

# **VI ENCONTRO VIRTUAL DO CONPEDI**

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I**

**FREDERICO THALES DE ARAÚJO MARTOS**

**JÉSSICA AMANDA FACHIN**

**AIRES JOSE ROVER**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

**Diretoria - CONPEDI**

**Presidente** - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

**Diretora Executiva** - Profa. Dra. Samyra Haydêe Dal Farra Napolini - UNIVEM/FMU - São Paulo

**Vice-presidente Norte** - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

**Vice-presidente Centro-Oeste** - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

**Vice-presidente Sul** - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

**Vice-presidente Sudeste** - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

**Vice-presidente Nordeste** - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

**Representante Discente:** Prof. Dra. Sinara Lacerda Andrade - UNIMAR/FEPODI - São Paulo

**Conselho Fiscal:**

Prof. Dr. Caio Augusto Souza Lara - ESDHC - Minas Gerais

Prof. Dr. João Marcelo de Lima Assafim - UCAM - Rio de Janeiro

Prof. Dr. José Filomeno de Moraes Filho - Ceará

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Prof. Dr. Valter Moura do Carmo - UNIMAR - São Paulo

**Secretarias**

**Relações Institucionais:**

Prof. Dra. Daniela Marques De Moraes - UNB - Distrito Federal

Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM - São Paulo

Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie - São Paulo

**Comunicação:**

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - Paraíba

Prof. Dr. Matheus Felipe de Castro - UNOESC - Santa Catarina

**Relações Internacionais para o Continente Americano:**

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

**Relações Internacionais para os demais Continentes:**

Prof. Dr. José Barroso Filho - ENAJUM

Prof. Dr. Rubens Beçak - USP - São Paulo

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicritiba - Paraná

**Eventos:**

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - Minas Gerais

Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC - Paraná

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - Mato Grosso do Sul

**Membro Nato** - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UMICAP - Pernambuco

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires Jose Rover; Frederico Thales de Araújo Martos; Jéssica Amanda Fachin – Florianópolis; CONPEDI, 2023.

Inclui bibliografia

ISBN: 978-65-5648-745-8

Modo de acesso: [www.conpedi.org.br](http://www.conpedi.org.br) em publicações

Tema: Direito e Políticas Públicas na era digital

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VI Encontro Virtual do CONPEDI (1; 2023; Florianópolis, Brasil).

CDU: 34



# VI ENCONTRO VIRTUAL DO CONPEDI

## DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

---

### **Apresentação**

O VI Encontro Virtual do CONPEDI, realizado em parceria com o Programa de Mestrado Profissional em "Direito, Sociedade e Tecnologias" das Faculdades Londrina e a Faculdade de Direito de Franca (FDF), ocorreu nos dias 20, 21, 22, 23 e 24 de junho de 2023. O evento teve como temática central "Direito e Políticas Públicas na Era Digital". As discussões realizadas durante o encontro, tanto nas diversas abordagens tecnológicas como nos Grupos de Trabalho (GTs), foram de grande relevância, considerando a atualidade e importância do tema.

Nesta publicação, os trabalhos apresentados como artigos no Grupo de Trabalho "Direito, Governança e Novas Tecnologias I", no dia 23 de junho de 2023, passaram por um processo de dupla avaliação cega realizada por doutores. A obra reúne os resultados de pesquisas desenvolvidas em diferentes Programas de Pós-Graduação em Direito, abordando uma parte significativa dos estudos produzidos no âmbito central do Grupo de Trabalho.

As temáticas abordadas refletem intensas e numerosas discussões que ocorrem em todo o Brasil. Elas destacam o aspecto humano da Inteligência Artificial, os desafios para a democracia e a aplicação do Direito no ciberespaço, bem como reflexões atuais e importantes sobre a regulação das plataformas digitais e as repercussões das novas tecnologias em diversas áreas da vida social.

Esperamos que, por meio da leitura dos textos, o leitor possa participar dessas discussões e obter um entendimento mais amplo sobre o assunto. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e na organização do evento, cujas contribuições inestimáveis foram fundamentais, e desejamos uma leitura proveitosa!

Prof. Dr. Aires Jose Rover - Universidade Federal de Santa Catarina/SC

Profa. Dra. Jéssica Fachin - Faculdades Londrina/PR

Prof. Dr. Frederico Thales de Araújo Martos - Faculdade de Direito de Franca/SP e Universidade do Estado de Minas Gerais/MG

# O DIREITO AO ESQUECIMENTO DIGITAL À LUZ DA LGPD BRASILEIRA E DA GDPR EUROPEIA

## DIGITAL RIGHT TO BE FORGOTTEN IN LIGHT OF BRAZILIAN LGPD AND EUROPEAN GDPR

Cildo Giolo Junior <sup>1</sup>  
Pablo Martins Bernardi Coelho <sup>2</sup>  
Manoel Ilson Cordeiro Rocha <sup>3</sup>

### Resumo

O direito ao esquecimento digital refere-se à capacidade dos indivíduos de solicitar a remoção de informações pessoais desatualizadas ou irrelevantes dos meios digitais. Tanto a GDPR europeia, assim como a LGPD brasileira, estabelece marcos legais para a proteção de dados, incluindo também diretrizes sobre o direito ao esquecimento. O tema tem sido objeto de muitas discussões nos Tribunais europeus, que, em suas decisões, têm inclusive estabelecido diretrizes e limites para sua aplicação. Da mesma forma, no Brasil, o assunto tem sido muito debatido e as decisões caminham no sentido de que o direito ao esquecimento não é absoluto e que está sujeito a certas condições e limitações. Desta forma, as comparações entre os regulamentos e julgamentos foram salutares para compreender que, tanto na Europa, quanto no Brasil, existe a necessidade de se equilibrar a privacidade individual com a liberdade de expressão e o interesse público na informação, bem como a importância de adaptar o conceito de esquecimento à realidade da era digital. A metodologia adotada foi a dedutiva com a utilização dos métodos bibliográfico e a utilização da jurisprudência para corroborar a necessidade de políticas públicas específicas.

