensão acima, "quem aparece como formador dos princípios do Direito europeu é o Direito Alemão" (CJF, 2011)[6].

Nessa linha, "O direito privado alemão que se tem hoje teve seus contornos mais claramente delineados a partir de 1900, quando o Códi-

[6] Com vistas a aprofundar a temática do direito alemão fazer referência ao artigo da Parte I "A nova lei de proteção de dados – uma visão crítica", de Thomas Hoeren e Stefan Pinelli, e ao artigo da Parte II, Seção III, "Direito à autodeterminação informativa e o exercício democrático: reflexões sobre as experiências alemã e brasileira", de Alice Lana e Marcelle Cortiano.

go Civil alemão (Bürgerliches Gesetzbuch - BGB) entrou em vigor" (PIRES, 2019, p. 95). Diz a autora (PIRES, 2019, p. 101) que o BGB compreenderia não uma, mas três cláusulas gerais de responsabilidade civil aquiliana. Ou seja, o tipo de responsabilidade civil objetiva decorrente da inobservância de norma jurídica, foco deste trabalho.

A primeira delas é uma cláusula acerca da violação de direitos subjetivos, cujo escopo é dado pelo § 823 I BGB que, de acordo com a tradução de Thatiane Pires (2019, p. 101) dispõe: "Aquele que, dolosamente ou por negligência, lesionar de forma antijurídica a vida, o corpo, a saúde, a liberdade, a propriedade ou um outro direito de alguém, está perante este obrigado à indenização dos danos resultantes".

A segunda cláusula geral se refere à responsabilidade pela violação de um direito objetivo, prevista no § 823 II BGB. Essa, de acordo com Pires (2019, pp. 101-102) impõe a obrigação de indenizar àquele que violar uma norma destinada à proteção de outrem. A mesma autora ainda traz a tradução do § II citado: "A mesma obrigação é imposta àquele que viola uma lei que se destina à proteção de outrem. Se, conforme o conteúdo da lei, a violação desta é possível mesmo sem culpa, então a obrigação de indenizar somente é imposta em caso de culpa".

Por fim, a terceira cláusula geral consta no § 826 BGB, a qual, de acordo com Pires (2019, p. 102) "obriga à indenização o responsável por causar dano a outrem de forma dolosa e contrária aos bons costumes". A tradução da norma jurídica, de acordo com a autora, assim dispõe: "Aquele que, de forma contrária aos bons costumes, causa dolosamente dano a outrem, é obrigado, perante este, à reparação do prejuízo".

Percebe-se, então, a previsão da responsabilidade civil nas modalidades objetiva e subjetiva no direito civil alemão. De forma semelhante acontece no Brasil, onde, nos termos do artigo 186 e 927, a obrigação de reparação se dá em decorrência do cometimento de ato ilícito, qual seja, violação e dano a outrem por ação ou omissão voluntária, negligência ou imprudência.

Assim, verifica-se a preferência do legislador brasileiro pela responsabilidade civil de forma subjetiva, requerendo a caracterização de dolo

ou culpa. Esta última pode ser na espécie de: i) imprudência- ato comissivo, onde o sujeito sem intenção de transgredir a norma, mas, por agir com inobservância do dever de cuidado, deve ser responsabilizado; ii) imperícia- similar à imprudência, mas espera-se o dever de cuidado devido à expertise do sujeito; iii) negligência- ato omissivo, em que o sujeito deixa de agir e, por consequência, causa dano à outrem.

À exceção, a responsabilidade civil objetiva é timidamente observada no Código Civil Brasileiro, embora reforçada posteriormente pelo Código de Defesa do Consumidor e tida como correção do conceito clássico e insatisfatório de culpa já superado (DA SILVA, 1974, p. 104) (FILHO, p. 159-170). Reforçando a preocupação, ainda atual, e apontando os desafios da sociedade moderna, versa Sergio Cavalieri Filho (2007, p. 16) que:

> "Por essa concepção clássica, todavia, a vítima só obterá a reparação do dano se provar a culpa do agente, o que nem sempre é possível na sociedade moderna. O desenvolvimento industrial, proporcionado pelo advento do maquinismo e outros inventos tecnológicos, bem como o crescimento populacional geraram novas situações que não podiam ser amparadas pelo conceito tradicional de culpa".

Dessa forma, a configuração da responsabilidade se dá pela soma do nexo causal ao dano, dispensando-se a comprovação de dolo ou culpa. Trata-se da opção do agente por exercer a atividade independentemente do risco, nesse sentido, Caio Mário:

> Em termos de responsabilidade civil, risco tem sentido especial, e sobre ele a doutrina civilista, desde o século passado vem-se projetando, com o objetivo de erigi-lo em fundamento de dever de reparar, com visos de exclusividade, ou com extremação da teoria própria, oposta à culpa.

Não se objetiva com este trabalho esgotar as teorias da responsabilidade civil, no entanto, defende-se que, apesar do sistema brasileiro

ser misto e abranger tanto a responsabilidade civil objetiva quanto a subjetiva, a reparação do dano não deveria depender da possibilidade de comprovação pela vítima de culpa do agente.

No que se refere à regulação da responsabilidade civil no Brasil e na Alemanha, percebe-se que ambos os sistemas normativos adotam a possibilidade subjetiva e objetiva, devendo ser analisada casuisticamente.

Assim, considerando-se a previsão do parágrafo único do art. 927 do Código Civil Brasileiro de que: "Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem" basilar a verificação de previsão legal ou situação prática que justifique a aplicação da responsabilidade civil objetiva em casos de violação de direitos no tratamento de dados pessoais.

## 3.2 A Responsabilidade Civil de acordo com a LGPD e o RGPD

Em âmbito europeu, o artigo 82, inciso 1, do RGPD deixa bem clara sua vinculação à responsabilidade civil aquiliana ao determinar que "qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indenização do responsável pelo tratamento ou do subcontratante pelos danos sofridos".

A lei continua no inciso 2 do mesmo artigo que qualquer controlador "que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento". O operador somente é responsabilizado pelos danos causados pelo tratamento caso não tenha cumprido as disposições legais relativas às obrigações específicas do operador ou caso não tenha seguido as instruções lícitas do controlador.

Por fim, a lei esclarece no inciso 3 do artigo 82 que o controlador ou o operador ficam isentos de responsabilidade caso provem que não

são de modo algum responsáveis pelo evento que deu origem aos danos. Isso significa que a lei adota uma postura mais vinculada à responsabilidade objetiva dos agentes de tratamento de dados, tal qual dispõem, especificamente os §§ I e II do artigo 823 do BGB. Porém, o RGPD abre margem para que se produza prova em contrário que possa eximir esses agentes caso ocorra algum tipo de evento danoso ao titular das informações utilizadas.

As disposições acerca da responsabilidade civil de acordo com a LGPD podem ser encontradas na sua Seção III do Capítulo IV, entre os artigos 42 e 45. Sobre o tema discorrem Mendes e Doneda (2018, p. 476):

> A consideração da responsabilidade dos agentes leva em conta, em primeiro lugar, a natureza da atividade de tratamento de dados, que a LGPD procura restringir às hipóteses com fundamento legal (art. 7º) e que não compreendam mais dados do que o estritamente necessário (princípio da finalidade, art. 6º, III) nem sejam inadequadas ou desproporcionais em relação à sua finalidade (art. 6º, II).

Nesse sentido, dispõe o artigo 42 da LGPD que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo". Nessa mesma linha, e tal qual o RGPD, a LGPD em seu artigo 42, § 1º, inciso I, prevê:

> O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Por fim, as hipóteses do artigo 43 da LGPD em que os agentes de tratamento não serão responsabilizados ocorrem quando eles provarem:

> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Em decorrência da maneira como a LGPD foi codificada, argumentam Mendes e Doneda (2018, p. 477) que isso justifica "o legislador optar por um regime de responsabilidade objetiva no art. 42, vinculando a obrigação de reparação do dano ao exercício de atividade de tratamento de dados pessoais". Tal regime de responsabilidade é o mesmo que pode ser observado no RGPD, conforme se demonstrou acima.

Nesse sentido, cabe verificar como se atribuiria a responsabilidade a um controlador ou operador que se trate de uma aplicação de Inteligência Artificial. Sendo um programa do tipo dependente do seu algoritmo, será que o modo como uma aplicação do tipo realiza tarefas de tratamento poderia ser programado na máquina? Sniesko e Melo (2020) ao tratar sobre uso legítimo trazem uma equação no que concerne ao uso legítimo:

> i) Se (Prp)Propósito > (NT)Necessidade de Tratamento + (DT)Direitos do Titular ∴ ao optar pelo legítimo interesse, há uma assunção de riscos pelo controlador
>
> ii) Se (Prp) ≤ (NT) + (DT) ∴ há uma hipótese de tratamento de dados pessoais mais confortável, valendo-se do legítimo interesse.

De acordo com os autores, isso significa que verificado "in casu, que o Propósito é maior do que a Necessidade mais os Direitos do Titular de dados (...), valer-se do legítimo interesse implicaria um cenário mais frágil ao controlador". Dessa forma, já se propõe a criação de uma série de instruções para o tratamento dos dados, ou seja, um algoritmo.

Assim, como demonstrado acima, se o operador age sem orientação do controlador, determinando se e como tratar certos dados, no que tange a esses dados específicos, o operador age e responderá como se controla-

dor fosse. Ao passo que, devido ao nível tecnológico de certas aplicações de IA, é possível que estas operem de forma não esperada, sendo o desafio jurídico encontrar correta e justamente a quem responsabilizar, verificando-se como se responsabilizaria um agente não-humano que pudesse realizar operações do tipo.

## 3.3 A Responsabilidade Civil da aplicação de IA que faça operações de tratamento de dados

Já há programas de computador que monitoram faxineiros, dizendo para eles qual quarto de hotel limpar e medindo quão rápido eles fazem isso. Do mesmo modo como já existem aplicações de IA que verificam quantos cliques no mouse ou quantas ligações um atendente de telemarketing faz por hora. Enquanto se vislumbra no horizonte a existência de caminhões automatizados, os robôs já chegaram na função de supervisores e de gerentes de empresas (DZIEZA, 2020).

Eles fazem isso através das técnicas abordadas acima: softwares programados com técnicas de *machine* ou *deep learning* que se utilizam de dados para determinar a melhor solução para determinado problema, tudo isso conforme regido em seu código. Com esses programas, coletam-se dados de clientes e funcionários e se interpretam eles com o objetivo de se otimizar a relação entre as partes.

Ainda que isso seja feito por uma aplicação de IA e que em alguns casos seja o próprio programa que determine, por exemplo, quantas entregas um trabalhador da Amazon deve fazer por hora (DZIEZA, 2020), com a edição da LGPD e do RGPD torna-se impossível de se deixar de atribuir a responsabilidade para um operador ou controlador humano. Isso porque essas aplicações dependem da interpretação de dados coletados e se esses dados forem pessoais eles serão abrangidos por ambas as leis.

Sobre o assunto, Dzieza (2020) ainda comenta:

> Poder-se-ia imaginar uma versão destes sistemas que coleta dados do local de trabalho, mas que seja anônima, agregada e apenas utiliza-

> da para melhorar os fluxos e processos de trabalho. Tal sistema teria algumas das eficiências que tornam estes sistemas atrativos, evitando ao mesmo tempo que os trabalhadores individualizados se vissem incomodados. Evidentemente, isso significaria renunciar a dados potencialmente valiosos. Exigiria o reconhecimento de que, por vezes, há valor na não coleta de dados, como meio de preservar o espaço para a autonomia humana.

Ou seja, caso não haja essa preocupação com a anonimização, aplicam-se as regras das leis de proteção de dados pessoais, pois afinal a aplicação de Inteligência Artificial é apenas uma ferramenta. A responsabilidade, no caso objetiva como se observou acima, recairá ao controlador e, subsidiariamente, ao operador dos dados. No que tange à importância que o sistema operacional pode ter para a definição do papel do agente no tratamento dos dados, logo, também sua responsabilização, já diria o ICO (2020):

> Se você estiver agindo como controlador e operador, deve assegurar-se de que seus sistemas e procedimentos distinguem entre os dados pessoais que você processa na sua qualidade de controlador e os que processa como operador em nome de outro controlador. Se alguns dos dados forem os mesmos, os seus sistemas devem ser capazes de distinguir entre estas duas capacidades, e permitir-lhe aplicar processos e medidas diferentes a cada um deles. Se não o puder fazer, é provável que seja considerado um controlador conjunto em vez de um operador para os dados que processa em nome do seu cliente.

A fim de harmonizar o uso da IA com o tratamento de dados pessoais de forma segura, pode-se valer do ensinamento de Teffé e Medon (2019, p. 304):

> "princípios éticos, padrões técnicos e normas de estrutura menos fechada ajudarão a garantir que o desenho e o desenvolvimento de tais tecnologias sejam orientados pela preocupação com a pessoa humana e busquem promover uma IA segura, justa e inclusiva.

Em suma, ainda que se faça uso de aplicações de inteligência artificial, os danos decorrentes de violações de direitos no tratamento de dados pessoais, assim como todos os outros danos, devem ser reparados. Nesse sentido, (FACCHINI NETO, 2003, p. 160-161):

> "O fato é que a teoria da responsabilidade civil comporta tanto a culpa como o risco. Um como o outro devem ser encarados não propriamente como fundamentos da responsabilidade civil, mas sim com meros processos técnicos de que se pode lançar mão para assegurar às vítimas o direito à reparação dos danos injustamente sofridos. Onde a teoria subjetiva não puder explicar e basear o direito à indenização, deve-se socorrer da teoria objetiva. Isto porque, numa sociedade realmente justa, todo dano deve ser reparado."

No que tange à responsabilidade civil sob aplicação de IA enquanto controlador ou operador conclui-se que a IA deve ser entendida como mera ferramenta a fim de auxiliar os agentes de tratamento de dados. Dessa forma, valendo-se da teoria objetiva da responsabilidade civil, ainda que carecendo de culpa, trata-se de atividade em que tanto controlador como operador assumem os riscos de seus atos e da execução das ferramentas que optam por utilizar. Portanto, no que diz respeito à responsabilidade civil, devem os agentes observar o efetivo cumprimento dos princípios legalmente previstos. Isso deve se dar tanto *a priori*, em atendimento ao princípio da prevenção, quanto *a posteriori*, à luz da responsabilização e prestação de contas, a fim de demonstrar a adoção de medidas eficazes, além da observância e o cumprimento das normas de proteção de dados pessoais.

## CONSIDERAÇÕES FINAIS

As aplicações de Inteligência Artificial são verdadeiras maravilhas tecnológicas que revolucionam o modo como a civilização executa todo tipo de atividade, da autonomização dos veículos às tarefas de gerência de empresas. Dito isso, elas não deixam de ser ferramentas, as quais são colocadas em atividade sob ordens de um controlador humano.

Nesse sentido, o item 1 deste trabalho abordou o funcionamento de uma aplicação do tipo. Definiu-se a IA como sendo a área de estudo focada em desenvolver máquinas capazes de emular o raciocínio humano e se abordou os três elementos que seriam necessários para seu bom funcionamento. O primeiro deles seria o *software*, sua programação, o que determina o que a aplicação irá realizar e que pode ser realizado por meio de técnicas como machine learning ou deep learning. O segundo elemento se trata do *hardware*, que é onde o programa de computador é executado. Por fim, o último elemento se trata dos dados, que funciona como o *input* necessário para que a aplicação de IA produza certo *output*.

Tratando-se de dados, sendo pessoais, eles caem sob a regência da LGPD e do RGPD, as mais recentes leis abordando as operações de tratamento de dados e tópico do item 2 do trabalho. Essas atribuem responsabilidade àqueles que realizem operações de tratamento de dados e atribuem em especial duas funções, a de controlador e a de operador. Controlador seria a pessoa física ou jurídica que determina as finalidades e os meios de tratamento de dados pessoais, enquanto que o operador seria a pessoa que trate os dados pessoais por conta do responsável pelo tratamento destes.

Sendo controlador e operador ambos pessoas físicas ou jurídicas, a lei também atribui a eles um regime de responsabilidade civil, conforme visto no item 3. Em análise à legislação brasileira e à europeia percebeu-se que o aplicável a esses agentes seria a responsabilidade objetiva. Ou seja, bastaria que o titular dos dados comprovasse ato danoso para poder pugnar por ressarcimento. Neste item, viu-se ainda que os atos praticados por uma aplicação de IA que atue como operador ou controlador de dados ainda teriam de ter sua responsabilidade atribuída a uma pessoa física ou jurídica.

Ainda que ferramentas revolucionárias, aplicações de IA continuam a ser instrumentos dos agentes de tratamento de dados. Elas já têm uma capacidade muito grande de gerir, classificar e alterar os dados que recebem, mas a legislação atual não abre para outro tipo de responsabilização civil que não a de agentes e operadores que sejam pessoas físicas ou jurídicas.

O próprio fato de a responsabilização ser objetiva já indica que é uma companhia ou órgão ou um membro destes que irá sofrer as consequências pelo mau uso da ferramenta. Só se vislumbraria a possibilidade dessas aplicações de IA terem algum tipo de responsabilização caso elas efetivamente atingissem a singularidade e pugnassem pelos seus direitos.

Essa foi a conclusão chegada nesse artigo, porém se reconhece que esse é um tema muito recente e, especialmente com as novas tecnologias, é inviável de se limitar a visão a apenas um tipo de tutela. Esperou-se com esse artigo trazer uma contribuição relevante para um tema que ainda exigirá muitas reflexões.

## REFERÊNCIAS

ALEMANHA. **Bürgerliches Gesetzbuch (BGB)**. Disponível em: https://www.gesetze-im-internet.de/bgb/. Acesso em: 20 set. 2020.

ASCENSÃO, José de Oliveira. **Direito Civil: Teoria Geral, vol. 1: Introdução. As Pessoas. Os Bens**. 3ª ed., São Paulo: Saraiva, 2010.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

_____. Lei n. 10.406, de 10 de janeiro de 2002. **Código Civil**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm.

BODIN DE MORAES, Maria Celina. **LGPD:** um novo regime de responsabilização civil dito "proativo". Editorial à Civilistica.com. Rio de Janeiro: a. 8, n.3, 2019. Disponível em: http://civilistica.com/lgpd-um-novo-regime/. Acesso em: 20 set. 2020.

CORMEN, Thomas H., LEISERSON, Charles E., RIVEST, Ronald L., STEIN, Clifford. **Algoritmos Teoria e Prática**. 2. Ed. Rio de Janeiro: Editora Campus, 2002.

CJF, Conselho da Justiça Federal. **Oliveira Ascensão traça um Panorama do Direito Civil Europeu**. 2011. Disponível em: https://www.cjf.jus.br/cjf/noticias/2011/novembro/oliveira-ascensao-traca-um-panorama-do-direito-civil-europeu. Acesso em: 20 set. 2020.

DZIEZA, Josh. **How Hard will the Robots Make Us Work?** 2020. Disponível em: https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon. Acesso em: 22 set. 2020.

ECONOMIST, The. **How Machine Learning Works**. 2015. Disponível em https://www.economist.com/the-economist-explains/2015/05/13/how-machine-learning-works?fsrc=scn/fb/te/bl/ed/. Acesso em: 28 ago. 2018.

FACCHINI NETO, Eugênio. **"Da responsabilidade civil no novo Código"**, in: SARLET, Ingo Wolfgang (org). O novo Código Civil e a Constituição. Porto Alegre: Liv. do Advogado, 2003.

FILHO, Sergio Cavalieri. **Programa de responsabilidade civil.** 3 ed. São Paulo: Malheiros, 2002.

GANDZ, Solomon. **The Origin of the Term "Algebra"**. The American Mathematical Monthly. 33 (9): 437–440. doi:10.2307/2299605. ISSN 0002–9890, 1926.

GARRETT, Filipe. **Computador e processador quântico:** sete coisas que você precisa saber. 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/03/computador-e-processador-quantico-sete-coisas-que-voce-precisa-saber.ghtml. Acesso em: 15 out. 2018.

GONÇALVES, Lukas Ruthes. **A Tutela Jurídica de Trabalhos Criativos feitos por Aplicações de Inteligência Artificial no Brasil**. Universidade Federal do Paraná, 2019.

ICO, Information Commissioner's Office. **How do you determine whether you are a controller or processor?** 2020. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/how-do-you-determine-whether-you-are-a-controller-or-processor/. Acesso em: 22 set. 2020.

KAUFMAN, Dora. **Os Meandros da Inteligência Artificial: Conceitos-chave para Leigos**. 2018. Disponível em: https://www.ab2l.org.br/os-meandros-da-inteligencia-artificial-conceitos-chave-para-leigos/. Acesso em: 28 ago. 2018.

KURZWEIL, Ray. **The Age of Intelligent Machines**. MIT Press, 1990.

MARR, Bernard. **Artificial Intelligence in the Workplace: How AI is Transforming your Employee Experience**. 2019. Disponível em: https://www.forbes.com/sites/bernardmarr/2019/05/29/artificial-intelligence-in-the-workplace-how-ai-is-transforming-your-employee-experience/#6f75fcb153ce. Acesso em: 20 set. 2020

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. Revista de Direito do Consumidor. vol. 120. ano 27. p. 469-483. São Paulo: Ed. RT, nov.-dez. 2018.

MCCARTHY, John; MINSKY, Marvin; ROCHESTER, Nathan; SHANNON, Claude (1955). **A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence**. Arquivado do original em 26 de agosto de 2007. Recuperado em 30 agosto de 2007.

MCCORDUCK, Pamela. **Machines Who Think.** (2nd ed.), Natick, MA: A. K. Peters, Ltd., ISBN 1-56881-205-1, 2004.

MICROSOFT. **The Microsoft approach to quantum computing**. 2018. Disponível em: https://cloudblogs.microsoft.com/quantum/2018/06/06/the-microsoft-approach-to-quantum-computing/. Acesso em: 15 out. 2018.

MORAVEC, Hans. **The Role of Raw Power in Intelligence**, 1976, retrieved 16 October 2008.

PEREIRA, Caio Mário da Silva. **Responsabilidade Civil**. Rio de Janeiro: Forense, 2001.

PIRES, Thatiane Cristina Fontão. **Desenvolvimento E Aplicação Da Compensatio Lucri Cum Damno No Direito Alemão:** O Problema Da Cumulação Da Indenização Com Vantagens Advindas Do Evento Danoso. Universidade Federal de Santa Catarina, 2019.

OSTP. **Preparing for the Future of Artificial Intelligence**. 2016. Executive office of the president. National Science and Technology Council. Washington, D.C. 20502.

ROOS, Teemu. **Elements of AI.** 2018. Disponível em: https://www.elementsofai.com/. Acesso em: 28/08/2018.

RUSSELL, Stuart; NORVING, Peter. **Artificial Intelligence:** A Modern Approach. 3. Ed. Harlow (UK): Pearson Education Limited, 2016.

SILVA, Wilson Melo da. **Responsabilidade sem culpa.** São Paulo: Saraiva, 1974.

SINDWANI, Prerna. **The Boss Machine is Here - AI is set to Eliminate Middle Management in 8 Years**. 2020. Disponível em: https://www.businessinsider.in/careers/news/the-boss-machine-is-here-ai-is-all-set-to-eliminate-middle-managers-in-8-years/articleshow/73474729.cms. Acesso em: 20 set. 2020.

SNIESKO, Thiago Reyes; MELO, Leonardo Albuquerque. **Equacionando o Legítimo Interesse na LGPD**. 2020. Disponível em: https://lbca.com.br/equacionando-o-legitimo-interesse-na-lgpd/#:~:text=S%C3%A3o%20alguns%20exemplos%20de%20aplica%C3%A7%C3%A3o. Acesso em: 20 set. 020.

TURING, Alan. **Computing Machinery and Intelligence.** Mind, LIX (236): 433–460, doi:10.1093/mind/LIX.236.433, 1950.

UNIÃO EUROPEIA. Regulation (EU) 2016/679. **General Data Protection Regulation (GDPR)**. Disponível em: https://gdpr-info.eu/. Acesso em: 20 set. 2020.

# Capítulo V

# PERFIL ALGORÍTIMICO E DISCRIMINAÇÃO DIGITAL: uma leitura a partir das normas europeias e brasileiras

*Ana Cristina Aguilar Viana*[1]

*Carolina Ferreira de Miranda*[2]



**RESUMO**

As novas tecnologias passam a ideia de serem neutras, mas são parciais e reproduzem no universo online em grande escala as discriminações do mundo offline. Diante disso, o presente trabalho tem como propósito examinar de que modo a legislação europeia e brasileira lidam com a questão da discriminação digital algorítmica. O trabalho é descritivo e comparativo. Parte-se de uma perspectiva metodológica de apreciação da leitura comparada entre as normas sobre o caso específico segundo um método que examina fatores que levam a criação e aplicação de uma norma. O artigo faz uma contextualização inicial, com descrições do perfil algoritmo (profiling) e tipos de discriminações, seguindo para exposição da normativa que trata sobre o objeto da pesquisa no RGPD (Regulamento geral de proteção de dados) e, posteriormente, na LGPD (Lei geral de proteção de dados). Ao fim, são traçadas noções comparativas, bem como disposições sobre serem ou não suficientes as normas elencadas ora analisadas.

**Palavras-chave:** Discriminação digital; decisões automatizadas; profiling – perfil algoritmo; LGPD; RGPD.

[1] Doutoranda em Direito na Universidade Federal do Paraná e na Paris 1 Panthéon-Sorbonne. Advogada e Professora. E-mail: anacristina_av@hotmail.com

[2] Bacharel em Direito na Universidade Dom Bosco/UniDom. Profissional com 17 anos de experiência no setor privado financeiro. Especialista em *Compliance*, Segurança da Informação e Fraudes Financeiras Digitais. Conhecimento em ferramenta de sistema neural, análise e investigação de fraudes. E-mail: kroldir@hotmail.com

## 1 INTRODUÇÃO

Conhecida como a "Poetisa do Código", Joy Buolamwini (2016) inicia o vídeo da sua palestra no site Ted.com com um exemplo prático: coloca-se de frente a um computador, que faz sua leitura facial, mas não a reconhece. Joy precisa então colocar uma máscara branca, em seguida a máquina a identifica. No vídeo, fica claro que isso ocorreu por conta da sua cor. "E por que isso acontece"? Indaga ela. Porque algoritmos criam vieses do mesmo modo daqueles criados por humanos. Usam, em regra, o mesmo tipo de reconhecimento genérico, o qual produz discriminações. A distinção entre o mundo real e o offline, pontua a Poetisa, "reside no fato que as máquinas podem disseminar obliquidades de modo massivo, o que pode ensejar em práticas discriminatórias de larga escala", exatamente o caso de Joy.

Esse exemplo coloca em causa um problema recorrente e preocupante das novas tecnologias. A discriminação digital algorítmica. Embora se vendam as tecnologias como neutras, elas não o são. Diante desse contexto, o presente trabalho tem como propósito examinar de que modo as normas europeia e brasileira, lidam com a questão da discriminação algorítmica. O trabalho é descritivo e crítico. Parte-se de uma perspectiva metodológica de apreciação da leitura comparada entre as normas sobre o caso específico segundo um método comparativo que examina os diversos fatores que levam a criação e aplicação de uma norma. No que se refere ao Direito comparado, deve-se partir de uma metodologia própria para análise, a fim de não incorrer em anacronismos, isto é, a pesquisa não pode estar limitada a uma comparação fria das normas. É preciso compreender o percurso histórico, contexto da norma.

Pierre Legrand (2018, p. 64) fala em "impossibilidade de transplantes legais", é dizer, de não se poder transplantar o direito de um país e colar em outro, sem atenção a outros critérios essenciais. O autor compreende que a interpretação da norma é um ato subjetivo o qual é carregado de elementos culturais. A interpretação, segundo ele, resulta de uma dada compreensão de uma regra que tem como condicionante uma série de

fatores, sendo que fatores distintos poderiam ensejar a outra interpretação. A regra, para ele, é necessariamente uma forma cultural constitutiva. Daí porque a impossibilidade de um simples "transplante" de uma norma (LEGRAND, 2018, p.115).

O artigo busca examinar as normativas europeias, especificamente o Regulamento Geral de Proteção de Dados (RGPD), bem como a Lei Geral de Proteção de Dados Brasileira (LGPD), tendo como pressupostos as disposições sobre método de comparação de Pierre Legrand. Antes, o trabalho faz uma contextualização inicial, com descrições do perfil algorítmico (*profiling*) e discriminações, seguindo para descrição da normativa que trata sobre o objeto da pesquisa no RGPD e, posteriormente, na LGPD. Ao fim, são traçadas noções comparativas, bem como disposições sobre serem suficientes as normas elencadas nas normas ora analisadas.

## 2 CONTEXTUALIZAÇÃO INICIAL: PERFIL ALGORITMO E DISCRIMINAÇÕES

A velocidade, profundidade, amplitude e variedade são características das novas tecnologias que provocam o universo jurídico. O advento das novas tecnologias digitais traz diversos desafios. Com a internet das coisas (IoT), inteligência artificial (IA) e *big data,* espera-se modificações substanciais.[3]

Gonçalves (2019, p. 33) fala que a IA se trata de uma área de estudo focada em resolver problemas (ou criar máquinas que desempe-

[3] A Internet das Coisas (IoT) é definida como uma rede onde objetos digitais e físicos são instrumentalizados com sensores o que permite acúmulo e troca de informação entre si, programado pela lógica de algoritmos. Segundo estimativas o impacto da IoT será de até US$ 11 trilhões até 2025 (LEMOS; ARAÚJO, 2018, p. 1-19). A inteligência artificial (IA) pode ser conceituada como campo de estudos, de conjunto, de técnicas e algoritmos computacionais e de métodos de reprodução da capacidade cognitiva humana. É esperado que os supercomputadores ultrapassem as capacitações em quase todas as áreas entre 2020 e 2060. Já a *Big data* é a locução que designa volume de dados estruturados ou não, que são armazenados em rede (HILLARD, 2012). Trata-se de termo que se refere não apenas à coleta de dados, mas também a própria análise destes (RGPD, 2018).

nhem essa função) que anteriormente somente a mente humana saberia responder. Desse modo, não se pode falar que exista "uma" ou "a" Inteligência Artificial. O que há são uma série de diferentes aplicações que se utilizam de tecnologia avançada com o fim de suprir a capacidade de raciocínio humano em um uso ou outro.

Essas tecnologias agem de modo conjunto e utilizam como matéria prima os dados. Atualmente, tudo pode ser fonte de dados. As curtidas, as pesquisas, as buscas realizadas nas redes, por satélites, fotos, vídeos, câmeras, GPS. Muitos são pessoais, como nome, endereço, conta bancária, e outros não. Essas tecnologias podem combinar qualquer tipo de informação e as recombinar, desde transações financeiras à tratamento médico e de seguros, etc. Pelo smartphone as pessoas preenchem diariamente dados para uso, resgate e criação de perfil. Tudo personalizado. Dados são obtidos, processados, analisados, vendidos e vendidos novamente (ZUBOFF, 2015).

Essa sistemática é realizada com amparo no chamado *profiling,* o perfil algoritmo. Ele pode ser definido como um modelo de análise inferencial que identifica correlações ou padrões no âmbito de um conjunto de dados extraídos. O perfil criado de uma pessoa é realizado por meio de decisões automatizadas realizadas em conformidade com padrões pré-estabelecidos e pré-determinados. O profiling pode ser utilizado para classificar uma pessoa enquanto componente de um determinado grupo. E se dá em diversas situações como emprego, marketing, policiamento, entre outros (MANN, 2019).

Como a *big data* abrange também o processamento, a análise, o exame, e a antecipação, os dados coletados - pessoais ou não - podem ser utilizados para finalidades distintas daquelas da pretensão original, como para prestação de serviços mais personalizados, no caso da publicidade, por exemplo (RGPD, 2018). A criação de um perfil de publicidade direcionada se faz mediante identificação de padrões que refletem o tipo da personalidade de uma pessoa. O produto "talvez você goste" é desenvolvido de acordo com informações coletadas de produtos que foram anteriormente selecionados.

A publicidade direcionada, no entanto, é apenas a ponta do iceberg. A técnica OCEAN de psicografia moderna, que traça cinco tipos de características para montar uma personalidade, é usada como exemplo pelo Conselho Europeu de modulação de comportamento. Trata-se de técnica por meio de dimensões da personalidade que vão desde a abertura da pessoa, sua extroversão e consciência, para delimitação do perfil onde se consegue traçar de que maneira uma pessoa pode se comportar. No caso das novas tecnologias, essas informações são colhidas e tratadas de acordo com o perfil obtido da extração de dados.

Esses perfis são então utilizados e comparados aos padrões da técnica OCEAN para interpretar as pessoas. Segundo o Manual Prático do RGPD, elaborado pela Agência dos Direitos Fundamentais da União Europeia e pelo Conselho da Europa, trata-se de uma técnica invertida, uma vez que as informações colhidas sobre o comportamento das pessoas são usadas para descrever a personalidade de alguém (RGPD, 2018). A criação da publicidade é realizada, portanto, de acordo com a personalidade e humor da pessoa, por meio de um processamento em tempo real. O Spotify (2015), por exemplo, ao inserir no cardápio de músicas a serem ouvidas uma playlist de acordo com o humor, repassa de modo automático tais informações para empresas que a utilizam para vendas de acordo com o temperamento da pessoa no momento.

Mas os dados são utilizados não apenas para publicidade direcionada, como igualmente para fazer previsões e direcionamento de decisões (ANDREJEVIC, 2014, p. 1673-1689). Trata-se da "hiper-relevância", método conhecido por acoplar uma vigilância onipresente e design de escolha algorítmica, com a autonomia e liberdade de escolha, por outro. Visto como oximoros, constrói-se um mundo perfeito de consumos personalizados (DARMODY; ZWICK, 2020). Segundo Soshanna Zuboff (2015), a problemática desse sistema de antecipação reside no fato que se trata de algo que visa produzir receitas e controle mercadológico.

Modelos mais recentes não apenas categorizam personalidades, mas analisam o comportamento por meio de padrões de voz e a intensidade com que as mensagens são digitadas ou ainda mesmo a tempe-

ratura corporal. A tomada de decisão de predição por essas tecnologias exige grande quantidade de dados e de seu processamento. Quanto mais se alimenta, mais se personaliza. A situação fica delicada quando se percebe que o uso desses mecanismos prejudica grupos específicos, criando, portanto, discriminações (LINDOSO, 2019, p. 45-46).

Oscar Gandy (2009) aponta a discriminação como o resultado de um processo tecnologicamente aperfeiçoado que começa com a identificação, procede através da classificação, e ganha impulso no ponto de avaliação. Ou seja, a discriminação se dá em diversas etapas do processo algoritmo. A discriminação ocorre inicialmente em decorrência dos dados reproduzirem o desenho arquitetado pelo operador, o qual é carregado de uma própria subjetividade decorrente de um sistema de ser designado socialmente. Preconceitos culturais do operador são inscritos no algoritmo, que por sua vez, trata-se de uma receita, a ser replicada pela inteligência artificial. Daí porque as tecnologias implicam na repetição das desigualdades já existentes.

Assim, as tecnologias não cooperam para a resolução de problemas sociais: aprofunda-os, reforçando desigualdades e preconceitos estruturais, perpetuando desigualdades de gênero, ameaçando empregos e introduzindo outros riscos atualmente desconhecidos e consequências não intencionais. Segundo Cathy O'Donnell (2018, p. 23), trata-se de "armas de destruição matemática".

Com efeito, as desigualdades que surgem das tecnologias são diversas e existem desde o início do uso massificado da internet. Por exemplo, embora tenha trazido a ideia de que o acesso a informação estava disponível para todas as pessoas ao redor do mundo, o seu alcance foi limitado a uma determinada parcela da população, considerando, ainda, que parcela significativa da população sequer tem acesso às comodidades da segunda revolução industrial, como energia elétrica (LERMAN, 2013, vol.66).

Além disso, a discriminação pode ser de modo direto ou indireto. A primeira se aplica nas situações em que uma pessoa foi tratada de modo

injusto com base em fundamentos protegidos, enquanto a discriminação indireta se trata de práticas que discriminam de modo indireto. Esta é difícil de detectar, ao ponto de que em muitos casos as pessoas não saberão que foram discriminadas. No âmbito do perfil algorítmico, sobretudo onde o *machine learning* é usado para criar novas histórias inferenciais, este problema excede até mesmo a questão da discriminação indireta. Ou seja, o perfil algorítmico dificulta a identificação de um resultado (MANN; MATZNER, 2019).

Por sua vez, a *behavioural discrimination* - discriminação comportamental, refere-se à prática adotada por empresas para personalizar e discriminar consumidores. Quanto mais vendedores personalizam preços e ofertas de produtos, mais difícil para os consumidores descobrir um preço geral de mercado e avaliar suas opções externas. Já a discriminação por associação se dá quando uma pessoa é tratada pior do que outras, o que pode acontecer com a não exibição de um anúncio, por exemplo, ou ainda mesmo, com base em seu relacionamento ou associação, como gênero, afinidade a um determinado grupo.

Cathy O'Donnell (2018, p. 23) exemplifica a questão da promoção e mérito que ocorre em buscas de emprego. Ao examinar o currículo de uma pessoa e conceder ao algoritmo que calcule com base no número de promoções e antiguidades, o que em tese, levaria de acordo com o mérito, isso estaria equivocado e não representaria chances equivalentes das pessoas. Isso porque o histórico cultural e social é patriarcal e etnográfico. Isto é, a maioria das pessoas que possuem uma qualificação elevada se encontram dentro de uma tipologia específica. Ou seja, será reproduzido, portanto, uma mesma lógica que se tomará como válida apenas para as pessoas que se enquadrem nesse critério, que já é limitado.

O algoritmo, portanto, vai além de repetir, reforçar as desigualdades, que já existem no mundo físico de questões culturais já existentes. Com efeito, as formas interseccionais de discriminação são relevantes para observação desses tipos de discriminação que ocorre com base em grupos e margens.

Há também dados colhidos que repetem preconceitos pré-existentes. Como, por exemplo, a porcentagem de pessoas negras que são presas por tráfico e por fumar maconha, que é mais elevada que a taxa de brancos. Essas porcentagens não são tidas como relevantes e se está automatizando inclusive tais decisões (O'DONELL, 2018, p. 23). Logo as novas tecnologias, além dos benefícios, também trazem perigos.

Os riscos para proteção de dados e privacidade foram destacados no Grupo de Trabalho do Artigo 29, nas resoluções do Parlamento Europeu e nos documentos de política do Conselho da Europa. Segundo eles, os riscos incluem o manuseio incorreto por pessoas e a manipulação, discriminação ou até mesmo opressão de indivíduos ou grupos específicos da sociedade. No Manual da legislação europeia, diz-se que o uso de dados pode levar a significativas violações de direitos e liberdades fundamentais que vão além do direito à privacidade, como no caso das discriminações, que se passa a examinar.

## 3 O TRATAMENTO AUTOMATIZADO E DISCRIMINAÇÕES NO RGPD E LGPD, TRAÇOS COMPARATIVOS

O percurso histórico das normas da União Europeia revela que a atenção à preocupação com a privacidade de proteção de dados não é recente, mas decorre de uma progressiva construção doutrinária e normativa sobre o tema. A questão relativa à proteção de dados marca presença normativa desde a década de 70, ao passo que no Brasil apenas na década de 90, de maneira esparsa. A preocupação com dados é mais recente, o que revela a diferença temporal no tratamento do tema, fator relevante para análise.

Nesse aspecto, essencial reconhecer o salto qualitativo que as normas europeias se encontram, pois estão mais amadurecidas, ao contrário do tratamento mais recente dado pelo Brasil. São questões que merecem participar do cotejo entre as normas. A partir daí, pode-se examinar de que modo o tratamento automatizado e as discriminações são tratadas nas normas, e, posteriormente suas lacunas.

## 3.1 Comparativo histórico e cultural: situando a realidade das normas examinadas

Na parte introdutiva do trabalho, indicou-se que o método comparativo escolhido seria o indicado por Pierre Legrand que pondera a necessidade de se observar o sistema no qual determinada norma foi enunciada, não sendo possível um simples transplante legal de um dispositivo para outro. Por isso, entende-se que inicialmente faz-se necessário um cotejo do histórico das legislações.

As primeiras leis relativas à proteção de dados pessoais datam da década de 1970 e são conhecidas como de primeira geração, incluindo-se aí a lei alemã (1970), a sueca (1973) o *Privacy Act* dos Estados Unidos (1974) e a lei francesa de liberdade de 1978. Além disso, a Diretiva 95/46/CE (1995) também era relativa ao tema. Na década de 80 foi adotada pela União Europeia a Convenção 108 que prevê de maneira específica a proibição do tratamento de dados sensíveis tais como dados sobre a raça, a opinião política, a saúde, as convicções religiosas, a vida sexual ou o registo criminal de uma pessoa".

A Convenção 108 foi uma das primeiras normas a tratar da proteção das pessoas e se refere ao tratamento automatizado de dados de carácter pessoal. A proposta é das partes adotarem medidas necessárias no direito interno com o fim de aplicar seus princípios, de modo a assegurar o respeito pelos direitos humanos fundamentais do indivíduo no que tange a proteção de dados.

Modernizada em 2018, a Convenção 108 trata especificamente das novas tecnologias e busca trazer proteção aos dados dos titulares no mundo digitalizado. Dois são os objetivos essenciais, isto é, responder aos desafios resultantes do uso das novas tecnologias e também reforçar a aplicação efetiva da Convenção. No artigo nono vem disposto, no que tange aos direitos das pessoas, que todos têm direito a "não estar sujeito a uma decisão que o afete significativamente, tomada unicamente com base no tratamento automatizado de dados, sem que o seu ponto de vista seja tido em conta".

Portanto, vê-se que na União Europeia as normas sobre proteção de privacidade e dados decorrem da década de 70, sendo uma preocupação dos países membros. No Brasil, o direito à privacidade é consolidado como um direito fundamental, ao estar inscrito na Constituição, no art. 5o, incisos X e XII, voltados à proteção da intimidade, da vida privada, da honra e da imagem das pessoas. Além disso, na Constituição também são estabelecidos o sigilo da correspondência e das comunicações telegráficas e telefônicas e de dados, assim como as previsões de habeas data no mesmo artigo, nos incisos LXIX, LXXII e LXXVII.

Lei que trata da questão de dados no Brasil é o Código de Defesa do Consumidor, a n.˚ 8.078 de 1990, a qual dispõe no art. 43 o direito ao consumidor de acesso às informações arquivadas sobre sua pessoa em bancos de dados e cadastros. Por sua vez, o art. 21 do Código Civil de 2002 insere a inviolabilidade da vida privada dentre os direitos de personalidade. A Lei de Acesso à Informação, Lei n˚ 12.527/2011 dispõe sobre o direito das pessoas em obterem informações como modo de garantir, ainda, transparência. Ainda, a Lei do Cadastro Positivo, Lei n˚ 12.414/2011 trata de informações em bancos de dados e prevê proteções a dados sensíveis de consumidores, como relativas à orientação sexual, gênero, entre outros.

A questão sobre o uso de dados teve sua regulação cotidiana, portanto, regulada pelo Código de Defesa do Consumidor (CDC), no artigo 6º, III, pela Lei do Cadastro Positivo, no seu art. 5º, VI, e finalmente, pela Súmula STJ nº 550 (2015).

Em 2014 foi publicado o Marco Civil da Internet – Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, assim como a versão europeia (RGPD Regulamento Geral de Proteção de Dados) de 2016. Finalmente, seguindo a tendência europeia, o Brasil publicou a Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018. A LGPD unifica e traz uma organização formal de um sistema de proteção. A tutela da privacidade e dados pessoais, portanto, existe no Brasil há algumas décadas, mas de modo esparso.

## 3.2 RGPD e LGPD: os dispositivos que tratam do tema das decisões automatizadas e discriminações e exame comparativo das normas

O RGPD traz artigos específicos acerca de decisões automatizadas, incluindo questões sobre *profiling*. A proteção contra decisões automatizadas está normatizada na legislação europeia no artigo 22:

> Art 22. 1. O titular dos dados tem o direito de não ser sujeito a uma decisão baseada apenas em processamento automatizado, incluindo criação de perfil, que produza efeitos jurídicos a seu respeito ou que o afete de forma semelhante.
>
> 2. O no 1 não se aplica se a decisão:
>
> 1. É necessário para celebrar ou executar um contrato entre o titular dos dados e o responsável pelo tratamento;
>
> 2. está autorizado pela legislação da União ou do Estado-Membro a que o responsável pelo tratamento está sujeito e que também estabelece medidas adequadas para salvaguardar os direitos e liberdades e interesses legítimos do titular dos dados; ou
>
> 3. é baseado no consentimento explícito do titular dos dados.

A normativa estabelece que o titular dos dados tem o direito de não se sujeitar a uma decisão automatizada, aí se incluindo a criação de perfil. Condiciona tal direito à decisão que produza efeitos jurídicos a seu respeito e o afete. Estatui também que os dados a serem protegidos são aqueles em que ele "é titular". No artigo XX, a norma confere proteção de dados ao titular de seus dados pessoais e pseudonimizados. O art. 4 define dados pessoais como qualquer informação relacionada a uma dada pessoa que seja identificada ou identificável, sendo a pessoa identificável, aquela que pode ser direta ou indiretamente identificada. Já a pseudonimização se trata de tratamento de dados pessoais ao ponto que deixam de ser considerados a uma pessoa específica, e não sejam a uma pessoa identificada ou identificável.

O regulamento ainda estabelece os casos nos quais a norma não se aplica, isto é, no caso de ser necessária a decisão para celebração ou execução de um contrato entre o titular de dados e o responsável pelo tratamento, quando há uma autorização legal ou quando se baseia no conseguimento explícito do titular.

Além do RGPD, a Convenção 108 Modernizada trata da proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal e especificamente das novas tecnologias. No artigo segundo, "c", vem definido o que são dados automatizados, que correspondem operações, efetuadas com a ajuda de processos automatizados, tais como registo de dados, sua aplicação a operações lógicas e ou aritméticas, além da modificação e extração.

Na norma ainda se discorre sobre novos direitos ao titular dos dados para permitir um controle mais efetivo dos seus dados pessoais na era dos dados. É o caso, por exemplo, das alíneas a), c) e. d) do artigo 1.o da Convenção que tratam do direito de não estar sujeito a uma decisão que o afete significativamente, com base unicamente no processamento automatizado de dados sem ter suas opiniões levadas em consideração, o direito de obter, mediante solicitação, conhecimento do raciocínio subjacente ao processamento de dados onde os resultados desse processamento lhe são aplicados, bem como o direito de objetar.

Além disso, dispõe-se questões específicas a dados sensíveis, isto é, que os dados caráter pessoal relativos à gênero, etnia, opinião política, convicção religiosa, entre outros, só serão tema de tratamento automatizado no caso de serem previstas garantias adequadas.

No caso do Brasil, a normativa que estabelece previsões específicas sobre proteção de dados é a Lei Geral de Proteção de Dados, a Lei 13.709/2018. O artigo que trata das questões automatizadas é o 20 e está disposto da seguinte maneira:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destina-

> das a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
>
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
>
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Seguindo a tendência do RGPD, a LGPD trata do direito daquele que for titular de dados de solicitar a revisão de decisões que forem realizadas de maneira isolada por meio de tratamento de dados e que afetem o seu interesse. Inclui-se nesse pedido de revisão as decisões que tratam de definição de perfil algorítmico.

Enquanto a normativa europeia estabelece que o titular de dados tem direito a não se sujeitar a uma decisão automatizada, incluindo aí a montagem de perfil, no caso brasileiro, a LGPD estabelece a possibilidade de revisão de uma decisão automatizada no caso de afetar seus interesses. Isto é, a proteção do RGPD é *ex ante,* ao passo que a norma brasileira trata de um momento posterior, relativa à possibilidade de revisão.

Ademais, no caso do RGPD as Diretrizes do Grupo de Trabalho (GT) do Artigo 29 sobre a tomada de decisão individual automatizada e criação de perfil para os fins do Regulamento 2016/679, conferem orientações acerca do dispositivo em questão do RGPD. Segundo o GT, o artigo 22 deve ser interpretado como uma proibição e não como um direito. Isto é, as pessoas estariam de modo automático protegidas dos efeitos potenciais que esse tipo de processamento pode ter. Denota-se, portanto, uma busca de proteção mais efetiva na norma europeia.

Ainda, o RGPD dispõe quais são os casos em que se está autorizado o uso automatizado, isto é, quando é necessário para celebração de

um contrato, quando é baseado no consentimento ou ainda quando tem sua autorização pela União ou um Estado-Membro da União Europeia. O RGPD esclarece (apenas nos casos em que dados pessoais não foram obtidos do titular dos dados), que o responsável pelo tratamento não é obrigado a fornecer essas informações ao titular dos dados quando "o fornecimento dessas informações se provar impossível ou não for possível". Tais ressalvas não estão dispostas na LGPD.

Sobre o tema, o Grupo de Trabalho do Artigo 29 em suas Diretrizes sobre tomada de decisões e perfil individuais automatizadas para os fins do Regulamento 2016/679, dispõe que a complexidade do processamento não deve, por si só, impedir o controlador de dados de apresentar esclarecimentos. O exercício do direito de objetar exige intervenção humana, permitindo os titulares dos dados a expressarem seu ponto de vista e contestarem a decisão apenas quando das decisões puramente automatizadas (RGPD, 2018, Art. 4).

Por sua vez, no art. 20 da LGPD existe indicação que o titular de dados possui a faculdade de solicitar a revisão das decisões que forem tomadas com base em tratamento automatizados, e que sejam afetas ao seu interesse, incluindo-se aí decisões que possam definir o seu perfil (profiling), e também questões relativas ao seu consumo, crédito ou ainda mesmo aspectos da personalidade.

O parágrafo 3º do art. 20, da LGPD indicava que a revisão da decisão automatizada deveria ser feita por pessoa natural, em conformidade com uma previsão de regulamentação por meio de uma autoridade nacional, que levaria em consideração não só a natureza, mas também o porte da entidade e as operações que ela realiza e seus fins.

Contudo, houve veto do §6˚ do projeto de lei que tratava especificamente da necessidade de revisão das decisões automatizadas. Justificou-se o veto ao argumento que a revisão por uma pessoa seria contrária ao interesse público, pois tornariam inviáveis modelos atuais de planos de negócios de empresas, o que, consequentemente, traria impactos nos créditos e negócios realizados por empresas e traria consequências nega-

tivas para os consumidores. Justificou-se, ainda com base no RGPD, que em tese estaria em conformidade com o art. 22.

No entanto, a exclusão da locução "pessoa natural" possibilita que um pedido de revisão automatizada seja realizado por outro sistema automatizado (SILVA; MEDEIROS, 2019). O veto, portanto, não apenas gera questionamentos como é contrário ao disposto no RGPD. Isso porque possibilitar que uma máquina realize a revisão de um processo decisório de outra máquina acaba por violar a transparência. O veto, além disso, distancia-se da normativa da união europeia que traz essa possibilidade (NETO, 2020).

Sob outro aspecto, a LGPD emprega uma abordagem mais agressiva no que tange ao direito de explicação, comparado o RGPD. Isso porque, enquanto a normativa europeia trata de regulação de decisões que tenham efeitos nas esfera jurídica do titular dos dados pessoais, no caso brasileiro, regulamentou-se que as decisões automatizadas que acabem por afetar interesses das pessoas, incluindo-se o perfil pessoal, mas também consumo e crédito e aspectos da personalidade, podem ensejar a revisão.

Segundo Isabela Ferraria e Daniel Becker (2017), essa consideração pode acabar mais por prejudicar do que beneficiar as pessoas. Isso porque, segundo eles o titular dos dados não possui interesse nas informações sobre código-fonte, ou ainda modelo estatístico, linhas de programação, mas sim o que ele pretende ter conhecimento é quais foram os dados da pessoa que foram utilizados para produzirem os resultados. Isto é, precisa ter uma compreensibilidade da análise dos dados, da motivação da decisão automatizada.

De qualquer maneira, no Manual Prático da Lei Geral de Proteção de Dados da União Europeia dispõe-se que o controle individual e a conscientização de seu processamento de dados pessoais são questões cruciais na análise de dados. Isto é, sem o conhecimento desses critérios não se sabe quem são os controladores ou o processador dos dados, o que impede que seja realizado de maneira efetiva os direitos estipulados na norma.

Ainda que as normas estabeleçam proteções de decisões automatizadas, restam diversas dúvidas. Uma delas, apontada por Monique Mann e Tobias Matzner (2019) reside no fato de que não existe um consenso acerca da definição dos perfis algoritmos ou inferências algorítmicas, especificamente se se tratam de dados pessoais. Essa definição possui relevância, pois existe uma distinção normativa entre os dados pessoais e os que são considerados anonimizados. A anonimização corresponde em processamento no qual se emprega um conjunto de técnicas de modo a tornar impossível, na prática (e em tese), identificar a pessoa por qualquer meio.

Isto é, de acordo com o artigo 4 do RGPD, as informações colhidas que geram as decisões automatizadas devem estar relacionadas a uma pessoa física identificada ou identificável. Isso significa que as decisões automatizadas que são protegidas são aquelas que atingem os dados pessoais e aqueles que são considerados como pseudonimizados. Nesta esteira, o Manual Prático da Lei Geral de Proteção de Dados da União Europeia indica que uma alternativa para proteção contra o profiling poderia reside na pseudonimização. Isso porque na lei geral de proteção dados Européia protege-se dados pessoais e pseudonimizados.

Sandra Wachter e Brent Mittelstadt (2018), por sua vez, observam que as orientações fornecidas pelo Grupo de Trabalho do Artigo 29 conferem suporte para inferências consideradas como dados pessoais, principalmente se houver potencial para impactar os direitos e interesses de um indivíduo identificável. No entanto, eles também apontam para as decisões conflitantes do Tribunal de Justiça Europeu que têm uma interpretação mais restrita dos dados pessoais.

Assim, o problema do RGPD é que ela se concentra principalmente na proteção no estágio de entrada quando os dados são coletados, mas dificilmente durante ou após a análise. A norma ignora, portanto, o fato de que ameaças imprevistas à privacidade podem surgir após a coleta de dados devido a análises inferenciais (WACHTER; MITTELSTADT, 2018)

Para os autores, embora o objetivo da lei de proteção de dados seja proteger a privacidade e a identidade, ela dificilmente regula como

e de acordo com quais parâmetros os dados são avaliados e avaliados. Portanto, as avaliações de indivíduos (por exemplo, previsões sobre desempenho no trabalho, liquidez financeira, expectativa de vida) estão fora do escopo do RGPD. Em vez disso, concede diferentes padrões de proteção, definidos contra categorias artificiais e fluentes, refletindo o status dos dados no ponto de coleta. Isto é, quando dados usados são anonimizados, não existe proteção por parte do RGPD. Ocorre que os dados anônimos podem ser usados como base para construir perfis e extrair inferências sensíveis (WACHTER; MITTELSTADT, 2018).

Assim, os dados pessoais acabam por excluir os dados anônimos, os dados sensíveis assim como o consentimento das pessoas. Isto é, nenhum dos direitos que estão estipulados no RGPD se aplicam aos dados anônimos. O mesmo se diz com relação a LGPD, que não inova neste sentido, reproduzindo uma falha existente no RGPD. Ocorre que, como explica Sandra Wachter (2018), qualquer dado que não seja identificado pode acabar sendo submetido a uma engenharia reversa e vincular a uma pessoa específica. Ou seja, existe a possibilidade de se relacionar o dado anônimo a pessoa que foi colhida. Além disso, mesmo os dados anônimos, podem acabar sendo utilizados para fins de criação de perfis de usuários. Assim, danos a privacidade e discriminação se mantêm, mesmo sem se identificar uma pessoa em específico.

Trata-se de um problema sensível que demonstra a falta de normas específicas que tratem da questão da discriminação, notadamente quando vinculadas aos dados anonimizados. Sandra Wachter (2018) pondera que o problema reside no fato que o RGPD e aqui pode-se estender essa racionalidade a LGPD, enfatiza no estágio da coleta de dados, mas não na maneira pela qual os dados são utilizados e seus efeitos sobre as pessoas.

Acrescente-se, que, ainda que o RGPD tenha sido projetada com a finalidade de se proteger o titular dos dados pessoais o Tribunal de Justiça Europeu não tem entendimento claro sobre se as inferências se enquadram ou não nessa proteção. A jurisprudência sobre o caso não é consistente. Caso julgado em 2014 excluiu conclusões acerca das garantias da Lei de Proteção de Dados, ao passo que, outro caso de 2017 atribuiu o

estatuto de "dados pessoais" às conclusões. No entanto, mesmo neste, o Tribunal não concedeu todos os direitos associados à proteção e mencionou que o RGPD não tem previsão sobre os direitos e a maneira pela qual os indivíduos são avaliados. A norma, ao contrário, teria sido criada tão somente para garantir que os dados recebidos sejam obtidos legalmente (WACHTER; MITTELSTADT, 2018).

No que tange aos dados sensíveis, na normativa europeia a proteção de dados tem uma proteção mais ampla, no que tange, por exemplo, a questão do consentimento aos usos que são permitidos sobre aos dados, ao processamento e categorização de dados confidenciais ou categorias especiais, descrevendo características relativas à saúde, etnia ou ainda mesmo crenças políticas. Assim, quando os dados pessoais podem ser utilizados para fins de permitir conclusão de atributos pessoais de uma pessoa, por meio de revelações em virtude das origens dos dados resgatados, é possível considerar como dados confidenciais. Mas, mais uma vez, Sandra Wachter (2018) pondera que "aplicação do artigo 9.º do RGPD (que define 'categorias especiais' de dados) se refere aos casos em que existe a intenção de inferir informações confidenciais".

Nadezhda Purtova (2015, p. 83-100), por sua vez, pondera que a diferenciação entre dados pessoais e não pessoais é irrelevante. Para ela, qualquer processamento de dados pode impactar as pessoas, de modo que qualquer dado deve ensejar proteção. Esse entendimento vai em conformidade com estudo realizado sobre discriminação das decisões automatizadas no caso de gênero, que segundo Maria Cristine Branco Lindoso (2019), a anonimização dos dados pessoais é muitas vezes um responsável de potencialização de discriminações, sobretudo em processos automatizados. Isso se deve em virtude que eliminar características das pessoas não se faz de maneira perfeita, o que incorre no fato que, por meio de correlações e inferências algorítmicas o usuário acaba sendo identificado.

O que ocorre é que existe a possibilidade do algorítmico no âmbito de um processo decisório sofrer uma contaminação de vieses prejudiciais de grupos marginalizados justo no momento em que processa a sua

função, seja preditiva, seja ótima ou seja ela histórica. Aí, o processo todo será reproduzido de maneira desigual, e não haverá como evitar uma discriminação (LINDOSO, 2019).

Já Monique Mann e Tobias Matzner (2019) ressalvam que os dados coletados para a receita algorítmica em um determinado local e tempo que possuem relação a pessoas específicas podem ser utilizados para construção de modelos de grupo a serem aplicados em contextos distintos. Logo, a privacidade que visa proteger uma pessoa acaba não sendo suficiente para uma dada proteção, vez que o resultado decorre de uma formulação realizada com base em um grupo e não de modo individual. Deste modo, para eles não há proteção normativa que combata o potencial discriminatório do perfil algorítmico.

Os autores sugerem uma regulamentação anti-discriminação específica que enfrente formas emergentes de discriminação de modo a trabalhar com a invisibilidade existentes. Com efeito, em *screening decisions* consta etapa substancial que corresponde em passar a fórmula matemática que resolverá o problema e será elencada enquanto um padrão. Trata-se do momento de criação do modelo segundo o qual ela deverá se espelhar. O problema, resta no fato que "há uma etapa fundamental no processo decisório, que diz respeito à fase de ensinar a fórmula matemática, ou seja, qual o problema será por ela resolvido e quais padrões deverão ser identificados para serem alcançados ou descartados durante esse processo" (LINDOSO, 2019).

Nesse aspecto específico, que trata justamente do código, da codificação, não existe proteção normativa nem no RGPD nem na LGPD. A abordagem, portanto, deve ser de uma revisão para se pensar em mecanismos de design plural e inclusivos, atentos a realidade (LINDOSO, 2019).

## 4 CONSIDERAÇÕES FINAIS

O exame comparativo relativo ao tema demonstrou um desenvolvimento mais amadurecido do RGPD que a LGPD no que tange ao tratamento dos dados pessoais, incluindo-se aí, a questão das decisões

automatizadas. Para além do RGPD, a União Europeia conta com uma Convenção normativa, a 108, que estabelece critérios essenciais de proteção no mundo datificado presente. Tal, contudo, é um processo que foi estabelecido de maneira gradual, uma maturação normativa. No Brasil, embora existam dispositivos sobre proteção de dados desde a Constituição, como o remédio do habeas data, e posteriormente, o código de defesa do consumidor, a legislação era esparsa e pouco eficaz. Assim, o tratamento da questão é recente.

De todo modo, o *profilling* é um problema no âmbito da proteção de dados nas legislações europeia e brasileira, e, não por outra razão, recebeu atenção das duas. Todavia, seu conteúdo não é bem disposto nas normas, e, além disso, a sua proteção reside no âmbito pessoal. No caso das discriminações algorítmicas, foi identificado que o *profilling* tem o condão de estabelecer discriminação em grupos, propagando em massa uma discriminação sobre um grupo todo.

O exame da norma em conjunto com a literatura sobre o tema mostra um resultado preocupante, isto é, as normas não dão conta de lidar com essa questão. Primeiro, pela própria definição das inferências e suas proteções. Além disso, as normas foram estabelecidas para a proteção de dados pessoais, e a discriminação algorítmica não se dá apenas de modo individual, mas de um grupo todo. Logo, há uma lacuna nesse sentido e ausência de proteção.

Assim, no que tange à discriminação em especifico, mesmo o RGPD possui problemas sensíveis de falta de proteção. Isso porque ficou demonstrado que os dados colhidos não se resumem nos dados pessoais e identificados, mas também em dados anonimizados, para além do próprio design do sistema, que já reproduz uma discriminação do mundo offline. Nesse sentido, entende-se tal como Nadezhda Purtova (2018, p. 83-100), que a saída deve ser a consideração de proteção de quaisquer dados sejam eles pessoais ou não. Além disso, compreende-se que o processo de design deve se dar de maneira plural, de forma a promover inclusão digital e assim lidar com a discriminação inerente do presente sistema.

Como já havia ressalvado Nadezhda Purtova (2018), o RGPD tem a predisposição de se tornar a "lei de tudo" do universo online, mas embora intencionado, sobressaltam lacunas. Daí porque, segundo ela, é imperioso abandonar a distinção entre dados pessoais e não pessoais para adotar o princípio de que todo processamento de dados deve desencadear proteção. Logo, embora o RGPD seja uma norma decorrente de um processo de amadurecimento normativo no âmbito da União Europeia, ela não traz proteção para a questão da discriminação algorítmica, tal como a LGPD brasileira.

Como pondera Sandra Wachter (2018) e Oscar Gandy (2009), categorizações desatualizadas de dados são ineficazes. Pessoal ou não pessoal reflete tão somente a natureza dos dados no momento em que são coletados, mas não tratam do uso subsequente dos dados e suas possíveis transformações. É justamente aí que se pode estabelecer inferências sobre orientação sexual e gênero, por exemplo. Ou seja, dos titulares dos dados não residem apenas no momento em que os dados são coletados. No entanto, tanto a legislação europeia, quanto a brasileira, não estabelecem proteções para esse momento a posteriori.

Vale lembrar que a proteção de dados se relaciona com determinadas ações, notadamente o "processamento" de dados, ao passo que a discriminação se refere a um resultado, que não dependem das ações que levaram a esse resultado (MANN; MATZNER, 2019). A solução apontada pela doutrina tem sido na regulamentação anti-discriminatória atenta a essas lacunas, bem como construção plural e diversificada desde o momento do design. Ao fim, o que mostra que os conselhos de Laurence Lessig (2206) sobre a rede devem ser sempre colocados como fundamentais no caso das novas tecnologias, isto é, o código é a lei. É necessário, portanto, pensar desde o código.

## REFERÊNCIAS

ANDREJEVIC, Mark. **The Big Data Divide**. International Journal of Communication. 8 (2014), 1673–1689. Disponível em: file:///C:/Users/Home/Downloads/2161-11851-1-PB.pdf

BUOLAMWINI, Joy. **How I'm fighting bias in algorithms,** 2016. Disponível em: https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms/discussion?.com&utm_medium=social&utm_campaign=tedspread#t-61876

CANUT, Letícia; MEDEIROS, Heloísa Gomes. Os algoritmos nas relações de consumo eletrônicas: análise do direito do consumidor à informação. GEDAI Grupo de Estudos de Direito Autoral e Industrial Prof. Dr. Marcos Wachowicz (organizador). **Anais do XI CODAIP. XI Congresso de Direito de autor e interesse Público Estudos de Direito de Autor e Interesse Público.** Curitiba: Universidade Federal do Paraná, 2017. Disponível em: http://www.gedai.com.br/sites/default/files/publicacoes/anais_xi_codaip-2017-gedai.pdf

DARMODY, Aron; ZWICK, Detlev. **Manipulate to empower:** Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism Big Data & Society, January–June: 1–12 2020. civilization. Disponível em: https://cryptome.org/2015/07/big-other.pdf

EUROPEAN UNION AGENCY, **Handbook on European data protection law** - 2018 edition. Disponível em: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

FERRARI, Isabela; BECKER, Daniel. **Algoritmo e preconceito**, 12/12/2017. JOTA. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/algoritmo-e-preconceito-12122017

GANDY, Oscar. **Engaging rational discrimination:** Exploring reasons for placing regulatory constraints on decision support systems. 2009. em: https://www.researchgate.net/publication/225235550_Engaging_rational_discrimination_Exploring_reasons_for_placing_regulatory_constraints_on_decision_support_systems

GOETTENAUER, Carlos Eduardo. Algoritmos, Inteligência Artificial, Mercados. Desafios ao arcabouço jurídico. In: FRAZÃO, Ana; CARVALHO, Angelo Gamba Prata de. **Empresa, Mercado e Tecnologia**. Belo Horizonte: Fórum, 2019.

GONÇALVES, Lukas Ruthes. **A Tutela Jurídica de Trabalhos Criativos feitos por Aplicações de Inteligência Artificial no Brasil**. Universidade Federal do Paraná, 2019.

LEGRAND, Pierre. **Como ler o direito estrangeiro**. Tradução de Daniel Wunder Hachem. São Paulo: Editora Concorrente, 2018.

LEMOS, André; ARAÚJO, Nayra Veras. **Cidadão Sensor e Cidade Inteligente: Análise dos Aplicativos Móveis da Bahia. Revista Famecos**, Porto Alegre, v. 25, n. 3, p. 1-19, setembro, outubro, novembro e dezembro de 2018.

LERMAN, Jonas. **Big data and Its Exclusions**. Stanford Law Review, v. 66, 2013. Disponível em: https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/66_stanlrevonline_55_lerman.pdf

LESSIG, Laurence. **Code, version 2.0.** Basic Books, New York, 2006.

LINDOSO, Maria Cristine Branco, **Discriminação de gênero em processos decisórios automatizados,** 2019. Disponível em: https://repositorio.unb.br/bitstream/10482/38524/1/2019_MariaCristineBrancoLindoso.pdf

MANN Monique, MATZNER Tobias. **Challenging algorithmic profiling:** The limits of data protection and anti-discrimination in responding to emergent discrimination. Big Data & Society. July 2019. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2053951719895805

MIKE2.0. Big Data Definition. In: **The open source methodology for Information Development**. Disponível em: http://mike2.openmethodology.org/. Acesso em: 01. out. 2018.

NETO, Thais. **LGPD e direitos do titular de dados pessoais**, 15/04/2020. Disponível em: https://direitoreal.com.br/artigos/lgpd-e-direitos-do-titular-de-dados-pessoais.

NEWSLOCKER – **Spotify to use playlists as proxy for targeting ads to activities, moods,** 16/04/2015. Disponível em: https://www.newslocker.com/en-us/profession/advertising/spotify-to-use-playlists-as-proxy-for-targeting-ads-to--activities-moods/.

O'DONNEL, Cathy. **Algorithmes, la bombe à retardement** – 2018, p. 23.

PURTOVA Nadezsha, The law of everything: Broad concept of personal data and future of EU data protection law. **Law, Innovation and Technology,** 2018, em: https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176

SILVA, Priscila; MEDEIROS, Juliana - **A polêmica da revisão (humana) sobre decisões automatizadas**, 10/12/2019. Disponível em: https://feed.itsrio.org/a-pol%C3%AAmica-da-revis%C3%A3o-humana-sobre-decis%C3%B5es-automatizadas-a81592886345

ZUBOFF Shoshana. **Big other: surveillance capitalism and the prospects of an information civilization**. Disponível em: https://cryptome.org/2015/07/big-other.pdf

# Seção IV

## Tratamento de dados pessoais pelo poder público: transparência versus privacidade

# Capítulo I

# O DEVER DE TRANSPARÊNCIA NO COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS E ENTIDADES DE DIREITO PÚBLICO – UM COMPARATIVO ENTRE O DIREITO EUROPEU E O DIREITO BRASILEIRO

*Luis Marcello Bessa Maretti*[1]

*Thiago Monroe*[2]

## SUMÁRIO



## RESUMO

Os dados pessoais assumem importância de caráter político e econômico na sociedade moderna. Dessa forma, o presente artigo analisa os sistemas de proteção de dados pessoais europeu e brasileiro, em especial o tratamento realizado pela Administração Pública, verificando as convergências e divergências. Como ponto central está a transparência com que os dados pessoais são compartilhados entre os Entes Públicos no Brasil, especialmente na esfera federal, regime jurídico que deveria ser tratado pelo artigo 28 da LGPD, vetado quando da promulgação da Lei, e, atualmente, regulado pelo Decreto nº 10.046/2019, que conforme será exposto, apresenta divergências com a LGPD criando um cenário de insegurança jurídica.

**Palavras-chave:** Dados pessoais. Compartilhamento. Poder Público. Transparência.

---

[1] Pós-Graduado em Direito do Estado/Constitucional pela Universidade Estadual de Londrina (2008). Pós-Graduado em Direito Tributário pela Uniasselvi (2011). Pós-Graduado em Administração Pública pela Fundação Getúlio Vargas (2016). Foi professor de Direito Tributário/Financeiro e Introdução ao Estudo do Direito na Universidade Estadual de Londrina. Lecionou Direito Tributário na Uninorte/PR e no Curso Jurídica preparatório para OAB em Londrina. Atualmente é Procurador da Fazenda Nacional em Curitiba, Coordenador da Divisão de Assuntos Judiciais da PFN/PR. Mestrado profissional em Direito em andamento pela Universidade Positivo.

[2] Mestrando em Direito, Tecnologia e Desenvolvimento pela Universidade Positivo.

## 1 INTRODUÇÃO

Há tempos vivencia-se um fenômeno complexo decorrente do célere avanço tecnológico que vem modificando o conceito de espaço-tempo e a forma de estar no mundo das pessoas e das instituições, com profundas modificações na maneira como vivem e se relacionam. Do advento das ferrovias, seguido pela introdução de um horário mundial – unificado e de validade global -; da disseminação de novos veículos de transporte – carros e aviões -; do célere avanço da tecnologia – internet ultrarrápida e aplicativos de comunicação em tempo real-; e, mais recentemente, da utilização de termos como pós-humano e singularidade; a relação do tempo com o espaço não é mais a mesma; vivencia-se uma nova era de evolução do homem para o pós-homem, integrado à máquina e a uma sociedade verdadeiramente da informação (ROSA, 2019, p.189-197).

Dentro desse cenário, debates envolvendo a proteção e o tratamento de dados pessoais e sensíveis dos indivíduos ganha corpo, não apenas na esfera privada, mas também no setor público – não raro permeado por percepções políticas –, ainda mais quando considerados como direitos fundamentais da personalidade humana protegidos constitucionalmente (DONEDA, 2011, p. 91-108).

Nesse contexto a democracia se define não apenas como "governo do povo", mas também como "governo em público", representando a transparência um elemento fundamental do processo democrático, da correção da vida pública em seu conjunto (RODOTÀ, 2003, p. 15), sendo a privacidade tida como um valor social (BOEHME-NESSLER, 2016, p.5).

Hodiernamente, a preocupação se volta ao uso e à disponibilidade que a base informacional de dados propicia ao Estado em sentido lato, especialmente quando consideradas as assimetrias entre o concreto e o abstrato, entre o real e o virtual, entre o possível e o desejável, decorrentes das diferenças entre os diversos entes e pessoas jurídicas de direito público. De um lado, processos e rotinas ineficientes, excessivamente burocráticas e avessas à modernização passam a fazer parte do passa-

do; de outro lado, clamores por adoção de padrões claros de eficiência e *accountability*, no resultado da ação, representam o período presente/futuro (RUEDIGER, 2006, p.233-256).

Nesse espectro, o uso ético, seguro e transparente de dados pessoais e sensíveis dos indivíduos pelos órgãos e entidades de direito público, mais que uma obrigação, é um dever corolário da cidadania e do Estado Democrático de Direito. O compartilhamento desses dados, justamente por se referirem a questões ligadas aos direitos da personalidade, deveria demandar, *prima facie*, o consentimento livre e expresso de seu titular, podendo essa regra ser mitigada, excepcionalmente, após critérios de proporcionalidade e razoabilidade, para situações específicas e necessárias ao atendimento do interesse público, ou à observância do direito de outro titular, previamente estabelecidas em lei, mas sempre de forma transparente.

E isso tem razão de ser, pois o Estado controla, ainda que não diretamente, diversos aspectos da vida das pessoas, merecendo elas terem direitos e garantias delineados pelo ordenamento jurídico. A privacidade está ligada a dignidade da pessoa humana, princípio também insculpido na Constituição da República Federativa do Brasil em seu art. 1º, inciso III (BARRETO JÚNIOR e FAUSTINO, 2019, p.302).

Essa nova fase se destaca por movimentos da sociedade civil e dos parlamentos em diversas partes do mundo visando conferir proteção jurídica aos dados pessoais e sensíveis dos indivíduos. Internacionalmente são proeminentes dois modelos principais – o americano e o europeu. Em poucas palavras, o modelo protetivo americano se destaca pelo patrimonialismo e pelo contratualismo, de caráter realista, em que basta o consentimento do indivíduo para legitimação do uso de seu dado pessoal como se mercadoria fosse (DONEDA, 2006, p. 372). Nos Estados Unidos, a propriedade privada exerce um papel central na construção da *privacy* circunscrevendo a esfera íntima da pessoa, usando a lógica do *trespass,* de violação-proteção de uma propriedade/espaço particular (MORAES, 2010, p. 2-3).

Por sua vez, no modelo europeu, o indivíduo possui direito à autodeterminação de sua esfera privada, detendo, portanto, caráter per-

sonalista (DONEDA, 2006, p. 372). Esse modelo dá mais ênfase à ligação entre os dados e as pessoas, especialmente onde "*os dados pessoais são elementos de personalidade de cada um; emanam dos indivíduos e revelam sua identidade e seus comportamentos, tal como tem elaborado o Tribunal Constitucional alemão desde 1983*" (ROCHFELD, 2018, p.73).

No velho continente, a preocupação com a proteção e o tratamento de dados pessoais não é nova. De início discreto, após a II Guerra Mundial, com a Declaração Universal dos Direitos Humanos, passando pela Convenção de Estrasburgo nº 108/1981 e pela Diretiva nº 95/46/CE, alcançou a União Europeia a sua legislação atual, representada precipuamente pelo Regulamento Geral sobre a Proteção de Dados (RGPD) nº 679/2016 que entrou em vigor em 25 de maio de 2018, bem como, mais diretamente, para o objeto desse artigo, pelo Regulamento nº 1725/2018.