**Palavras-chave:** Direito ao esquecimento, Lgpd, Gdpr, Posicionamento dos tribunais, Privacidade

### Abstract/Resumen/Résumé

The right to digital oblivion refers to the ability of individuals to request the removal of outdated or irrelevant personal information from digital media. Both the European GDPR and the Brazilian LGPD establish legal frameworks for data protection, also including guidelines on the right to be forgotten. The subject has been the subject of many discussions

---

<sup>1</sup> Pós-Doutor pela Universidade de Coimbra. Doutor e Mestre em Direito. Professor da Faculdade de Direito de Franca e da Universidade do Estado de Minas Gerais.

<sup>2</sup> Doutor em História pela UNESP. Mestre em História pela UNESP. Professor de Direito na Universidade do Estado de Minas Gerais.

<sup>3</sup> Pós-Doutorando pela FGV-SP. Doutor em Direito pela Universidade de Lisboa. Mestre em Direito pela UNESP. Professor da Faculdade de Direito de Franca.

in the European Courts, which, in their decisions, have even established guidelines and limits for its application. In the same way, in Brazil, the subject has been much debated and the decisions are moving in the direction that the right to be forgotten is not absolute and that it is subject to certain conditions and limitations. In this way, comparisons between regulations and judgments were salutary to understand that, both in Europe and in Brazil, there is a need to balance individual privacy with freedom of expression and the public interest in information, as well as the importance of adapt the concept of forgetting to the reality of the digital age. The methodology adopted was deductive with the use of bibliographic methods and the use of jurisprudence to corroborate the need for specific public policies.

**Keywords/Palabras-claves/Mots-clés:** Right to be forgotten, Lgpd, Gdpr, Courts position, Privacy

## 1 INTRODUÇÃO

“[...] the digitization and disclosure of life’s personal details will forever tether us to all our past actions, making it impossible, in practice, to escape them.” (MAYER-SCHÖNBERGER, 2009)

A era digital trouxe consigo inúmeros avanços na maneira como nos comunicamos e acessamos informações. No entanto, a crescente facilidade com que dados pessoais podem ser compartilhados e armazenados online também levanta preocupações sobre privacidade e proteção de dados. Neste contexto, o direito ao esquecimento digital emerge como um tópico relevante e desafiador. Este direito visa permitir que indivíduos solicitem a remoção de informações pessoais desatualizadas ou irrelevantes de meios digitais. A aprovação da Lei Geral de Proteção de Dados (LGPD) no Brasil e do Regulamento Geral de Proteção de Dados (GDPR) na União Europeia reflete a crescente importância da proteção de dados pessoais e do direito ao esquecimento.

A justificativa deste estudo é analisar o direito ao esquecimento digital à luz da LGPD brasileira e da GDPR europeia, destacando as semelhanças e diferenças entre os dois regimes, a fim de identificar as melhores práticas e desafios em ambas as jurisdições. Além disso, busca compreender como tribunais e órgãos reguladores têm lidado com questões relacionadas ao direito ao esquecimento, contribuindo assim para o debate jurídico e acadêmico sobre o tema.

Os objetivos deste paper incluem examinar os princípios e disposições do direito ao esquecimento na LGPD e na GDPR; analisar a jurisprudência e as decisões regulatórias relacionadas ao direito ao esquecimento no Brasil e na União Europeia; identificar os desafios e as melhores práticas na aplicação do direito ao esquecimento em ambas as jurisdições; e discutir a necessidade de políticas públicas específicas para abordar o direito ao esquecimento digital.

O direito ao esquecimento digital, relacionado à remoção de informações pessoais desatualizadas ou irrelevantes em meios digitais, é abordado tanto pela LGPD brasileira quanto pela GDPR europeia. A análise caso a caso tem sido a abordagem comum dos tribunais ao lidar com o direito ao esquecimento digital.

Para atingir esses objetivos, a metodologia adotada compreende uma abordagem dedutiva, utilizando métodos bibliográficos para revisar literatura acadêmica, legislação e documentos oficiais relevantes. Além disso, será realizada uma análise de casos e decisões jurisprudenciais nos âmbitos brasileiro e europeu para identificar tendências e desafios na aplicação do direito ao esquecimento digital.

## **2 OS MARCOS REGULATÓRIOS DE PROTEÇÃO DE DADOS NA EUROPA E NO BRASIL**

Importante se demonstrar o contexto de proteção de dados europeu e brasileiro, visto que o foco da presente pesquisa é fazer um corte diametral verificando como o assunto é tratado em ambas as legislações, nada mais apropriado do que demonstrar as conjunturas e realidades de ambos os regulamentos.

A Lei Geral de Proteção de Dados ou LGPD brasileira, foi aprovada em agosto de 2018 e entrou em vigor em setembro de 2020 (Lei nº 13.709). Esta lei tem como principal objetivo garantir a privacidade e proteção dos dados pessoais dos cidadãos brasileiros, estabelecendo regras e diretrizes claras para o tratamento e uso dessas informações por parte de empresas e órgãos públicos. Ela foi inspirada no *General Data Protection Regulation* – GDPR (UNIÃO EUROPEIA, 2016) da porque ambos os regulamentos têm objetivos e abordagens semelhantes na proteção de dados pessoais e na garantia da privacidade dos indivíduos. Por sua vez, a GDPR, que entrou em vigor em maio de 2018, tem sido considerada uma das legislações mais abrangentes e rigorosas em termos de proteção de dados e privacidade no mundo.

Diz-se que a LGPD brasileira foi influenciada no *General Data Protection Regulation* (GDPR) europeia porque ambos os regulamentos têm objetivos e abordagens semelhantes na proteção de dados pessoais e na garantia da privacidade dos indivíduos. A GDPR, que entrou em vigor em maio de 2018, tem sido considerada uma das legislações mais abrangentes e rigorosas em termos de proteção de dados e privacidade no mundo.

Com a crescente importância da proteção de dados e o exemplo do GDPR, o Brasil percebeu a necessidade de implementar uma legislação específica para regular e proteger os dados pessoais dos cidadãos. A LGPD (Lei Geral de Proteção de Dados) foi então promulgada em agosto de 2018 e entrou em vigor em setembro de 2020.

### **2.1 Antecedentes Normativos da GDPR**

Antes da implementação do Regulamento Geral de Proteção de Dados (GDPR) em maio de 2018, a legislação europeia sobre proteção de dados e privacidade era regida principalmente pelas seguintes normas:

A Convenção para a Proteção de Pessoas Singulares relativamente ao tratamento automatizado de dados de carácter pessoal, Convenção 108: Embora não seja uma legislação

específica da União Europeia, a Convenção 108, adotada em 1981 pelo Conselho da Europa, estabeleceu princípios gerais de proteção de dados para seus Estados-membros. A Convenção 108 foi a primeira vinculação legal internacional sobre proteção de dados pessoais e continua sendo um importante instrumento no campo da proteção de dados. (UNIÃO EUROPEIA, 1981)

A Diretiva de Proteção de Dados (95/46/EC): Adotada em 1995, esta diretiva estabeleceu as bases para a proteção de dados pessoais na União Europeia. A Diretiva de Proteção de Dados estabeleceu regras sobre o processamento e o fluxo de dados pessoais e introduziu conceitos como o consentimento do titular dos dados e a obrigação de informar. Cada Estado-membro implementou a diretiva em sua própria legislação nacional. (UNIÃO EUROPEIA, 1995)

A Diretiva de Privacidade e Comunicações Eletrônicas (2002/58/EC), também conhecida como Diretiva *e-Privacy*: Esta diretiva, adotada em 2002 e posteriormente revisada em 2009, abordava especificamente a proteção de dados e a privacidade no contexto das comunicações eletrônicas. Ela estabelecia regras sobre o uso de cookies, o envio de comunicações comerciais por e-mail e a proteção de dados em serviços de telecomunicações. (UNIÃO EUROPEIA, 2002)

Legislações nacionais: Antes do GDPR, cada país da União Europeia tinha sua própria legislação para a proteção de dados pessoais, com base nas diretrizes estabelecidas pela Diretiva de Proteção de Dados (95/46/EC). Por exemplo, na França, a legislação relevante era a Lei de Proteção de Dados de 1978 (modificada em 2004), enquanto na Alemanha, a Lei Federal de Proteção de Dados (BDSG) desempenhava um papel semelhante (KUNER, 2007).

O GDPR foi criado para unificar e fortalecer a proteção de dados na União Europeia, substituindo a Diretiva de Proteção de Dados e harmonizando a legislação de proteção de dados entre os Estados-membros. Ele estabelece requisitos mais rígidos para o processamento de dados pessoais e aumenta significativamente as sanções para o não cumprimento das normas de proteção de dados.

## **2.2 Antecedentes Normativos da LGPD**

Por outro lado, os antecedentes legislativos da LGPD (Lei Geral de Proteção de Dados) brasileira podem ser encontrados tanto na legislação nacional quanto nas diretrizes e regulamentações internacionais, incluindo:

A Constituição Federal de 1988: A Constituição do Brasil já estabelecia a proteção à privacidade como um direito fundamental (artigo 5º, 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;). Embora não fosse específica para a proteção de dados pessoais, a Constituição criou o alicerce para o desenvolvimento de leis nessa área.

O Código de Defesa do Consumidor (Lei 8.078/1990), também estabeleceu normas de proteção e defesa do consumidor e inclui disposições relacionadas à proteção de dados pessoais, como a obrigatoriedade de informações claras e adequadas sobre o uso de dados pessoais dos consumidores (artigo 43).

O Marco Civil da Internet (Lei 12.965/2014), ao estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, muito embora não seja específica para a proteção de dados pessoais, ela aborda aspectos de privacidade e define responsabilidades e obrigações para provedores de acesso e de conteúdo.

Além da influência já aqui narrada da GDPR (Regulamento Geral de Proteção de Dados) da União Europeia, que entrou em vigor em maio de 2018, o Brasil também foi inspirado por diretrizes e recomendações internacionais, como as Diretrizes da OCDE (Organização para a Cooperação e Desenvolvimento Econômico) sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais foram adotadas pela primeira vez em 1980 e atualizadas em 2013. Essas diretrizes servem como um conjunto de princípios comuns para os países membros e não membros desta organização, na proteção de dados pessoais e no equilíbrio da privacidade com outros interesses, como a livre circulação de informações, estabelecendo princípios norteadores para a limitação de coleta de dados, limitações sobre o uso, segurança e transparência, responsabilidade, participação pessoal, dentre outros (OCDE, 2013). Estas orientações, que merecem uma atenção maior em outra pesquisa, têm sido um marco importante no desenvolvimento de leis e regulamentações de proteção de dados em todo o mundo, e seus princípios podem ser encontrados tanto na LGPD brasileira, como em outras legislações de proteção de dados, como a GDPR europeia.

### **2.3 Semelhanças e Diferenças entre a LGPD da GPDR**

Apesar de contextos geopolíticos díspares, no que tange ao texto das normas, a LGPD brasileira e a GDPR europeia compartilham diversas semelhanças, como: ambas as leis aplicam-se não apenas às empresas e organizações estabelecidas em seus respectivos territórios, mas também às organizações localizadas fora de suas fronteiras, desde que processem dados de residentes do Brasil ou da União Europeia; tanto a LGPD quanto a GDPR estabelecem princípios-chave para o processamento de dados pessoais, como legalidade, lealdade,

transparência, limitação de finalidade, minimização de dados, exatidão, limitação de armazenamento, integridade e confidencialidade. Ambas as legislações preveem a figura do controlador e do operador de dados e estabelecem suas responsabilidades e obrigações.

Por outro lado, a LGPD e a GDPR exigem que as organizações obtenham o consentimento explícito dos indivíduos para o processamento de seus dados pessoais, com algumas exceções previstas em lei.

Ambas as leis estabelecem os direitos dos titulares dos dados, como o direito de acesso, retificação, oposição, eliminação, portabilidade e informação sobre o processamento de seus dados pessoais.

Os dois regulamentos previam a criação de autoridades nacionais de proteção de dados com o objetivo de supervisionar e aplicar as respectivas leis. Entre nós, a Lei nº 13.709, de 14 de agosto de 2018, criou a Autoridade Nacional de Proteção de Dados (ANPD), dentre outras providências. Na Europa, O Comité Europeu para a Proteção de Dados (CEPD) foi criado pela própria GDPR. O comitê é composto pelos representantes das autoridades nacionais de proteção de dados de todos os Estados-Membros da UE e tem como objetivo garantir a coerência na aplicação do regulamento de proteção de dados em toda a UE, bem como promover a cooperação entre as autoridades nacionais de proteção de dados.

Muito embora a LGPD e a GDPR compartilhem muitos aspectos e princípios comuns, existem inúmeras diferenças entre os regulamentos, originárias das particularidades que refletem o contexto legal, cultural e político específico de cada região.