Do lado de cá do oceano atlântico, esse novo paradigma é representado pela Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) aprovada em 14 de agosto de 2018 e que entrou em vigor em setembro de 2020, estando suspensa a aplicação das sanções até agosto de 2021, por força da Lei nº 14.010/2020.

A lei brasileira, inspirada pelo modelo europeu, busca disciplinar, inclusive nos meios digitais, o tratamento de dados pessoais tanto por pessoa natural, como por pessoa jurídica, seja ela de direito público ou de direito privado.

Outrossim, possui a legislação pátria a finalidade de proteger os direitos fundamentais de liberdade, de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural.

Como se vê, a LGPD se aplica tanto à Administração Direta como à Administração Indireta de todos os entes da Federação. "*Deixar o setor público fora do alcance da LGPD seria um verdadeiro atentado aos direitos fundamentais*" (ROSSO, 2019, p. 4). E com razão, uma vez que, como visto alhures, o Estado exerce papel determinante, mesmo que indiretamente, na vida das pessoas, sendo de suma importância a inclusão da Administração Pública no ato normativo regulador do tratamento de dados

pessoais e sensíveis dos indivíduos por impor um ônus a toda a esfera pública a envidar esforços, inclusive financeiros, na proteção e no uso adequado, transparente e ético desses dados.

Mas será que a LGPD, no tocante ao compartilhamento de dados pessoais entre órgãos e entidades de direito público possui a mesma disciplina que sua fonte inspiradora europeia representada pelo RGPD e pelo Regulamento nº 1725/2018? Haveria distinção de tratamento do tema entre o Brasil e os países da União Europeia? Eis o que veremos a seguir.

## 2 O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO NA EUROPA

Como mencionado, a União Europeia desde o ano de 1995, através da Diretiva nº 95/46/CE, conta com legislação específica sobre a proteção de dados. Ainda, desde o ano de 2001, já existia legislação acerca do tratamento de dados pessoais pela Administração Pública, consubstanciada no Regulamento nº 45/2001.

A União Europeia então em 2016 adotou o RGPD como norma geral e para o tratamento de dados realizado pela Administração Pública, adotou o Regulamento nº 1725/2018. Assim, o presente tópico abordará a regulamentação europeia sobre os dados, em especial a parte referente à Administração Pública e o dever de transparência.

### 2.1 O Regulamento Geral sobre a Proteção de Dados – RGPD nº 679/2016

As regras relativas à proteção de dados pessoais e sua livre circulação são precipuamente disciplinadas, no âmbito da União Europeia, pelo Regulamento Geral sobre a Proteção de Dados (RGPD) nº 679/2016, que os considera como um direito fundamental devendo o tratamento ser concebido para servir as pessoas. Ao defini-los, o RGPD adotou um con-

ceito expansionista, em que o dado pessoal pode se referir a qualquer tipo de informação que permita a identificação do indivíduo, ainda que não de forma imediata ou direta (POLIDO; DOS ANJOS; BRANDÃO; MACHADO e OLIVEIRA, 2018, p.8).

Como regra, de acordo com o RGPD, os dados pessoais são recolhidos para finalidades determinadas, explícitas e legítimas, demandando o consentimento de seu titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades, salvo para fins de arquivo de interesse público, ou para fins de investigação histórica, científica ou para fins estatísticos.[3]

O tratamento deverá ser transparente, de fácil acesso e compreensão, formulado numa linguagem clara e simples, inclusive por meio eletrônico num sítio *web,* informando-se ao titular da operação de tratamento e de suas finalidades.[4] Demais disso, os dados pessoais devem ser conservados de forma que permita a identificação de seus titulares apenas durante o período necessário para as finalidades para as quais são tratados, ressalvadas, novamente, as hipóteses de conservação para fins de arquivo de interesse público, ou para fins de investigação histórica, científica ou para fins estatísticos.[5]

Por fim, se o tratamento for necessário por motivos de interesse público importante, deverá esse ser proporcional ao objetivo visado, respeitando a essência do direito à proteção dos dados pessoais e prevendo medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados.[6]

Nesse caso, o próprio RGPD, já prevendo a necessidade de regulamentação específica e melhor detalhada, excepcionou algumas hipóteses do âmbito de sua aplicação, dentre elas, o tratamento de dados pessoais quando efetuado pelas autoridades competentes para efeitos penais, in-

3 União Europeia**. Regulamento (UE) 2016/679**. Artigos 5º., 1, *b.*

4 União Europeia**. Regulamento (UE) 2016/679**. Considerandos nº 39, 58 e 60.

5 União Europeia**. Regulamento (UE) 2016/679**. Artigos 5º., 1, *e.*

6 União Europeia**. Regulamento (UE) 2016/679**. Artigos 9º., 2, *g.*

cluindo a salvaguarda e a prevenção de ameaças à segurança pública[7] – caso em que regida pela Diretiva nº 680/2016 –; e, para fins desse artigo, o tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da própria União Europeia, isto é, pela esfera pública – caso em que até pouco tempo era disciplinado pelo Regulamento nº 45/2001[8] e atualmente regido pelo Regulamento nº 1725/2018 que o revogou.

Em que pese direcionar o tratamento de dados pessoais pelos órgãos e entidades públicos a outro diploma normativo, o RGPD deixou claro que o Regulamento nº 45/2001 (sucedido pelo Regulamento nº 1725/2018) deveria ser adaptado aos princípios e regras da novel legislação, a fim de assegurar uma proteção uniforme e coerente das pessoas[9], aumentando a segurança jurídica para os titulares desses dados (IGF, 2019, p.1-2), sendo, portanto, de curial importância essa análise preliminar das principais diretivas trazidas pelo RGPD acima realizada.

Essa orientação, aliás, encontra guarida na jurisprudência do Tribunal de Justiça da União Europeia, e está expressamente contida no considerando nº 5 do Regulamento nº 1725/2018 que estabelece:

> (5) Uma abordagem coerente da proteção dos dados pessoais e a livre circulação dos mesmos na União implicam uma harmonização, tão ampla quanto possível, das regras de proteção de dados adotadas a nível das instituições, dos órgãos e dos organismos da União com as regras de proteção de dados adotadas para o sector público nos Estados-Membros. Sempre que as disposições do presente regulamento sigam os mesmos princípios que as disposições do Regulamento (UE) 2016/679, de acordo com a jurisprudência do Tribunal de Justiça da União Europeia («Tribunal de Justiça»), esses dois conjuntos de disposições deverão ser interpretados de forma homogénea, sobretudo porque o regime do presente regulamento deverá ser entendido como equivalente ao regime do Regulamento (UE) 2016/679.[10]

---

7 União Europeia**. Regulamento (UE) 2016/679**. Artigos 2º., 2, *d.* c/c 10..

8 União Europeia. **Regulamento (UE) 2016/679**. Artigo 2º., 3.

9 União Europeia**. Regulamento (UE) 2016/679**. Artigos 2º., 3 c/c 98.

10 União Europeia. **Regulamento (UE) 2018/1725**. Considerando nº 5.

Isso posto, veja-se, por conseguinte, a legislação específica destinada à proteção e ao tratamento de dados pessoais no âmbito da esfera pública pelo direito europeu.

## 2.2 O Regulamento nº 1725/2018.

Em 23 de maio de 2018, apenas dois dias antes da entrada em vigor do RGPD, representantes do Parlamento europeu e do Conselho concordaram em fazer uma nova regulamentação para o tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União Europeia até então prevista no Regulamento nº 45/2001, cujo objetivo era oferecer aos seus cidadãos o mesmo tratamento dado pelo RGPD quando interagindo com o setor público (DELOITTE, 2019, p.3).

Esses trabalhos redundaram na aprovação do Regulamento nº 1725/2018, que revogou tanto o Regulamento nº 45/2001 como a Decisão nº 1247/2002, a partir de 11 de dezembro de 2018[11], sendo um diploma especialmente dedicado à proteção das pessoas físicas – não aplicável às pessoas jurídicas (ABAJO, 2018, p.1-3) – no tocante ao tratamento e à livre circulação de seus dados pessoais pelas instituições e pelos órgãos e organismos da União Europeia, devendo, como outrora consignado, de acordo com a jurisprudência do Tribunal de Justiça da União Europeia, nos casos em que não haja distinção expressa, ser interpretado de acordo com a mesma orientação dada ao RGPD.

Com efeito, dentre as linhas mestras do Regulamento nº 1725/2018, merece ser destacado o seu considerando nº 20 que traz garantias aos indivíduos em linha com o quanto estabelecido pelo RGPD. De acordo com esse considerando, elaborado com base nos artigos que compõem o Capítulo II do Regulamento em referência, o tratamento de dados pessoais deverá ser efetuado de forma lícita e leal, bem como deverá ser feito de forma transparente, adequada e limitada ao necessário atendimento das finalidades para os quais são tratados, exigindo-se que o titular dos

[11] União Europeia. **Regulamento (UE) 2018/1725**. Artigo 99.

dados seja informado da operação de tratamento de dados e das suas finalidades.

A respeito do dever de transparência transcreva-se um pequeno excerto do referido considerando:

> (20) O tratamento de dados pessoais deverá ser efetuado de forma lícita e leal. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes digam respeito são recolhidos, utilizados, consultados ou sujeitos a outros tipos de tratamento, e em que medida é que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações e as comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento e sobre as finalidades a que o tratamento dos dados se destina, e às informações adicionais destinadas a assegurar que o tratamento dos dados seja efetuado com lealdade e transparência em relação às pessoas singulares em causa e salvaguarde o seu direito a obter a confirmação e a comunicação dos dados pessoais tratados que lhes digam respeito.[12]

Demais disso, o tratamento de dados pessoais para finalidades distintas daquelas para as quais os dados tenham sido inicialmente recolhidos – disciplinado em seu artigo 6º – só será lícito se for compatível com as finalidades para as quais tenham sido inicialmente obtidos. Se o tratamento for necessário para o exercício de funções de interesse público ou para o exercício da autoridade pública de que o responsável pelo tratamento esteja investido, o direito europeu poderá determinar e definir as tarefas e as finalidades para as quais o tratamento posterior será considerado compatível e válido, garantindo ao titular o direito de oposição. De acordo com o considerando nº 25:

---

[12] União Europeia. **Regulamento (UE) 2018/1725**. Considerando nº 20.

> (25) (...)A fim de apurar se a finalidade de um tratamento posterior é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento, após ter cumprido todos os requisitos de licitude do tratamento inicial, deverá ter em atenção, nomeadamente: a existência de uma ligação entre tais finalidades e a finalidade do tratamento posterior previsto; o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, com base na sua relação com o responsável pelo tratamento; a natureza dos dados pessoais; as consequências do tratamento posterior previsto para os titulares dos dados; e a existência de garantias adequadas tanto nas operações de tratamento iniciais como nas operações de tratamento posteriores previstas.[13]

Nesse diapasão, o Regulamento nº 1725/2018 também confere especial atenção aos dados pessoais dito sensíveis, que:

> São dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (PINHEIRO, 2018, p.26).

Segundo o Regulamento em comento esses dados pessoais, sem prejuízo da aplicação dos princípios e regras gerais, só deverão ter tratamento se as condições específicas no Diploma normativo definidas estiverem reunidas.[14]

Veja, porém, que os direitos fundamentais até o momento aduzidos, à semelhança do que já previsto para o RGPD, não são absolutos. De acordo com a Decisão UE nº 969/2020 de 3 de julho do corrente ano,

---

13 União Europeia. **Regulamento (UE) 2018/1725**. Considerando nº 25.

14 União Europeia. **Regulamento (UE) 2018/1725**. Artigo 10.

> (7) Em determinadas circunstâncias, é necessário conciliar os direitos dos titulares de dados ao abrigo do Regulamento (UE) 2018/1725 com a necessidade da Comissão de realizar as funções de controlo, investigação, auditoria ou consulta do RPD e com a necessidade de confidencialidade do intercâmbio de informações com outros serviços da Comissão, bem como com o pleno respeito dos direitos e liberdades fundamentais de outros titulares de dados. (...)
>
> (14) Por estas razões, a Comissão pode ter de invocar os motivos das limitações a que se refere o artigo 25.o, n.o 1, alíneas c), g) e h), do Regulamento (UE) 2018/1725 para os aplicar às operações de tratamento de dados efetuadas no âmbito das funções de controlo, investigação, auditoria ou consulta do RPD previstas no artigo 45.o do mesmo regulamento.

Embora a Decisão UE nº 969/2020 tenha confirmado o entendimento de que os direitos protegidos pelo Regulamento nº 1725/2018 – e por corolário lógico pelo RGPD – não são absolutos, pois devem ser considerados em relação à sua função na sociedade e ser equilibrados, em conformidade com os princípios da razoabilidade e da proporcionalidade, com outros direitos fundamentais[15], em nenhum momento ela os deixa desprotegidos, ao contrário, trata-se apenas de compatibilização com os direitos de outros indivíduos e o interesse público eventualmente envolvidos.

Aliás, importante esclarecer que

> Assim como o RGPD para o setor privado, o Regulamento (UE) 2018/1725 deixa pouco espaço para interpretação: seu conteúdo e aplicabilidade se resumem à criação de uma cultura de *accountability*, uma vez que o controlador deve ser capaz de demonstrar conformidade com o regulamento e deve ser responsável por isso. Para esse efeito, o controlador deve implementar as medidas técnicas e organizacionais adequadas (DELOITTE, 2019, p.4).

[15] União Europeia**. Regulamento (UE) 2016/679**. Considerando nº 4.

Desse modo, visto em linhas gerais os normativos a respeito do tratamento de dados pessoais pelas instituições e pelos órgãos e organismos dados pela União Europeia, passa-se ao estudo da regulamentação brasileira sobre o assunto.

## 3 O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO NO BRASIL

O Brasil até a promulgação da LGPD caminhava em passos lentos acerca da proteção dos dados pessoais; como exemplo, apenas com a promulgação do Marco Civil da Internet - MCI (Lei nº 12.965/2014), através do inciso II, do artigo 3º, surge no texto legal o termo "privacidade", sendo anteriormente referenciado como "intimidade e vida íntima".

Contudo, a LGPD quando teve vetado seu artigo 28, passou a ser omissa sobre o compartilhamento de dados pessoais entre a Administração Pública. Para suprimir aludida omissão, ao menos na esfera federal, promulgou-se o Decreto nº 10.046/2019 que como será exposto abaixo, não é suficiente para suprir o veto e, ainda, representa insegurança jurídica, pois divergente das disposições constantes na própria LGPD e seu paradigma, o RGPD.

### 3.1 A Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018)

No Brasil, em 14 de agosto de 2018, foi editada a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), diploma legal responsável por preencher uma grande lacuna no direito pátrio relativa à existência de uma regulamentação especificamente dirigida ao tratamento de dados pessoais, cuja importância cresce dia após dia na nova era digital decorrente do avanço da sociedade da informação. Nesse contexto:

> Em vários aspectos a LGPD assemelha-se ao regulamento europeu sendo uma dessas semelhanças a sua aplicação multisetorial e trans-

> versal, ou seja, a lei aplica-se às pessoas naturais e às pessoas de direito público e privado, respeitadas algumas peculiaridades de cada setor para qualquer operação de tratamento de dados pessoais (ROSSO, 2019, p.1).

O diploma pátrio, fortemente influenciado pelo seu paradigma europeu, igualmente agrega uma categoria aos dados pessoais, aqueles dito sensíveis. Esses dados pessoais sensíveis estão diretamente correlacionados com um núcleo fundamental de direitos da personalidade e encontra limites protetivos dentro do conceito de cidadania e de Estado Democrático de Direito.

Em terras tupiniquins, a LGPD, embora inclua o Estado dentro de seus preceitos, reserva à legislação específica, ainda não promulgada, o tratamento de dados pessoais quando realizado para fins exclusivos de segurança pública, defesa nacional ou atividades de investigação e repressão de infrações penais.[16]

Nesse diapasão, a legislação pátria exige que as atividades de tratamento de dados pessoais observem a boa-fé e alguns princípios basilares, semelhantes ao seu paradigma europeu, dentre os quais se destacam, a finalidade, a adequação e a necessidade do tratamento, que deverá ser voltado a propósitos legítimos, específicos, explícitos e informados ao titular, bem como compatíveis com esses propósitos, limitados ao mínimo necessário para a realização de suas finalidades; o livre acesso enquanto perdurar o tratamento, garantindo-se a prestação de informações claras e precisas sobre a realização do tratamento bem como dos seus respectivos agentes, que deverão utilizar os dados de forma segura, sem discriminação, adotando-se medidas de proteção contra a ocorrência de danos, que, acaso verificados, serão objeto de responsabilização e prestação de contas.[17]

---

16 BRASIL. Planalto. **Lei nº 13.709, de 14 de agosto de 2018**. Artigo 4º.

17 BRASIL. Planalto. **Lei nº 13.709, de 14 de agosto de 2018**. Artigo 6º

Sobre o tema, e conferindo ênfase ao tratamento de dados pelo Estado, muito embora possa independer do consentimento do titular quando for indispensável para o cumprimento de obrigação legal ou para a consecução de políticas públicas legalmente estabelecidas (GEDIEL, 2008, p.141-153)[18] o tratamento de dados pessoais deve atender à finalidade pública e ao interesse público, respeitados os princípios supra aludidos. Compartilhando desse entendimento, o Ministério Público Federal, emitiu em seu "Roteiro de Atuação" o seguinte entendimento:

> De outro lado, o tratamento de dados pessoais por entes públicos deve ser sempre atrelado ao atendimento de sua finalidade pública e à persecução do interesse público, devendo haver ainda a explicitação das hipóteses em que realizam o referido tratamento – com especificação dos procedimentos e práticas usados.
>
> Além disso, o uso compartilhado de dados pessoais pelo Poder Público deve sempre respeitar os princípios da proteção de dados pessoais, especificados no art. 6º da LGPD (MPF, 2019, p. 25).

Outrossim, mister destacar que,

> A LGPD tornou obrigatória a observância dos princípios *Privacy By Design* e *Privacy By Default*, pelos quais as entidades (públicas e privadas) devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais desde a fase de concepção do produto ou do serviço até a sua execução (BONFIM, 2019, p.4-5).

Trata-se do programa de governança em privacidade cujo objetivo é estabelecer regras de boas práticas a serem aplicadas pelos agentes no tratamento dos dados, considerando a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular.[19]

---

[18] BRASIL. Planalto. **Lei nº 13.709, de 14 de agosto de 2018**. Artigo 11, II..

[19] BRASIL. Planalto. **Lei nº 13.709, de 14 de agosto de 2018**. Artigo 50.

A importância do Estado sobre o tema é tão grande que merece relevo o fato da LGPD ter conferido ao tratamento de dados pessoais pelo Poder Público um capítulo específico, dividido em duas seções. Fala-se aqui do Capítulo IV da Lei nº 13.079/2018, aplicável aos órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, o Judiciário e o Ministério Público, bem como às autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.[20] Para as empresas públicas e as sociedades de economia mista que atuem em regime de concorrência, aplicável o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares.[21]

Em razão disso, "*deve o ente público identificar sob qual condição atua, uma vez que as consequências de atuar em regime concorrencial ou regime de finalidade pública são diferentes, desde os requisitos (...) até às sanções (...)* (ROSSO, 2019, p.2).

Ademais, os dados pessoais deverão ser mantidos em formato interoperável e estruturados para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral, devendo o seu uso compartilhado, atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da LGPD.

Aqui chega-se ao ponto nodal do presente artigo. Parece não haver dúvidas, em um primeiro momento e com base em tudo o que até aqui desenvolvido, que o Estado tem o dever de ser transparente, princípio expressamente elencado pela LGPD, quando no uso compartilhado de dados pessoais, seja na hipótese excepcional de transferência para enti-

[20] BRASIL. Planalto. **Lei nº 13.709, de 14 de agosto de 2018**. Artigo 23.

[21] BRASIL. Planalto. **Lei nº 13.709, de 14 de agosto de 2018**. Artigo 24.

dades privadas[22], seja na hipótese de compartilhamento entre órgãos e entidades de direito público. Aliás, a LGPD é clara ao conceituar o princípio da transparência:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> (...)
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;[23]

Nesse sentido, temos que:

> Estritamente no caso do setor público, o tratamento dos dados pessoais deverá ser realizado para atender à finalidade pública referente ao órgão, com o fim de executar as competências ou atribuições legais estabelecidas para o serviço público (art. 23, caput). Para isso deve haver transparência quanto à base normativa utilizada e ao uso, aos procedimentos e às finalidades para os quais os dados são coletados, tratados e utilizados (art. 23, inc. I) (GONÇALVES, 2019, p. 112).

Tanto assim é verdade que o Parlamento brasileiro aprovou a LGPD com regra expressa garantindo a *publicidade* na comunicação e no uso compartilhado de dados pessoais entre órgãos e entidades de direito público. Assim se encontrava estabelecida a norma legal:

> Art. 28. A comunicação ou o uso compartilhado de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos do inciso I do *caput* do art. 23 desta Lei.[24]

---

22 BRASIL. Planalto. **Lei nº 13.709, de 14 de agosto de 2018**. Artigos 26 e 27.

23 BRASIL. Planalto. **Lei nº 13.709, de 14 de agosto de 2018**. Artigo 6º.

24 BRASIL. Poder Executivo. **Mensagem nº 451, de 14 de agosto de 2018**.

Referida norma fora objeto de veto presidencial, sob a alegação de que a publicidade irrestrita da comunicação ou do uso compartilhado de dados pessoais entre órgãos e entidades de direito público, imposta pelo dispositivo, poderia tornar inviável o exercício regular de algumas ações públicas como as de fiscalização, controle e polícia administrativa.[25]

Com a devida vênia, parece haver confusão entre os termos publicidade e transparência. De fato, embora a regra seja a publicidade dos atos pelo Poder Público, ela, à luz do caso concreto, pode ser mitigada, quando, por exemplo, estivermos diante da proteção da privacidade do titular dos dados pessoais, hipótese em que a anonimização, defendida no artigo seguinte desta obra, localizado na parte II, seção IV, pode ser uma boa solução (MACOHIN, Aline; CARNEIRO, João Victor Vieira, 2020, p. 14-16). Todavia, e o dever de transparência na comunicação e no uso compartilhado dos dados pessoais entre órgãos e entidades de direito público? Ele se mantém? Quais os efeitos do veto presidencial? O tratamento jurídico pátrio seria distinto daquele conferido pela União Europeia?

## 3.2 O Veto Presidencial ao Artigo 28 da LGPD e a Regulamentação do Compartilhamento de Dados na Esfera Pública Federal pelo Decreto nº 10.046/2019

Considerando o seu paradigma europeu, a resposta deveria estar em consonância com ele. Como regra o Poder Público deve obediência ao dever de transparência quando do compartilhamento de dados entre órgãos e entidades de direito público. A publicidade é que poderia ser restringida, quando se relacionar a atividades que já se encontrem fora do espectro de abrangência da LGPD, a saber, segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, bem como quando for necessária, com esteio nos princípios da proporcionalidade e da razoabilidade, a confidencialidade

[25] BRASIL. Poder Executivo. **Mensagem nº 451, de 14 de agosto de 2018**.

no compartilhamento dos dados com vistas a atender um determinado interesse público, hipótese em que ficaria deferida para um momento posterior a divulgação da informação, ou, ainda, quando for necessária a compatibilização com o direito de outros titulares de dados e o próprio respeito à privacidade de seu titular.

Essa conclusão possui razão de ser, já que a transparência do Estado deve ser ativa, garantindo efetividade às regras e princípios estabelecidos pela LGPD, pois, "*as proteções trazidas pela lei são mais que obrigações legais, são direitos dos cidadãos que merecem ser respeitados*" (KARL, 2020, p. 61-62). Com o veto presidencial ao artigo 28 da LGPD, havia um vácuo no disciplinamento da matéria e apreensão quanto à não observância do dever de transparência pelo Estado.

A questão, porém, ganhou novos contornos, com a edição do Decreto nº 10.046/2019 que dentre outros assuntos, disciplinou a governança no compartilhamento de dados no âmbito da administração pública federal, que inclui a direta, a autárquica, a fundacional e os demais Poderes da União.

Inicialmente denota-se que as finalidades previstas no referido Decreto destoam daquelas estabelecidas pela LGPD. Por um lado, observa-se que o foco do Decreto em comento encontra-se na administração pública federal; por outro, infere-se que o foco da LGPD é na proteção do indivíduo quando do tratamento de seus dados pessoais, direito fundamental protegido pela Constituição. Nesse sentido,

> Em uma primeira análise ao decreto, é possível tomar como conclusão que este veio mais voltado a ser uma solução à burocracia enraizada na administração pública do país, mas aborda de forma superficial quando se trata do assunto do momento: proteção de dados pessoais e os possíveis riscos gerados pelo seu tratamento. Ou seja, gozou o decreto de boas intenções – facilitar a vida daquele que espera uma administração pública célere, no entanto, acabou por desconsiderar importantes princípios da lei específica de 2018 (GALDINO JUNIOR, 2019, p. 1-2).

Outrossim, enquanto a LGPD se refere a dados pessoais e sensíveis, o Decreto fez menção a atributos biográficos, biométricos e cadastrais, conceitos que não encontram correspondente direto na legislação aprovada pelo Parlamento, demandando um esforço interpretativo de compatibilização. Sobre o tema,

> Há muitos pontos conflitantes quando se analisa o decreto 10.046 frente à LGPD, a começar pela própria segmentação dos dados pessoais. Enquanto a LGPD fala em "dados pessoais" e "dados pessoais sensíveis", o decreto classifica os dados dos cidadãos em "cadastrais", "biográficos", "biométricos" e "atributos genéticos". Para a LGPD, dados relacionados à origem étnica, opinião política, genética e biometria de uma pessoa, por exemplo, são dados sensíveis e requerem um tratamento especial por parte de empresas e órgãos públicos (PAIVA, 2019, p. 1-6).

No que se refere ao compartilhamento de dados pelos órgãos e entidades de direito público, objetivando colmatar a lacuna deixada pelo veto presidencial ao artigo 28 da Lei nº 13.709/2018, o Decreto nº 10.046/2019 estabeleceu as seguintes diretrizes:

> I - a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;
>
> II - o compartilhamento de dados sujeitos a sigilo implica a assunção, pelo recebedor de dados, dos deveres de sigilo e auditabilidade impostos ao custodiante dos dados;
>
> III - os mecanismos de compartilhamento, interoperabilidade e auditabilidade devem ser desenvolvidos de forma a atender às necessidades de negócio dos órgãos e entidades de que trata o art. 1º, para facilitar a execução de políticas públicas orientadas por dados;
>
> IV - os órgãos e entidades de que trata o art. 1º colaborarão para a redução dos custos de acesso a dados no âmbito da administração pú-

> blica, inclusive, mediante o reaproveitamento de recursos de infraestrutura por múltiplos órgãos e entidades;
>
> V - nas hipóteses em que se configure tratamento de dados pessoais, serão observados o direito à preservação da intimidade e da privacidade da pessoa natural, a proteção dos dados e as normas e os procedimentos previstos na legislação; e
>
> VI - a coleta, o tratamento e o compartilhamento de dados por cada órgão serão realizados nos termos do disposto no art. 23 da Lei nº 13.709, de 2018.[26]

Da leitura das diretrizes acima, chama atenção que o Decreto em referência considera possível o compartilhamento de dados não pessoais, já que aos pessoais garante a observância do direito à intimidade e à privacidade, remetendo a sua proteção, às normas e aos procedimentos da legislação, que, dentre outros, abarca a própria LGPD.

Ademais, importante destacar que o último inciso do artigo 3º do Decreto nº 10.046/2019 trouxe norma semelhante àquela prevista no artigo 28 da LGPD objeto de veto presidencial. Eis o cotejo entre elas:

> **Artigo 28 da LGPD objeto de veto**
>
> Art. 28. A comunicação ou o uso compartilhado de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos do inciso I do *caput* do art. 23 desta Lei.
>
> **Artigo 3º, VI, do Decreto nº 10.046/2019**
>
> Art. 3º O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes:
>
> (...)
>
> VI - a coleta, o tratamento e o compartilhamento de dados por cada órgão serão realizados nos termos do disposto no art. 23 da Lei nº 13.709, de 2018.

[26] BRASIL. Poder Executivo. **Decreto nº 10.046/2019.** Artigo 3º.

Tal fato poderia afastar a preocupação quanto à não observância do dever de transparência pelo Estado. Todavia, o próprio Decreto, em seus artigos seguintes, ao disciplinar o compartilhamento de dados em três níveis – amplo, restrito, e específico – limitou, novamente, não apenas a publicidade, mas também a transparência que deveriam nortear a atuação do Poder Público, tendo, uma vez mais, como foco a Administração Pública e não os titulares de dados objeto de compartilhamento.

Para o compartilhamento amplo, partiu-se do pressuposto que os dados são públicos não sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado. Já o compartilhamento restrito e o compartilhamento específico envolveriam dados protegidos por sigilo. A diferença é que no primeiro a concessão de acesso aos órgãos e entidades da administração pública federal deve demandar a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados e estabelecidos pelo Comitê Central de Governança de Dados; no segundo, a concessão de acesso aos órgãos e entidades da administração pública federal deve demandar hipóteses e fins previstos em lei, cujo compartilhamento e regras sejam definidos pelo gestor de dados.

No ponto, uma vez mais as normas previstas no Decreto em comento parecem estar em choque com a LGPD, já que enquanto o primeiro determina a criação de um Comitê Central de Governança de Dados constituído apenas por representantes indicados pelo poder executivo; o segundo estabelece a criação da Autoridade Nacional de Proteção de Dados (ANPD), composta por um conselho diretor com cinco membros, todos indicados pelo presidente da República, mas que, uma vez escolhidos, não podem ser livremente por ele demitidos. Ambos os órgãos teriam atribuições sobrepostas, cujo impasse pode desencadear litígios a serem decididos pelo Poder Judiciário (PAIVA, 2019, p.2).

Nesse contexto, muito embora tenha o Decreto nº 10.046/2019 procurado solucionar a lacuna deixada pelo veto presidencial ao artigo 28 da Lei nº 13.709/2018, acabou esse diploma se afastando do escopo e dos princípios da LGPD e de seu paradigma europeu, e nessa parte, alvo

de críticas, pois, como elencado anteriormente, as proteções estabelecidas pela lei são mais que meras obrigações legais, são, em verdade, direitos dos cidadãos que merecem ser respeitados. Ser transparente significa "*dar publicidade quanto à motivação, ao uso e à finalidade para o qual os dados foram coletados, conferindo maior controle ao cidadão sobre as ações adotadas, sendo, também, uma forma de accountability*" (GONÇALVES, 2019, p. 114).

Ainda sobre o tema, merece destaque a recente decisão proferida em 13 de agosto de 2020 pelo Supremo Tribunal Federal na ADI 6529, em que a Corte, por maioria de votos, deferiu parcialmente a medida cautelar requerida para estabelecer que os órgãos componentes do Sistema Brasileiro de Inteligência - SISBIN somente podem fornecer dados e conhecimentos específicos à Agência Brasileira de Inteligência - ABIN quando for comprovado o interesse público da medida, em decisão motivada, afastando qualquer possibilidade desses dados atenderem a interesses pessoais ou privados.[27]

Outrossim, mesmo diante da existência de interesse público, em razão da limitação aos direitos fundamentais, decidiu a Corte Constitucional ser imprescindível a instauração de procedimento formal e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.[28]

## 4 CONSIDERAÇÕES FINAIS

Como se vê da detida análise da questão posta, diante do célere avanço tecnológico vivenciado pela nossa sociedade da informação, e a contínua aproximação na relação espaço/tempo, a proteção e o trata-

[27] BRASIL. Supremo Tribunal Federal. **ADI 6529. Medida Cautelar**. Decisão proferida em 13.08.2020.

[28] BRASIL. Supremo Tribunal Federal. **ADI 6529. Medida Cautelar**. Decisão proferida em 13.08.2020.

mento dos dados pessoais e sensíveis dos indivíduos no Estado Democrático de Direito são uma realidade a ser debatida.

As ferramentas tecnológicas desenvolvidas para a coleta de dados pessoais e sensíveis dos indivíduos somente encontraria guarida no ordenamento jurídico quando acompanhada do consentimento livre e expresso de seu titular. Seu tratamento pelo Estado, outrossim, deveria ser reservado estritamente às questões ligadas ao atendimento do interesse público e aos preceitos ligados à ética, transparência e *accountability,* sob pena de malferimento das disposições democráticas.

Dentro dos dois principais modelos mundiais de proteção dos dados pessoais e sensíveis dos indivíduos, destacam-se o americano e o europeu, tendo sido esse último escolhido pela legislação pátria como paradigma a ser seguido. No ponto, a União Europeia tem como pilar o Regulamento Geral sobre a Proteção de Dados – RGPD nº 679/2016 que, aliada à jurisprudência do Tribunal de Justiça lá instalado, passou a tratar a proteção de dados pessoais no âmbito do Poder Público, por meio do Regulamento nº 1725/2018, adaptado aos princípios e regras do RGPD, a fim de assegurar uma proteção uniforme e coerente dos indivíduos.

Dentre as principais diretrizes, observa-se que o tratamento de dados pessoais deverá ser efetuado de forma lícita, leal, transparente, adequada e limitada ao necessário atendimento das finalidades para os quais são tratados, informando-se ao titular dos dados da operação e de suas finalidades.

Embora a proteção não seja absoluta, pois considerada, nos termos da Decisão UE nº 969/2020, a sua função e seu equilíbrio com outros direitos fundamentais, em nenhum momento houve um esvaziamento da proteção, mas sim uma compatibilização com os direitos de outros indivíduos e o interesse público eventualmente envolvidos.

No Brasil, editada a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), em vários aspectos assemelhada ao direito europeu, incluiu o Estado dentro de seus preceitos, reservando a ele um capítulo específico, dividido em duas seções. No ponto destaca-se o fato de que o

uso compartilhado dos dados pessoais dos indivíduos deve atender a políticas públicas, respeitados os princípios de proteção elencados no art. 6º a LGPD, incluindo-se o dever de transparência.

Em que pese tal fato, a norma legal que conferia publicidade ao compartilhamento de dados entre órgãos e entidades do poder público foi objeto de veto presidencial sendo a hipótese posteriormente disciplinada pelo Decreto nº 10.046/2019.

Do cotejo entre os dois diplomas normativos, chegou-se à conclusão de que há um descompasso entre eles. Por um lado, o Decreto tem como foco a administração pública federal, instrumento voltado à própria burocracia estatal; por outro, a LGPD busca a proteção do indivíduo quando do tratamento de seus dados pessoais e sensíveis, direito fundamental protegido pela Constituição.

Nesse diapasão, no tocante à observância do dever de transparência pelo Estado quando do compartilhamento de dados pessoais dos indivíduos, novamente a frustração é a tônica. Dividido em três níveis – amplo, restrito, e específico – a publicidade e a transparência que deveriam nortear a atuação do Poder Público, foram novamente restringidas.

Se para o compartilhamento amplo, partiu-se do pressuposto que os dados são públicos não sujeitos a nenhuma restrição de acesso, para os compartilhamentos restrito e específico, a regra é o sigilo, cuja concessão de acesso aos órgãos e entidades da administração pública federal deve demandar prévio regramento pelo Comitê Central de Governança de Dados ou pelo gestor de dados, respectivamente, nada se referindo ao conhecimento e ao consentimento do titular dos dados.

Porém, esse posicionamento tem sido objeto de ponderação e controle pela Corte Constitucional brasileira. Em recente decisão, o Supremo Tribunal Federal, por maioria de votos, deferiu parcialmente a medida cautelar requerida para estabelecer que os órgãos componentes do Sistema Brasileiro de Inteligência - SISBIN somente podem fornecer dados e conhecimentos específicos à Agência Brasileira de Inteligência - ABIN quando for comprovado o interesse público da medida, em decisão mo-

tivada, afastando qualquer possibilidade desses dados atenderem a interesses pessoais ou privados.

Outrossim, ainda que diante da existência de interesse público, em razão da limitação aos direitos fundamentais, imprescindível a instauração de procedimento formal e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

E esse posicionamento da Corte Constitucional faz parte do sistema político de freios e contrapesos especialmente quando diante da constatação que as proteções estabelecidas pela Carta Magna e pela LGPD são mais que meras obrigações legais, representam, na realidade, direitos dos indivíduos que merecem ser respeitados e observados.

Nesse contexto, ainda que necessária, a mitigação da publicidade merece ser tratada de forma transparente, ocasião em que a anonimização dos dados pessoais seja, quiçá, uma boa solução para o desenlace da questão e cujo tópico é melhor desenvolvido no artigo seguinte deste livro.

## REFERÊNCIAS

ABAJO, Joaquín. **2018 despide el año com um nuevo reglamento en matéria de protección de datos**. Disponível em https://www.hyaip.com/es/espacio/2018-despide-el-ano-con-un-nuevo-reglamento-en-materia-de-proteccion-de-datos/. Acesso em: 07 set. 2020.

BARRETO JUNIOR, Irineu Francisco Barreto; FAUSTINO, André. **Aplicativos de serviços de saúde e proteção de dados pessoais dos usuários**. Revista Jurídica, vol. 01, nº 54, Curitiba, 2019, p. 292-316. Disponível em: http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3311/371371803. Acesso em: 02 set. 2020.

BOEHME-NESSLER, Volker **Privacy: a matter of democracy. Why democracy needs privacy and data protection**. Disponível em: https://doi.org/10.1093/idpl/ipw007. Acesso em: 28 ago. 2020.

BONFIM, Natália Bertolo. **O tratamento de dados pessoais pelo Poder Público**. Disponível em https://www.migalhas.com.br/depeso/299940/o-tratamento-de-dados-pessoais-pelo-poder-publico. Acesso em: 03 set. 2020.

BRASIL. Ministério Público Federal. **Sistema Brasileiro de Proteção e Acesso a Dados Pessoais.** Disponível em http://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3. Acesso em: 03 set. 2020.

_____. Planalto. **Lei nº 13.709/2018**. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 19 ago. 2020.

_____. Poder Executivo. **Mensagem nº 451, de 14 de agosto de 2018**. Disponível em https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-veto-156214-pl.html. Acesso em: 03 set. 2020.