No que diz respeito à abrangência geográfica, apesar de o GDPR se aplicar a todos os membros da União Europeia, e a LGPD ser uma lei federal brasileira, ambas as leis têm efeitos extraterritoriais, ou seja, se aplicam a entidades internacionais que oferecem serviços ou coletam dados de indivíduos nos respectivos territórios.

Ambas as leis exigem uma base legal para o tratamento de dados pessoais, o GDPR prevê seis bases legais, incluindo o consentimento, o cumprimento de obrigações legais, a execução de um contrato, a proteção de interesses vitais, o interesse público e o interesse legítimo. A LGPD lista dez bases legais, que são similares às do GDPR, mas incluem algumas especificidades, como a proteção à saúde e a realização de estudos por órgãos de pesquisa.

O GDPR estabelece autoridades de proteção de dados em cada país membro da União Europeia e não uma só supranacional. Autoridades de proteção de dados: A GDPR exige que os países membros da UE tenham autoridades de proteção de dados independentes. No Brasil, a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), que era vinculada à Presidência da República. Transformada em autarquia com status de agência reguladora em

outubro do ano passado por meio do Decreto Nº 11.348, de 01 de janeiro de 2023. Assim, embora seja autônoma, não é completamente independente do governo federal.

O GDPR exige a nomeação de um Encarregado de Proteção de Dados (DPO) em determinadas circunstâncias, como quando a organização realiza tratamento de dados em larga escala, trata dados sensíveis ou monitora sistematicamente indivíduos. A LGPD, por sua vez, exige que todas as organizações nomeiem um DPO, independentemente do tamanho ou natureza dos dados tratados.

O GDPR exige que as violações de dados sejam notificadas às autoridades de proteção de dados em até 72 horas após a descoberta. A LGPD não estabelece um prazo específico, mas determina que a notificação deve ocorrer em um prazo razoável, a ser definido pela ANPD.

Os dois regulamentos definem e protegem dados sensíveis, mas a GDPR tem uma lista mais ampla de categorias, incluindo dados biométricos e genéticos, enquanto a LGPD tem uma lista mais limitada, com uma abordagem mais focada em informações que podem levar à discriminação. Ambas exigem o consentimento explícito do titular dos dados para o processamento de suas informações sensíveis, salvo algumas exceções, como cumprimento de obrigações legais, proteção da vida, tutela da saúde, entre outras. As leis estabelecem que o consentimento deve ser claro, informado e específico quanto ao propósito de processamento desses dados.

Apesar dessas diferenças na categorização de dados sensíveis, ambos os regulamentos buscam proteger informações que podem levar à discriminação ou a outros danos aos titulares dos dados, e impõem requisitos mais rigorosos em relação ao consentimento e às condições para o tratamento desses dados.

### **3 DIREITO AO ESQUECIMENTO**

Embora o conceito de direito ao esquecimento digital seja relativamente recente, vários acadêmicos e especialistas em proteção de dados têm contribuído para a discussão e a definição do termo. A distinção não meramente semântica entre o direito ao esquecimento digital e o direito ao esquecimento comum, embora ambos estejam relacionados à proteção da privacidade e à reputação do indivíduo.

O direito ao esquecimento comum é mais amplo e pode ser aplicado tanto no ambiente digital quanto no físico. Ele se refere ao direito de uma pessoa de ter informações desatualizadas, irrelevantes ou prejudiciais sobre ela removidas ou esquecidas, permitindo que

a pessoa siga em frente sem ser prejudicada por eventos passados. O direito ao esquecimento comum pode se estender a registros públicos, arquivos de instituições e outros registros físicos.

Por outro lado, o direito ao esquecimento digital refere-se especificamente à remoção de informações pessoais desatualizadas ou irrelevantes dos meios digitais, como sites, mecanismos de busca e redes sociais. Ele reconhece o poder e o alcance da internet e a facilidade com que as informações podem ser disseminadas e armazenadas online, tornando-se acessíveis a um público amplo e permanecendo disponíveis indefinidamente. O direito ao esquecimento digital busca garantir que as pessoas possam ter maior controle sobre sua presença online e impedir que informações pessoais potencialmente prejudiciais continuem a afetá-las no futuro.

Os princípios fundamentais da LGPD, como a finalidade, a necessidade, a transparência e a segurança, sustentam o conceito de direito ao esquecimento. A LGPD limita a retenção de dados a prazos estabelecidos em lei ou até que a finalidade do tratamento seja alcançada (artigo 16) e inclui o direito à eliminação dos dados pessoais tratados com o consentimento do titular (artigo 18, III), conforme se demonstra:

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.

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: [...]

- III - correção de dados incompletos, inexatos ou desatualizados;

A GDPR, por sua vez, aborda o direito ao esquecimento de forma mais explícita, com uma seção específica dedicada ao tema, o artigo 17 trata do chamado "Direito ao apagamento" ou "ao esquecimento". De acordo com este artigo, os titulares dos dados têm o direito de solicitar o apagamento de seus dados pessoais quando uma série de condições é atendida, como quando os dados não são mais necessários para a finalidade original, o consentimento foi retirado, ou o tratamento é ilícito, conforme se evidencia abaixo:

Artigo 17. Direito ao apagamento dos dados («direito a ser esquecido»)

1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:

- a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
- b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;
- c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2;
- d) Os dados pessoais foram tratados ilicitamente;
- e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
- f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1.

2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º 1, toma as medidas que forem razoáveis, incluindo de carácter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.

3. Os n.ºs 1 e 2 não se aplicam na medida em que o tratamento se revele necessário:

- a) Ao exercício da liberdade de expressão e de informação;
- b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;
- c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.º, n.º 2, alíneas h) e i), bem como do artigo 9.º, n.º 3;
- d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1, na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou
- e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Vários autores vêm explorando o tema do direito ao esquecimento digital. Em 2009, Viktor Mayer-Schönberger (p. 121-132), ao explorar os impactos negativos da memória digital duradoura, já discutia a importância do esquecimento na era digital, argumentando a favor do direito ao esquecimento como uma forma de proteger a privacidade e permitir que as próprias pessoas controlem as suas informações pessoais online.

O autor defende a ideia de que o esquecimento tem um valor importante na sociedade, ao permitir que as pessoas aprendam com os erros, superem o passado e se reinventem.