_____. Poder Executivo. **Decreto nº 10.046/2019.** Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 03 set. 2020.

_____. Supremo Tribunal Federal. **ADI 6529. Medida Cautelar**. Decisão proferida em 13.08.2020. Disponível em http://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837. Acesso em: 08 set. 2020

DELOITTE. **Delloitte´s view on the implementation of regulation (EU) 2018/1725 – the 'GDPR for European Union Institutions'**. Disponível em https://www2.deloitte.com/be/en/pages/risk/articles/gdpr-for-eu-institutions.html. Acesso em: 07 set. 2020.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Revista Espaço Jurídico, Joaçaba, v. 12, n. 2, p.91-108, jul/dez.2011.

_____. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro, Renovar, 2006.

GALDINO JUNIOR, Roberto. **O decreto 10.046/19 e a lei geral de proteção de dados no Brasil.** Disponível em https://www.migalhas.com.br/depeso/313686/o-decreto-10046-19-e-a-lei-geral-de-protecao-de-dados-no-brasil. Acesso em: 08 set. 2020.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção Jurídica de Dados Pessoais: A Intimidade Sitiada entre o Estado e o Mercado. **Revista da Faculdade de Direito – UFPR**, Curitiba, n. 47, 2008.

GONÇALVES, Tânia Carolina Nunes Machado. **Gestão de Dados Pessoais e Sensíveis pela Administração Pública Federal:** Desafios, Modelos e Principais Impactos com a Nova Lei**.** Disponível em www.uniceub.br/arquivo/144ng_20190730051313*pdf?AID=3007. Acesso em: 19 ago. 2020.

GUNTHER, Luiz Eduardo; COMAR, Rodrigo Thomazinho; RODRIGUES, Luciano Ehlke. **A Proteção e o Tratamento dos Dados Pessoais Sensíveis na Era Digital e o Direito à Privacidade:** Os Limites da Intervenção do Estado. Disponível em: http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/3972/371372300. Acesso em: 19 ago. 2020.

INSPEÇÃO-GERAL DE FINANÇAS - IGF. **Tratamento de Dados Pessoais para efeitos do exercício de competências penais**. Disponível em https://www.igf.gov.pt/anexos-informacao-tecnica/anexos-protecao-de-dados-pessoais-rgpd/ficha-informativa-diretiva-2016_680-e-lei-59_2019-pdf.aspx+&cd=1&hl=p-t-BR&ct=clnk&gl=br&client=safari. Acesso em: 26 ago. 2020.

KARL, Éryta Dallete Fernandes. Compliance e LGPD: Uma exigência também para a Administração Pública *in* **Compliance no Setor Público**. Organizadores Marcelo Zenkner e Rodrigo Pironti Aguirre de Castro. Belo Horizonte, Forum, 2020.

MACOHIN, Aline; CARNEIRO, João Victor Vieira. Web Crawling e Web Scraping em sites de tribunais: publicidade processual e proteção de dados pessoais nas experiências europeia e brasileira *in* **Proteção de Dados Pessoais em Perspectiva**: LGPD e RGPD na Ótica do Direito Comparado. Organizador: Marcos Wachowicz**.** Acesso em: 09 out. 2020.

MORAES, Maria Celina Bodin de. Ampliando os direitos da personalidade. In: _____. **Na medida da pessoa humana:** estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010.

PAIVA, Fernando. **Uma análise do conflito entre LGPD e o decreto 10.046.** Disponível em https://www.mobiletime.com.br/noticias/07/11/2019/o-conflito-entre-lgpd-e-o-decreto-10-046-em-analise/. Acesso em: 08 set. 2020.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018. São Paulo: Saraiva Educação, 2018.

POLIDO, Fabrício B. Pasquot; DOS ANJOS, Lucas Costa; BRANDÃO, Luíza Couto Chaves; MACHADO, Diego Carvalho; OLIVEIRA, Davi Teofilo Nunes. **GDPR e suas repercussões no direito brasileiro.** Disponível em: https://irisbh.com.br/publicacoes/gdpr-e-suas-repercussoes-no-direito-brasileiro/. Acesso em: 07 set. 2020.

RODOTÀ, Stefano. Democracia y protección de datos. **Cuadernos de Derecho Público**, núms 19-20 (mayo-diciembre 2003).

ROCHFELD, Judith. **C**omo qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 10, n. 1, p. 61-84, maio 2018.

ROSA, Hartmut. **Aceleração:** a transformação das estruturas temporais na Modernidade; traduzido por Rafael H. Silveira. São Paulo, editora Unesp, 2019.

ROSSO, Angela Maria. **LGPD e o setor público:** aspectos gerais e desafios. Disponível em https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico-aspectos-gerais-e-desafios. Acesso em: 26 ago. 2020.

RUEDIGER, Marco Aurélio. Perspectivas da governança na era da informação: Estado e Sociedade Civil *in* **Estado e Gestão Pública:** Visões do Brasil Contemporâneo. Organizadores Paulo Emilio Matos Martins e Octavio Penna Pieranti. 2ª edição. FGV. 2006.

UNIÃO EUROPÉIA. **Diretiva 95/46/CE**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 19 ago. 2020.

_____. **Regulamento UE 2016/679**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1528874672298&uri=CELEX:32016R0679. Acesso em: 19 ago. 2020.

_____. **Regulamento (UE) 2016/680**. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680. Acesso em: 26 ago. 2020.

_____. **Regulamento (UE) 2018/1725**. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32018R1725. Acesso em: 07 set. 2020.

_____. **Decisão (UE) 2020/969**. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2020.213.01.0012.01.POR&toc=OJ:L:2020:213:TOC. Acesso em: 07 set. 2020.

# Capítulo II

# *WEB CRAWLING* E *WEB SCRAPING* EM SITES DE TRIBUNAIS: publicidade processual e proteção de dados pessoais nas experiências europeia e brasileira

*Aline Macohin*[1]

*João Victor Vieira Carneiro*[2]

## SUMÁRIO



## RESUMO

A coleta de dados disponibilizados em sites públicos, em especial através de técnicas de *web crawling* e *web scraping*, possibilita alimentar bases de dados para diversas finalidades. A partir do cruzamento desses dados entre si ou com outras bases de dados, é possível inferir informações adicionais sobre pessoas, órgãos públicos ou empresas, por exemplo. Com a crescente informatização do processo judicial no Brasil, estas técnicas vêm sendo aplicadas para a extração de informações do texto de decisões judiciais e documentos processuais. Neste contexto, o presente artigo busca avaliar o aparente conflito entre o direito à proteção de dados e o princípio da publicidade dos atos processuais, demonstrando experiências positivas na União Europeia e apontando para futuros desafios no cenário brasileiro.

**Palavras-chave:** web crawling; web scraping; decisões judiciais; processo eletrônico; proteção de dados.

[1] Doutoranda em Direito na UFPR, Mestre em Computação Aplicada pela UTFPR, Advogada e Analista de Sistemas. Pesquisadora nos Grupos de Pesquisa E-Justiça (UFPR) e Lawgorithm (USP). Website: http://www.macohin.adv.br

[2] Graduando em Direito na UFPR. Membro do Grupo de Estudos de Direito Autoral e Industrial (GEDAI/UFPR) e do grupo Direito, Biotecnologia e Sociedade (BIOTEC/UFPR). Pesquisador de iniciação científica. Website: https://joaovvcarneiro.github.io

## 1 INTRODUÇÃO

A coleta de dados disponibilizados em sites públicos, em especial através de técnicas de *web crawling* e *web scraping*, possibilita alimentar bases de dados para fins acadêmicos e comerciais, dentre outros. A partir do cruzamento desses dados entre si ou com outras bases de dados, é possível inferir informações adicionais sobre pessoas, órgãos públicos ou empresas, por exemplo. Com a entrada em vigência da Lei Geral de Proteção de Dados (LGPD), surgem dúvidas sobre sua aplicação à coleta e processamento de dados que, conquanto relativos a pessoas naturais, são tornados públicos pelo Estado pela necessidade de transparência.

Neste contexto, uma relevante questão surge quanto aos dados públicos de processos judiciais. Os dados constantes em decisões judiciais, embora disponibilizados de forma textual e não estruturada, podem trazer informações significativas se processados por meio de algoritmos. As fontes de dados para este tipo de informação podem ser os sites dos tribunais ou ainda os diários eletrônicos do poder judiciário.

A análise informatizada de dados do Poder Judiciário pode auxiliar tanto magistrados quanto advogados e servidores públicos. No lado dos tribunais é possível viabilizar mais racionalidade, celeridade e efetividade à prestação jurisdicional. Já para os advogados, muitas aplicações podem se mostrar atrativas, principalmente no que se refere a justiça preditiva: pode-se, por exemplo, determinar a posição dominante de um tribunal sobre casos específicos, verificar quais acórdãos e obras doutrinárias costumam ser referenciados, e até mesmo calcular a probabilidade de sucesso em uma ação judicial.[3]

A coleta e processamento de dados disponíveis *online* é facilitada por sistemas como os de *web crawling* e *web scraping*, que automatizam parte do trabalhoso processo de navegar e extrair informações de uma

[3] Sobre estas e outras aplicações propiciadas pela informática jurídica, recomenda-se a introdução histórica feita por MAGALHÃES (2005) a respeito da inteligência artificial no direito.

grande quantidade de páginas *web*. As duas técnicas diferem entre si na medida que, enquanto *web crawlers* automatizam o *download* de grande quantidade de páginas, as ferramentas de *scraping* analisam pormenorizadamente as informações de cada arquivo obtido. Um sistema de *webcrawler*, segundo Olston e Najork (2010) é definido da seguinte forma:

> Um rastreador web (também conhecido como robô ou «spider") é um sistema para download em massa de páginas da web. Os rastreadores da web são usados para diversos fins. Mais proeminentemente, eles são um dos principais componentes dos mecanismos de pesquisa da web, sistemas que montam um corpus de página da web, indexam-nas e permitem que os usuários façam consultas ao índice e encontrem as páginas da web que correspondem às consultas. (OLSTON; NAJORK, 2010, p. 176, tradução nossa).

Os *crawlers*, portanto, servem para navegar entre *hyperlinks* na Internet, ou ainda na hierarquia de arquivos em servidores *web*. A análise do conteúdo das páginas vasculhadas, por sua vez, demanda ferramentas aptas a navegar internamente pela estrutura dos documentos extraídos. Aqui se mostram úteis as ferramentas de *web scraping*, termo definido da seguinte forma por Chandrika et al (2020):

> Web scraping é um conceito que pode ser usado para extrair dados de um site que está hospedado online. As ferramentas de web scraping acessam a Internet por meio de protocolos (ou seja, HTTP/HTTPS) ou por meio dos navegadores que normalmente usamos. A maior parte da extração de dados é feita pelo software ou script e é um processo automatizado. Portanto, também pode ser referido como web crawling. As ações realizadas pelo web scraper podem ser consideradas como um ato de cópia dos dados, mas o produto final está na forma exigida, de que precisamos. (CHANDRIKA et al, 2020, p. 853, tradução nossa).

Um sistema de *web crawling* faz o download de páginas *web* e, analisando o conteúdo interno de cada uma, retira os *links* nela citados, reiterando a operação a cada página até esgotar os *hyperlinks* disponíveis. Já um sistema de *web scraping* é desenvolvido para extrair informações específicas nas páginas obtidas, descartando aquilo que não se mostra útil a dada finalidade. A partir dos dados coletados mediante a técnica de *web scraping*, é possível aplicar ainda outras técnicas, como a mineração de dados, para a descoberta de padrões e informações relevantes em meio a grandes massas de dados.

Os dados coletados e utilizados por essas aplicações, entretanto, podem ser de caráter pessoal, o que levanta questionamentos relacionados aos sistemas processuais eletrônicos e à publicação virtual de decisões. Torna-se necessário, destarte, verificar a viabilidade do uso de tais tecnologias sem violar direitos personalíssimos e fundamentais das partes envolvidas. Em virtude da busca de informações por diversas empresas, principalmente lawtechs, mostra-se pertinente buscar um equilíbrio entre a privacidade dos cidadãos e a divulgação de dados pessoais decorrente da publicidade dos atos processuais.

Questões como as acima nortearão o percurso do presente trabalho, o qual, partindo dos conceitos expostos acima, buscará aprofundar a discussão sobre o uso destas técnicas computacionais de coleta e análise de dados judiciais. Preliminarmente, é essencial destacar alguns pontos relativos à publicidade dos atos judiciais, demonstrando outrossim como se desenvolveu a informatização do processo judicial no direito brasileiro. Será empreendido, outrossim, um cotejo com a experiência europeia neste tema, de modo a apontar possíveis caminhos para a proteção de dados no Brasil.

É mister, de antemão, delimitar a abordagem comparatista a ser aqui adotada, pois não se pretende meramente comparar trechos do Regulamento Geral de Proteção de Dados europeu (RGPD) com a LGPD. A trajetória legislativa europeia[4] e as disposições do RGPD são

[4] O tema origina profícuas discussões, dado o protagonismo legislativo europeu nesta seara jurídica; contudo, não há como pormenorizar aqui as nuances históricas do ramo, dado

o grande exemplo tomado pelo legislador brasileiro quando da redação dos projetos que deram luz à LGPD.[5] Não obstante, uma exegese destas normas não seria útil à presente análise, e tampouco proveitosa como metodologia de pesquisa jurídica. Como aponta LEGRAND (2018, p. 64), aquele que utilizar o direito comparado como ferramenta deve superar a visão de que o direito de um país se restringe aos termos de suas leis. Deste modo, busca-se aqui observar a *experiência* europeia na padronização de registros judiciais e sua compatibilização com os preceitos da proteção de dados pessoais.

## 2 O EQUILÍBRIO ENTRE TRANSPARÊNCIA E A PROTEÇÃO DE DADOS NO PODER JUDICIÁRIO

O princípio da publicidade é um dos pilares do Direito Público brasileiro, de modo que para possibilitar o controle do governo pelos cidadãos, o Poder Público deve atuar de modo transparente. Esse princípio constitucionalmente previsto tornou-se mais sólido com o advento da Lei de Acesso à Informação (Lei 12.527/2011), que assegura aos cidadãos o direito de saber como estão atuando os agentes públicos, como utilizam os recursos públicos, e o que motiva suas decisões (SALGADO, 2017). A lei dispõe que os órgãos e entidades públicas respondem[6] pelos danos decorrentes da divulgação não autorizada ou a utilização indevida de informações sigilosas ou pessoais (MEIRELLES, 2016, p. 103). Destarte, o acesso a dados pessoais, ainda que públicos por sua natureza, resulta em uma decisão sobre a (não-)interferência na construção da história e da memória coletiva, quando em conflito com o direito à proteção de dados pessoais (CARNEIRO, 2019).

o escopo deste artigo. Cf. neste sentido as lições de DONEDA (2011) sobre as gerações legislativas na proteção de dados pessoais.

5 Cf. a análise de VERONESE e MELO (2018) sobre o Projeto de Lei brasileiro 5.276/2016 em relação com o RGPD. Este PL, em conjunto com o PL 4.060/2012, constituiu grande parte do que viria a ser o texto da LGPD.

6 Cabendo direito de regresso ou apuração de responsabilidade funcional.

Por integrar o Poder Público, o Poder Judiciário também se sujeita às previsões da Lei de Acesso à Informação (LAI). Mas antes disso, se sujeita ao princípio constitucional da publicidade dos atos processuais,[7] compreendida como a liberdade de acesso aos atos integrantes do procedimento e sua documentação (YARSHELL, 2014, p 133).

Como explicita CUEVA (2019, p. 136), neste âmbito a publicidade processual é regra e o sigilo, exceção. A publicidade não é absoluta, encontrando restrições quando em conflito com outras situações. A Constituição Federal, neste sentido, prevê que a publicidade dos atos processuais só é passível de restrição quando a defesa da intimidade ou o interesse social[8] o exigirem (arts. 5º, LX e 93, IX).

Essa possibilidade de ponderação se torna um tema crítico com a aceleração tecnológica e a crescente informatização do processo judicial no Brasil. Este fenômeno traz consigo ganhos e riscos: ao passo que se ampliam as possibilidades de controle social do exercício da jurisdição, eventuais fragilidades nos sistemas processuais podem permitir fraudes e violações à intimidade (YARSHELL, 2014, p. 136).

O contexto por que passa o Poder Judiciário demanda, portanto, maior deste atenção à compatibilização entre transparência e a proteção dos dados pessoais, como apontam LANGENEGGER e GOBATTO (2019, p. 146). Os autores demonstram que diversas informações presentes em andamentos processuais, decisões e outros documentos podem ser classificadas como dados pessoais, a exemplo de CPF, endereço e profissão das partes (LANGENEGGER; GOBATTO, 2019, p. 146). Sua disponibilização em formato eletrônico possibilita que programas automatizem sua coleta e análise, o que traz uma série de consequências para o ramo da proteção de dados pessoais, consoante se verá adiante.

---

7 O ato processual é "toda conduta dos sujeitos do processo que tenha por efeito a criação, modificação ou extinção de situações jurídicas processuais", podendo-se citar como exemplos o oferecimento de uma denúncia, uma petição inicial, um interrogatório ou uma sentença (CINTRA; GRINOVER; DINAMARCO, 2011, p. 361).

8 O conceito de «interesse social» é amplo, devendo ser densificado pelo legislador ordinário, que consequentemente adquire certa discricionariedade na delimitação das situações que, por sua sensibilidade, merecem segredo (SCHREIBER, 2013, p. 140).

## 2.1 A informatização do processo judicial no Brasil

A adoção de sistemas processuais eletrônicos no direito brasileiro remete ao ano de 2006, quando, por meio da Lei 11.419, passou-se a admitir o uso de meios eletrônicos na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais.[9] A justificativa para a regulamentação se baseava, sobretudo, na insatisfação da população brasileira em relação à morosidade do sistema judiciário (PEGORARO JÚNIOR, 2019, p. 78). O artigo 14 da Lei prevê que os sistemas processuais eletrônicos deverão usar, preferencialmente, "programas com código aberto, acessíveis ininterruptamente por meio da rede mundial de computadores, priorizando-se a sua padronização".

Percebe-se, portanto, um estímulo à interoperabilidade[10] e à garantia de disponibilidade dos sistemas. A adoção de programas de código aberto (*open source*)[11] não se confunde com o desenvolvimento de sistemas processuais sob tais licenças. A inclusão do trecho pelo legislador foi provavelmente motivada pela redução dos gastos de desenvolvimento, além da maior segurança dos softwares de código aberto.[12] Deste modo, tal preferência não se estende ao produto final, cujo código-fonte pode ser

9 Conquanto não abrangessem a totalidade do processo judicial e seus atos, normas anteriores a Lei 11.419 já possibilitaram o uso de recursos eletrônicos. Muito antes disso, a Lei 8.245/1991 (Lei do Inquilinato) já possibilitava a citação por meio eletrônico, mediante telex ou fac-símile. (PEGORARO JÚNIOR, 2019, p.80).

10 A padronização permitiria que diferentes sistemas observem um mesmo conjunto de especificações técnicas, jurídicas e organizacionais. Isto favorece sua interoperabilidade, que para SERBENA (2017, passim) pode ser compreendida, de modo simplificado, como a capacidade de comunicação eficiente entre aplicações e bases de dados distintos.

11 Por open source entende-se um programa cuja licença permite o acesso e a modificação do código-fonte, dentre outras permissões. A diferença para o termo software livre (free ou libre software), como escreve STALLMAN (2002, p. 76), é que este é um movimento social direcionado à liberdade e emancipação dos usuários, enquanto aquele é somente uma metodologia de desenvolvimento. Portanto, todo software livre é open source, mas nem todo software open source é livre.

12 A "Lei de Linus", cunhada pelo hacker Eric S. RAYMOND (1999, p. 29), afirma que "com olhos suficientes, todos os erros se tornam óbvios" (*given enough eyeballs, all bugs are shallow*). Dito de outro modo, o argumento do autor significa que, ao possibilitarem a revisão do código-fonte por mais pessoas, os softwares open source têm falhas de segurança e bugs mais rapidamente corrigidos. De qualquer modo, a frequente atualização desses sistemas

tornado confidencial. Os três maiores sistemas processuais eletrônicos do Judiciário brasileiro (PJe, e-Proc e Projudi) têm seu código-fonte fechado,[13] o que obsta maior transparência quanto ao seu funcionamento interno e sua segurança. A necessidade da promoção de padrões abertos e software livre no Poder Público é um debate extremamente necessário, mas que não caberia no escopo desta investigação.[14]

A vigência do Código de Processo Civil de 2015 foi um grande passo na informatização do direito processual brasileiro, ampliando certas previsões da Lei de 2006 e regulamentando a realização de diversos atos processuais por meio eletrônico. A partir da leitura do relatório Justiça em Números, do Conselho Nacional de Justiça (CNJ), torna-se evidente a consolidação do processo eletrônico no Brasil, de modo que 90% dos novos casos judiciais são ajuizados de modo virtual. É nítida, contudo, uma disparidade entre regiões do país e entre segmentos do Poder Judiciário. A adesão beira os 100% na Justiça Trabalhista, mas na Justiça Eleitoral somente três tribunais apresentam mais de 30% de novas ações ingressadas eletronicamente. A Justiça Estadual apresenta desigualdades: a título de exemplo, 37,5% dos novos processos ingressam eletronicamente no TJES, contra os 100% do TJPR e outros seis estados (CNJ, 2020, p. 112-119).

## 2.2 O acesso público a informações processuais e decisões judiciais

A informatização do processo judicial traz consigo a disponibilidade de informações processuais por meio da Internet, com variável grau de controle ao seu acesso. Conforme exposto anteriormente, no

já se mostra uma vantagem para o Judiciário, que se exime da necessidade de arcar com os custos contínuos de desenvolvedores.

13 A título de exemplo, Ministro Dias Toffoli, presidente do Conselho Nacional de Justiça, enviou em 2019 um ofício ao TRF-4 determinando que este não compartilhe o código-fonte do sistema e-Proc com outros tribunais. Cf. Disponível em: https://www.conjur.com.br/2019-out-29/cnj-determina-trf-abstenha-ceder-codigo-sistema.

14 Cf., por exemplo, HEXSEL (2002).

ordenamento brasileiro a publicidade dos atos processuais é a regra, sendo sua restrição possível apenas em situações excepcionais. Neste sentido dispõe o texto constitucional, conforme a modificação da Emenda Constitucional nº 45/2004:

> Art. 5º, LX - a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem;
>
> [...]
>
> Art. 93, IX - todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação;

Além da Constituição, a Lei 11.419/2006 aborda este tema, ao prever a disponibilização dos dados de processos judiciais e oficializar os diários como fonte de dados oficial:

> Art. 4º Os tribunais poderão criar Diário da Justiça eletrônico, disponibilizado em sítio da rede mundial de computadores, para publicação de atos judiciais e administrativos próprios e dos órgãos a eles subordinados, bem como comunicações em geral.
>
> [...]
>
> § 2º A publicação eletrônica na forma deste artigo substitui qualquer outro meio e publicação oficial, para quaisquer efeitos legais, à exceção dos casos que, por lei, exigem intimação ou vista pessoal.
>
> [...]
>
> § 5º A criação do Diário da Justiça eletrônico deverá ser acompanhada de ampla divulgação, e o ato administrativo correspondente será publicado durante 30 (trinta) dias no diário oficial em uso.

Esta mesma lei prevê em seu artigo 11, §7, uma certa restrição quanto ao acesso de processos por pessoas não vinculadas, desde

que demonstrem interesse para fins de registro. Entretanto, nada é mencionado sobre o acesso automatizado.

Quanto ao Código de Processo Civil, este prevê em seu artigo 193 que os atos processuais sejam produzidos, comunicados, armazenados e validados por meio eletrônico. Além disso também é garantida sua publicidade, com respectivo acesso e participação das partes e seus procuradores, inclusive facilitados por meio da acessibilidade e interoperabilidade dos sistemas, serviços, dados e informações que o Poder Judiciário administre (art. 194 e 195 do CPC).

A Resolução nº 121/2011 do Conselho Nacional de Justiça (CNJ) afirma que prescinde de cadastro a consulta a certos tipos de informações processuais, quais sejam: 1) número, classe e assunto do processo; 2) nome das partes e advogados; 3) movimentação processual; 4) inteiro teor das decisões, sentenças, votos e acórdãos (CUEVA, 2019, p. 137).

O acesso integral ao conteúdo dos autos pode ser feito pelas partes, por seus advogados e por membros do Ministério Público (MP) — todavia, ainda é prevista a possibilidade de advogados, procuradores e membros do MP acessarem a totalidade dos atos e documentos, mesmo sem habilitação no processo, mediante demonstração de interesse para fins de registro (CUEVA, 2019, p. 137). As consultas públicas dos sistemas processuais recebem algumas restrições em situações que envolvam processos criminais, após o trânsito em julgado da decisão absolutória, da extinção de punibilidade ou do cumprimento da pena; ou nos processos sujeitos à apreciação da Justiça do Trabalho (Art. 4º).

Além da previsão legislativa sobre a disponibilização de informações, há também algumas ressalvas quanto ao acesso automatizado. Vale citar, como exemplo, o que previa a Resolução n. 136/2014 do Conselho Superior da Justiça do Trabalho:

> Art. 38. O uso inadequado do sistema que cause redução significativa de sua disponibilidade poderá ensejar o bloqueio total do usuário, de forma preventiva ou temporária.

> § 1º Considera-se uso inadequado do sistema, para fins do caput deste artigo, as atividades que configurem ataques ou uso desproporcional dos ativos computacionais, devidamente comprovados.
>
> § 2º Na hipótese do caput, deverá ser procedido imediato contato com o usuário bloqueado para identificação da causa do problema e reativação no sistema e, em caso de advogado, a comunicação à respectiva Seccional da Ordem dos Advogados do Brasil.
>
> § 3º A automatização de consultas ao sistema deve ser feita mediante utilização do modelo nacional de interoperabilidade, previsto na Resolução Conjunta CNJ/CNMP nº 3, de 16 de abril de 2013

Esta resolução do CSJT permitia apenas a consulta automatizada mediante o modelo nacional de interoperabilidade,[15] restringindo o acesso ao Ministério Público, defensoria pública, advocacia pública ou advogado.[16] Dada a redação do §1º, é possível afirmar que práticas de web scraping e web crawling poderiam ser enquadradas como usos inadequados do sistema processual eletrônico trabalhista.

## 2.3 O papel do Conselho Nacional de Justiça

O Código de Processo Civil atribui ao Conselho Nacional de Justiça, através do artigo 196, a responsabilidade para regulamentar a prática e a comunicação oficial de atos processuais por meio eletrônico, disciplinando a incorporação progressiva de novos avanços tecnológicos e editando, para esse fim, os atos que forem necessários. Devido a isto, neste tópico iremos abordar a evolução das normas sobre o tema deste trabalho.

O Conselho Nacional de Justiça, através da Portaria Nº 63 de 26/04/2019, buscou definir um grupo de trabalho para tratar a política

[15] CONSELHO NACIONAL DE JUSTIÇA. Modelo Nacional de Interoperabilidade. Disponível em: https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/comite-nacional-de-gestao-de-tecnologia-da-informacao-e-comunicacao-do-poder-judiciario/modelo-nacional-de-interoperabilidade/

[16] CONSELHO NACIONAL DE JUSTIÇA. Tutorial MNI. Disponível em: https://www.cnj.jus.br/wiki/index.php/Tutorial_MNI#consultarProcesso

de acesso às bases de dados processuais dos tribunais, principalmente quando se trata de sua utilização para fins comerciais. Como fruto das discussões desse grupo, deu origem a recomendações aos tribunais sobre a Lei Geral de Proteção de Dados Pessoais (LGPD).[17] Outras preocupações relatadas pelo CNJ, quanto à tratativa dos dados do poder judiciário se refere a repercussões econômicas e de segurança[18].

Este assunto também foi tema de uma audiência pública, realizada em setembro de 2019, para colher sugestões que subsidiassem a política de acesso aos bancos de dados dos tribunais, em relação aos temas:

> **1)** Lei Geral de Proteção de Dados: direito à intimidade e anonimização;
>
> **2)** Critérios de acesso às bases de dados dos tribunais para a incorporação progressiva de novos avanços tecnológicos nos diversos setores do Sistema de Justiça: desafios da inovação;
>
> **3)** Os dados e as startups jurídicas;
>
> **4)** A proteção dos dados pessoais e o acesso aos processos judiciais não exclusivo a partes e advogados: academia, imprensa, etc.;
>
> **5)** Disponibilização de dados massivos e assimetria de acesso: em busca de modelos para compatibilizar demanda e recursos investidos;
>
> **6)** Lei Geral de Proteção de Dados: a figura do encarregado nos tribunais, composição, perfil, requisitos e vedações (artigo 5º, VIII, da LGPD).[19]

Fruto do trabalho da comissão do CNJ previamente citada, em agosto de 2020 o CNJ publicou a Recomendação Nº 73 de 20/08/2020, que orienta os órgãos do Poder Judiciário brasileiro sobre medidas

---

17 CONSELHO NACIONAL DE JUSTIÇA. CNJ prepara recomendação sobre proteção de dados. Disponível em https://www.cnj.jus.br/cnj-prepara-recomendacao-sobre-protecao-de-dados/

18 CONSELHO NACIONAL DE JUSTIÇA. Grupo inicia trabalho para regulamentar acesso a bases de dados do Judiciário. Disponível em: https://www.cnj.jus.br/grupo-inicia-trabalho-para-regulamentar-acesso-a-bases-de-dados-do-judiciario/

19 Audiência Pública sobre Política de Acesso às Bases de Dados Processuais dos Tribunais. Disponível em: https://www.cnj.jus.br/agendas/audiencia-publica-sobre-politica-de-acesso-as-bases-de-dados-processuais-dos-tribunais/

preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD, como instituir um padrão nacional de proteção de dados pessoais existentes nas suas bases. Para definição deste padrão, destacaram-se algumas atividades como **a)** plano de ação sobre direitos do titular, gestão de consentimento e retenção de dados e cópia de segurança; **b)** disponibilizar no site dos tribunais informações básicas sobre a aplicação da Lei Geral de Proteção de Dados aos tribunais, incluindo os requisitos para o tratamento legítimo de dados, as obrigações dos controladores e os direitos dos titulares; **c)** criação de formulário para exercício de direitos dos titulares de dados pessoais; **d)** elaborar política de privacidade para navegação no website da instituição em relação à Lei Geral de Proteção de Dados Pessoais; **e)** Registros de tratamentos de dados pessoais contendo finalidade, base legal, descrição dos titulares, categoria de dados e destinatários, prazo de conservação, entre outros.

As recomendações já passaram a ser observadas, por exemplo, pelo Tribunal de Justiça de São Paulo, que por meio da Portaria nº 9.918/2020, publicada em setembro de 2020, instituiu a Política de Privacidade e Proteção de Dados no Poder Judiciário do Estado de São Paulo.[20] Neste sentido, é possível constatar que o Conselho Nacional de Justiça poderá ser um importante ator na implementação de políticas de proteção de dados nos tribunais brasileiros.

## 3 ACESSO E PROCESSAMENTO DE DADOS DE PROCESSOS JUDICIAIS – ABORDAGEM TÉCNICA

Com as informações processuais disponibilizadas online, estes dados se tornaram objeto de interesse por empresas, profissionais da área e acadêmicos para acesso e processamento automatizado. A partir dos documentos e informações coletadas, pode-se utilizar diversos

[20] Cf. a íntegra da portaria em: https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=120680

sistemas de *web scraping* e *web crawling* para subsidiar a mineração de dados e texto, detectando padrões e inferindo novos dados.

Para fins de compreensão, abaixo podem ser verificadas duas imagens que representam o funcionamento de um *web crawler* (figura 1) e o funcionamento de um *web scraper* (figura 2).

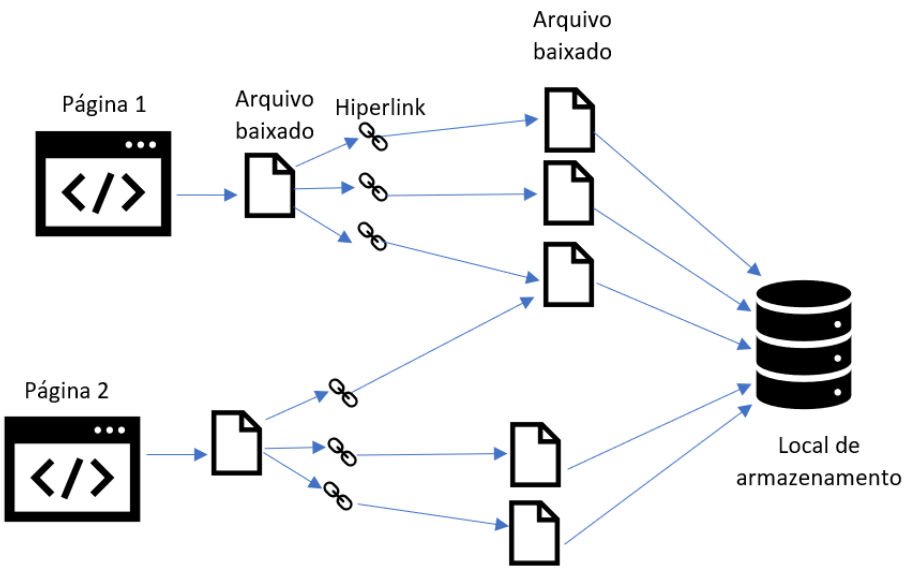



**Figura 1** - demonstra o funcionamento de um web crawler que busca armazenar a totalidade de páginas de um determinado site a partir dos hiperlinks existentes. Fonte: Própria.

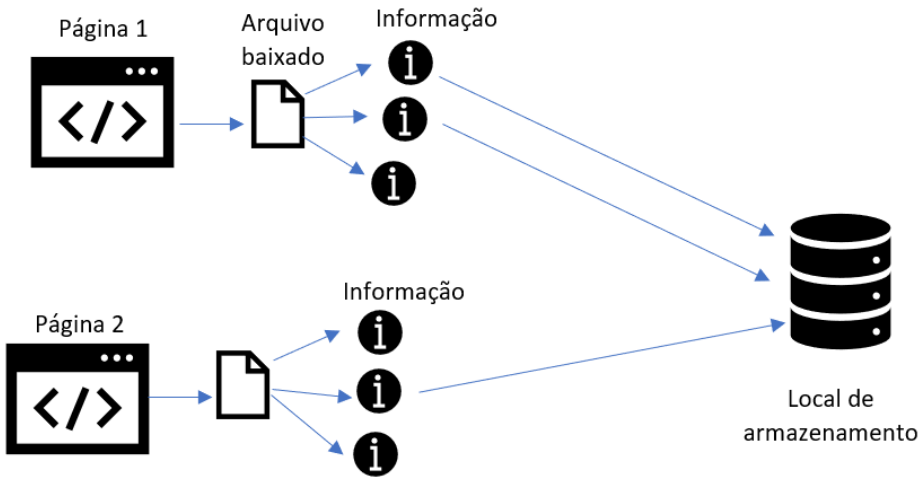



**Figura 2** - demonstra o funcionamento de um web scraper que busca baixar um conjunto de páginas pré-determinado que podem conter as informações específicas buscadas. O web scraper pode se utilizar, opcionalmente, da busca por hiperlinks ou ainda buscar as informações a partir de um conjunto de arquivos já baixados pelo web crawler. Fonte: Própria.

Um exemplo prático, no contexto de sites de tribunais cujo objetivo é obter decisões dos tribunais, seria identificar qual página contém publicamente as decisões, ou ainda um sistema de busca que permite encontrá-las. Após a identificação dessa página, verifica-se como o tribunal disponibiliza as urls (endereços) das decisões.

Para fins exemplificativos, cita-se a página do Superior Tribunal de Justiça, que disponibiliza sua busca de decisões a partir da página "Jurisprudência do STJ".[21] A partir dessa página é possível verificar dois hiperlinks para cada decisão encontrada, permitindo-se visualizar a íntegra do acórdão (arquivo HTML) ou baixá-lo em formato PDF. Com

[21] SUPERIOR TRIBUNAL DE JUSTIÇA. Jurisprudência do STJ. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp

essas informações e conhecimento de programação para automatizar essa rotina, é possível executar os passos da figura 1, ao fim dos quais terão sido baixados todos os arquivos de decisões.

Se por algum motivo, não desejássemos ter a íntegra das decisões e apenas o número do processo e o nome do relator, executaríamos os passos da figura 2, em que, além de baixar essa página, esta seria lida em busca dessas informações específicas que seriam armazenadas, descartando-se o resto.

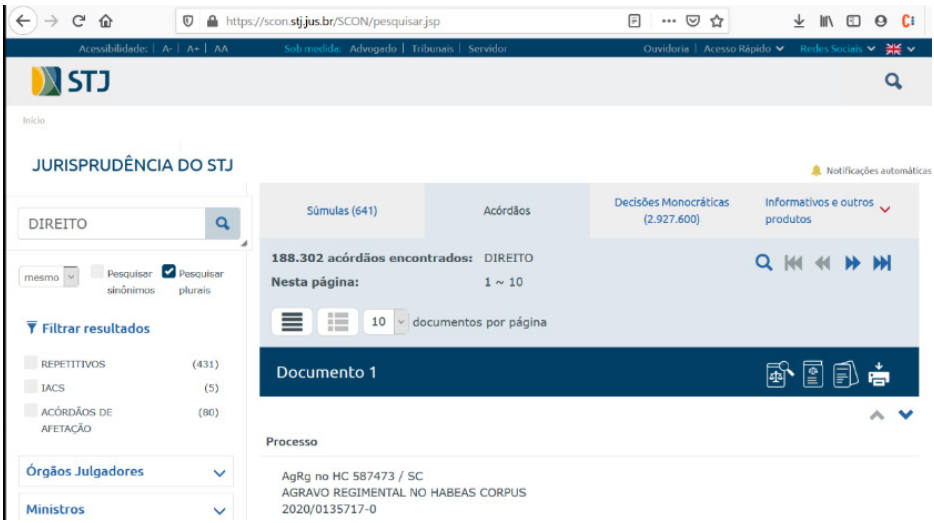



**Figura 3** - Sistema de busca do Superior Tribunal de Justiça e formas como são disponibilizados os acórdãos. Fonte: Site do STJ.