Contudo, a era digital, com sua memória quase perfeita, tornou o esquecimento muito mais difícil. Afirmar que: "Without the capacity to forget, we all become less forgiving of others and ourselves, less able to live and learn, and less able to change and adapt." (2009, p. 131).

Sugere algumas abordagens para reintroduzir o esquecimento na era digital, incluindo a ideia de um "prazo de validade" dos dados, em que as informações seriam automaticamente excluídas após um período de tempo determinado, e o empoderamento dos indivíduos para controlar melhor seus próprios dados.

Neste mesmo sentido, BERNAL (2014, p. 215), sugere um equilíbrio entre a privacidade dos indivíduos e outros interesses, como a liberdade de expressão e o interesse público. Ele argumenta que o direito ao esquecimento é uma faceta essencial do direito à privacidade na era digital, sugerindo que o direito ao esquecimento deveria ser visto como uma maneira de proteger a autonomia individual e permitir que as pessoas controlem sua presença digital. Também examina o impacto do direito ao esquecimento na liberdade de expressão e no acesso à informação, defendendo que é necessário encontrar um equilíbrio adequado entre esses direitos, para que a privacidade não se torne uma desculpa para a censura ou a supressão da verdade. Por fim, explora as dificuldades práticas e técnicas associadas à implementação do direito ao esquecimento na era da internet. Ele destaca que a remoção de informações dos mecanismos de busca, como exigido pelo direito ao esquecimento, não significa que a informação deixe de existir na internet, mas apenas que se torna mais difícil de ser encontrada.

Paralelamente a este autor, MANTELERO (2013) analisa a proposta da União Europeia para o Regulamento Geral de Proteção de Dados (GDPR) e as raízes do direito ao esquecimento. Ele examina o conceito e a evolução do direito ao esquecimento, as perspectivas legais e as implicações práticas relacionadas a esse direito.

Embora ele não forneça uma definição literal específica do direito ao esquecimento, ele descreve o conceito como uma evolução dos direitos já existentes no âmbito da proteção de dados pessoais e privacidade. Ele examina o direito ao esquecimento em termos de sua relação com os direitos de oposição, cancelamento e bloqueio de dados pessoais e aborda a necessidade de equilibrar o direito ao esquecimento com outros direitos fundamentais, como a liberdade de expressão. A discussão deste autor sobre o direito ao esquecimento é mais focada nos aspectos legais e regulatórios, bem como nos desafios práticos relacionados à sua implementação e aplicação. Ele não fornece uma definição literal única do direito ao esquecimento, mas sim uma análise aprofundada das implicações, limitações e contexto desse conceito. (MANTELERO, 2013)

Para Luciano FLORIDI, o direito ao esquecimento não é um direito absoluto de apagar informações indiscriminadamente, mas sim um direito relacionado à exclusão de dados pessoais que não são mais relevantes ou necessários e quando o processamento dos mesmos já não é mais legal.

The right to be forgotten should be correctly interpreted as the right to have one's personal data deleted when there is no longer any need to process them (and control over such data has been regained), or when personal data are no longer being processed lawfully (2013, p. 11).

Em outra obra, esse mesmo autor argumenta que estamos passando pela "quarta revolução", uma revolução da informação que está remodelando a realidade humana. Ele explora como a digitalização das informações está alterando a maneira como vivemos, nos relacionamos e nos entendemos como seres humanos. Nesse contexto, ele aborda questões sobre a natureza da privacidade e como a sociedade deve se adaptar e abordar os desafios éticos emergentes na era digital. Assim, Embora não discuta diretamente o direito ao esquecimento neste livro, seus argumentos sobre privacidade, identidade e a crescente importância da informação podem ser aplicados ao debate sobre o direito ao esquecimento. (FLORIDI, 2014).

Por sua vez, Meg Leta JONES examina a evolução do direito ao esquecimento, principalmente na Europa, e sua aplicabilidade em outros contextos, incluindo os Estados Unidos. Ela descreve a origem histórica do direito ao esquecimento como um desenvolvimento que tem suas raízes no direito civil francês, principalmente no "droit à l'oubli" (direito de ser esquecido). Esse direito inicialmente estava relacionado à ideia de que criminosos reabilitados deveriam ter a oportunidade de reintegrar-se à sociedade sem serem constantemente lembrados de seu passado. Além disso, as primeiras discussões sobre privacidade na imprensa e na literatura jurídica no final do século XIX e início do século XX também contribuíram para o desenvolvimento do direito ao esquecimento. (JONES, 2016)

Aborda ela também, a complexidade do direito ao esquecimento e os desafios em equilibrar os interesses conflitantes, como o direito à privacidade e a liberdade de expressão. Argumenta que o direito ao esquecimento não deve ser visto como um conceito monolítico, mas como um conjunto de direitos e obrigações que podem ser adaptados para diferentes contextos legais e sociais, afirmando:

The right to be forgotten is, at its core, a mechanism of information control that, depending on implementation, may challenge the importance of free speech in the information society or better balance speech and privacy rights. (JONES, 2016, p.132).

Indo além, a autora define o direito ao esquecimento como um conjunto de direitos e obrigações que permite aos indivíduos controlar a disseminação de informações pessoais no ambiente digital e solicitar a remoção de dados que não são mais relevantes, corretos ou necessários. Ela argumenta que o direito ao esquecimento não é um conceito monolítico, mas uma série de regras e normas que podem ser adaptadas a diferentes contextos legais e sociais:

Even as we create and make sense of a digital reality, making choices among the many options on the matrix and determinations along the information life cycle will need to fit within the socio-technical legal cultures. This is particularly true of laws that revolve around forgiveness, privacy, and speech—all of which are laden with different meanings and deeply rooted in cultural norms of justice, utility, and human flourishing. (JONES, 2016, p.137)

Ao longo do tempo, o direito ao esquecimento evoluiu, expandindo-se além de sua origem no contexto da reabilitação criminal para abranger a proteção da privacidade dos indivíduos no ambiente digital. Assim, seguindo a mesma esteira de MAYER-SCHÖNBERGER (2009), JONES (2016) destaca como os avanços tecnológicos e a crescente quantidade de informações pessoais disponíveis online aumentaram a importância e a relevância do direito ao esquecimento.

Em discordância com os autores aqui demonstrados, CASTELLS (2012) contrasta ao afirmar que o direito ao esquecimento é uma ideia equivocada e perigosa, pois representa uma ameaça à liberdade de expressão e à transparência na esfera pública. Em sua visão, a informação é um bem coletivo que deve ser compartilhado e debatido, e não um direito exclusivo de determinadas pessoas ou grupos. Embora Castells não aborde exclusivamente o tema do direito ao esquecimento, ele discute esse tema de forma crítica e elaborada. Segundo o autor, o direito ao esquecimento pode ser utilizado como uma ferramenta de censura e controle da informação, permitindo que pessoas e empresas apaguem informações relevantes e verdadeiras que possam ser incômodas ou prejudiciais para a sua imagem pública. Além disso, ele argumenta que o direito ao esquecimento é incompatível com a natureza das novas tecnologias de informação e comunicação, que permitem a armazenagem e disseminação de informações em larga escala e em tempo real.

Para Castells (2012), a solução para os problemas decorrentes do uso indevido de informações pessoais e da privacidade na era digital não está em um direito ao esquecimento, mas sim em mecanismos mais eficazes de proteção da privacidade e de regulação do uso da informação. Ele defende, por exemplo, a criação de normas mais rigorosas de proteção de dados pessoais e de transparência na coleta e uso de informações por empresas e governos.

Muito embora a privacidade e a proteção de dados pessoais sejam importantes na era digital, o direito ao esquecimento é uma ideia equivocada que pode ser utilizada para limitar a liberdade de expressão e a transparência na esfera pública. Ele argumenta que, em vez de apagar informações ou restringir o acesso a elas, é preciso criar mecanismos mais eficazes de proteção de dados pessoais e de regulação do uso da informação, que permitam o compartilhamento de informações relevantes e verdadeiras sem prejudicar a privacidade e a dignidade das pessoas. (CASTELLS, 2012).

Esses autores contribuem para a discussão sobre o direito ao esquecimento digital e comum, a partir de diferentes perspectivas, explorando aspectos como a preservação da privacidade, a proteção da reputação, o interesse público na informação e o equilíbrio com a liberdade de expressão. A literatura sobre o tema é vasta e está em constante evolução à medida que a tecnologia e a normatização relacionada à proteção de dados avançam.

#### **4 PRECEDENTES JUDICIAIS**

A intenção deste tópico de pesquisa é demonstrar um retrato do pensamento jurisprudencial sobre o tema nos tribunais pelo mundo. Como já foi dito acima, quando se propôs analisar as diferenças e semelhanças dos regulamentos de proteção de dados, cada posicionamento jurisprudencial simboliza uma realidade local e não mundial. Todavia, não podemos nos esquecer que problema aqui tratado é de escala mundial, todavia, cada país é soberano e irá tratar a questão de acordo com as suas especificidades.

O direito ao esquecimento digital é um conceito que se refere à capacidade de um indivíduo solicitar a remoção de informações pessoais, desatualizadas ou prejudiciais, disponíveis na internet, especialmente em mecanismos de busca. Este direito busca equilibrar o interesse público na disseminação de informações e a proteção da privacidade e reputação do indivíduo.

O direito ao esquecimento digital ganhou destaque em alguns países, especialmente na União Europeia, onde várias decisões judiciais favoráveis foram proferidas.

Um marco importante na evolução do direito ao esquecimento foi um caso espanhol de 2014. O Tribunal de Justiça da União Europeia (TJUE), que interpreta o direito europeu para garantir que este é aplicado da mesma forma em todos os países da União Europeia, julgou o Google Spain SL e Google Inc. contra a Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, decidindo que os indivíduos têm o direito de solicitar a remoção de links para informações pessoais desatualizadas ou irrelevantes em motores de busca como o

Google. Neste caso, um cidadão espanhol, Mario Costeja González, solicitou que informações sobre um leilão de imóveis relacionado ao seu nome fossem removidas do Google, pois a dívida havia sido resolvida há muito tempo e a informação era prejudicial à sua reputação. Essa decisão influenciou diretamente a inclusão do direito ao esquecimento na GDPR (General Data Protection Regulation), formalizando o direito ao esquecimento no âmbito legal europeu (UNIÃO EUROPEIA, 2012).

O processo contra o Facebook foi apresentado no mesmo dia em que o Regulamento Geral de Proteção de Dados (GDPR) entrou em vigor na União Europeia, em 25 de maio de 2018.

Em 2018, o ativista de privacidade austríaco Max Schrems ganhou uma ação contra o Facebook na Áustria, na qual o tribunal determinou que o Facebook deveria remover publicações e comentários caluniosos sobre o autor que haviam se espalhado pela plataforma. Schrems apresentou suas queixas na Áustria, Bélgica, França e Alemanha, por meio de sua organização sem fins lucrativos chamada NOYB (None of Your Business). O foco do processo estava relacionado ao consentimento forçado. Schrems alegou que o Facebook e outras empresas coagem os usuários a concordar com seus termos de serviço, incluindo a coleta e uso de dados pessoais, para acessar os serviços das plataformas. Segundo ele, isso violava as disposições do GDPR, que exigem que o consentimento seja dado de forma livre, informada e específica. O resultado deste caso específico é que o Facebook enfrentou investigações e possíveis sanções por parte das autoridades de proteção de dados na Europa. (KUCHLER, 2018).

No caso da Commission Nationale de l'Informatique et des Libertés (CNIL) contra o Google (França), em sua decisão de 13 de maio de 2014, a agência francesa de proteção de dados ordenou que o Google aplicasse a remoção de informações dos resultados de busca em todas as versões do mecanismo de busca, não apenas nas versões europeias (FRANÇA, 2014). No entanto, após anos de disputa legal, em 2019, o TJUE decidiu a favor do Google, afirmando que a empresa não era obrigada a aplicar o direito ao esquecimento globalmente. O tribunal determinou que o Google precisava garantir que os links fossem removidos dos resultados de busca na UE, mas que a CNIL não tinha autoridade para exigir a remoção dos links em escala global (UNIÃO EUROPEIA, 2019). Essa decisão estabeleceu marcos importantes para o direito ao esquecimento e sua aplicação fora das fronteiras europeias.

Assim, muito embora o direito ao esquecimento seja mais desenvolvido e aplicado na União Europeia, outros países também estão começando a discutir e considerar esse direito em

suas legislações e jurisprudências, levando em conta os desafios de equilibrar a liberdade de expressão, o interesse público e os direitos de privacidade dos indivíduos.