## 4 ACESSO E PROCESSAMENTO DE DADOS DE PROCESSOS JUDICIAIS – ABORDAGEM JURÍDICA

Como exposto anteriormente, as políticas de acesso aos dados constantes em decisões e processos judiciais podem consubstanciar violações aos direitos à privacidade e proteção de dados. A utilização comercial dos dados pessoais, por exemplo, possibilita o perfilamento das pessoas envolvidas em processos judiciais. O perfilamento, ou

*profiling*, consiste na construção de perfis ou modelos determinísticos relacionados com dados pessoais (CARVALHO et al, 2020, p. 80). No que tange ao tema do presente artigo, o perfilamento poderia ser realizado a partir do nome das partes, juízes, advogados que constem na decisão judicial e seu respectivo conteúdo.

Estes e outros problemas demandam uma postura regulatória pautada em princípios[22] e atenta à necessidade de ponderação entre transparência jurisdicional e privacidade dos cidadãos. Neste sentido, cumpre tecer algumas considerações sobre a experiência europeia e os futuros desafios brasileiros no tema sob análise.

A experiência da União Europeia: a anonimização pode ser um caminho?

No âmbito da União Europeia percebem-se distintas abordagens à publicidade dos atos processuais, considerando a pluralidade de Estados que a integram. A maior parte de seus Estados-membros mantêm uma postura de seleção *negativa* das decisões a serem publicadas: a regra é sua divulgação, excetuadas algumas situações ou categorias de decisão previstas em lei. A postura minoritária, adotada por cerca de um quinto dos Estados-membros, é a de seleção *positiva*, segundo a qual somente devem ser publicadas as decisões que atenderem a certos requisitos previstos em lei. (BO-ECLI, 2017).

A coleta e processamento de dados judiciais eletrônicos no âmbito europeu é objeto de debates datados e mais aprofundados do que os observados no Brasil. A padronização dos registros de processos judiciais no continente é promovida por meio do *European Case-Law Identifier*, um formato de estruturação de metadados sobre decisões. Neste sentido,

[22] Vale mencionar os princípios da Inteligência Artificial levantados por um grupo de pesquisadores nesta área, denominados Asilomar AI principles. Ao todo, 23 princípios são elencados, mas de acordo com o estudo de caso discutido neste artigo – acesso, armazenamento e processamento automatizado de decisões judiciais – cita-se os que têm relação com o tema: a) transparência judiciária; b) valores humanos; c) privacidade pessoal; e d) liberdade e privacidade. Apesar da proposta deste artigo não envolver diretamente Inteligência Artificial, ele envolve a obtenção e tratamento de dados que podem subsidiar um sistema deste tipo. Cf.: https://futureoflife.org/ai-principles/

busca-se construir um protocolo comum de referências a julgamentos por tribunais de diferentes países, para facilitar a busca, citação e intercâmbio de tais documentos (OPIJNEN, 2011).

O projeto *Building on ECLI*, co-fundado com a União Europeia e ativo entre 2015 e 2017, acompanhou a implementação do ECLI nos Estados-membros, emitiu relatórios sobre o padrão e o promoveu junto a juristas e profissionais de TI (OPIJNEN, 2019, p. 82-83). Em um de seus relatórios, o projeto apontou alguns aspectos da proteção de dados pessoais na publicação de decisões, dando especial ênfase às práticas de anonimização[23] na sua 12ª Recomendação: «em princípio, todas as decisões judiciais publicadas na Internet deveriam ser anonimizadas» (BO-ECLI, 2017, p. 148, tradução nossa).

Na prática, vários países europeus já anonimizam há algum tempo as decisões,[24] tendo em vista que a exposição dos dados pessoais das partes do processo não cumprem os principais propósitos da publicidade das decisões: a transparência do processo decisório e a divulgação de avanços jurisprudenciais (OPIJNEN, 2019, p. 85). A opção pelo termo anonimização, todavia, é questionável,[25] pois ainda há possibilidade de reidentificar as partes por meio de «quase-identificadores» (*quasi-identifiers*),[26] por exemplo; dito isto, na maior parte dos casos ocorre

[23] Anonimização é o processo que busca eliminar de uma base de dados os elementos identificadores de pessoas naturais, por meio de técnicas como: supressão, generalização, randomização e, de modo incompleto, a pseudonimização, que para muitos não chega a ser considerada uma técnica de anonimização (BIONI, 2020, p. 62).

[24] Em 2017, dentre os países da UE apenas a Grécia não tinha alguma forma de anonimização nas decisões de suas jurisdições civil/criminal. Cerca de 70% dos países tinham alguma forma de anonimização nas jurisdições constitucionais e administrativas (BO-ECLI, 2017, p. 23)

[25] Por teoricamente não identificar uma pessoa natural, um dado anonimizado não é considerado um dado pessoal, inclusive no texto da LGPD. Deve-se notar, todavia, que é extremamente difícil (senão impossível) uma completa e irreversível anonimização de um dado (BIONI, 2020, p. 63-65).

[26] Um «quase identificador» (*quasi-identifier)* é uma combinação de atributos que pode levar indiretamente à identificação de um indivíduo; se analisados o contexto do caso, seu desfecho («culpado/inocente», por exemplo), e informações genéricas sobre as partes do processo (idade, gênero, estado civil etc.) é possível reidentificar o titular dos dados (ALLARD; BÉZIAUD; GAMBS, 2020, p. 3).

somente a pseudonimização dos dados. Não obstante a possível imprecisão conceitual, as técnicas empregadas servem para, ao menos, tornar menos explícita a relação da decisão com as partes cujos dados foram ocultados: isto impede, a título de exemplo, que uma busca por um nome na Internet retorne dentre os resultados uma decisão judicial.

Entretanto, conforme menciona-se em um relatório da organização de pesquisa brasileira *Lawgorithm*, o momento em que se deve se realizar o procedimento não é algo uníssono entre os Estados-membros da União Europeia:

> Muito embora a prática de anonimização seja generalizada entre os países-membro, há diferenças quanto a sua política, i.e. se a anonimização ocorre por padrão (default) ou por decisão judicial, ex officio ou mediante requisição das partes. (MARANHÃO, 2020, p. 20)

Em 2019, a França publicou uma lei que gerou repercussão mundial, principalmente entre os pesquisadores de dados do poder judiciário. A Lei Francesa n. 2019-222, apesar de continuar mantendo as decisões judiciais públicas, impacta as aplicações referentes à justiça preditiva. No artigo 33, a referida Lei incluiu cláusulas sobre a ocultação do nome das partes e terceiros nas decisões e a ocultação de elementos que permitam identificar as partes, onde se incluem os juízes e membros do cartório, quando suscetível de comprometer a segurança e privacidade destes.

A ocultação do nome dos juízes se dá pela justificativa abaixo e ainda prevê sanções no caso de realizada:

> Os dados de identidade dos magistrados e membros do cartório não podem ser reutilizados com o objetivo ou efeito de avaliar, analisar, comparar ou prever as suas reais ou supostas práticas profissionais. A violação desta proibição é punível com as penas previstas nos artigos 226-18, 226-24 e 226-31 do Código Penal, sem prejuízo das medidas e sanções previstas na Lei n.º 78-17 de 6 de Janeiro de 1978 relativa às tecnologias da informação, arquivos e liberdades. (Tradução nossa).

Pelo que também se verifica nesta lei, a realização de *web scraping* e *web crawling* nesses casos pode ser ilícita por sua natureza repetitiva e sistemática, de acordo com o seguinte trecho:

> Art. L. 10-1.-Terceiros podem obter cópia das sentenças, sob reserva de pedidos abusivos, nomeadamente pelo seu número ou pela sua natureza repetitiva ou sistemática.
>
> Os elementos que permitem a identificação das pessoas singulares referidas na sentença, quando são partes ou terceiros, são ocultados se a sua divulgação for suscetível de infringir a segurança ou o respeito pela vida privada dessas pessoas ou dos seus comitiva. (Tradução nossa).

Dada a natureza restritiva da legislação francesa, apesar de proibir a construção de perfis estatísticos de magistrados, esta não proíbe a realização de estatísticas por tribunal. Portanto, ainda que não se realize o perfilamento decisional de cada magistrado, as orientações de cada corte seguem passíveis de quantificação.

## 4.1 A Lei Geral de Proteção de Dados e o dilema brasileiro

Expostos alguns aspectos do cenário europeu, cumpre abordar a legislação brasileira de proteção de dados. Preliminarmente, é necessário destacar as hipóteses de tratamento de dados pessoais que fundamentariam o tratamento de dados processuais por terceiros.

As hipóteses amplas para os tratamentos são previstas no artigo 7º da LGPD. Dentre estas, mostra-se relevante a possibilidade de tratamento para a realização de estudos por órgãos de pesquisa, o que viabilizaria, por exemplo, novos estudos jurimétricos com base em decisões judiciais. Conquanto seja em tal hipótese garantida sempre que possível a anonimização dos dados pessoais, trata-se de uma anonimização *a posteriori*, dado que a decisão utilizada, quando tornada

pública, não realizara tal procedimento. É imperioso, portanto, que o direito brasileiro passe a se atentar à possibilidade de anonimizar ou pseudonimizar os dados pessoais no conteúdo das decisões, conforme mostra a experiência europeia.

De todo modo, o tratamento de dados pessoais de acesso público é também referido pela LGPD. Em especial, cabe evidenciar o que dispõe o Art. 7, §§ 3º e 7º:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
>
> § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

Como aponta Marcel Leonardi, os *dados de acesso público* são aqueles cuja divulgação pública é obrigatória por lei (INTERNETLAB, 2016). Aqui reside, portanto, sua diferença em relação a categorias como os *dados manifestamente públicos*, por exemplo.[27] Deste modo, é possível concluir que o tratamento dos dados pessoais oriundos de decisões judiciais pode ser enquadrado na previsão do Art. 7º, §3º.

Deste modo, o terceiro que realizar o tratamento destes dados adquire o dever de considerar a finalidade e o interesse público que justificaram sua disponibilização. Ainda deve se observar a boa-fé, caracterizada, *in casu*, pelo atendimento às legítimas expectativas dos

[27] «Em termos conceituais, dados de acesso público são distintos dos manifestamente públicos. Neste último, a disponibilização da informação se daria por iniciativa do próprio titular e não por terceiros e, por fim, o seu acesso não teria qualquer tipo de restrição» (BIONI, 2020, p. 257).

titulares (LIMA, 2019, p. 187). Sobre o tratamento de dados de acesso público, transcreve-se pertinente lição de Bruno Bioni:

> Em todos esses casos, o que define a (i)legalidade do tratamento dos dados é a sua *compatibilidade* com a finalidade e o interesse público pelo qual tais dados são de acesso público. É necessária, portanto, uma *análise contextual* para saber por que houve publicização da informação, o que calibrará os possíveis (re)usos que dela podem ser feitos (BIONI, 2020, p. 257).

A argumentação de Bioni indica que, no caso analisado no presente artigo, posteriores tratamentos devem observar a finalidade que motivou a divulgação dos dados pessoais: o princípio constitucional da publicidade dos atos processuais. Se este, como visto anteriormente, surge para garantir a transparência da atividade jurisdicional, é difícil avaliar em que situações isto fundamentaria o tratamento dos dados pessoais por terceiros. E mesmo antes disso, a exposição de dados pessoais decorrente da divulgação de uma decisão, em grande parte dos casos, não é indispensável para a consecução da finalidade desta publicação.[28] Desta forma, surgem dúvidas quanto à possibilidade de violações ao princípio da necessidade[29] e da prevenção.[30]

---

[28] O que reforça a viabilidade da anonimização como paliativo no conflito entre a publicidade dos atos judiciais e a proteção de dados pessoais: "[...] most civil law countries have always followed a strict anonymisation policy for public databases, generally based on the view that personal data of applicants, defendants and witnesses do not serve the primary goals of publication: transparency of the judicial decision process and spreading knowledge about jurisprudential developments." (OPIJNEN, 2019, p. 85).

[29] Princípio que remonta à doutrina alemã de proteção de dados pessoais, sendo elencado no artigo 6º, III, da LGPD como um dos princípios para o tratamento de dados pessoais no Brasil. Conforme ensina DONEDA (2011, p. 1146): "[os] riscos inerentes ao tratamento de dados pessoais fizeram com que fosse desenvolvida a noção pela qual esta atividade deva ser realizada somente quando seus objetivos não possam ser obtidos de forma alternativa. Daí resultou a formulação do princípio da necessidade, que vincula o tratamento ao fato de este ser indispensável para a consecução de sua finalidade".

[30] Princípio definido no Art. 6º, VIII da LGPD como "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais". A exposição massiva poderia, neste sentido, possibilitar posteriores abusos.

## 5 CONSIDERAÇÕES FINAIS

Feita a argumentação acima, nota-se que a Lei Geral de Proteção de Dados deverá gerar impasses quando em conflito com o dever de transparência do poder público. No presente artigo, deu-se um enfoque ao princípio da publicidade dos atos processuais, que visa a possibilitar o controle da atividade jurisdicional pela população, impedindo abusos por magistrados e permitindo o acompanhamento de avanços jurisprudenciais.

Consoante supracitado, este princípio de previsão constitucional e infraconstitucional só é afastado para tutelar a intimidade em casos excepcionais, e não como regra. Mas com a crescente informatização do processo judicial brasileiro, fenômeno observável há mais de uma década, a intimidade passa a ser passível de violações outrora inimagináveis.

O uso abusivo das técnicas de *web scraping* e *web crawling* parece encontrar um terreno fértil com a ampla divulgação de dados pessoais em decisões judiciais públicas e, em certos casos, outros documentos processuais. Estas duas técnicas computacionais possibilitam a extração de informações presentes em páginas *web*: por meio do *crawling*, vasculham-se as relações entre *hyperlinks* contidos nas páginas, de modo a baixá-las em grande quantidade; por meio do *scraping*, analisa-se o conteúdo de cada página individualmente, encontrando em sua estrutura interna informações relevantes.

Tais algoritmos podem ser utilizados para diversas finalidades, muitas delas benignas. Por exemplo, o projeto Brasil.IO se utiliza deles para realizar a coleta de dados disponibilizados por órgãos públicos, buscando estruturá-los de modo "amigável" para serem consultados pela população geral.[31] O controle de arbitrariedades na atividade jurisdicional por meio da análise dos dados judiciais é também algo positivo. Sob outro aspecto, todavia, é questionável a divulgação irrestrita dos dados

[31] Em muitos casos, porém, os dados são dispostos de maneira que dificulta seu tratamento, o que demanda certa cautela e, frequentemente, pedidos fundamentados na Lei de Acesso à Informação. Cf. https://brasil.io/manifesto/

pessoais das partes, sobretudo quando desnecessária para a consecução da finalidade do tratamento, o que configuraria violação ao princípio da necessidade previsto na LGPD.

A partir do texto exposto, verifica-se que a experiência europeia pode servir como um ponto de partida para uma inserção mais qualificada deste debate no ordenamento brasileiro. O uso de técnicas de anonimização e pseudonimização em boa parte dos tribunais europeus já é presente em boa parte dos Estados-membros da União Europeia há muitos anos. Apontou-se nesta investigação que, por meio de tais técnicas, torna-se viável resguardar a intimidade das partes, o que não obstaria a divulgação da decisão para a concretização do princípio da publicidade. Atentar-se à trajetória europeia é algo imperioso para aqueles atentos à construção de uma cultura de proteção de dados pessoais no Brasil. A transferência internacional de dados, por exemplo, é imprescindível à inserção do país no cenário globalizado da sociedade informacional.

A legislação brasileira, ao abordar o tratamento de dados pessoais de acesso público, aponta o dever de observância da finalidade que originou sua divulgação. Contudo, como apontado, o princípio da necessidade previsto na LGPD levanta dúvidas quanto à imprescindibilidade da exposição de dados pessoais nestes casos, em especial quando seu acesso pelo público geral ocorre sem quaisquer restrições. O desenvolvimento e a resolução destas e outras questões deverão ser observados nos próximos anos, com a criação da Autoridade Nacional de Proteção de Dados e com novas orientações do Conselho Nacional de Justiça.

## REFERÊNCIAS

ALLARD, Tristan; BÉZIAUD, Louis; GAMBS, Sébastien. **Online publication of court records**: circumventing the privacy-transparency trade-off. [S.l.], 2020. Disponível em: https://arxiv.org/abs/2007.01688. No prelo.

ASILOMAR CONFERENCE. **Asilomar AI principles**. Future of Life Institute, 2017. Disponível em: https://futureoflife.org/ai-principles/

BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BO-ECLI. **On-line publication of court decisions in the EU**: Report of the policy group of the project «Building on the European Case Law Identifier». [s.l.], 2017.

CARNEIRO, João Víctor Vieira. Proteção de dados pessoais e direito à informação: impasses na gestão de arquivos públicos e o caso dos documentos da ditadura (1964-1985). **Revista do Arquivo do Estado de São Paulo**, n. 9, p. 52-59, 2019.

CARVALHO, Luiz Paulo; OLIVEIRA, Jonice; CAPPELLI, Claudia. **Pesquisas em Análise de Redes Sociais e LGPD**: análises e recomendações. In: BRAZILIAN WORKSHOP ON SOCIAL NETWORK ANALYSIS AND MINING (BRASNAM), Porto Alegre: Sociedade Brasileira de Computação, p. 73-84, 2020.

CHANDRIKA, G.; RAMASUBBAREDDY, Somula; GOVINDA, Kharisma; SWETHA, E... **Web Scraping for Unstructured Data Over Web**. Embedded Systems and Artificial Intelligence. Advances in Intelligent Systems and Computing, v. 1076. Singapore: Springer, pp.853-859, 2020.

CINTRA, Antonio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. **Teoria Geral do Processo**. 27. ed. São Paulo: Malheiros, 2011.

CONSELHO NACIONAL DE JUSTIÇA. **Audiência Pública sobre Política de Acesso às Bases de Dados Processuais dos Tribunais**. Disponível em: https://www.cnj.jus.br/agendas/audiencia-publica-sobre-politica-de-acesso-as-bases-de-dados-processuais-dos-tribunais/

CONSELHO NACIONAL DE JUSTIÇA**. Grupo inicia trabalho para regulamentar acesso a bases de dados do Judiciário**. Disponível em: https://www.cnj.jus.br/grupo-inicia-trabalho-para-regulamentar-acesso-a-bases-de-dados-do-judiciario/

CONSELHO NACIONAL DE JUSTIÇA**. CNJ prepara recomendação sobre proteção de dados.** Disponível em: https://www.cnj.jus.br/cnj-prepara-recomendacao-sobre-protecao-de-dados/

CONSELHO NACIONAL DE JUSTIÇA. **Justiça em Números 2020**. Relatório (ano-base 2019). Brasília: CNJ, 2020. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2020/08/WEB-V3-Justi%C3%A7a-em-N%C3%BAmeros-2020-atualizado-em-25-08-2020.pdf

CONSELHO NACIONAL DE JUSTIÇA. **Modelo Nacional de Interoperabilidade**. Disponível em https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/comite-nacional-de-gestao-de-tecnologia-da-informacao-e-comunicacao-do-poder-judiciario/modelo-nacional-de-interoperabilidade/

CONSELHO NACIONAL DE JUSTIÇA. **Portaria Nº 63 de 26/04/2019**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/2890.

CONSELHO NACIONAL DE JUSTIÇA. **Tutorial MNI**. Disponível em: https://www.cnj.jus.br/wiki/index.php/Tutorial_MNI#consultarProcesso

CUEVA, Ricardo Villas Bôas. Proteção de Dados Pessoais no Judiciário. **Revista do Advogado**, n. 144, p. 134-140, nov. 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, 2011.

DONEDA, Danilo. Princípios de proteção de dados pessoais. In: TORRES, R.; GALDINO, F.; KATAOKA, E. (orgs.). **Dicionário de princípios jurídicos**. Rio de Janeiro: Elsevier, p. 1141-1148, 2013.

HEXSEL, Roberto A. **Software Livre**: propostas de ações de governo para incentivar o uso de software livre. Curitiba: Universidade Federal do Paraná, 2002. Disponível em: http://www.inf.ufpr.br/ppginf/Relatorios_Tecnicos/RT_DINF004_2002.pdf

INTERNETLAB. **O que são dados públicos?** 13 jul 2016. Disponível em: https://www.internetlab.org.br/pt/opiniao/o-que-sao-dados-publicos/

LANGENEGGER, Natalia; GOBBATO, Andréa. Compatibilização da Lei de Acesso à Informação com a Lei Geral de Proteção de Dados Pessoais: desafios no âmbito do Poder Judiciário. **Revista do Advogado**, v. 39, n. 144, 2019.

LEGRAND, Pierre. **Como ler o direito estrangeiro**. Tradução por D. W. Hachem. São Paulo: Contracorrente, 2018.

LIMA, Caio César Carvalho. Do tratamento de dados pessoais. In: MALDONADO, V. N.; BLUM, R. O. (coords.). **LGPD:** Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, p, 179-214, 2019.

MAGALHÃES, R.V. Inteligência artificial e direito – uma breve introdução histórica. **Revista Direito e Liberdade**, v. 1, n. 1, p. 335-370, 2010.

MARANHÃO, Juliano (coord.)**. Acesso a dados de processos judiciais no Brasil**. São Paulo: Lawgorithm, jul. 2020. Disponível em: https://lawgorithm.com.br/wp-content/uploads/2020/08/ReportAcessoDadosJudiciario20200731.pdf

MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro**. 42. ed. São Paulo: Malheiros, 2016.

OLSTON, Christopher; NAJORK, Marc. Web Crawling. **Foundations and Trends in Information Retrieval**, v. 4, n. 3, pp. 175–246, 2010.

OPIJNEN, Marc van. European Case Law Identifier: indispensable asset for legal information retrieval. In: BIASIOTTI, M. A.; FARO, S. (eds.). **From Information to Knowledge - Online Access to Legal Information**: Methodologies, Trends and Perspectives. Amsterdam: IOS, p. 91-103, 2011.

OPIJNEN, Marc van. The EU Council Conclusions on the Online Publication of Court Decisions. In: PERUGINELLI, G.; FARO, S. (eds.). **Knowledge of the Law in the Big Data Age:** Frontiers in Artificial Intelligence and Applications. Amsterdam: IOS, p. 81-90, 2019.

PEGORARO JUNIOR, Paulo Roberto. **O processo eletrônico e a evolução disruptiva do direito processual civil**. Curitiba: Juruá, 2019.

RAYMOND, Eric. The Cathedral and the Bazaar. **Knowledge, Technology & Policy**, v. 12, n. 3, pp. 23-49, 1999.

SALGADO, Eneida Desiree. **Princípio da publicidade.** In: CAMPILONGO, C. F.; GONZAGA, A. A.; FREIRE, A. L. (coords.). Enciclopédia jurídica da PUC-SP. São Paulo: PUC-SP, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/37/edicao-1/principio-da-publicidade

SERBENA, Cesar Antonio. A título de introdução: o desafio da interoperabilidade do processo eletrônico no Brasil. In: SERBENA. C. A. (Coord.). **Interoperabilidade dos Sistemas de Processo Eletrônico no Brasil**. Curitiba: E-Justiça UFPR, 2017, p. 07-10.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Jurisprudência do STJ**. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp

STALLMAN, Richard**. Why Open Source misses the point of Free Software**. In: ___. Free Software, free society: Selected essays of Richard M. Stallman. Boston:

Free Software Foundation, 2002, p. 75-82. Disponível em: http://www.gnu.org/doc/Press-use/fsfs3-hardcover.pdf

VERONESE, Alexandre; MELO, Noemy. O Projeto de Lei 5.276/2016 em contraste como Novo Regulamento Europeu (2016/679 UE). **Revista de Direito Civil Contemporâneo**, v. 14, p. 71-72, 2018.

YARSHELL, Flavio Luiz. **Curso de Direito Processual Civil.** São Paulo: Marcial Pons, 2014.

# Seção V

## Transferência internacional de dados: extraterritorialidade e elementos de conexão

# Capítulo I

# TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS: A extraterritorialidade do RGPD europeu e seus impactos

*Bruna Homem de Souza Osman*[1]

*Jessica Aparecida Soares*[2]

## SUMÁRIO



## RESUMO

O estudo trata sobre a extraterritorialidade do RGPD da União Europeia quando da transferência internacional de dados pessoais a partir da decisão Schrems II do Tribunal de Justiça da União Europeia (TJUE) e analisar suas possíveis influências na LGPD brasileira. Utiliza da análise comparada para identificar diferenças e similaridades entre as legislações da União Europeia e do Brasil relacionadas a proteção e transferência internacional de dados pessoais. Identifica-se que a LGPD tem influências do RGPD, com semelhantes mecanismos de salvaguarda para a transferência transfronteiriças de dados pessoais, assegurando proteção aos titulares de dados além dos limites de seu território. Identifica na LGPD os mesmos embasamentos presentes na decisão Schrems II, que são suficientes para questionar e invalidar fluxo de dados pessoais transfronteiriços do Brasil para os Estados Unidos ou para outros países terceiros. Assim até que existam Tratados Internacionais que harmonizem conflitos relacionados às transferências transnacionais de dados e sua respectiva proteção, entende-se que o Brasil poderá caminhar em diversos sentidos, inclusive aplicar a LGPD por extensão territorial, para garantir aos titulares de dados maior efetividade dos seus direitos e maior segurança jurídica na ordem internacional.

**Palavras-chaves:** Dados pessoais; transferência internacional; extraterritorialidade; Regulamento Geral de Proteção de Dados (RGPD).

[1] Advogada. Mestra em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie (2017). Professora do Centro Universitário Dinâmica das Cataratas - UDC. Pesquisadora do Grupo de Estudos em Direito Autoral e Industrial (GEDAI).

[2] Mestra em Sociedade, Cultura e Fronteiras pela Universidade Estadual do Oeste do Paraná - UNIOESTE (2017). Professora das Faculdades Unificadas de Foz do Iguaçu – UNIFOZ. Pesquisadora do Grupo de Estudos em Direito Autoral e Industrial (GEDAI).

## INTRODUÇÃO

No que tange ao ambiente digital existe atualmente circulação de dados pessoais que ultrapassam as fronteiras territoriais dos países. O Regulamento 2016/679 do Parlamento Europeu e do Conselho, denominado como Regulamento Geral de Proteção de Dados (RGPD) da União Europeia (UE) reconhece a transferência de dados pessoais para países não pertencentes à UE.

Da mesma forma, no Brasil, a Lei n° 13.709/18, também denominada como Lei Geral de Proteção de Dados (LGPD) existe a previsão sobre o fluxo transfronteiriço de dados.

O RGPD e a LGPD são legislações similares, no entanto, é possível identificar em cada qual especificidades que visam garantir, tanto no território da UE quanto do Brasil, a partir do cumprimento de determinados requisitos, a proteção aos dados pessoais na transferência internacional de dados.

Recentemente a sentença proferida pelo Tribunal de Justiça da União Europeia (TJUE) no processo C-311/18 (*Schrems II*) garante que os mecanismos e as garantias de proteção de dados pessoais do RGPD sejam aplicados nas transferências transfronteiriças de dados à países terceiros.

Assim, analisa-se na presente pesquisa os efeitos da aplicação do RGPD em âmbito extraterritorial, bem como os impactos da decisão *Schrems II* para países terceiros. Da mesma forma é realizada a análise em relação aos impactos da decisão *Schrems II* nas transferências internacionais de dados pessoais entre Brasil e os Estados Unidos.

Como objetivo pretende-se refletir sobre a extraterritorialidade do RGPD quando da transferência internacional de dados pessoais a partir da decisão *Schrems II* do TJUE e analisar suas possíveis influências na Lei Geral de Proteção de Dados em vigência no Brasil.

Para tanto, investiga-se os principais instrumentos legislativos europeus em matéria de proteção de dados pessoais e as fontes da extraterritorialidade do Regulamento Geral de Proteção de Dados (RGPD). Verifi-

ca-se o conceito de extraterritorialidade e o âmbito de aplicação material e territorial do RGPD. Estuda-se a invalidação do acordo *Safe Harbor* e a invalidação do acordo *Privacy Shield*, para ser possível apreender os impactos destas decisões em países terceiros, como no caso do Brasil.

A partir destas colocações surge a pergunta norteadora: Em que medida a decisão proferida pelo Tribunal de Justiça da União Europeia (TJUE) no processo C-311/18 (*Schrems II*) amplia a extraterritorialidade do Regulamento Geral de Proteção de Dados (RGPD) vigente na União Europeia e quais os seus impactos em países terceiros?

Como hipótese tem-se que com a aplicação dos mecanismos e garantias do RGPD é evidenciada a ampliação da territorialidade da União Europeia.

A pesquisa, quanto à metodologia, baseia-se em estudo de caso, com emprego de acórdãos de Tribunais relacionados à temática em exame, como também é aplicada a técnica bibliográfica, sendo utilizados livros, artigos e legislação. Ainda se emprega a análise comparada para identificar diferenças e similaridades entre as legislações da União Europeia e do Brasil relacionadas a proteção e transferência de dados pessoais.

## 1 PRINCIPAIS INSTRUMENTOS LEGISLATIVOS EUROPEUS EM MATÉRIA DE PROTEÇÃO DE DADOS PESSOAIS E FONTES DA EXTRATERRITORIALIDADE DO REGIME GERAL DE PROTEÇÃO DE DADOS

Inicialmente o estudo analisa os primórdios da sistemática de proteção de dados na Europa vez que esta reflete na atual ordenação de proteção de dados da União Europeia, a qual abrange inclusive a transferência internacional de dados pessoais.

Em especial após a Segunda Guerra Mundial, em uma "sociedade mundializada que se caracteriza por mudanças tecnológicas rápidas" (PARLAMENTO EUROPEU, 2020), desperta na Europa uma particular atenção para a proteção das pessoas no ambiente privado e familiar, de forma

que passaram a ser necessárias proteções para os seres humanos a fim de que as pessoas ficassem resguardadas de intromissões estatais.

Neste contexto europeu, evidenciaram-se alguns instrumentos, como por exemplo a Convenção Europeia dos Direitos do Homem (CEDH), assinada em 4 de novembro de 1950 em Roma – com vigência a partir de 1953 - , que é um tratado internacional ao abrigo do qual os Estados Membros do Conselho da Europa[3] garantem os direitos fundamentais, civis e políticos, não apenas aos seus próprios cidadãos, mas também a qualquer pessoa que se encontre sob sua jurisdição.

O artigo 8º[4] da CEDH consagra o direito ao respeito pela vida privada e familiar, pela inviolabilidade do domicílio e de correspondência, assim corrobora incontinente com a manutenção da privacidade do ser humano e com a não intervenção estatal nesta esfera.

Outro mecanismo é a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, que foi o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados. Visa garantir a todas as pessoas singulares "[...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal que lhes digam respeito (proteção dos dados)" (CONSELHO DA EUROPA, 1981).

---

[3] O Conselho da Europa foi fundado em 1949 tendo Bélgica, Dinamarca, França, Irlanda, Itália, Luxemburgo, Países Baixos, Noruega, Suécia e Reino Unido como Estados membros, atualmente integra 47 Estados membros que ratificaram a Convenção Europeia dos Direitos do Homem.

[4] O artigo 8º da Convenção Europeia dos Direitos do Homem (CEDH) dispõe sobre o direito ao respeito pela vida privada e familiar, estabelecendo que "qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência", ainda com previsão de que "não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros" (CORTE EUROPEIA DOS DIREITOS HUMANOS, 1950).

O documento, "além de fornecer garantias em relação à coleta e processamento de dados pessoais, [...] proíbe o processamento de dados sensíveis sobre raça, política, saúde, religião, vida sexual, antecedentes criminais, etc., na ausência de salvaguardas legais"(CONSELHO DA EUROPA, 1981).

A partir das garantias listadas acima, esta "Convenção também consagra o direito do indivíduo de saber que as informações sobre ele são armazenadas e, se necessário, de corrigi-las. As restrições aos direitos consagrados na Convenção só são possíveis quando interesses superiores (por exemplo, segurança do Estado, defesa, etc.) estão em jogo" (CONSELHO DA EUROPA, 1981).

Ressalta-se que a Convenção 108 do Conselho da Europa visa evitar abusos da coleta e tratamento de dados pessoais e é o primeiro instrumento "[...] internacional vinculativo que impõe algumas restrições aos fluxos transfronteiriços de dados pessoais para Estados onde a regulamentação legal não oferece proteção equivalente" (CONSELHO DA EUROPA, 1981).

A Convenção 108 está em vigência até a presente data e não se limitou somente aos 47 Estados membros do Conselho da Europa, mas também a não membros do Conselho da Europa, ou seja, Argentina, Burkina Faso, Cabo Verde, Ilhas Maurício, México, Marrocos, Senegal, Tunísia (CONSELHO DA EUROPA, 2020).

Salienta-se que com a vigência plena do Regulamento Geral de Proteção de Dados (RGPD) 2016/679, a Convenção 108 de 1981 está sendo revisada para a adequação ao RGPD, com o intuito de alargar o seu âmbito de aplicação, aumentar o nível de proteção de dados e melhorar a sua eficácia.

De grande relevância a Carta dos Direitos Fundamentais da União Europeia (CDFUE) de 18 de dezembro de 2000 que prioriza o ser humano e baseia-se "[..] nos valores indivisíveis e universais da dignidade do ser humano, da liberdade, da igualdade e da solidariedade", da mesma maneira é assentada "nos princípios de democracia e do Estado de direito"

e visa criar "um espaço de liberdade, de segurança e de justiça", em especial, "à luz da evolução da sociedade, do progresso social e da evolução científica e tecnológica" (PARLAMENTO EUROPEU, 2000).

Frente a estes princípios e valores, os artigos 7° e 8°[5] da CDFUE reconhecem o respeito pela vida privada e proteção dos dados pessoais como direitos fundamentais estritamente relacionados, mas distintos.

Em relação a Convenção Europeia dos Direitos do Homem (CEDH) de 1950 a Carta dos Direitos Fundamentais da União Europeia (CDFUE) do ano 2000 passa a tutelar a proteção de dados de caráter pessoal. Veja-se que a CEDH protegia apenas o direito à vida privada e familiar.

Pondera-se que na Europa o tema da proteção de dados pessoais ganha maior ênfase nos anos 2000, pois havia preocupação com questões relacionadas ao tratamento de dados, o qual deveria ser realizado apenas com finalidade específica e com o consentimento da pessoa interessada ou mediante outro fundamento legítimo previsto em lei, com possibilidade do titular dos dados acessá-los e retificá-los quando necessário, devendo o cumprimento destas regras ficar sujeito a fiscalização de uma autoridade independente.

Neste contexto é seguro ponderar que estas orientações da CDFUE influenciaram os Tratados e legislações subsequentes e repercutiram no atual sistema de proteção de dados europeu[6].

---

5 Carta dos Direitos Fundamentais da União Europeia (2000/C 364/01) de 18 de dezembro de 2.000 estabelece no artigo 8° a proteção de dados pessoais, enfatizando que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito, que esses dados devem ser objeto de um tratamento leal para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto em lei, sendo que todas as pessoas tem o direito de ter acesso aos dados que forem recolhidos que lhes digam respeito e de obter a respectiva retificação. Ainda prevê que o cumprimento destas regras fica sujeito a fiscalização de uma autoridade independente (PARLAMENTO EUROPEU. 2000).

6 Vale lembrar que o Código de Defesa do Consumidor (Lei n° 8.078, de 11 de setembro de 1990) da mesma forma foi inovador relativamente aos bancos de dados e cadastros de consumidores ao determinar no artigo 43 e seguintes que o consumidor "[...] terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes", que os dados dos cadastros devem ser "objetivos, claros, verdadeiros", não podendo conter informações ne-

No Tratado sobre o Funcionamento da União Europeia (TFUE)[7] o artigo 16° "[...] contém uma nova base jurídica para as regras de proteção de dados aplicáveis a todas as atividades abrangidas pelo direito da UE. Reconhece-se no n.º 1 o direito à proteção de dados de caráter pessoal e no nº 2 uma competência específica da UE para legislar sobre a matéria. Este artigo, tal como configurado pelo Tratado de Lisboa, permite que a UE disponha de um único instrumento para regular a proteção de dados incluindo no domínio da cooperação policial e judiciária em matéria penal." (ARAÚJO; OLIVEIRA, [201-?]).

Salienta-se que "a reforma do quadro jurídico da proteção de dados da UE, proporcionada pela nova redação do art. 16º[8] do TFUE, prevê uma mudança substancial das regras da UE sobre a matéria. A reforma apoia-se em duas propostas legislativas: um regulamento que estabelece o quadro geral da UE em matéria de proteção de dados (e que substitui a Diretiva 95/46/CE); e uma diretiva que enuncia as regras relativas à proteção de da-

gativas pelo prazo superior a cinco anos (CDC art. 43 § 1°), dependendo "a abertura de cadastro, ficha, registro e dados pessoais e de consumo" de prévia comunicação por escrito ao consumidor, quando não solicitada por ele (CDC art. 43 § 2°), autorizando ainda o consumidor a exigir a imediata correção de seus dados sempre que encontrar inexatidão nos seus dados e cadastros no prazo de cinco dias úteis (CDC art. 43 § 3°). Caso haja descumprimento total ou parcial destas obrigações as pessoas jurídicas serão compelidas a cumpri-las e a reparar os danos causados aos consumidores (CDC art. 22). Elucida-se ademais que o Código de Defesa do Consumidor estabelece duas infrações penais, a primeira no artigo 72, definindo que "impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros". A segunda no artigo 73 que "deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata. Em ambas as situações a pena é de detenção de um a seis meses e multa (BRASIL, 1990).