No Brasil, o direito ao esquecimento tem sido debatido no âmbito jurídico e há decisões tanto em instâncias inferiores, assim como o tema já chegou a ser analisado pelo Supremo Tribunal Federal (STF). A mais alta casa do Poder Judiciário, analisou a questão do direito ao esquecimento no contexto dos casos Doca Street, Aida Curi e de outros similares (RE 1.010.606 e RE 1.015.797), firmando repercussão geral sobre o tema.

Para contextualizar, o caso Doca Street aborda o direito ao esquecimento. Nesse caso, o réu, Raul Fernandes do Santos, conhecido como Doca Street, foi condenado pelo assassinato de Ângela Maria Diniz, em 1976. O caso foi veiculado pela Rede Globo em um episódio do programa "Linha Direta Justiça" em 2004, e Doca Street moveu uma ação alegando violação de seu direito ao esquecimento. O caso Aida Curi, também relacionado na decisão da corte, envolvia a família da vítima e a Rede Globo, sendo ingressada ação contra a emissora por veicular em um programa jornalístico, a história do assassinato de Aida Curi, ocorrido em 1958. A família alegou que a divulgação do caso violava seu direito ao esquecimento da vítima.

O julgamento ocorreu no Supremo Tribunal Federal (STF), e em fevereiro de 2021, o STF, por 9 votos a 1, decidiu que o direito ao esquecimento não está previsto na Constituição brasileira, e que limitar a liberdade de expressão em nome do direito ao esquecimento poderia resultar em censura. A decisão reforçou que cada caso deve ser analisado individualmente e que é preciso equilibrar interesses como a privacidade, a dignidade da pessoa humana e a liberdade de expressão. (BRASIL, 2021)

Assim, o STF consolidou o pensamento de que o direito ao esquecimento não pode ser utilizado para suprimir informações de interesse público e que cada caso deve ser analisado individualmente, considerando a adequação, a necessidade e a proporcionalidade da medida. Essa decisão do STF estabelece um importante precedente no que diz respeito ao direito ao esquecimento no Brasil, destacando a importância do equilíbrio entre a proteção da privacidade e a liberdade de expressão. Todavia, deve-se salientar a necessidade de equilibrar os interesses envolvidos, incluindo a liberdade de expressão e a proteção da privacidade, de forma a garantir a proporcionalidade e a adequação das medidas adotadas em cada caso específico.

Aqui se demonstra apenas a ponta do iceberg. Muitas são as decisões que envolvem o tema. Muitas no sentido da adoção do direito ao esquecimento e outras contrárias.

Neste sentido, como demonstra Jorida Xhafaj, as decisões dos tribunais são inúmeras. Inúmeros também são as colisões destas decisões com o direito ao esquecimento, assim como com o direito da privacidade, da liberdade de expressão, da publicidade, do interesse público,

dentre outros direitos protegidos universalmente. A maneira de como serão efetuadas as limitações e exceções, levantam a questão sobre o estabelecimento de mecanismos ou autoridades especializadas em analisar os pedidos de remoção de listagens, antes que os mecanismos de busca processem cada um deles, evitando-se assim que os questionamentos cheguem ao judiciário.

The lack of clarity about the scope and substance of the limitation and exceptions to be made in view of the right to be forgotten raises the question concerning the establishment of mechanisms or authorities that are specialized in scrutinizing the delisting requests before the search engines administrate each of them. Otherwise, the appliance of the principle of proportionality will still remain in ambiguity and the dilemma in every of the reviewed case will suffer from the pressure of social needs or lack of transparency. (XHFAJ, 2018).

Caso contrário, a aplicação do princípio da proporcionalidade continuará ambígua, e o dilema em cada caso analisado sofrerá com a pressão das necessidades sociais ou falta de transparência.

## **7 CONSIDERAÇÕES FINAIS**

O direito ao esquecimento digital é um tema complexo que envolve o equilíbrio entre a proteção da privacidade, a dignidade da pessoa humana e a liberdade de expressão e informação. Tanto a LGPD brasileira quanto a GDPR europeia fornecem marcos legais para a proteção de dados pessoais, incluindo disposições relacionadas ao direito ao esquecimento, embora haja diferenças nas abordagens e no tratamento dos dados sensíveis.

Ambas as regulamentações exigem que os controladores de dados ponderem os direitos à privacidade e reputação dos indivíduos com o interesse público na informação e a liberdade de expressão, destacando a importância do equilíbrio entre esses valores fundamentais no contexto digital.

As informações hoje, graças aos buscadores da internet, simplesmente não se apagam. O esquecimento desempenharia um papel significativo na sociedade, possibilitando que as pessoas aprendam com os equívocos, superem seu passado e se reinventem. No entanto, a era digital e sua memória quase infalível tornaram o esquecimento muito mais desafiador. Algumas propostas visam reintroduzir o esquecimento no contexto digital, como a ideia de estabelecer um certo prazo de existência para os dados, no qual as informações seriam automaticamente removidas após um período específico, além de capacitar os indivíduos a gerenciarem de forma mais eficaz seus próprios dados.

O conceito de direito ao esquecimento tem sofrido evoluções na sociedade da informação. Os autores mencionados trazem diferentes perspectivas sobre o direito ao esquecimento, abordando aspectos como o equilíbrio entre privacidade e liberdade de expressão, a história e evolução do direito ao esquecimento, e as implicações práticas de sua aplicação. Apesar das diferenças, os conceitos lidam com o equilíbrio entre a privacidade e a reputação dos indivíduos e outros direitos e interesses, como a liberdade de expressão e o interesse público. Em ambos os casos, a aplicação do direito ao esquecimento depende de uma análise caso a caso, levando em consideração as circunstâncias específicas e os direitos envolvidos. Todavia, esse pensamento não uníssono, existindo vozes que criticam e contrariam o reconhecimento legal do direito ao esquecimento, considerando que a adoção dessa ideia pode ser utilizada para restringir a liberdade de expressão e o acesso à informação, prejudicando a transparência e a democracia na esfera pública.

Os tribunais europeus têm respaldado o direito ao esquecimento, como demonstrado pelos casos Max Schrems contra o Facebook e CNIL contra o Google e no caso inaugural Google Spain SL e Google Inc. contra a Agencia Española de Protección de Datos (AEPD). Esses casos, dentre outros, estabeleceram diretrizes e limites para sua aplicação desse direito.