7 O Tratado sobre o Funcionamento da União Europeia (TFUE) foi assinado em 18 de dezembro de 2007 e entrou em vigência em 01 de dezembro de 2009, também é denominado como Tratado de Lisboa.

8 Estabelece o artigo 16° do Tratado dobre o funcionamento da União Europeia (TFUE) Artigo 16 no n° 1 que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" e no n°2 que "o Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes" (EUR-LEX, 2012).

dos pessoais tratados para efeitos de prevenção, investigação, deteção ou repressão de infrações penais e atividades judiciárias conexas (e que substitui a Decisão-Quadro 2008/977/JAI16)" (ARAÚJO; OLIVEIRA, , [201-?]).

A Diretiva 95/46/CE não mais subsisti nos dias de hoje, mas até 25 de maio de 2018 era o texto de referência no âmbito europeu em matéria de proteção de dados pessoais, instituía um quadro regulamentar a fim de estabelecer um equilíbrio entre um nível elevado de proteção da vida privada das pessoas e a livre circulação de dados pessoais no interior da União Europeia. Para este efeito, fixava limites estritos à coleta e à utilização de dados pessoais e solicita a criação, em cada Estado membro, de um organismo nacional independente encarregado do controle de todas as atividades relacionadas com o tratamento de dados pessoais.

A substituição da Diretiva 95/46/CE pelo Regulamento (UE) 2016/679[9] foi imprescindível pois havia multiplicidade de sistemas no âmbito da União Europeia, sendo necessário estabelecer uma unidade através de um modelo homogêneo[10].

Esta unidade foi instituída pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, denominado como Regulamento Geral de Proteção de Dados (RGPD) da União Europeia (UE)[11], que atingiu a eficácia plena em 25 de maio de 2018 e "[...]estabelece as regras relativas ao tratamento, por uma pessoa, em empresa ou uma organização, de dados pessoais relativos a pessoas na UE" (COMISSÃO EUROPEIA, 2020).

Identifica-se no RGPD duas seções, na primeira 173 Considerandos e, na segunda parte, 99 artigos, os quais devem ser analisados conjuntamente vez que os conteúdos são difusos.

---

9 Observa-se que o Parlamento Europeu, órgão legislativo da União Europeia, sanciona dois tipos de documentos, quais sejam: a Diretiva, que corresponde à uma proposição para que os países da União Europeia efetivem a transposição da matéria da Diretiva para a lei nacional de cada país e, o Regulamento, que tem força de lei e se aplica automaticamente aos Estados membros da EU, sem a necessidade de transposição.

10 O artigo 16° da TFUE atribui competência específica à UE para legislar em matéria de proteção de dados.

11 Denominado em inglês como *General Protection Regulation (GDPR)*

O RGPD apresenta definições[12], princípios e regras. Representa inovação legislativa pois além de ter aplicação na União Europeia tem aplicação extraterritorial, podendo ser aplicado integralmente a terceiros países em hipóteses específicas.

## 2 CONCEITO DE EXTRATERRITORIALIDADE E ÂMBITO DE APLICAÇÃO MATERIAL E TERRITORIAL DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS.

O tema da extraterritorialidade foi revisitado com maior frequência a partir da vigência do Regulamento (EU 2016/679) do Parlamento Europeu e do Conselho de 27 de abril de 2016, denominado Regulamento Geral de Proteção de Dados (RGPD) relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Apesar dos atos administrativos, judiciais e legislativos dos Estados serem emanações da jurisdição soberana do próprio Estado, é necessário analisar toda a extensão e alcance destes atos fora das suas fronteiras, principalmente em situações de violação dos direitos fundamentais, uma vez que em especial nas últimas décadas o fator da globalização fez culminar na "internacionalização da vida quotidiana" (FONSECA, 2019).

Assim se faz indispensável esclarecimentos prévios do conceito de extraterritorialidade.

A extraterritorialidade judicial de um Estado é para Dulce Lopes (2015, p.38) "o conjunto de situações em que o Estado está habilitado, usualmente por via unilateral, a dizer o direito aplicável a situações internacionais".

Já para Fernando Loureiro Bastos (2016, p.442) a "extraterritorialidade determina que as normas de uma determinada ordem jurídica pos-

[12] O Regulamento Geral de Proteção de Dados traz 26 definições, dentre eles o conceito de tratamento de dados e privacidade.

sam vir a produzir efeitos no espaço geográfico de uma ordem jurídica distinta".

Cedric Ryngaert (2015, p. 6) define extraterritorialidade como situações "em que um Estado regula assuntos que, tendo uma ligação com outro Estado, não são de preocupação exclusivamente doméstica".

Percebe-se assim, que a extraterritorialidade judicial de um Estado é um meio de regular alguma conduta além das fronteiras de um Estado, mas que são de interesse deste, ou seja, prepondera e a norma jurídica estrangeira em prejuízo da norma vigente no país em que foi configurada a controvérsia.

Tem-se que os atos administrativos, judiciais e legislativos da União Europeia teoricamente possuem o mesmo grau de hierarquia dos instrumentos atos administrativos, judiciais e legislativos dos outros Estados no cenário internacional.

Consequentemente, a UE se sujeita às mesmas regras e limites de competência estabelecidos pelo Direito Público Internacional aos demais Estados quando exercem jurisdição extraterritorial (FONSECA, 2019, p.8).

Mas com a evolução das relações nacionais e transnacionais existe impulsionamento à jurisdição extraterritorial, justamente poque existe a necessidade da UE manter sua autoridade e proteger os indivíduos em situações que "[...] certos atos cometidos além-fronteira violam normas imperativas nacionais e internacionais ou tem implicações sérias do território nacional" (FONSECA, 2019, p.11).

Decorre da situação de "sociedade de risco global" (LOUREIRO, 2001) e do crescimento desmedido de acontecimentos internacionais expressivos que demandam pronta intervenção, essencialmente quando amparam direitos fundamentais do ser humano.

Maria da Graça Almeida de Eça do Canto Moniz Adão da Fonseca (2019, p. 13-14) observa que:

> "segundo a teoria dos deveres de proteção de direitos fundamentais, em especial as considerações a propósito dos "perigos com conexões

> internacionais", isto é, "diretamente causados por Estados estrangeiros ou com origem nos respetivos territórios", vigora um relativo consenso quanto à tese de que a entidade do foro não se deve demitir do dever de proteção apenas porque a fonte da ameaça ou perigo se encontra no estrangeiro pelo que se tem pugnado pela aplicação de um "princípio da irrelevância da origem da ameaça". Cabe sempre à entidade do foro ponderar a utilidade social e económica de atividades perigosas (mesmo quando a sua origem é no estrangeiro) com as probabilidades de estas causarem danos jusfundamentais de difícil mensuração e valoração, mesmo que tal implique decidir, isolada e unilateralmente, questões de elevada complexidade sem que a entidade do foro disponha de todos os dados e num ambiente de incerteza" (FONSECA 2019, p. 13-14).

Como observa Jorge Pereira da Silva (2015), "para ameaças que transcendem as fronteiras do Estado, torna-se necessário que este promova soluções institucionais e normativas que transcendam a escala puramente nacional".

Maria da Graça Almeida de Eça do Canto Moniz Adão da Fonseca (2019, p. 14) elucida que nem sempre "[...] os esforços a nível da cooperação internacional, diplomáticos e institucionais", ou através da estruturação do sistema de Direito Internacional Público seja possível resolver demandas de âmbito global ou transnacional, de forma que os Estados reinventam ou adaptam regras ou recorrem às vias que estão ao seu alcance no plano doméstico para resolverem os novos desafios, a fim de o Estado manter a sua autoridade e proteger os indivíduos.

No âmbito digital é fácil identificar a inadequação de aplicação da jurisdição exclusivamente territorial, por isso, a UE faz uso da técnica da "extensão territorial" (FONSECA, 2019, p. 20-21) em áreas de regulação que operam num contexto de grande interdependência internacional, que incidem sobre operadores económicos transnacionais e nas quais a cooperação internacional é frágil e morosa que se caraterizada por três elementos centrais, quais sejam:

> "(i) Parte de um nexo ou gancho territorial com a UE que pode resultar de vários fatores, como a introdução de um produto ou a prestação de serviços por um operador ou prestador estrangeiro no mercado interno, a sua presença temporária no território da UE, entre outros fatores;
>
> (ii) A imposição de condições a esse acesso, ao mercado interno ou ao território da União, que passam pela apreciação da conformidade e respeito do DUE, quanto às operações e à atividade desenvolvidas no mercado interno da UE, mas também quanto à sua performance no estrangeiro;
>
> (iii) A criação de "esferas concêntricas de intervenção regulatória" incidentes sobre vários níveis, três externos, micro (atividades económicas transnacionais), intermédio (o conteúdo do direito estrangeiro) e macro (a evolução do DIP) e um nível interno". (FONSECA (2019, p. 20-21)

Ao analisar o artigo 2° relativo ao âmbito de aplicação material, bem como o artigo 3° concernente ao âmbito de aplicação territorial do Regulamento Geral de Proteção de Dados (RGPD) é possível identificar que a mencionada técnica da extensão territorial foi adotada.

O RGPD garante o livre fluxo de dados pessoais entre os Estados membros da UE, mas no corpo do seu texto legal também reconhece a transferência de dados de um Estado membro para outro país fora do espaço econômico europeu, desde que estejam os dados pessoais transferidos adequadamente protegidos.

Por esta razão, no caso de transferência internacional de dados, além da proteção prevista no RGPD, exige-se condições extras, podendo aquela somente se evidenciar se estiver embasada em uma decisão de adequação (RGPD, Art. 45°), ou diante de garantias adequadas (RGPD, art. 46°), através de regras vinculativas aplicáveis às empresas (RGPD, Art. 47°), a partir de transferências ou divulgações não autorizadas pelos direito da União (RGPD, Art. 48°), mediante derrogações para situações específicas (RGPD, Art. 49°), ou ainda, diante de cooperação internacional no domínio da proteção de dados pessoais (RGPD, Art. 50°).

Atém-se especificamente o presente estudo às transferências de dados pessoais internacionais embasadas em decisões de adequação, que são emitidas pela Comissão Europeia (CE) e dizem respeito ao nível de proteção garantido pelo país terceiro para onde os dados serão transferidos.

Para avaliar o nível de adequação de cada país, a CE leva em consideração a legislação geral e setorial vigente naquele país, o respeito pelos direitos humanos e pelas liberdades fundamentais, como também, a existência e funcionamento efetivo de uma ou mais autoridade independente de proteção de dados.[13]

Dentre os países considerados seguros, cita-se como exemplo Israel, Argentina, Nova Zelândia, Suíça e Uruguai. Observa-se que até julho de 2020 os Estados Unidos estavam nesta lista limitado ao acordo *Privacy Schield*.

Segundo a Comissão Europeia (2017) e o Parlamento Europeu (2017) as decisões de adequação tem como objetivo, encontrar o equilíbrio entre a estabilidade financeira, a proteção dos investidores e os benefícios em manter os mercados financeiros da UE globalmente abertos e, promover a convergência regulatória e melhorar a cooperação da supervisão com outros parceiros.

As decisões de adequação proporcionam que a regulamentação da União Europeia tenha incidência na arquitetura de governança e nas atividades dos operadores econômicos estrangeiros que atuam ou pretendam atuar no mercado interno da União Europeia.

Assim, estes operadores econômicos passam a aderir às decisões de adequação como condicionante para ter acesso ao mercado interno da União Europeia.

Elucidam sobre esta situação Abraham Newman e Eliot Posner (2015, p. 1316 e ss) que "as normas de equivalência incentivam empresas internacionalmente ativas a pressionar reformas regulatórias nos países

[13] Até o mês de outubro de 2020 o Brasil ainda não é considerado pela Comissão Europeia um país adequado. Observa-se que mesmo após o estabelecimento da Autoridade Nacional de Proteção de Dados (ANPD) poderá ainda não ser reconhecido como um país seguro pela eventual falta de independência da ANPD.

de origem". Assim, a UE instiga alterações no ordenamento jurídico de países terceiros, atuando como dinamizador de normas.

O posicionamento da UE de induzir pressão nos países terceiros no sentido de aproximar estas legislações com a europeia está de acordo com um princípio que rege a sua atuação externa, qual seja, o princípio da responsabilidade[14], que traduz um objetivo de longa data dos seus órgãos de incrementar a visibilidade e a eficácia da sua atuação internacional no sentido de torná-la uma potência capaz de marcar eticamente a globalização (RANGEL DE MESQUITA, 2011, p. 184).

Com relação ao âmbito de aplicação material das decisões de adequação, o artigo 44° do RGPD dispõe que qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou para uma organização internacional somente será realizada se, sem prejuízo das outras disposições do RGPD, as condições estabelecidas em uma decisão de adequação forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional.

Portanto, as decisões de adequação não podem ir em desencontro com os princípios e regras do RGPD, visto que estas

[14] O princípio da responsabilidade é enunciado na Declaração de Laeken, em 2001, e acolhido pelo TL por via do elenco de objetivos da UE em matéria de atuação externa no art. 3.º, n.º 5 e no art. 21.º do TUE. De onde se pode ler, respetivamente, "Nas suas relações com o mundo, a União afirma e promove os seus valores e interesses e contribui para a proteção dos seus cidadãos. Contribui para a paz, a segurança, o desenvolvimento sustentável do planeta, a solidariedade e o respeito mútuo entre os povos, o comércio livre e equitativo, a erradicação da pobreza e a proteção dos direitos do Homem (...) bem como para a rigorosa observância e o desenvolvimento do direito internacional, incluindo o respeito dos princípios da Carta das Nações Unidas" e, alia, "A ação da União na cena internacional assenta nos princípios que presidiram à sua criação, desenvolvimento e alargamento, e que é seu objetivo promover em todo o mundo: democracia, Estado de direito, universalidade e indivisibilidade dos direitos do Homem e das liberdades fundamentais, respeito pela dignidade humana, princípios da igualdade e solidariedade e respeito pelos princípio da Carta das Nações Unidas e do direito internacional. (...)" (COMISSÃO EUROPEIA, 2001)

> "regras destinam-se a proteger todos os cidadãos da UE contra violações da privacidade e dos dados num mundo cada vez mais baseado em dados, criando simultaneamente um quadro mais claro e mais coerente para as empresas. Os direitos de que beneficiam os cidadãos incluem: um consentimento claro e positivo do tratamento dos seus dados e o direito de receber informações claras e compreensíveis sobre o mesmo; o direito a ser esquecido — um cidadão pode solicitar que os seus dados sejam suprimidos; o direito a transferir os dados para outro prestador de serviços (por exemplo, a mudança de uma rede social para outra); e o direito de saber se os seus dados foram pirateados. As novas regras aplicam-se a todas as empresas que operam na UE, mesmo que essas empresas tenham sede fora dela. Além disso, será possível impor medidas corretivas — tais como advertências e ordens — ou impor sanções às empresas que violem as regras" (PARLAMENTO EUROPEU, 2020).

Frisa-se que as regras do RGPD "[...] não se aplicam ao tratamento de dados por motivos exclusivamente pessoais ou no exercício de atividades domésticas, desde que não haja qualquer ligação com uma atividade profissional ou comercial. Quando uma pessoa utiliza os dados pessoais fora da sua esfera pessoal, por exemplo para o exercício de atividades socioculturais ou financeiras, a legislação relativa à proteção de dados tem de ser respeitada" (COMISSÃO EUROPEIA, 2020). Do mesmo modo, as regras do RGPD não se aplicam ao tratamento de dados pessoais de pessoas falecidas ou de pessoas coletivas.

Por fim, no plano interno, a extensão territorial serve para proteger o funcionamento do mercado da União, garantir a sua estabilidade e integridade e condicionar o acesso de operadores econômicos estrangeiros.

Condicionando esse acesso, a UE protege interesses próprios (de consumidores, investidores, cidadãos e indivíduos em geral) sempre que os serviços e produtos estrangeiros comportem riscos para os valores ou interesse que mobilizaram o legislador a conformar a atividade privada no seu espaço econômico.

A criação de um mercado interno dando origem a uma forma de territorialidade interna e a efetividade da regulação aplicável a esse mercado, exigem a externalização e a aplicação das decisões de adequação, que atuam como uma técnica legislativa de extensão territorial, garantindo o comércio internacional e a sujeição da atuação privada de âmbito transnacional às vinculações jurídico-públicas que garantam a preservação e a promoção de traços essenciais do ordenamento jurídico da União Europeia.

## 3 ACORDO *SAFE HARBOR*: A DEMANDA DA UNIÃO EUROPEIA POR PADRÕES DE PRIVACIDADE DE DADOS MAIS ELEVADOS (*SCHREMS I*).

Como visto anteriormente, a Diretiva 95/46/CE do Parlamento Europeu e do Conselho visava garantir um alto nível de proteção para a privacidade dos indivíduos em todos os Estados membros e também garantia o livre fluxo dos serviços da sociedade da informação na UE, promovendo a confiança dos consumidores e minimizando as diferenças entre as regras dos Estados membros.

A Diretiva 95/46/CE condicionava que quase a totalidade da coleta, uso e transferência de dados se submetesse aos regramentos de cada um dos Estados membros da UE e que cada um destes Estados membros monitorassem os procedimentos relacionados aos dados através de sua autoridade independente de proteção de dados.

Nos termos do artigo 25° da Diretiva 95/46/CE as transferências de dados pessoais para países terceiros[15] somente seriam permitidas a partir do momento que estes países assegurassem níveis adequados de proteção de dados.

Ocorre que, apesar das transferências de dados entre a União Europeia e países terceiros serem comuns, os padrões americanos não eram

[15] Países não pertencentes ao Espaço Econômico Europeu.

considerados adequados pela UE, ameaçando a continuidade da transferência de dados pessoais entre a União Europeia e os Estados Unidos.

Após negociações foi emitido pelo Departamento de Comércio dos Estados Unidos o acordo denominado *Safe Harbor*, reconhecido pela Comissão Europeia como adequado para garantir um nível adequado de proteção aos dados pessoais.

Assim uma empresa ou organização americana, além de cumprir princípios e requisitos relativos ao consentimento, tratamento, transferência e segurança, deveria anualmente apresentar declaração de compliance[16].

Mas em 2013, os padrões americanos foram questionados, principalmente após a divulgação do caso Edward Snowden que trouxe à baila a intensa atividade de vigilância da Agência de Segurança Nacional dos Estados Unidos (NSA).

À luz destas informações divulgadas amplamente através de mídia a validade do acordo *Safe Harbor* foi questionada em 2013 no caso conhecido com *Schrems*[17] *v. Irish Data Protection Commissioner*, sob o argumento principal de que os servidores do *Facebook* baseados na UE não protegiam adequadamente a transferência de seus dados pessoais para os servidores nos Estados Unidos.

Especificamente, Maximillian Schrems alegou que o Facebook não poderia ter transferido seus dados pessoais de acordo com a legislação da União Europeia porque a Agência de Segurança Nacional dos Estados Unidos havia interceptado essas transferências.

Para chegar às suas conclusões o Tribunal de Justiça da União Europeia (TJUE) baseou-se principalmente nos artigos 25.º e 28.º da Diretiva

---

16 O programa de compliance teve origem no início do século XX e pode ser compreendido como um programa que cria, monitora e faz "[...] cumprir um código de conduta com regras claras que visam conduzir a organização a realizar negócios limpos, éticos e de acordo com as leis vigentes" (CARVALHO, 2018, p. 4).

17 Maximilian Schrems é ativista de proteção de dados na ONG *Not on Your Bussiness* (NOYB), disponível no sítio eletrônico https://noyb.eu, que funde práticas de direito do consumidor, ativistas de privacidade, *hackers* e iniciativas de tecnologia para melhor aplicação do RGPD.

95/46/CE, bem como nos artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE).

O artigo 25.º da Diretiva 95/46/CE estabelecia que as transferências de dados para países terceiros somente são permitidas se esse país garantir um nível adequado de proteção de dados e se a Comissão estiver autorizada a emitir decisão de adequação. Já o artigo 28.º da mesma Diretiva exigia que os Estados membros criassem pelo menos uma autoridade pública para monitorizar o cumprimento.

Os artigos 7.º, 8.º e 47.º da CDFUE protegiam respectivamente, os direitos individuais à privacidade, à proteção de dados e a um recurso efetivo e, a um julgamento justo.

Em última análise o TJUE considerou o acordo *Safe Harbor* inválido em outubro de 2015, interpretando o termo "nível de proteção adequado" do artigo 25° da Diretiva 95/46/CE de modo a exigir que países terceiros forneçam níveis de proteção de direitos e liberdades essencialmente equivalentes aos garantidos na União Europeia por força da Diretiva 95/46/CE, como também à luz da CDFUE.

Portanto, o TJUE concluiu que o acordo de adequação *Safe Harbor* não atendia ao requisito de nível de proteção equivalente porque permitia aos Estados Unidos desconsiderar os princípios do acordo *Safe Harbor* quando em conflito com a segurança nacional ou interesse público, minando assim o direito fundamental à privacidade nos termos do artigo 7° da CDFUE.

O TJUE também considerou que o acordo *Safe Harbor* possuía cláusulas de adequações conflitantes com o artigo 47° da CDFUE porque não fazia referência à existência de regras ou proteções legais dos Estados Unidos destinadas a limitar a interferência deste na privacidade de dados.

Ademais o TJUE concluiu que, nos termos do artigo 25.º da Diretiva 95/46/CE, a Comissão Europeia devia avaliar as legislações nacionais e os compromissos internacionais de um país terceiro antes de tomar uma decisão sobre as normas de proteção de dados do país. Fatos estes não

evidenciados no momento do reconhecimento da adequação do Acordo *Safe Harbor* pela Comissão Europeia.

Esta decisão gerou incertezas para milhares de empresas e organizações americanas que dependiam da cláusula de adequação *Safe Harbor* para realizar legalmente transferências de dados pessoais.

Também como resultado da insegurança gerada as empresas com bases ou filiais na União Europeia que realizavam transferências transnacionais de dados pessoais para os Estados Unidos passaram a se utilizar das cláusulas contratuais padrão como alternativa para autorização das operações.

Mas em fevereiro de 2016, em substituição ao acordo *Safe Harbor,* foi publicada decisão de adequação pela Comissão Europeia considerando o acordo *Privacy Shield* adequado, tendo em vista que este refletia os requisitos necessário de adequação estabelecidos pelo TJUE na decisão do processo *Schrems v. Irish Data Protection Commissioner,* ou seja, viabilizava a proteção de dados pessoais exigida pelo RGPD para as transferências internacionais de dados pessoais da UE para os Estados Unidos.

## 4 INVALIDAÇÃO DO ACORDO *PRIVACY SHIELD* E A PROTEÇÃO EXTRATERRITORIAL DAS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PELO GDPR (*SCHREMS II*).

Desde 2016 o acordo *Privacy Shield*[18] era considerado por uma decisão de adequação da Comissão Europeia adequado para a transferência internacional de dados pessoais entre os Estados Unidos e a União Europeia.

Apesar dos Estados Unidos não ser considerado um país adequado para a transferência de dados internacionais, as empresas americanas poderiam aderir voluntariamente aos princípios e salvaguardas do acordo e

[18] No site da internet do Privacy Shield (https://www.privacyshield.gov/welcome) é possível encontrar a lista das empresas americanas que cumpriram os requisitos de proteção de dados nas transferências de dados pessoais da UE aos Estados Unidos.

se valerem das transferências transnacionais de dados pessoais de indivíduos situados na UE para esses negócios e organizações localizados nos Estados Unidos.

Contudo, a decisão de 16 julho de 2020, proferida pelo Tribunal de Justiça da União Europeia (TJUE) no processo C-311/18 (*Schrems II*) anulou a decisão de adequação do acordo *Privacy Shield* utilizado como base legal para a transferência internacional de dados.

Consoante a compreensão do TJUE, os programas de vigilância implementados pelo governo dos Estados Unidos violam desproporcionalmente os direitos à privacidade e à proteção de dados garantidos pelo RGPD, em virtude de não anunciarem de maneira aberta e transparente as limitações aos poderes conferidos aos serviços de inteligência, de forma a evidenciar abusos pelas autoridades públicas, que por sua vez não se limitam ao estreitamente imprescindível para a garantia da segurança nacional.

Ademais, o TJUE entende que o ordenamento jurídico e as práticas dos Estados Unidos não se adequam ao RGPD por não garantirem aos titulares dos dados medidas judiciais ou outros recursos eficientes que permitam a reivindicação da proteção de seus dados contra o acesso e uso abusivo por autoridades públicas, nem o direito de pleitear a retificação ou exclusão de seus dados.

Assim, o TJUE compreendeu que estas práticas e a legislação não se adequam ao RGPD e que o acordo *Privacy Shield* não é eficiente o suficiente para evitar ou abrandar estas questões, e, portanto, não representa um mecanismo legal válido para legitimar a transferência de dados de indivíduos localizados na UE para os Estados Unidos.

Ainda, no que tange as cláusulas contratuais padrão[19] o TJUE reconheceu no caso *Schrems II* que antes das transferências dos dados pessoais para países terceiros, deve o controlador de dados[20] analisar se os

[19] As cláusulas contratuais padrão são denominadas como *standard contractual clauses* (SCC) e estão previstas do Regulamento n° 2016/279 (Regulamento Geral de Proteção de Dados – RGPD) no artigo 46.

[20] O RGPD designa o controlador de dados como *data controller* que corresponde a pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, sozinho ou em

dados pessoais transferidos terão as garantias de proteção previstas no RGPD, ou seja, está sob a responsabilidade do controlador adotar medidas de salvaguarda adicionais. Caso contrário, o controlador de dados poderá ser impedido pelas autoridades de proteção de dados dos países membros da UE de transferir dados para os Estados Unidos.

O TJUE salientou em sua decisão que essa análise deve ser realizada de forma ativa e frequente, devendo o controlador descontinuar o fluxo de transferência dos dados caso as condições no país de destino sejam modificadas.

Esta decisão traz consequências políticas e comerciais internacionais entre UE e Estados Unidos pois as empresas americanas deverão aplicar uma nova camada de proteção e diligência nos fluxos transfronteiriços de dados, com padrões de proteção de dados ainda mais elevados, em especial ao acesso dos dados pelas autoridades públicas.

Assim, verifica-se a abrangência extraterritorial do RGPD, a partir da aplicação da técnica legislativa de extensão territorial, onde a UE pressiona alterações no ordenamento jurídico dos Estados Unidos através de condicionantes que incidem na arquitetura de governança e operações dos controladores e receptadores dos dados pessoais.

## 5 IMPACTOS DA DECISÃO *SCHREMS II NO BRASIL (PAÍS TERCEIRO)*

No mundo atualmente temos bilhões de usuários de internet e multiplicidade de modelos regulatórios de proteção de dados pessoais com dificuldades de harmonização.

O modelo da UE é unificado e através do RGPD - Regulamento (UE) 2016/679 torna-se aplicável aos Estados membros da UE e aos membros do Espaço Econômico Europeu (EEE), englobando Islândia, Liechtenstein e Noruega. Já o modelo americano é setorial, portanto, não é unificado.

conjunto com outros, tomam as decisões sobre as atividades de processamento de dados. Importante constatar que figura diferente é a do processador de dados (*data processor)* que é responsável pelo processamento de dados em nome do controlador.

No Brasil, com a vigência do RGPD, entendeu-se necessário estabelecer parâmetros balizados com o padrão europeu de proteção de dados, sendo promulgada a Lei n° 13.709 de agosto de 2018[21], que subsiste como um modelo unificado, ou seja, aplica-se uniformemente em todo o país.

Uma das principais disposições do RGPD está relacionada à sua aplicação extraterritorial em casos em que empresas, ainda que não estabelecidas na UE, efetuem atividades relacionadas ao tratamento de dados pessoais de titulares que se encontram no seu território, quando o tratamento se relacionar à oferta de bens ou serviços, sejam eles remunerados ou não, ou ao controle do seu comportamento, desde que ocorrido na União Europeia.

Esta disposição impacta nas pessoas físicas ou jurídicas, públicas ou privadas brasileiras que se enquadrem nas condições do parágrafo anterior, posto que deverão se submeter às condições da UE sob pena de lhes serem aplicadas penalidades impostas às violações aos seus dispositivos.

A legislação brasileira tem muitas influências do RGPD, tanto assim que a LGPD no artigo 33 e seguintes adotou mecanismos de salvaguarda semelhantes na transferência transfronteiriças de dados pessoais, assegurando proteção aos dados pessoais para além dos limites de seu território.

Os dados pessoais de brasileiros, com a vigência da LGPD somente poderão ser transferidos para países que tenham nível adequado de proteção de dados, sendo esta análise efetivada pela Autoridade Nacional de Proteção de Dados (ANPD).

A ANPD foi criada pela Lei n° 13.853 de 8 de julho de 2019, é atualmente um órgão vinculado ao governo e está subordinado à Presidência da República, portanto, não é independente, de modo que o Brasil continuará a ser considerado pela Comissão Europeia um país inadequado,

[21] A Lei n° 13.709/18, também denominada como Lei Geral de Proteção de Dados (LGPD) entrou em vigência parcial, ressalvadas as multas administrativas que poderão ser aplicadas a partir de 01 de agosto de 2020.

vez que em desconformidade com o RGPD, o que o torna incapacitado para transacionar dados pessoais com países da UE[22].

A ANPD[23] deverá levar em consideração na análise se a legislação dos países terceiros, estão alinhadas e em convergência com a legislação brasileira, caso contrário os dados pessoais originários do Brasil somente poderão ser transferidos internacionalmente mediante a legitimação das transferências pela ANPD pela aplicação de outros mecanismos, como por exemplo: cláusulas contratuais específicas, cláusulas contratuais padrão, consentimento expresso e informado, códigos de conduta, selos, mecanismos de certificação, entre outros.

Veja-se, portanto, que analogamente ao RGPD, a Lei Geral de Proteção de Dados (LGPD) dispõe que a Autoridade Nacional de Proteção de Dados (ANPD) irá definir o conteúdo das cláusulas-padrão contratuais e sua adequação à legislação brasileira.

Além disso, a LGPD no artigo 6° estabelece princípios que devem ser levados em conta quando do tratamento de dados pessoais, quais sejam, finalidade, adequação, livre acesso, qualidade dos dados, transparência, segurança, prevenção, necessidade, não discriminação e, responsabilização e prestação de contas.

Quanto ao princípio da responsabilidade disposto no artigo 6°, inciso X, está definido que o agente controlador de dados deve demonstrar a "[...] adoção de medidas eficazes e capazes de comprovar a observância

[22] A definição da Autoridade Nacional de Proteção de Dados está definida no artigo 5°, inciso XIX da LGPD e corresponde ao "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento[...]" da LGPD em todo o território nacional. Observa-se que na Seção II, Capítulo I desta obra existe estudo sobre o papel e função das Autoridades Nacionais de Proteção de Dados, com contextualização da ANPD brasileira.

[23] A ANPD avaliará o nível de proteção na transferência internacional de dados pessoais para países ou organismos internacionais levando em consideração os requisitos do artigo 34 da LGPD, quais sejam: "I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional; II - a natureza dos dados; III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei; IV - a adoção de medidas de segurança previstas em regulamento; V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e VI - outras circunstâncias específicas relativas à transferência. (BRASIL, 2018)

e o cumprimento das normas de proteção de dados pessoais e, inclusiva, da eficácia dessas medidas".

Portanto, quando da utilização de mecanismos de transferência de dados, como no caso de uso de cláusulas-padrão, compete ao controlador "verificar a observância das próprias instruções e das normas sobre os dados pessoais do titular e informar ao operador para que este realize o tratamento segundo as instruções fornecidas" (FRANCO, 2020, p.129).

As normas aqui tratadas são as contidas na LGPD, como também a Constituição Federal e toda a legislação vigente, a exemplo, o Código Penal, Código de Processo Civil, Códigos Penal e Civil, Código do Consumidor, porque nos casos de infrações penais, civis e administrativas, poderão serão responsabilizados o controlador e operador (FRANCO, 2020).

Desta forma, percebe-se que a LGPD aduz no corpo do seu texto legal os mesmos embasamentos presentes na decisão *Schrems II* para questionar e invalidar fluxo de dados pessoais transfronteiriços do Brasil para os EUA ou do Brasil para países terceiros.

Por conseguinte, significa dizer que está expressamente imposto ao controlador importante carga de responsabilidade, que deve ser observada e poderá ser questionada tanto no âmbito administrativo, quanto no judiciário, da mesma forma que aconteceu no caso *Schrems II,* na decisão TJUE.

Este mecanismo de proteção, pode, de modo semelhante, a partir da vigência da LGPD, ocasionar insegurança jurídica para as pessoas jurídicas ou físicas no atinente a transferência internacional de dados pessoais com operação no território brasileiro, haja visto que muitas delas se utilizam de servidores para armazenar dados que estão localizados em nuvem no território dos Estados Unidos.

Deste modo, o acórdão na decisão *Schrems II* do TJUE desperta reflexão sobre a legitimidade e ameaças advindas da legislação de vigilância dos Estados Unidos, em razão de uso e tratamento abusivos por autoridades públicas norte-americanas dos dados pessoais originários do Brasil.

Constata-se que não existe atualmente discussão judicial no Brasil neste sentido, mas a decisão *Schrems II* do TJUE conduz de imediato a reflexão sobre a possibilidade do Brasil se alinhar com o entendimento da UE e confrontar os Estados Unidos, ou, de forma contrária, do Brasil se indispor com a UE.

Em ambas as situações serão evidenciadas consequências políticas e econômicas.

Todavia, o Brasil poderá inovar e traçar seu próprio caminho em termos de soberania.

Mas caso o Brasil se alinhe com a posição da UE será possível reconhecer a aplicação extraterritorial da LGPD, corroborando com pressões da UE para alterar o ordenamento jurídico dos Estados Unidos, de modo a garantir padrões de proteção de dados mais elevados em situações que envolvem a transferência transfronteiriça de dados pessoais.

De qualquer forma, face a coexistência de distintos e múltiplos arranjos legais, urge a estipulação de princípios e normas globais a fim de garantir a estabilidade e harmonização das transferências internacionais e nível adequado de proteção dos dados pessoais.

## CONSIDERAÇÕES FINAIS

Os dados pessoais circulam em ambiente digital e ultrapassam as fronteiras territoriais dos países, com isto, existe preocupação com a proteção dos dados pessoais que levaram a União Europeia e diversos países do globo a promulgarem legislações com vista a garantir direitos aos titulares de dados tanto no ambiente interno, quanto no ambiente externo de seus territórios.

A sistemática de proteção de dados europeia reflete na sistemática de países terceiros e está respaldada na Convenção Europeia dos Direitos do Homem (CEDH), na Convenção 108 do Conselho da Europa, na Carta dos Direitos Fundamentais da União Europeia (CDFUE), no Tratado sobre o Funcionamento da União Europeia (TFUE), e no Regulamen-

to (UE) 2016/679 do Parlamento Europeu e do Conselho, denominado como Regulamento Geral de Proteção de Dados (RGPD) que atingiu a eficácia plena em 25 de maio de 2018.

O RGPD é inovador, engloba as definições, princípios e regras, tem aplicação na União Europeia e extraterritorial, uma vez que pode ser aplicado integralmente a terceiros países em hipóteses específicas.

A aplicação extraterritorial de uma lei é questão que pode demandar diversas discussões, justamente porque alcança a soberania de outro Estado, especialmente quando é preponderante a norma jurídica estrangeira.

Apesar de no cenário internacional os atos administrativos, judiciais e legislativos da União Europeia possuírem o mesmo grau de hierarquia dos instrumentos atos administrativos, judiciais e legislativos dos outros Estados, decorre da situação de risco global a necessidade de um Estado exercer jurisdição extraterritorial, principalmente em situações que envolvem a proteção dos direitos fundamentais.

A UE faz uso da técnica da extensão territorial para proteger a privacidade dos dados e efetivar as garantir previstas no RGPD ao impor condições aos operadores econômicos transnacionais, dentre elas, cita-se as decisões de adequação, que são emitidas pela Comissão Europeia (CE) e dizem respeito ao nível de proteção garantido pelo país terceiro para onde os dados serão transferidos.

As decisões de adequação levam em consideração a legislação geral e setorial vigente naquele país, o respeito pelos direitos humanos e pelas liberdades fundamentais, como também, a existência e funcionamento efetivo de uma ou mais autoridade independente de proteção de dados. Identicamente proporcionam que a regulamentação da UE tenha incidência na arquitetura de governança e nas atividades dos operadores econômicos estrangeiros que atuam ou pretendam atuar no mercado interno da União Europeia. Desta forma, as empresas estrangeiras impulsionam mudanças regulatórias nos países de origem.

O acordo denominado *Safe Harbor*, foi inicialmente reconhecido pela Comissão Europeia como adequado para garantir um nível adequado

de proteção aos dados pessoais. Mas no ano de 2016 foi invalidado no processo conhecido como *Schrems I* por não garantir a proteção exigida pelo RGPD para as transferências internacionais de dados pessoais da UE para os Estados Unidos.

Em substituição, desde o ano de 2016 persistia o acordo *Privacy Shield* que teve a sua validade questionada no TJUE no caso denominado *Schrems II*.

Da mesma forma este acordo foi declarado em julho de 2020 como não mais adequado para embasar as transferências internacionais de dados entre UE e Estados Unidos, justamente porque os programas de vigilância implantados pelo governo norte-americano violam desproporcionalmente os direitos à privacidade e à proteção de dados garantidos pelo RGPD.

No caso *Schrems II* o TJUE reconhece ainda quanto às cláusulas contratuais padrão (outro mecanismo previsto no RGPD para a transferência de dados internacional), a responsabilidade do controlador de dados analisar de forma ativa e frequente as condições do fluxo transfronteiriços e, adotar medidas de salvaguardas adicionais com o objetivo de garantir a proteção dos dados pessoais transferidos nos termos do RGPD.

Esta decisão pressiona alterações no ordenamento jurídico dos Estados Unidos, sendo possível observar a abrangência extraterritorial do RGPD, a partir da aplicação da técnica legislativa de extensão territorial.

No Brasil a Lei n° 13.709 de agosto de 2018[24], subsiste como um modelo unificado e tem muitas influências do RGPD, tanto que adotou mecanismos de salvaguarda semelhantes na transferência transfronteiriças de dados pessoais, assegurando proteção aos dados pessoais para além dos limites de seu território.

Os dados pessoais de brasileiros, com a vigência da LGPD somente poderão ser transferidos para países que tenham nível adequado de proteção de dados, sendo esta análise efetivada pela Autoridade Nacional de

[24] A Lei n° 13.709/18, também denominada como Lei Geral de Proteção de Dados (LGPD) entrou em vigência em setembro de 2020, ressalvadas as multas administrativas que poderão ser aplicadas a partir de 01 de agosto de 2020.

Proteção de Dados (ANPD). Analogamente ao RGPD, a LGPD dispõe que a ANPD definirá o conteúdo das cláusulas-padrão contratuais e sua adequação aos princípios e à legislação brasileira, devendo o controlador de dados demonstrar efetivamente a adoção destas adequações nos fluxos transfronteiriços, inclusive pelo operador dos dados pessoais.

Assim, tem-se na LGPD os mesmos embasamentos presentes na decisão *Schrems II,* que são suficientes para questionar e invalidar fluxo de dados pessoais transfronteiriços do Brasil para os EUA, tendo em vista o uso e tratamento abusivos por autoridades públicas norte-americanas dos dados pessoais originários do Brasil.

Ao Brasil restam as opções de se alinhar ao entendimento da UE e confrontar os Estados Unidos, ou, de forma contrária, do Brasil se indispor com a UE.

Outro caminho é o Brasil trilhar seu próprio caminho impondo a aplicação extraterritorial da LGPD, corroborando com pressões da UE para alterar o ordenamento jurídico dos Estados Unidos, de modo a garantir padrões de proteção de dados mais elevados em situações que envolvem a transferência transfronteiriça de dados pessoais.

Até a efetiva existência de princípios e normas globais que garantirão a estabilidade e harmonização das transferências internacionais de dados, advirão custos e entraves para validação e adequação da legislação brasileira à legislação estrangeira ou vice-versa, o que poderá ser entendido em um primeiro momento como uma barreira, mas certamente garantir-se-á aos titulares de dados maior efetividade dos direitos fundamentais e maior segurança jurídica na ordem internacional.

## REFERÊNCIAS

ARAÚJO, Alexandra Maria Rodrigues; OLIVEIRA, José Sebastião. **A transferência de dados pessoais para países terceiros acompanhada de uma decisão de adequação no Direito da união Europeia.** [201-?]). Disponível em: http://www.publicadireito.com.br/artigos/?cod=5b8f9c769baebee0. Acesso em: 15 set. 2020.

BASTOS, Fernando Loureiro**. Algumas notas sobre globalização e extraterritorialidade.** Liber Amicorum Fausto de Quadros, vol. I, 2016, p. 442.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 15 set. 2020.

_____. **Lei n°13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 set. 2020.

_____. **Lei n° 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 18 set. 2020.

CARVALHO, Adriana Barreira de. Ética & Compliance. In: Coriolano Almeida Camargo, Cleórbete Santos (Org.). **Direito digital:** novas teses jurídicas. Rio de Janeiro: Lumen Juris, 2018, p. 4.

COMISSÃO EUROPEIA. **Para que serve o Regulamento Geral sobre a Proteção de Dados (RGPD)?** 2020. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_pt. Acesso em: 10 set. 2020.

_____. *Commission Staff Working Document****. Equivalence decisions in financial services policy****: an assessment*, 27 de fevereiro de 2017, Disponível em: https://ec.europa.eu/info/sites/info/files/eu-equivalence-decisions-assessment-27022017_en.pdf. Acesso em: 22 set. 2020.

_____. **Conclusões da Presidência Conselho Europeu de Laeken**, 14 e 15 de dezembro de 2001. Disponível em: https://ec.europa.eu/commission/presscorner/detail/pt/DOC_01_18. Acesso em: 20 set. 2020

CONSELHO DA EUROPA. **Convenção 108 de 28 de janeiro de 1981**. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em: 16 set. 2020.

_____. **Mapa de assinaturas e ratificações do Tratado 108.** Convenção para a proteção de indivíduos com relação ao processamento automático de dados

pessoais. 2020. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=Bm5k3R88. Acesso em: 12 set. 2020.

CORTE EUROPEIA DOS DIREITOS HUMANOS. **Convenção Europeia dos Direitos Humanos.** 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf.Acesso em: 15 set. 2020.

EUR-Lex. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32016R0679. Acesso em: 10 set. 2020.

_____. **Versão Consolidada do Tratado da União Europeia e do Tratado sobre o Funcionamento da União Europeia 212/C 326/01**. Jornal Oficial nº C 326 de 26/10/2012 p. 0001 - 0390. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12012E/TXT&from=EN. Acesso em: 14 set. 2020.

FONSECA, Maria da Graça almeida de Eça do Canto Moniz Adão da. **A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia.** 2019. Tese de Doutorado. Disponível em: https://run.unl.pt/bitstream/10362/89180/1/Fonseca_2019.pdf. Acesso em: 15 set.2020.

FRANCO, Paulo Alves. **Lei Geral de Proteção de Dados Comentada.** Leme, SP: Imperium Editora, 2020, p. 129.

LOPES, Dulce. **Eficácia, Reconhecimento e Execução de Atos Administrativos Estrangeiros**, Policopiado, 2015, p. 38.

LOUREIRO, João. **Da sociedade técnica de massas à sociedade de risco – Prevenção, precaução e tecnociência**: algumas questões juspublicístas", Estudos em homenagem ao Prof. Doutor Rogério Soares, Coimbra Editora, 2001.

NEWMAN, Abraham; POSNER, Elliot. ***Putting the EU in its place****: policy strategies and the globat regulatory context.* JEEP, vol. 22, n° 9, 2015, p.1316 e ss.

PARLAMENTO EUROPEU. **Fichas técnicas sobre a União Europeia. Proteção dos Dados Pessoais.** 2020. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em: 11 set. 2020.

PARLAMENTO EUROPEU. **Carta dos Direitos Fundamentais da União Europeia** (2000/C 364/01) de 18 de dezembro de 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 19 set. 2020.

_____. **Briefing**: Third-country equivalence in EU banking legislation, 12 de julho de 2017, disponível em http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/587369/IPOL_BRI(2016)587369_EN.pdf, consultado no dia 30 de setembro de 2018.

RANGEL DE MESQUITA, Maria J. **A Actuação Externa da União Europeia depois do Tratado de Lisboa**, Almedina, 2011, p. 184.

SILVA, Jorge Pereira da. **Deveres do Estado de Proteção de Direitos Fundamentais**, Universidade Católica, Lisboa, 2015.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão do Tribunal (Grande Câmara) no Processo C-311/18 do TJUE de 16 de julho de 2020.** Disponível no link: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9710189. Acesso em: 12 set. 2020.

_____. **Acórdão do Tribunal (Grande Câmara) no Processo C-362/14 do TJUE de 6 de outubro de 2015**. Disponível no link: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d61f6b2122d377439c962fde383b0f9c39.e34KaxiLc3qMb40Rch0SaxyMbxv0?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=944110. Acesso em: 10 set. 2020.

RYNGAERT, Cedric. ***Jurisdiction in International Law.*** Oxford University Press, 2015, p. 6.

# Capítulo II

# OS ELEMENTOS DE CONEXÃO NAS RELAÇÕES JURÍDICAS CONSUMERISTAS E CONTRATUAIS: Análise de sua aplicação na LGPD e no RGPD

*Marcos Wachowicz*[1]

*Luciana Reusing*[2]

## SUMÁRIO



**RESUMO**

Em maio de 2018 entrou em vigor o RGPD 2016/679. O RGPD é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Económico Europeu. Regulamenta também a exportação de dados pessoais para fora da UE e EEE. Em agosto de 2018 no Brasil, foi editada a Lei 13.709, denominada LGPD, o texto é inspirado na legislação europeia (RGPD) e estabelece também que empresas que tenham como atividade centrada no tratamento sistemático de dados pessoais seja obrigada a ter um Encarregado pelo Tratamento de Dados Pessoais – Data Protection Officer (DPO). A questão norteadora do artigo se encontra na Governança Global da Internet na ceara do Direito Internacional Privado, na análise dos elementos de conexão para uma correta aplicação da legislação RGPD e/ou LGPDP nas relações jurídicas consumeristas e contratuais estabelecidas online.

**Palavras-chave:** Direito Internacional, Elementos de Conexão, Relações Jurídicas Online, Regulamento Geral sobre Proteção de Dados na União Europeia, Lei Geral de Proteção de Dados Pessoais.

[1] Professor de Direito no Curso de Graduação da Universidade Federal do Paraná - UFPR e docente no Programa de Pós-Graduação-PPGD da Universidade Federal do Paraná - UFPR. Doutor em Direito pela Universidade Federal do Paraná-UFPR. Mestre em Direito pela Universidade Clássica de Lisboa - Portugal. Professor da Cátedra de Propriedade Intelectual no Institute for Information, Telecommunication and Media Law - ITM da Universidade de Münster - ALEMANHA (2018). Coordenador-lider do Grupo de Estudos em Direito Autoral e Industrial - GEDAI / UFPR vinculado ao CNPq.

[2] Mestre em Ciência Tecnologia e Sociedade pelo Instituto Federal do Paraná, Pós-Graduada em Direito Penal e Processo Penal com ênfase em prática jurídica, Advogada, Professora Universitária, Pesquisadora do Grupo de Estudos em Direito Autoral e Industrial- GEDAI/UFPR vinculado ao CNPq.

## INTRODUÇÃO

Na Sociedade Informacional[3] a computação se desenvolve através do uso das Tecnologias da Informação e Comunicação (TICs), em especial por meio de redes[4] de conexão e transmissão de dados, conhecida como Internet, qual se popularizou e institucionalizou a chamada Governança Global. Esta é definida por Rosenau (2000), como as atividades apoiadas em objetivos comuns, que podem ou não derivar de responsabilidades legais que implicam em um controle transnacional de proteção às relações internacionais por meio da internet.

As pesquisas do Instituto Brasileiro de Geografia e Estatística do Brasil – IBGE, apontam que 116 milhões[5] de pessoas estão conectadas á internet, sendo que ao redor do mundo o número de usuários alcança 4 bilhões[6] de conexões online.

Aos 23 de junho de 2014 entrou em vigor o Marco Civil da Internet brasileiro (MCI), mediante a lei ordinária 12.965. Tratase de regulação le-

---

3 Gostaria de apresentar a distinção analítica adotada no presente estudo que foi feita por CASTELLS entre as noções de Sociedade de Informação e Sociedade Informacional com conseqüências similares para economia da informação e economia informacional. (...) Minha terminologia tenta estabelecer um paralelo com a distinção entre indústria e industrial. Uma sociedade industrial (conceito comum na tradição sociológica) não é apenas uma sociedade em que há indústrias, mas uma sociedade em que as formas sociais e tecnológicas de organização industrial permeiam todas as esferas de atividade, começando com as atividades predominantes localizadas no sistema econômico e na tecnologia militar e alcançando os objetos e hábitos da vida cotidiana. Meu emprego dos termos sociedade informacional e economia informacional tenta uma caracterização mais precisa das transformações atuais, além da sensata observação de que a informação e os conhecimentos são importantes para nossas sociedades. Porém, o conteúdo real de sociedade informacional tem de ser determinado pela observação e análise." CASTELLS, Manuel. **A sociedade em rede**. vol. I São Paulo : Paz e Terra, 1999, p. 46.

4 McNeill (2000) esclarece que as redes de informação são características recorrentes das sociedades humanas em diferentes tempos da história, e a Internet conforme Kurose e Ross (2010) como tecnologia capaz de interligar computadores, localizações geográficas e diferentes usuários.

5 Instituto Brasileiro de Geografia e Estatística. https://www.ibge.gov.br/

6 TecMundo. https://www.tecmundo.com.br/internet/126654-4-bilhoes-pessoas-usam-internet-no-mundo.htm

gislativa setorial, contendo normas de diversas naturezas agrupadas em razão de sua cobertura material: a internet e seu uso.[7]

A internet se tornou uma tecnologia indispensável para a concretização de diversas relações pessoais onde se incluem as de caráter jurídico consumeristas e contratuais, que trazem ao Direito Interno e ao Internacional Privado, desafios na determinação da lei aplicável na proteção de dados dos usuários em detrimentos dos elementos de conexão clássicos.

Essa importância se reflete na promulgação da Lei 13.709 no Brasil, editada em agosto de 2018 denominada Lei Geral de Proteção de Dados Pessoais (LGPDP ou LGPD), tem seu texto inspirado na atual Legislação Europeia sobre o tema (Regulamento Geral de Proteção de Dados – RGPD), ora aplicável a todos os indivíduos na União Europeia ao Espaço Econômico Europeu, com efeito sobre a exportação de dados pessoais para fora da UE e EEE.

Esses efeitos são decorrentes da exigência do RGPD[8] de que qualquer companhia de fora da UE, que queira tratar informações de europeus precisa se adaptar à legislação comunitária.

No mesmo sentido essa condição existe expressamente no art. 3.° e seus incisos da LGPD, o qual especifica que a lei brasileira de proteção de dados se aplica a qualquer operação de tratamento de dados pessoais, realizada por pessoa física ou jurídica de direito público ou privado, independente do meio, do país de sua sede ou do país onde estejam localizados, desde que verse sobre dados pessoais que tenham sido coletados no Brasil ou em qualquer outra operação de tratamento que seja realizado em nosso país. A LGPD no art. 5., inciso X dispõe ainda sobre o trata-

---

7 Wachowicz, Marcos; Fontoura Costa, José.Augusto. **C**láusulas contratuais nulas no Marco Civil da Internet. In **Revista da Faculdade de Direito da Universidade Federal de Minas Gerais - UFMG**, Belo Horizonte, n. 68, pp. 477-496, jan./jun. 2016. Acesso em: 15 de março de 2019: http://www.gedai.com.br/wp-content/uploads/2016/12/artigo_clausulas_contratuais_nulas_marco_civil_internet-1.pdf

8 General Data Protection Regulation - GDPR. Termo em inglês utilizado para referir-se ao Regulamento Geral de Proteção dos Dados Pessoais, embora seja importante observar que a consistência com a abreviatura empregada em língua portuguesa em uma das versões originais do Regulamento seja RGDP.

mento e a coleta de dados, englobando a recepção, acesso, transmissão, entre outras operações que envolvem os dados pessoais, será a autoridade nacional, o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional

Ademais, na própria LGPD em seu art. 33, I, estabelece sobre a transferência internacional de dados pessoais somente será permitida para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Por outro lado, o artigo 11 da Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet (MCI), já estabelecia que em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra ou tenha seus efeitos em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

A legisção brasileita (MCI) desde 2014 determina expressamente que será competência da juridição brasileira relações que envolvam empresas situadas fora do Brasil, desde que a operação envolva dados pessoais de usuários ou internautas brasileiros[9]. Antes do MCI se um

[9] Lei nº 12.965/2014 - Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

provedor de Internet não estivesse situado fisicamente no país, não seria aplicada a lei brasileira, porém, agora, mesmo que a atividade seja exercida por pessoa jurídica situada no exterior, será aplicada a lei brasileira (PINHEIRO, 2016,p, 87)

Assim, a analise dos Elementos de Conexão nas relações jurídicas consumeristas e contratuais à luz da LGPD e/ou RGPD se torna essencial, ainda, mais se considerar a hipótese que se lança é a possibilidade de um entrave na aplicabilidade das legislações LGPD e/ou RGPD, sobre as relações jurídicas consumeristas e/ou contratuais *online*, face as potenciais dificuldades oriundas dos elementos clássicos de conexão do Direito Internacional Privado, que são um fator determinante de internacionalidade e multiterritorialidade mesmo no cenário digital.

Deste modo, o referido artigo busca o analisar numa perspectiva da Governança Global os elementos de conexão para uma correta aplicação das legislações LGPD e/ou RGPD na proteção jurisdicional a consumidores e contratos celebrados pela internet *"e-commerce"*.

A abordagem do tema, será dividido em 4 tópicos: (i) Internet e os Desafios para o Direito, (ii) Os Contratos Virtuais e a Proteção de Dados Pessoais, (iii) Análise dos Elementos Clássicos de Conexão no Direito Internacional Privado e sua relação com o *e-commerce* na Proteção de Dados, e; (iv) Lei Geral de Proteção de Dados Pessoais (LGPD) e/ou Regulamento Geral para Proteção de Dados (RGPD) no "*e-commerce*".

## 1 INTERNET E OS DESAFIOS PARA O DIREITO

A nova ordem mundial nas relações internacionais do século XXI se perfaz pelo uso massivo das novas Tecnologias da Informação e Comunicação (TIC's), a exemplo da Internet na capacidade de compartilhar em tempo real a mesma informação a milhões de pessoas desde que conectadas a uma rede. Para Silva (2010) as TIC's concedem as pessoas uma

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

capacidade de firmar contato direto com a informação, por meio de um processo autônomo de escolha, atemporal e sem barreiras territoriais.

Conforme pontua Azevedo (2006), a internet é uma rede[10], é o espaço planetário mais importante pelo volume de informação e acesso disponível, comumente definida como a rede remota internacional de ampla área geográfica que proporciona transferência de arquivos e dados para milhões de usuários ao redor do mundo.

Aprofundando em outras definições, para Bachelard (1996) expõe como a Internet, tem por objetivo buscar o outro para melhor conhecer e também questionar as relações com o mundo, capaz de tratar e expandir dados como aponta Bush (2011), e interagir com outras áreas do conhecimento (MENDONÇA, 2014). Tateoki (2017), aponta que na Sociedade Informacional a Internet representa a maior revolução de conforto e comodidade para contratar bens e serviços, condicionando a sociedade com a capacidade de interconectividade e interatividade em todo o planeta, com o barateamento do custo das TIC's, bem como, o aumento da capacidade de armazenamento de dados propiciando um enorme fluxo de informações. Portanto a Sociedade Informacional está condicionada e transformada por todas as evoluções tecnológicas.

A partir da troca de protocolos pela rede, a Internet dá origem ao ciberespaço que para Lévy (2000), como espaço de comunicação, organização, sociabilidade e também de transação, podendo constituir-se numa sociedade de informação.

A sociedade Informacional é um contexto global do século de aceitação de relação entre indivíduos, que para Castells (1999) é a habilidade ou inabilidade de uma sociedade dominar ou incorporar as tecnologias seja como ferramentas aplicáveis ou processos a serem desenvolvidos.

Na mesma proporção que o fenômeno Internet alcança milhões de usuários no Brasil e no mundo na chamada Sociedade Informacional, surge concomitantemente o chamado cidadão consumidor, haja vista o poder de realizar todo o tipo de operações (KOHN e MORAES 2007).

[10] Conforme Leite (2015) rede em inglês significa "web", tendo por entendimento uma "teia de aranha", capaz de conectar diversos computadores pelo mundo.

Vislumbra-se o poder do cidadão consumidor de contratar bens e serviços em qualquer lugar do mundo de forma *online,* qual se espera da parte contratada a boa-fé[11], informações claras e principalmente a proteção dos seus dados, por se tratar de negócio jurídico a distância (MARQUES, 2004).

Para Castells (1999), tal fenômeno é uma revolução tecnológica, com base na informação que transformou o pensar, o produzir, o comunicar, o viver, o morrer, fazer guerra, amor e o negociar, na sociedade atual de consumo.

A internet conforme Castells (2003) possibilitou a comunicação com várias pessoas de forma simultânea, em qualquer lugar do planeta, a qualquer momento, resultando em um mundo novo denominado Galáxia da Internet, expressão que visa demonstrar sua amplitude como sistema de informação, bem as transformações culturais, econômicas, políticas e sociais que resultam desta tecnologia.

Deste modo Castells (1999) introduz a chamada sociedade em rede qual se expressa por estar conectada, promovendo interações afronteiriças pela interconexão de interesses em comuns que modificam os processos de contratação de bens e consumo.

Nesse prisma para Baudrillard (2010) através da sociedade de redes, surge a sociedade de consumo, definida como a vida cotidiana, da qual sobrevém a necessidade de comprar o novo, exigindo do consumidor o fornecimento de seus dados pessoais para celebrar os contratos virtuais.

Tal exigência cominada com a larga utilização da Internet traz ao Direito uma constante inquietação (VICENTE, 2010, p.193) no tocante ao Comércio Eletrônico e responsabilidade empresarial, seja na proteção de dados quanto uma tutela especifica, bem como na legislação a ser aplicada em caso de conflitos de normas diante das possiveis relações consumeristas e contratuais virtuais.

---

[11] Marques (2004) diz que "a confiança é um elemento central da vida em sociedade e, em sentido amplo, é à base da atuação/ação organizada do indivíduo," o que remete a dizer que a boa fé anda ao lado do princípio confiança, buscando trazer para uma relação jurídica, um equilíbrio.

## 2 OS CONTRATOS VIRTUAIS E A PROTEÇÃO DE DADOS PESSOAIS

As relações contratuais se perfazem conforme aponta Diniz (1993) através do contrato que é basicamente um acordo entre duas ou mais vontades que se manifestam na conformidade de uma determinada ordem jurídica, estabelecendo interessses entre as partes que o celebram, com o fim de adquir, modificar ou extinguir relações jurídicas de natureza patrimonial.

Contudo, as relações consumeristas e/ou contratuais realizadas *online,* podem ser denominadas de contratos virtuais, pois conforme Leal (2009) trata-se de contratação eletrônica interativa, ou seja, são contratos executados por computador, o acordo de vontades entre partes não se dá por meio eletrônico, servindo o computador apenas para a execução, ajustes ou implementação do acordo já aperfeiçoado. Afirmando ainda, que no momento em que tais informações são disponibilizadas na Internet considerar-se-á feita a oferta ao público e, consequentemente, manifesta a vontade do fornecedor. Por outro lado, frisa Leal (2009) a vontade do consumidor será manifestda no momento que este acessa o sistema aplicativo e com ele interage, preenchendo os campos eletrônicos em determinado site na Internet, sendo que, ao confirma os dados o consumidor conclui a sua aceitação.

Assim o contrato virtual se perfaz pela acesso, interação e aceite do usuário por algum meio virtual[12], computador ou *smartphone,* conectados a uma rede de Internet, objetivando uma nova forma de negociar produtos e serviços nacionais ou estrangeiros, pelo *e-commerce*[13], que para Lawand (2003) é uma nova forma de escambo.

---

12 Para Glanz (apud ANDRADE, 2004), o contrato eletrônico é aquele celebrado por meio de programas de computador ou aparelhos com tais programas.

13 Os sites de comércio eletrônico devem disponibilizar, em local de destaque e de fácil visualização, a razão social ou nome completo do fornecedor, bem como o número do CPF ou CNPJ, se pessoa física ou jurídica, objetivando diminuir o risco do consumidor na contratação ou compra pela internet, bem como permitir que o referido site seja corretamente identificado podendo responder por suas ações e omissões. Decreto nº 7962 de 15 de março de 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm. Acesso em: 11 de mar. 2019.

> Para Klee (2014), o *e-commerce* se traduz como Comércio Eletrônico, sendo este toda e qualquer forma de transação comercial em que as partes interagem eletronicamente, sem contato físico nas relações entre partes que se desenvolvem a distância por via eletrônica.
>
> Para Diniz (2008), o contrato virtual opera na relação entre o internauta e o estabelecimento comercial virtual, mediante a transmissão de dados pessoais, que se perfaz na declaração de vontade constituindo deveres e obrigações jurídicas.

A Convenção de Strasbourg de 1981[14] formulado pelo Conselho Europeu, definiu que dados pessoais como qualquer informação relativa a uma pessoa singular identificada ou susceptivel de identificação.

Castro (2005) define dados pessoais como qualquer informação numérica, alfabética, gráfica, fotográfica ou acustica, que independente do seu suporte som ou imagem, com a capacidade de identificar uma pessoa ou torna-la indentificável, o que se coaduna ao artigo 1º da LGPDP[15].

Contudo os dados pessoais conforme Limberg (2007), são divididos em sensíveis e não-sensíveis e diferenciados pelo seu potencial ofensivo de causar dano aos direitos fundamentais[16] do indivíduo, especialemen-

---

[14] Convenção nº 108 para a prteção das pessoas em relação ao tratamento de dados pessoais.

[15] Artigo 5º, I, da LGPDP dado pessoal é informação relacionada a pessoa natural identificada ou identificável.

[16] Conforme artigo 5º, X da Constituição Federal Brasileira de 1998, preceitua que são inviolávies o direiro a intimidade, a vida privada, a honra e a imagem das pessoais, assegurando-lhes o direito de intenização pelo dano material decorrente de sua violação, assim como o Código Civil no artigo 21 ao delcarar que a vida privada da pessoa natural ´inviolável, sendo que o juiz pode a requerimento do interessado adotar providencias para impedir ou fazer cessar ato contrário a esta norma, assim como o artigo 8, da Carta dos Direitos Fundamentais da União Européia que protege os dados pessoais, a intimidade e a vida privada: 1. Todas as pessoas tem direito à protecçªo dos dados de carater pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas tem o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O

te a sua dignidade, intimidade e privacidade, como informações de raça, credo, orientação sexual e saúde.

Rodatà (1995), enfatiza que a proteção de dados em especial ao dados sensíveis, serve para evitar discriminações, trazendo as relações equilíbrio, igualdade, ou má utilização quando armazenados.

Para tanto a proteção aos dados pessoais, se estende ao consumidor pois muitas das informações fornecidas nas relações jurídicas *online,* são pessoais sensíveis por tratar-se de valores emanados de determinada configuração social como descreve Limberger (2007), e portanto devem ser protegidas[17] desde sua fase précontratual.

Tal preceito da proteção, também é abarcado por Schmidt Neto (2016), ao relacionar os dados pessoais fornecidos pelo consumidor ao princípio da confiança, como a base para uma ação organizada e transparente.

Assim sendo, a importância na proteção de dados pessoais do consumidor, também se deve ao fato de evitar "fraudes" virutais, ou seja, lesões na quebra do sigilo de informações como aponta Salgarelli (2010), por meio de sistemas criptográficos, certificadores, árbitros virtuais, etc.

O ato de proteger dados pessoais está intrinsecamente ligado aos direitos de personalidade[18], a dignidade da pessoa humana[19]

cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

17 Declaração Universal dos Direitos dos Homens de 1948. Artigo 12: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação, contra as intromissões ou ataques toda pessoa tem direito a proteção da lei".

18 O Direito a Privacidade também está regulado no Novo Código Civil brasileiro, no Capítulo dos Direitos da Personalidade, em seu artigo 21, estabelece que „a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma". No entanto, é importante destacar que quando o interesse público predominar sobre o particular, a inviolabilidade da privacidade também reclama certas restrições, obrigando à análise caso a caso. Em algumas situações encontramos exceções à proteção legal como em pessoas dotadas de notoriedade (SERPRO, 2014).

19 É um princípio construído pela história tem buscado como bem maior proteger o ser humano contra qualquer forma de desprezo observando a declaração de Kant: [...] Mas o homem não é uma coisa. (KANT, 2008).

e ao direito de privacidade[20] como bem elenca Mendes e Branco (2011), alcançando os comportamentos e acontecimentos das relações pessoais mas também os comerciais que não se desaja publicidade.

Sarti (2016), enfatiza que os dados pessoais devem ser utilizados de acordo com o consentimento do consumidor, que passa a ser o sujeito de direito ao controle de suas próprias informações, ou seja, de expor ou não a sua intimadade[21].

Conforme jurisprudência do STJ, o consentimento é direito do consumidor de controle de suas informações, não podendo ser utilizada ou obtida por meios inadquados.

> "Com o desenvolvimento da tecnologia, passa a existir um novo conceito de privacidade, sendo o consentimento do interessado o ponto de referência de todo o sistema de tutela da privacidade, direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem". (REsp 1168547 / RJ RECURSO ESPECIAL 2007/0252908-3 Ministro LUIS FELIPE SALOMÃO (1140) T4 - QUARTA TURMA 11/05/2010 DJe 07/02/2011).[22]

Deste modo, um terceiro não poderá sem o consentimento do consumidor *online* obter, tratar e expor dados pessoais se não autorizados, do contrário poderá ter amparo legal.

Assim sendo *e-commerce,* na questão de proteção de dados, acaba abrangendo ao menos a legislação de dois estados, e observando o recorte espacial deste estudo, no Brasil com o Código de Defesa do

---

[20] Conforme Mendes e Branco (2010), o direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. O objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas.

[21] Para Marques (2010), o direito à intimidade é aquele que preserva-nos do conhecimento alheio, reserva-nos a nossa própria vivência.

[22] Jusbrasil. https://stj.jusbrasil.com.br/jurisprudencia/19128034/recurso-especial-resp-1168547-rj-20070252908-3-stj

Consumidor e a Lei de Proteção de Dados Pessoais (LGPD), e na Europa com o Regulamento Geral de Proteção de Dados (RGPD).

Por esse prisma, é possível que os contratos virtuais, gerem questões conflituosas em detrimento de qual legislação a ser aplicada em casos concretos, na possibilidade de não precisar ao certo por exemplo o local ou o momento da celebração do contrato ou até mesmo a identificação das partes.

## 3 ANÁLISE DOS ELEMENTOS CLÁSSICOS DE CONEXÃO NO DIREITO INTERNACIONAL PRIVADO E SUA RELAÇÃO COM O *E-COMMERCE* NA PROTEÇÃO DE DADOS.

Antes de abordar os elementos de conexão no Direito Internanacional Privado e sua relação com o *e-commerce*[23] na proteção de dados, é de extrema importância conceituar o referido direito, já que se destina a regular as relações internacionais entre particulares.

Para Correia (2000) o Direito Internacional privado, se define como um ramo da ciência jurídica no qual se formulam princípios e regras para determinar qual a lei de qual ordenamento jurídico será aplicável a um caso concreto nas relações jurídico-privadas de caráter internacional, com isso assegura o reconhecimento no Estado do foro das situações jurídicas puramente internas de questões que possuam elementos de estraneidade na órbita de outros sistemas de Direito estrangeiro (situações internacionais de conexão única, situações relativamente internacionais).

Deste modo, além de regular as regras e princípios aplicáveis nos casos de solução de conflito de leis no espaço o Direito Internacional Privado, é o ramo do direito que desafia o princípio da territorialidade das leis na medida em que fixa os critérios da aplicação do direito alienígena, e questionando: Quando aplicar? Em que caso aplicar? E qual o limite de sua aplicação?

---

[23] Regulamentado pela a Lei nº 8.078, de 11 de setembro de 1990, que passa a dispor sobre a contratação no comércio eletrônico, (BRASIL, 1990). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acesso em: 20 fev. de 2019.

Apresentado o conceito de Direito Internacional Privado, é importante trazer a luz o questionamento deste estudo: Qual legislação deve ser aplicada LGPD e/ou RGPD nas possíveis relações jurídicas consumeristas e contratuais plurilocalizadas na proteção de dados do *e-commerce*?

No objetivo de responder a tal questionamento, a abordagem dos elementos de conexão do Direito Internacional Privado, se torna o fator determinante para a correta aplicação legal, pois como declara Del'Omo (2010) os elementos de conexão são os elos capazes apontar a lei a ser aplicada no caso concreto.

Assim sendo, as relações jurídicas do *e-commerce* e a proteção de dados quando ligadas a mais de um sistema legal, ou seja, plurilocalizadas deve-se primeiramente verificar qual é o elemento de conexão para posteriormente se aplicar o sistema legal correto.

Elencando um possível caso prático: Um brasileiro residindo na Espanha, assina virtualmente uma autorização a uma empresa Alemã, para que esta use de seus dados para fins apenas de contrato de compra e venda.

Contudo se a empresa Alemã liberar tais dados pessoais a terceiros que tem sede na Inglaterra, qual lei será aplicada em caso de responsabilização pelo tratamento de dados?

E se o contratante ora brasileiro ainda residente na Espanha, alegar que a autorização assinada do uso de seus dados pessoais com a contratada no caso empresa Alemã não estava clara, qual a lei a ser aplicada?

Em caso de revogação da autorização dada à contratada empresa Alemã para o uso de seus dados, o contratante brasileiro ao retorno para o Brasil, toma conhecimento de que seus dados foram expostos a terceiros, qual legislação a ser aplicada?

Em todos os países acima mencionados se aplica o RGPD, a exemplo do caso de vazamento de dados dento da UE a responsabilidade sobre os danos prevista nos artigos. 79-82 do RGPD. Ademais, o art. 6

do RGPD estabelece quando se pode utilizar os dados e realizar o tratamento (a exemplo da a execução de um contrato, cumprimento de obrigações legais, saúde, legítimo interesse, dentre outros). Como também dispõe quando o tratamento de dados não encontrar base legal neste artigo, o tratamento pelas empresas somente deve acontecer com consentimento manifestado do consumidor, devendo este compreender o alcance e deve concordar com cada uma das finalidades. O art. 7 do RGPD especifica a possibilidade de tratamento de dados pelo consentimento expresso.

A questão ganha maiores complexidades quando envolve empresas e consumidores de países que estejam fora do âmbito do Espaço Schengen cujos Estados-Membros integram a União Europeia, garante a liberdade de circulação num território que engloba 26 países, com mais de 400 milhões de cidadãos.

Ressalte-se, o RGPD no que envolver países terceiros e extraterritorialidade, prevê que mesmo o dado pessoal de um europeu seja transferido para fora da União Europeia, esta operação deve ser adequadamente protegida. A regra básica é pela proibição de transferência internacional de dados pessoais, salvo se as condições impostas do RGPD tenham sido satisfeitas, a saber: (i) decisão de adequação (art 45); (ii) ter garantias apropriadas (art. 46); (iii) através de regras vinculativas aplicáveis às empresas (art. 47); (iv) mediante derrogações ou exceções (art.49); ou ainda, (v) diante a cooperação internacional no domínio da proteção de dados pessoais (art. 50).

O RGPD especifica no art. 49, a possibilidade de transferência internacional de dados se houver o consentimento explicito do titular de dados, se a transferência de dados for para a execução de um contrato e formação de contratos, ou ainda se houver interesse público.

Logo, havendo transferência internacional para fora do Espaço Schengen, de dados de cidadãos europeus, dependendo do caso pode ser aplicado mais de um ordenamento jurídico, bem como, se poderia atrair a lei específica de um país terceiro não se aplicando a LGPD e/ou RGPD.

Questões jurídicas controvertidas decorrente da plurilocalidade certamente surgirão em com o fluxo de negócios internacionais pela Internet e da transferência de dados pessoais além das fronteiras territoriais dos Estados.

Ocorre que, muitas vezes uma atividade negocial pode ser iniciada a partir de um determinado país africano, envolvendo armazenamento, guarda e tratamento de dados, cuja comunicação envolve terminal de usuário domiciliado na Argentina, que acessa um serviço hospedado num servidor nos Estados Unidos, porém sem que se conheça o local específico, vez que os dados se encontram na computação em nuvem (*cloud computing*). O armazenamento de dados em *cloud computing* é feito em serviços que podem ser acessados de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de programas específicos, independentemente da plataforma em que estejam as partes envolvidas.

Portanto, será sempre, diante de um caso concreto, seja este de "*e-commerce*" ou de proteção, que se abrirá questionamentos sobre conflitos de jurisdição (MOTA, BUHIGUES, PALAO MORENO, 2019, p.95), sobre qual legislação a ser aplicada ante a plurilocalidade dos consumidores e dos contratos, e que partir dos elementos de conexão segundo a Lei de Introdução das Normas do Direito Brasileiro (LINDB), Pessoas, Casamento, Bens ou Coisas, Sucessão, Fatos ou Negócios e Processo Judicial, é que irão indicar a lei a ser aplicada decorrente das espécies dos elementos de conexão, que são:

(i) **Lei do local do Dano** *(lex loci damni):* o lugar em que se manifestaram as consequências do ato ilícito, para reger a obrigação de indenizar a quem foi atingido pela conduta delitiva.

(ii) **Local da Prática do Ato** *(lex loci actus),* o lugar onde e ocorre o fato ilícito, irá determinar o local da relação jurídica. Com isso a lei aplicada será daquele local, onde aconteceu o ato ilícito.

(iii) **Lei do Domicílio** *(lex domicili),* aplicar-se a lei do lugar onde as partes estão domiciliadas, se em lugar diferentes, irá prevalecer o domicilio do réu, sendo que o entendimento para domicilio como o lugar onde a pessoa possui sua maior ocupação de vida.

(iv) **Local da Execução do Contrato** *(lex loci executionis),* institui-se como parte da sede de uma relação jurídica e estabelece que a norma a ser utilizada seja a do território onde o contrato será pactuado para reger sua interpretação e seus efeitos.

(v) **Lei do Lugar do Foro** *(lex fori),* adotado nos casos em que há incompatibilidade espacial de normas judiciais entre as partes, ou seja, a lei local estabelecerá as condições da ação.

(vi) **Lei do Lugar da Coisa** *(lex rei sitae)*, em conflitos de posses de bens, será aplicada o regulamento do país em que se encontram situados os bens imóveis.

(vii) **Lei do Lugar da Realização do Ato Jurídico** *(lex loci actus)*: lei do local da realização do ato jurídico para reger sua substância.

(viii) **Lei do Local da Realização das Formalidades do Casamento** *(lex loci celebrations)*: lei do local em razão das formalidades e impedimentos do casamento.

(ix) **Lei do Local do Cumprimento das Obrigações** *(lex loci solutionis)*: a lei a ser aplicada é a do local em que as obrigações devem ser cumpridas.

(x) **Lei do Local da Moeda** *(lex monetae):* a lei a ser aplicada é a do Estado em cuja moeda a obrigação legal foi expressa.

(xi) **Lei da Nacionalidade da Pessoa** *(lex patrie):* a lei a ser aplicada é a da nacionalidade da pessoa por reger seu estatuto pessoal, que alcancem seu nascimento, poder familiar, morte, personalidade e capacidade jurídica.

(xii) **Lei da Autonomia da Vontade das Partes** *(lex voluntautis)*: a lei a ser aplicada é a aquela livre e consciente escolhidas pelos pactuantes.