No entanto, desde então, vários tribunais europeus proferiram decisões divergentes em relação ao direito ao esquecimento. Alguns tribunais têm considerado que o direito ao esquecimento não pode ser aplicado a informações que são de interesse público ou que são relevantes para o exercício da liberdade de expressão e de informação. Outros tribunais têm adotado uma abordagem mais ampla e têm concedido o direito ao esquecimento em casos em que as informações pessoais dos indivíduos foram usadas de forma inadequada ou injusta.

Percebe-se que ainda é um assunto complexo e controverso nos tribunais europeus, sendo que a interpretação e aplicação desse direito pode variar dependendo do caso específico em análise e a geopolítica envolvida.

No Brasil, a discussão sobre o direito ao esquecimento ainda está evoluindo, como evidenciado pelos casos Aida Curi e Doca Street julgados pelo STF, nos quais o direito ao esquecimento não foi reconhecido como um direito constitucionalmente garantido.

Diante deste cenário, é crucial que pesquisadores, legisladores e profissionais do direito continuem a estudar e debater o direito ao esquecimento digital, tanto no contexto da LGPD brasileira quanto da GDPR europeia. A análise comparativa entre as duas legislações pode fornecer insights valiosos para o desenvolvimento de políticas públicas e abordagens legais equilibradas, que levem em consideração os diversos interesses em jogo e garantam a

proteção adequada dos direitos fundamentais dos indivíduos, bem como a preservação da liberdade de expressão e informação na era digital.

Há a necessidade de se equilibrar a privacidade individual com a liberdade de expressão e o interesse público na informação, bem como a importância de adaptar o conceito à realidade da era digital. O direito ao esquecimento não deve ser entendido como uma ferramenta de censura, mas sim como um mecanismo de proteção à privacidade em casos específicos.

O direito ao esquecimento não é absoluto e está sujeito a certas condições e limitações. O controlador de dados pode se recusar a excluir os dados pessoais do titular em determinadas circunstâncias, como quando a retenção dos dados é necessária para o exercício de direitos à liberdade de expressão e informação, para o cumprimento de uma obrigação legal ou para a defesa de um direito em processo judicial. Um titular dos dados pode solicitar o apagamento de seus dados pessoais. Assim, solicitar a remoção de informações pessoais dos mecanismos de busca se essas informações forem inadequadas, irrelevantes, desatualizadas ou excessivas. Assim, deve se analisar o direito ao esquecimento digital com uma abordagem crítica e ponderada, examinando suas implicações, limitações e a necessidade de equilibrar este direito com outros direitos fundamentais na sociedade.

## REFERÊNCIAS

BERNAL, Paul. **Internet privacy rights: Rights to Protect Autonomy**. Cambridge: Cambridge University Press, 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/113709.htm). Acesso em 10/01/2023.

BRASIL. **Supremo Tribunal Federal**. RE 1010606. Rel. Min. Dias Toffoli. D. 11/02/2021. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5091603>. Acesso em 06/01/2023.

CASTELLS, Manuel. **Redes de indignação e esperança: Movimentos Sociais na Era da Internet**. Zahar, 2012.

FLORIDI, Luciano. "The Right to Be Forgotten": a Philosophical View. (2013). Disponível em: <https://philpapers.org/archive/FLOQRT.pdf>. Acesso em 10/04/2023.

FLORIDI, Luciano. **The fourth revolution: How the Infosphere is Reshaping Human Reality**: Oxford University Press, 2014.

FRANÇA, Commission Nationale de l'Informatique et des Libertés (CNIL). 2014. Disponível em: <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000030746525/>. Acesso em: 10/04/2023.

JONES, Meg Leta. **Ctrl + z - The Right to Be Forgotten**. ISBN 9781479876747. New York: New York University Press, 2016.

KUCHLER, Hannah. Max Schrems: the man who took on Facebook — and won. **Financial Times**. 05/04/2018 Disponível em: <https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544>. Acesso em 06/02/2023.

KUNER, Christopher. **European data protection law: Corporate Compliance and Regulation**. 2. Ed. Oxford: Oxford University Press, 2007.

MANTELERO, Alessandro. The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten' (June 28, 2013). **Computer Law & Security Review**, Volume 29, Issue 3, June 2013, Pages 229–235, Disponível em: <https://ssrn.com/abstract=2473151>. Acesso em 09/04/2023.

MAYER-SCHÖNBERGER, Viktor. **Delete: The Virtue of Forgetting in the Digital Age**. ISBN 978-0-691-15036-9. New Jersey: Princeton University Press, 2009.

OCDE. **Guidelines on Privacy Protection and Cross-Border Flows of Personal Data**. 2013. Disponível em: <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>. Acesso: em 08/04/2023.

UNIÃO EUROPEIA, **Convenção 108**, adotada em 1981. Disponível em: [https://www.europarl.europa.eu/ftu/pdf/pt/FTU\\_4.2.8.pdf](https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf). Acesso em 04/02/2023.

UNIÃO EUROPEIA, **Directiva 95/46/CE do Parlamento Europeu e do Conselho**, de 24 de outubro de 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em 04/02/2023.

UNIÃO EUROPEIA, **Directiva 2002/58/CE do Parlamento Europeu e do Conselho**, de 12 de julho de 2002. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002L0058>. Acesso em 04/02/2023.

UNIÃO EUROPEIA, **Tribunal de Justiça da União Europeia (TJUE)**. Caso Google Spain SL x AEPD. (2012) Disponível em: <https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT>. Acesso em: 09/04/2023.

UNIÃO EUROPEIA, **General Data Protection Regulation (GDPR)**. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&qid=1681040227005&from=EN>. Acesso em 10/01/2023.

UNIÃO EUROPEIA, **Tribunal de Justiça da União Europeia (TJUE)**. Comissão Nacional de Informática e Liberdades (CNIL) contra Google LLC. (2019) Disponível em:

<https://curia.europa.eu/juris/document/document.jsf?docid=218106&doclang=FR>. Acesso em: 09/04/2023.

XHAF AJ, Jorida. **The right to be forgotten**: A Controversial Topic Under the General Data Protection Regulation. (2018). UBT International Conference. 271. Disponível em: <https://doi.org/10.22364/iscflul.7.26>. Acesso em: 09/04/2023.