(xiii) **Lei do Bem Móvel** *(mobilia sequuntur personam):* a lei a ser aplicada para bens móveis e a do local em que o proprietário está domiciliado.

(xiv) **Lei do Local da Celebração do Contrato** *(lex loci contractus):* a lei a ser aplicada é a do local da celebração do contrato, ou seja, onde ele foi assinado para reger sua interpretação e aplicação.

Deste modo, na forma tradicional de contratos, conforme a Lei de Introdução as Normas do Direito Brasileiro (LINDB)[24] nº 4657/42, o artigo 9º§2º[25] traz *"lex loci"* como a regra geral dos contratos, ou seja, a lei aplicada é a do lugar em que o contrato foi celebrado.

Porém nas transações virtuais onde pode não se conhecer ao certo a localização ou a identidade dos contratantes decorre a aplicabilidade da *"lex fori",* em razão da localização de um computador, servidor ou responsável pela conexão.

Ressaltando, que em se tratando de dados pessoais com o Marco Civil da Internet (art. 11), a jurisdição brasileira será a competente, sempre que de algum modo envolvam dados de usuários ou internautas brasileiros.

Contudo, se as leis, atos e sentenças, bem como quaisquer declarações de vontade que ofendam a soberania nacional, a ordem pública e

---

[24] A referida Lei de Introdução as Normas de Direito Brasileiro de 2010 (LINDB), alterou a nomenclatura da Lei de Introdução ao Código Civil de 1942 (LICC). BRASIL. Decreto-lei nº 4.657, de 4 de setembro de 1942. **Lei de Introdução às Normas do Direito Brasileiro**. Diário Oficial da União, Brasília, DF, 9 set. 1942. Disponível em: www.planalto.gov.br/ccivil/Decreto-Lei/Del4657. Acesso em: 11 de mar. 2019.

[25] Art. 9º Para qualificar e reger as obrigações, aplicar-se-á a lei do país em que se constituirem.
§ 2º A obrigação resultante do contrato reputa-se constituida no lugar em que residir o proponente.
BRASIL. **Lei de Introdução as Normas do Direito Brasileiro**. (LINDB). Lei nº 12.376 de 2010. Disponível em: www.planalto.gov.br/ccivil/Decreto-Lei/Del4657. Acesso em: 11 de mar. 2019.

os bons costumes, perderam sua eficácia conforme o artigo 17[26] da LINDB (BRASIL, 1942).

Entretanto na União Europeia, o apreço é ao Regulamento Roma 593 de 2008, também denominado Roma I, e o Regulamento de Roma 864 de 2007, ou Roma II, que tratam da lei aplicável a matérias civis e comerciais.

O Roma I trata das chamadas obrigações contratuais, assegurando o princípio da liberdade de eleição da lei a ser aplicada, que no seu artigo 3º na primeira parte[27] determina que ao contrato seja aplicada a lei escolhida pelas partes, *"lex fori"* e na segunda parte[28] que essa escolha pode ser alterada a qualquer tempo bastando à manifestação do comum acordo.

Em caso de omissão quanto à eleição do foro para dirimir eventuais lides, o artigo 4º conforme suas alíneas "a e b" estabelecem que a lei a ser aplicada seja a do país onde reside o vendedor e/ou prestador de serviço[29], "*lex domicili"* em contratos de compra e venda ou prestação de serviço.

---

[26] Art. 17**.** As leis, atos e sentenças de outro país, bem como quaisquer declarações de vontade, não terão eficácia no Brasil, quando ofenderem a soberania nacional, a ordem pública e os bons costumes. Disponível em: www.planalto.gov.br/ccivil/Decreto-Lei/Del4657. Acesso em: 11 de mar. 2019.

[27] Regulamento 593/2008 de 11 de julho de 2007. Artigo 3 - Liberdade de escolha - 1. O contrato rege-se pela lei escolhida pelas partes. A escolha deve ser expressa ou resultar de forma clara das disposições do contrato, ou das circunstâncias do caso. Mediante a sua escolha, as partes podem designar a lei aplicável à totalidade ou apenas a parte do contrato." sobre a lei aplicável às obrigações contratuais (Roma I). Jornal Oficial da União Europeia, Estrasburgo, 04/07/2008. P. 5.

[28] Regulamento 593 de 11 de julho de 2007. Artigo 3 – 2. Em qualquer momento, as partes podem acordar em subordinar o contrato a uma lei diferente da que precedentemente o regulava, quer por força de uma escolha anterior nos termos do presente artigo, quer por força de outras disposições do presente regulamento. Qualquer modificação quanto à determinação da lei aplicável, ocorrida posteriormente à celebração do contrato, não afecta a validade formal do contrato, nos termos do artigo 11.o, nem prejudica os direitos de terceiros." sobre a lei aplicável às obrigações contratuais (Roma I). Jornal Oficial da União Europeia, Estrasburgo, 04/07/2008. P. 5.

[29] Regulamento 593 de 11 de julho de 2007. Artigo 4º - Lei aplicável na falta de escolha: 1. Na falta de escolha nos termos do artigo 3º e sem prejuízo dos artigos 5º a 8º, a lei aplicável aos contratos é determinada do seguinte modo: a) O contrato de compra e venda de mercadorias é regulado pela lei do país em que o vendedor tem a

Entretanto nas obrigações de caráter extracontratual, o Regulamento a ser observado é o Roma II, qual estabelece que a lei aplicável seja a do país onde ocorrer o dano *"lex loci damni"*[30] , porém se ambas as partes possuem domicílio no mesmo país a lei é a do local onde residem *"lex domicili",* artigo 4º segunda parte.

Portanto, notório é o avanço das legislações para a proteção das relações jurídicas consumeristas e contratuais do *e-commerce* e da proteção de dados sejam no Brasil com a Lei Geral de Proteção de Dados Pessoais (LGPD), ou na União Europeia com o Regulamento Geral para Proteção de Dados (RGPD), haja vista o objetivo comum de disciplinar segurança no ambiente virtual.

## 4 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E/OU REGULAMENTO GERAL PARA PROTEÇÃO DE DADOS (RGPD) NO "*E-COMMERCE*".

O recorte espacial deste artigo abrange o Brasil com a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Europa (União Europeia) com o Regulamento Geral de Proteção de Dados (RGPD), no impacto ao *digital due process*[31] e na sociedade de informação[32] nos possíveis

sua residência habitual; b) O contrato de prestação de serviços é regulado pela lei do país em que o prestador de serviços tem a sua residência habitual." sobre a lei aplicável às obrigações contratuais (Roma I). Jornal Oficial da União Europeia, Estrasburgo, 04/07/2008. P. 5.

30 Regulamento 864 de 11 de julho de 2007. "2. Todavia, sempre que a pessoa cuja responsabilidade é invocada e o lesado tenha a sua residência habitual no mesmo país no momento em que ocorre o dano, é aplicável a lei desse país."relativo à lei aplicável às obrigações extracontratuais (Roma II). Jornal Oficial da União Europeia, Estrasburgo, 31/07/2007. P: 5.

31 Segundo Antunes, Rosa, Biazatti, Vilela e Porto (2017) *digital due process* compreende uma constelação de transformações das regras jurídicas para garantir o devido processo legal, nos conflitos gerados pelos meios de comunicação e informação eletrônica.

32 A sociededade da informação resulta desses acontecimentos, viabilizando-se a comunicação mais rápida e a obtenção adequeda de dados. Verifica-se a concenntração de empresas mundiais de informação, (LISBOA, 2001).

conflitos de norma das relações jurídicas do *e-commerce* na proteção de dados.

As primeiras regulamentações sobre proteção e tratamento de dados são elencadas na Declaração Universal dos Direitos Humanos em 1948[33] e na Convenção Europeia dos Direitos Humanos de 1950[34], posteriormente a Lei de Proteção de Dados Pessoais do Land de Hesse Alemanha (1970) e a Data Legen na Suíça (1973), (BRASIL, 2010).

Já em 1981 é aprovada pelo Conselho da Europa a Convenção 108[35], que veio reforçar o assunto sobre proteção de dados[36], e a Diretiva 95/46 de 1995[37] considerada o marco regulatório para os países

---

33 Artigo 12°: - Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei.

34 Artigo 8º: - Direito ao respeito pela vida privada e familiar. 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

35 Convenção 108, para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal. (Artigo 2º - Definições: para os fins da presente Convenção: a) «Dados de carácter pessoal» significa qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação («titular dos dados»); **b)** «Ficheiro automatizado» significa qualquer conjunto de informações objeto de tratamento automatizado; **c)** «Tratamento automatizado» compreende as seguintes operações, efetuadas, no todo ou em parte, com a ajuda de processos automatizados: registo de dados, aplicação a esses dados de operações lógicas e ou aritméticas, bem como a sua modificação, supressão, extração ou difusão; **d)** «Responsável pelo ficheiro» significa a pessoa, singular ou coletiva, autoridade pública, serviço ou qualquer outro organismo competente, segundo a lei nacional, para decidir sobre a finalidade do ficheiro automatizado, as categorias de dados de carácter pessoal que devem ser registadas e as operações que lhes serão aplicadas.

36 Para Fromholz (2000) a Diretiva 95/46/EC era parte de uma estratégia europeia de diferenciação dos Estados Unidos na regulação da proteção de dados, evitando desenvolver normas vinculativas e/ou rígidas sobre o tema, em uma perspectiva liberal e de auto regulação.

37 Diretiva 95/46/CE 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.

membros da União Europeia[38], definindo dados pessoais no artigo 2º como:

> "qualquer informação relativa a uma pessoa singular identificada ou identificável pessoa em causa; é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social."

A referida diretiva, trouxe importante debate sobre transferência internacional de dados, definindo critérios e padrões entre países, porém sem previsões de aplicações extraterritoriais, mas criando as autoridades centrais ora responsáveis pela fiscalização, legislação e arbitragem a proteção de dados pessoais (GUIDI, 2017).

Contudo em 2016 a Diretiva nº95/46 que influenciou a proposta do Marco Normativo a Privacidade e da Proteção de Dados Pessoais no Brasil hoje LGPDP, é substituida pelo Regulamento nº 679/2015, denominado Regulamento Geral de Proteção de Dados – (RGPD) norma interna e aplicável aos 28 Estados Membros.

O novo Regulamento Geral tem por finalidade pacificar os conflitos originados das interações virtuais, sendo reconhecida pela Comissão Europeia como *Digital Single Market*[39], ou seja, uma estratégia ante a globalização das tecnologias e serviços na internet.

O RGPD, nos seus onze primeiros artigos, compreendem as garantias fundamentais que asseguram uma aplicação a longo prazo, mesmo estando suscetivel as influências do desenvolvimento tecnologócio (GUIDI, 2017).

---

38 A União Europeia é uma união econômica e política de características únicas, constituída por 28 países europeus que, em conjunto, abarcam grande parte do continente europeu, foi criada logo após a Segunda Guerra Mundial. A intenção inicial era incentivar a cooperação econômica, partindo do pressuposto de que se os países tivessem relações comerciais entre si, se tornariam economicamente dependentes uns dos outros, reduzindo, assim, os riscos de conflitos.

39 Conforme a EUROPEAN COMMISION. Digital Single Market.

Abrange conceitos considerados chaves para a hermeneutica juridica, como dado pessoal[40], processamento[41], consentimento[42], e tantos outros que definem a aplicabilidade do próprio RGPD.

O conceito de dados pessoais para o RGPD, é extensivo por tratar-se de qualquer infornação que identifique um indivíduo além do seu nome, imagem, telefone ou e-mail, abrangendo a localização do usuário e do IP da máquina, bem como a proibição dos dados sensíveis[43] que alcançam etnia, raça, religião, dados genéticos.

Verifica-se conforme Zarski (2017) que o conceito de dados trazido pelo RGPD, demonstra sua preocupação em adaptar a legislação com a velocidade da evolução da tecnológica, se opondo a outrora condição reducionista[44], alcançando também os dados sensíveis quanto ao con-

40 De acordo com o artigo 4 (1) do Regulamento Geral de Proteção de Dados (RGPD) nª 2016/679 do Parlamento Europeu e do Conselho (UE), dadaos pessoais, são relativos a informação de uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

41 De acordo com o artigo 4 (2) do Regulamento Geral de Proteção de Dados (RGPD) nº 2016/679 do Parlamento Europeu e do Conselho (UE), processamento é uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

42 De acordo com o artigo 4 (11) do Regulamento Geral de Proteção de Dados (RGPD) nº 2016/679 do Parlamento Europeu e do Conselho (UE), consentimento do titular dos dados é uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

43 De acordo com o artigo 9, do Regulamento Geral de Proteção de Dados (RGPD) nº2016/670, é proibido o processamento de dados pessoais revelando origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, ou filiação sindical, e processamento de dados genéticos, dados biométricos com a finalidade de identificar unicamente uma pessoa singular, dados relativos à saúde ou dados relativos a um sexualidade ou orientação sexual de uma pessoa.

44 Conforme Zarski (2017), a literatura profissional fala em 4 volumes, sobre proteção de dados coletados, a variedade de fontes, a velocidade que a análise consegue ser feita, e a

sentimento, a coleta, a fiscalização e a responsabilização inidivualizada (princípio da responsabilidade)[45] e cominações de sanções.

Evidencia-se também no RGPD o surgimento dos chamados novos direitos informacionais oriundos dos desdobramenos da internet, como o direito ao esquecimento e a oposição ao tratamento de dados, direito de portabilidade de dados para transferência de dados pessoais, proteção de dados por design e por definição[46].

O RGPD também abrange as questões de extraterritorialidade, ou seja, é aplicada tanto para os estabelecimentos[47] nos limites dos territorios da União Europeia, quanto as empresas que operam o tratamento de dados fora dos limites territoriais, conforme o artigo 3(1)[48].

Milard (2013) aponta que o RGPD ainda no artigo 3, alcança aqueles que utilizam da computação em nuvem por arranjos pelos quais recursos computacionais são fornecidos de modo flexível e independentemente

---

veracidade da informação final que é atingida, de acordo com o conselho europeu a diretiva 95/46 revogada conceituava dados pessoais como nome, imagem, endereço, e-mail, telefone e identificação pessoal.

45 O princípio da responsabilidade norteia a gestão de dados por empresas e entes da administração pública, quais são civilmente responsabilizadas pelo armazenamento e proteção de todos os dados pessoais, decorrendo obrigação de reparar os danos causados aos titulares das informações coletadas e armazenadas decorrente de violação ou vazamento. O RGPD, estabelece no Artigo 33: "Em caso de violação dos dados pessoais, o responsável pelo tratamento deve, sem demora injus-tificada e, se exequível, no prazo de 72 horas após ter tomado conhecimento, notificar a violação dos dados pessoais à autoridade de supervisão competente nos termos do artigo 55.º, a menos que seja improvável que a violação de dados pessoais resulte num risco para os direitos e liberdades das pessoas singulares".

46 UNIÃO EUROPEIA. **Tribunal de Justiça da União Europeia**. Grande Secção. Processo C-131/12, Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González. Luxemburgo, 13/05/2014.Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT

47 UNIÃO EUROPEIA. O conceito de estabelecimento se "estende a toda atividade real e efetiva ainda que mínima exercida mediante uma instalação estável. Court of Justice of European Union. Third Chamber. Case C-230/14, Weltimmo s. r. o. v. Nemzeti Adat-védelmi és Információszabadság Hatóság. Luxemburgo, 01/10/2015. Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT

48 Artigo 3(1), GPDR: „O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União".

da localização, que permitem uma rápida e ininterrupta alocação de recursos sob demanda, incluindo o subcontratante ou operador atuantes em qualquer fase do tratamento de dados pessoais.

Contudo para De Hert e Czerniawski (2017), o artigo 3 (2) é a maior conquista da reforma, por incidir sua aplicabilidade na proteção de dados das pessoas residentes na União Europeia, ainda que tenha sido efetuado por responsável/operador não estabelecidos no território europeu, mas que as operações de tratamento se relacionarem à oferta de bens ou serviços, independentemente da exigência de pagamento e ao monitoramento do seu comportamento, desde que tal conduta ocorra no espaço territorial da UEA.

Deste modo é inconteste que o monitoramento e a publicidade comportamental, para a coleta de informações pessoais por entidades responsáveis mesmo que estabelecidas fora do território da UEA, incidirá as normas do RGPD.

Na questão de extraterritorialidade para a transferência de dados, o RGPD disciplina nos artigos 44 a 50[49] a condição de cedente, na disponibilidade das informações pessoais ao agente responsável ou operador, ou seja, a coleta de dados, a transmissão pelo cedente ao recepetor no Estado estrangeiro, e o tratamento de dados para sua armazenagem (GIMENEZ, 2015).

Observa-se portanto a exigencia de se ter um cedente ora responsável/operador, e a aplicação automática do RGPD, e um receptor de dados que diante da incerteza da aplicabidade da normativa, aplica-se uma prévia verificação do nível de proteção do país ou organização de destino afim de resguardar conforme Piroddi (2016), o risco de ofensa a direitos e liberdades fundamentais dos cidadãos da União Européia.

[49] Princípio Geral da Transferência normatiza a transferência de dados pessoais em tratamento ou destinada a ser processada após a transferência para um país terceiro ou para uma organização internacional só deve ocorrer se, sem prejuízo das outras disposições do presente regulamento, forem cumpridas as condições estabelecidas no presente capítulo. com o responsável pelo tratamento e o processador, incluindo as transferências subsequentes de dados pessoais do país terceiro ou de uma organização internacional para outro país terceiro ou para outra organização internacional, a fim assegurar que o nível de proteção das pessoas singulares garantido pelo presente regulamento não seja infirmado (RGPD, 2016).

Após a análise do nível de proteção do país ou organização receptor de dados, a uma decisão de adequação[50], ou seja, a comissão européia impõem condições como apresentação de garantias adequadas ou regras empresarias vinculativas, capaz de gerar a responsabilidade organizacional quanto a previsão de programas de privacidade, *data protection officer,* relatório de impacto, regras e códigos de conduta, normas comparativas, orientações, independentemente da sua localização ou jurisdição, suscetíveis a revisão no período mínimo de quatro em quatro anos (PIRODDI, 2016).

Entretanto Albrecth (2017), ressalta que dentre os inúmeros pontos positivos do RGPD, elencada pela doutrina majoritária em razão da busca incessante pelo aprimoramento da proteção de dados como direito fundamental ou de privacidade, há uma minoria de doutrinadores, que aponta para um desiquilibrio entre o RGPD e o cenário tecnológico atual e futuro como fator limitar de novas tecnologias baseadas principalmente na inteligência artificial.

Contudo os fatores de impacto do RGPD alcançam a legislação brasileira a LGPD, denominada de Lei Geral de Proteção de Dados Pessoais, nº 13.709/2018[51], fonte de inúmeros debates legislativos desde 2010, baseados na imagem e semelhança da legislação europeia na proteção

[50] A transferência de dados pessoais para um país terceiro ou uma organização internacional pode ter lugar quando a Comissão tiver decidido que o país terceiro, um território ou um ou mais sectores especificados nesse país terceiro ou a organização internacional em questão garantem um nível adequado de proteção, não se tratando de uma autorização específica, mas sim uma adaptação qual deverá ser verificada o respeito aos direitos humanos e liberdades fundamentais, legislação específica do Estado quando a proteção de dados e segurança pública, regras de transferência de dados, existencia de autoridade de supervisão e execução, outros compromissos internacinais de proteção de dados (RGPD, 2016).

[51] BRASIL. Lei nº 13.709 de agosto de 2018. Dispões sobre a proteção de dados e altera a Lei nº 12.965 de 23 de abril de 2014, Marco Civil da Internet. Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 18 de mar. 2019.

de dados como direito fundamental, mais distante da preocupação com aplicação extraterritorial (MONTEIRO, 2017).

Deste modo, um dos aspectos mais importantes da LGPD após agosto de 2020, quando da sua entrada em vigor é o impacto transversal e multissetorial, no setor público ou privado, para pessoas física ou jurídica, independente do meio, país sede ou do país em que os dados estejam localizados, e que o tratamento seja realizado em território nacional com obejtivo de ofertar ou fornecer bens e serviços (LGPD, 2018).

Assim sendo toda a empresa ou entidade estrangeira, com filial no Brasil, que ofertar ou fornecer bens e serviços ao mercado nacional, coletando ou tratando dados localizados em território brasileiro, estará sujeito à nova lei, não podendo os dados pessoais usados de maneira indiscriminada (LGPD, 2018).

No *e-commerce* a LGPD se insere no contextos contratuais impedindo que os dados pessoais sejam coletados ou utilizados sem o consentimento do seu titular, percebendo aos consumidores direito de questionar serviços de edição ou exclusão de suas informações, portabilidade, além de aplicar penalidades financeiras que variam de 2% do faturamento da empresa até 50 milhões por infração cometida (LGPD, 2018).

Portanto, entre o RGPD e a LGPD no *e-commerce*, a base legal a ser aplicada será aquela adestrida as claúsulas contratuais entre exportador e importador de dados, garantindo assim uma maior efetividade da proteção aos direitos fundamentais e de privacidade dos seus titulares nas relações jurídicas consumeristas e contratuais estabelecidas online.

## 5 CONSIDERAÇÕES FINAIS

O artigo ora desenvolvido, não possui a pretensão de exaurir a questão da análise dos elementos clássicos de conexão do Direito Internacional, para uma correta aplicação da legislação LGPD e/ou RGPD nas relações jurídicas consumeristas e contratuais estabelecidas online, que se encontra delimitada na esfera da Governança Global.

Isso porque a evolução das tecnologias da informação e comunicação (TICs), trazem ao Direito Interno e Internacional a frequente preocupação de atualizar suas legislações a fim de acompanhar as novas relações de consumo e contratuais realizadas por pessoas físicas ou jurídicas, públicas ou privadas no *e-commerce*.

Para tanto, tal preocupação se reflete na promulgação da Lei 13.709 de 2018 no Brasil, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), vigente apenas em agosto de 2020, com texto inspirado na atual Legislação Europeia sobre o tema (Regulamento Geral de Proteção de Dados – RGPD) de 2016.

Inconteste que ambas as legislações independentemente do espaço geográfico ou organizacional em que forem aplicadas ou aplicáveis, trará impacto considerável a sociedade como poucas leis fizeram, haja vista sua característica peculiar de ser ao mesmo tempo transversal e multisetorial.

Destarte, vale a ressalva de que ambas legislações buscam nas suas questões particulares de territorialidade ou de extraterritorialidade, a concretização do *e-commerce* nas relações consumeristas e contratuais, na proteção de dados como direito fundamental, bem como no fomento por novas tecnologias.

Diante do exposto pela análise jurídica e reflexiva ao tema, é possível verificar a preocupação seja pela União Europeia ou pelo Brasil, de que suas legislações estejam o mais próximo de condizerem com as evoluções quase que em tempo real da tecnologia e das relações por elas geradas como o *e-commerce*, principalmente na proteção de dados, a fim de obstar eventuais danos aos titulares das informações.

Contudo, não se pode olvidar de que o direito ao possuir estreita relação com as tecnologias, já que está se trata de um sistema de informação, necessita de meio eficaz e formal, objetivando amparo jurídico e equilíbrio entre as partes envolvidas no processo para satisfazer as demandas da sociedade *on-line*.

## REFERÊNCIAS

ALBRECHT, J. P. How the GDPR Will Change the World. **European Data Protection Law Review**, v. 2, n. 3, p. 287–289, 2017.

ANTUNES, L. D; ROSA, M.; BIAZETTI, B. O. de.; VILELA, P.; PORTO, O. **Jurisdição e conflitos de lei na era digital. Quadro político-normativo de regulamentação na internet.** Instituto de Referência em Internet e Sociedade. Disponível em: file:///E:/M%20e%20L/artigo/texto%202.pdf. Acesso em: 04 mar. 2019.

AZEVEDO, F.A. **Mídia e democracia no Brasil:** revelações entre o sistema de mídia e o sistema político. Opinião Pública, Campinas, vol. 12, nº 1, Abril/Maio, 2006, p. 88-113.

BACHELARD, G. **A formação do espírito científico:** contribuição para uma psicanálise do conhecimento. Rio de Janeiro: Contraponto, 1996.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 24 fev. 2019.

BRASIL. **Código Civil.** Lei nº 10.406 de 10 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 25 fev. 2019.

BRASIL. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia.** Escola Nacional de Defesa do Consumidor; coord. Danilo Doneda. Brasília: SDE/DPDC, 2010.

BRASIL. ***E-commerce*.** Lei nº 8.078, de 11 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acesso em: 20 fev. 2019.

BRASIL. **Contratação no Comércio Eletrônico.** Decreto nº 7962 de 15 de março de 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato20112014/2013/Decreto/. Acesso em: 20 fev. 2019.

BRASIL. IBGE- **Instituto Brasileiro de Geografia e Estatística.** Disponivel em: https://www.ibge.gov.br/. Acesso em: 14 fev. 2019.

BRASIL. LICC. Decreto-lei nº 4.657, de 4 de setembro de 1942. **Lei de Introdução ao Código Civil. Diário** Oficial da União, Brasília, DF, 9 set. 1942. Disponível em: www.planalto.gov.br/ccivil/Decreto-Lei/Del4657. Acesso em: 11 de mar. 2019.

BRASIL. LINDB. **Lei de Introdução as Normas do Direito Brasileiro.** Lei nº 12.376 de 2010. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Lei/L12376.htm#art2. Acesso em: 11 mar. 2019.

BRASIL. JUSBRASIL. **Jurisprudências.** Disponível em: Jusbrasil. https://stj.jusbrasil.com.br/jurisprudencia/19128034/recurso-especial-resp-1168547-rj--20070252908-3-stj. Acesso em: 26 fev. 2019.

BRASIL. ONU. **Organização Nacional das Nações Unidas.** Disponível em: https://computerworld.com.br/2018/07/12/10-mudancas-que-nova-lei-de-protecao-de-dados-pessoais-deve-trazer-ao-cotidiano/. Acesso em: 24 fev. 2019.

BRASIL. ONU. **Declaração Universal dos Direitos Humanos.** Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/. Acesso em: 28 fev. 2019.

BRASIL. SERPRO. **Serviço Brasileito de Proteção de Dados.** Disponível em: http://www.serpro.gov.br/. Acesso em: 20 fev. 2019.

BRASIL. Lei nº 13.709 de agosto de 2018. **Dispões sobre a proteção de dados e altera a Lei nº 12.965 de 23 de abril de 2014, Marco Civil da Internet.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 18 mar. 2019.

BUSH, V. **As we may think, 1945. Tradução de Luana Villac. Revista Latina Americana de Psicopatologia Fundamental.** São Paulo, v.14, n.1. mar. 2011. Disponível em: http://www.fundamentalpsychopathology.org.br/pagina-revista-latinoamericana-de psicopatologia-fundamental-108. Acesso em: 24 fev. 2019.

CASTELLS, M. **A galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Jorge Zahar, 2003.

CASTELLS, M. **La Era de la información: economi´a, sociedad y cultura**. México: Siglo Veintiuno Editores, 1999.

CASTRO, C. S. e. **Direito da informática, privacidade e dados pessoais.** Coimbra: Edições Almedina, 2005.

CORREIA, A. F. – **Lições de Direito Internacional Privado**, 1ª edição, Almedina, Coimbra:–2000.

DE HERT, P.; CZERNIAWSKI, M. **Expanding the European data protection scope beyond territory.** cit. , p. 239. Vide, tam-bém, BU-PASHA, S. Cross-border issues

under EU data protection law with regards to personal data protection. In: Information & Communications Technology Law, v. 26, n. 3, p. 218, 2017.

DEL'OLMO, F. S. de. **Curso de Direito Internacional Privado.** Rio de Janeiro: Forense, 2010.

DINIZ, M. H. **Tratado teórico e prático dos contratos.** São Paulo: Saraiva, vol. 1. 1993.

DINIZ, M. H. **Curso de direito civil brasileiro** : teoria das obrigações contratuais e extracontratuais. 24. ed. rev., atual. e ampl. de acordo com a reforma do CPC e com o Projeto de Lei n. 276/2007. São Paulo: Saraiva, 2008.

DUMAS, V. **A origem da Internet. História Viva.** Disponível em: http://revistahistorien.blogspot.com/2011/08/origem-da-internet.html. Acesso em: 14 de fev. 2019.

EUROPA. **Carta dos Direitos Fundamentais da União Europeia. Jornal Oficial das Comunidade Euopeias. 18.12.2000.**

Disponível em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 25 fev. 2019.

EUROPA. **Convenção Europia dos Direitos do Homem**. Tribunal Europeu dos Direitos do Homem Council of Europe. Strasburg. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 14 mar. 2019.

EUROPA. **Directiva 95/46/CE**. 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. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 14 mar. 2019.

EUROPA. **Regulamento (CE) nº 593/2008 do Parlamento Europeu e do Conselho, de 11 de julho de 2007, sobre a lei aplicável às obrigações contratuais (Roma I).** Jornal Oficial da União Europeia, Estrasburgo, 04/07/2008. P. 5. Disponível em: https://goo.gl/QGFZqy. Acesso em: 14 mar. 2019.

EUROPA. **Regulamento (CE) nº 864/2007 do Parlamento Europeu e do Conselho, de 11 de julho de 2007, relativo à lei aplicável às obrigações extracontratuais (Roma II).** Jornal Oficial da União Europeia, Estrasburgo, 31/07/2007, p: 5. Disponível em: https://goo.gl/fW4wkd. Acesso em: 14 mar. 2019.

EUROPEAN COMMISION. **Digital Single Market**. Disponível em: https://goo.gl/GX1HpK. Acesso em: 14 mar. 2019.

FROMHOLZ, J. The European Union data privacy directive. **Berk. Tech. Law Journal**, v. 15, 2000. p. 461-484.

RGPD. **Regulamento Geral de Proteção dos Dados Pessoais**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679. Acesso em: 14 mar. 2019.

GIMÉNEZ, A. O. **La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita.** Madrid: Agencia Española de Protección de Datos, 2015. p. 61; BU-PASHA, S. Cross-border issues under EU data protection law with regards to personal data protection.cit, p. 214.

GLANZ, S. **Contrato Eletrônico, 2004, p. 29.** In: ANDRADE, Ronaldo Alves de. Contrato Eletrônico, São Paulo, Editora Manole, 2004.

GUIDI, G. **Modelos regulatórios para proteção de dados pessoais**. Disponível em: http://www.itsrio.org/wp-content/uploads. Acesso em: 13 mar. 2019.

KANT, I. **Fundamentação Da Metafísica Dos Costumes E Outros Escritos**. São Paulo: Martin Claret, 2008.

KLEE, A. E. L. **Comércio eletrônico**. São Paulo: Editora Revista dos Tribunais, 2014.

KONH, K. ; MORAES C. H. de. **O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade da Informação e da Sociedade Digital.** Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação XXX Congresso Brasileiro de Ciências da Comunicação – Santos – 29 de agosto a 2 de setembro de 2007. Disponível em: https://www.intercom.org.br/papers/nacionais/2007/resumos/R1533-1.pdf. Acesso em: 14 fev. 2019.

KUROSE, J. F.; ROSS, K. W. **Redes de computador e a Internet: uma abordagem top-down.** São Paulo: Addison Wesley, 2010.

LAWAND, J. J. **Teoria geral dos contratos eletrônicos.** São Paulo: Editora Juarez de Oliveira, 2003.

LEAL, S. R. C. S. do. **Contratos eletrônicos: validade jurídica dos contratos via internet.** 1.ed. São Paulo: Atlas, 2009.

LEGIS. CNPD. **Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatixado de Dados de Caráter Pessoal.** Disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 20 fev. 2019.

LEITE, B.S. **Tecnologias no ensino de química: teoria e prática na formação docente.** Curitiba: Appris, 2015.

LÉVY, P. **A Revolução contemporânea em matéria de comunicação**. In: MARTINS, Francisco Menezes; SILVA, Juremir Machado da (Orgs.). Para navegar no século XXI. Porto Alegre: Sulina/Edipucrs, 2000.

LISBOA, R. S. **A inviolabilidade de correspondência na Internet.** In: LUCCA, N. de; SIMÃO FILHO, A. Direito e Internet. Aspectos Jurídicos Relevantes. Bauru, SP: Edipro, 2001.

MARQUES, C. L. **Confiança no comércio eletrônico e a proteção do consumidor: (um estudo dos negócios jurídicos de consumo no comércio eletrônico).** São Paulo: Revista dos Tribunais, 2004.

MCNEILL, W. H. **Information and transportation nets in world history. World-System History: The Social Science of Long-Term Change.** R. A. DENEMARK. London, UK, Routledge, 2000.

MENDES, G. ; B, P. G. G. **Curso de Direito Constitucional.** 7 ed. São Paulo: Saraiva, 2011.

MENDONÇA, E. **Epistemologia, Tecnologia, Paradigma: as origens da Ciência da Informação.** Datagramazero, Rio de Janeiro, v. 15, 2014. Disponível em: http://www.brapci.inf.br/index.php/article/download/51760. Acesso em: 20 fev. 2019.

MICHAELIS, **Dicionário de Português Online.** Disponível em: https://www.google.com/search?ei=iv5yXOyrO7nB5OUPofm1yAY&q=site+dodicionario+mikaelis&oq=site+dodicionario+mikaelis&gs_l=psyab.3..33i10.7431.9043..9815...1.0..0.158.989.0j8.....0....1..gws-wiz.....0i71j0i13j0i13i30.J3o_MQHgSuQ. Acesso em: 14 fev. 2019.

MILLARD, C. (Ed.). **Cloud Computing Law.** E-book. Tradução livre do orginal: "an arrangement whereby computing resources are provided on a flexible, location-independent basis that allows for rapid and seamless allocation of resources on demand." Oxford: Oxford University Press, 2013.

MONTEIRO, R. L. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Artigo Estratégico 39**, Instituto Igarapé, dez. 2018.

MOTA, Carlos Esplugues; BUJIGUES, José L. I.; PALAO MORENO, Guillhermo. **Derecho Internacional Privado.** 13a ed. Tirant lo Blanch: Valência, 2019.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6 ed. São Paulo: Saraiva, 2016

PIRODDI, P. **I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati**. In: RESTA, Giorgio; ZENO-ZENCOVICH, Vincezo (Coord.). La protezione transazionale dei dati personali. Roma: Roma-Tre Press, 2016. p. 198-199.

RODOTÀ.S. **Tecnologia e diritti.** Bologna: Il Mulino, 1995.

ROSENAU, J. **Governança, ordem e mudança na política mundial.** In: ROSENAU, J.; CZEMPIEL, E. O. Governança sem governo: ordem e transformação na política mundial. Brasília, DF: Unb, 2000.

SALGARELLI, K. C. **Direito do consumidor no comércio eletrônico: uma abordagem sobre confiança e boa-fé.** 1 ed. São Paulo: Ícone, 2010.

SARTORI, E. C. M. **Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na Internet.** Revista de Direito Civil Contemporâneo | vol. 9/2016. Out - Dez / 2016. p. 59.

SCHMIDT NETO. A. P. **Contratos na sociedade de consumo: vontade e confiança.** São Paulo: Editora Revista dos Tribunais, 2016.

TATEOKI, V. A. **A proteção de dados pessoais e a publicidade comportamental.** Revista Juris UniToledo, Araçatuba, SP, v. 02, n. 01, p. 62/75, jan./mar. 2017. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/113-2706-1-pb.pd. Acesso em: 14 fev. 2019.

TECMUNDO. **Bilhões de Pessoas usam internet no mundo.** Disponível em: https://www.tecmundo.com.br/internet/126654-4-bilhoes-pessoas-usam-internet-no-mundo.htm. Acesso em: 14 fev. 2019.

UNIÃO EUROPEIA. **A União Europeia**. Disponível em: https://goo.gl/fz7U3z. Acesso em: 13 mar. 2019.

UNIÃO EUROPEIA. **Tribunal de Justiça da União Europeia.** Grande Secção. Processo C-131/12, Google Spain SL, Google Inc. c. Agencia Española de Protección

de Datos (AEPD), Mario Costeja González. Luxemburgo, 13/05/2014.Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT. Acesso em: 13 mar. 2019.

UNIÃO EUROPEIA. **O conceito de estabelecimento se "estende a toda atividade real e efetiva ainda que mínima exercida mediante uma instalação estável. Court of Justice of European Union. Third Chamber.** Case C-230/14, Weltimmo s. r. o. v. Nemzeti Adat-védelmi és Információszabadság Hatóság. Luxemburgo, 01/10/2015. Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT. Acesso em: 13 mar. 2019.

VICENTE, Dário Moura. **Direito Internacional Privado**. Vol. I, II e III. Editora Almedina, 2010, Coimbra.

WACHOWICZ, Marcos; FONTOURA COSTA, José Augusto. **Cláusulas contratuais nulas no Marco Civil da Internet.** In Revista da Faculdade de Direito da Universidade Federal de Minas Gerais - UFMG, Belo Horizonte, n. 68, pp. 477-496, jan./jun. 2016. Acesso em: 15 de março de 2019: http://www.gedai.com.br/wp-content/uploads/2016/12/artigo_clausulas_contratuais_nulas_marco_civil_internet-1.pdf

O livro **"PROTEÇÃO DE DADOS PESSOAIS EM PERSPECTIVA: LGPD e RGPD na ótica do direito comparado"** é fruto de trabalho de pesquisa desenvolvido pelo Grupo de Estudos de Direito Autoral e Industrial – GEDAI, dentro das atividades acadêmicas realizadas no Programa de Pós-Graduação em Direito da Universidade Federal do Paraná – PPGD/UFPR.

O leitor perceberá que tem diante de seus olhos uma obra coesa, com interconexões internas entre seus capítulos, que dialogam entre si, erigindo um pensamento jurídico uniforme e sistêmico, cujas partes se complementam e harmonizam.

Apoio:

CAPES

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

GEDAI
Grupo de Estudos de Direito Autoral e Industrial
Universidade Federal do Paraná

PPGD
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
Mestrado, Doutorado e Pós-doutorado

GEDAI
PUBLICAÇÕES