O CENÁRIO JURÍDICO DA PROTEÇÃO DE DADOS: DO CONTEXTO GLOBAL À REALIDADE BRASILEIRA

João Pedro Ignácio Marsillac[1]

Olivia Oliveira Guimarães[2]

RESUMO

O artigo aborda a evolução do direito à privacidade para a proteção de dados pessoais, destacando a influência do Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. Em seguida, analisa a Lei Geral de Proteção de Dados (LGPD) brasileira, ressaltando suas semelhanças e distinções em relação ao GDPR, como a ampliação das bases legais e a criação da Autoridade Nacional de Proteção de Dados (ANPD). O texto explora o papel das tecnologias, como a criptografia, a anonimização e a pseudonimização, como ferramentas essenciais para a segurança e a efetivação da privacidade por design. Por fim, discute os direitos do titular de dados, como os direitos de acesso, retificação, exclusão e portabilidade, e os desafios práticos para sua implementação, sublinhando a importância da ANPD para a fiscalização e a garantia do cumprimento das leis.

Palavras-chave: Anonimização, Autodeterminação informativa, GDPR, LGPD, Privacidade por design.

[1] Integrante do programa de Pós-Doutorado da Faculdade de Direito da USP. Doutor e mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie, Especialista em Direito Público e em Direito e Processo do Trabalho. Pesquisador do GPMAT – Grupo de Pesquisa Meio Ambiente do Trabalho – USP e do Grupo de Pesquisa Estado e Economia – Mackenzie. E-mail. joao.pedro@adv.oabsp.org.br

[2] Advogada. Especialista em Direito Tributário pela Escola Brasileira de Direito. Mestra em Direito pela Universidade de Passo Fundo e pela Universidade de Alicante, na Espanha. Doutoranda em Direito Político e Econômico pelo Instituto Presbiteriano Mackenzie.

THE LEGAL LANDSCAPE OF DATA PROTECTION: FROM THE GLOBAL CONTEXT TO THE BRAZILIAN REALITY

ABSTRACT

This article addresses the evolution of the right to privacy in the protection of personal data, highlighting the influence of the European Union's General Data Protection Regulation (GDPR). It then analyzes the Brazilian General Data Protection Law (LGPD), highlighting its similarities and differences in relation to the GDPR, such as the expansion of legal bases and the creation of the National Data Protection Authority (ANPD). The text explores the role of technologies, such as encryption, anonymization, and pseudonymization, as essential tools for security and the implementation of privacy by design. Finally, it discusses data subject rights, such as the rights of access, rectification, deletion, and portability, and the practical challenges of their implementation, emphasizing the importance of the ANPD for monitoring and ensuring compliance with the law.

Keywords: Anonymization, Informational self-determination, GDPR, LGPD, Privacy by design.

INTRODUÇÃO

A proteção de dados pessoais, em sua forma moderna, representa uma evolução fundamental do conceito tradicional de privacidade. A crescente digitalização e a coleta massiva de informações transformaram o direito à privacidade, que agora se manifesta como o direito à autodeterminação informativa. Essa transformação é evidenciada pela necessidade de o indivíduo manter o controle sobre o uso de suas informações.

Essa mudança de paradigma exigiu uma resposta legal robusta, com a União Europeia tomando a liderança ao promulgar o Regulamento Geral sobre a Proteção de Dados (GDPR). O GDPR foi concebido como um marco regulatório abrangente, com base no direito fundamental à proteção de dados, visando unificar a legislação dos países-membros e criar um padrão global. O chamado "efeito Bruxelas" do GDPR reverberou globalmente, influenciando outras jurisdições a criarem suas próprias legislações para garantir a interação no comércio digital.

No Brasil, a resposta a esse cenário global veio com a aprovação da Lei Geral de Proteção de Dados (LGPD). A LGPD não surgiu no vácuo, mas como um resultado direto da necessidade de o país se alinhar às melhores práticas internacionais e de conferir segurança jurídica ao ambiente digital. Sua promulgação foi fundamental para posicionar o Brasil como um ator confiável no mercado global, demonstrando compromisso com os direitos fundamentais dos cidadãos.

Este artigo explora como a proteção de dados transcendeu o direito à privacidade, tornando-se uma questão de autodeterminação informativa. Para isso,

analisa as nuances das legislações brasileira e europeia e o papel essencial da tecnologia na efetivação desses direitos. Por fim, discute os direitos do titular de dados, destacando os desafios práticos de sua implementação e o papel da Autoridade Nacional de Proteção de Dados (ANPD) na garantia da aplicação da lei.

O CENÁRIO JURÍDICO DA PROTEÇÃO DE DADOS: DO CONTEXTO GLOBAL À REALIDADE BRASILEIRA

A proteção de dados pessoais, em sua forma moderna, representa uma evolução fundamental do conceito tradicional de privacidade. A crescente digitalização e a coleta massiva de informações transformaram o direito à privacidade, que agora se manifesta como o direito à autodeterminação informativa (Doneda, 2019). Essa transformação é evidenciada pela necessidade de o indivíduo manter o controle sobre o uso de suas informações. (Bioni, 2020).

Essa mudança de paradigma exigiu uma resposta legal robusta, e a União Europeia tomou a liderança com a promulgação do Regulamento Geral sobre a Proteção de Dados (GDPR), formalmente o Regulamento (UE) 2016/679. O GDPR não foi apenas uma atualização das diretivas anteriores; ele foi concebido como um marco regulatório abrangente, com base no direito fundamental à proteção de dados (European Union, 2016). Seu objetivo principal era unificar a legislação dos países-membros e, assim, criar um padrão global de governança de dados (Pérez, 2018).

O GDPR introduziu princípios inovadores, como o da privacidade por design e por padrão, que obriga as organizações a incorporar a proteção de dados desde a concepção de seus sistemas e serviços (Artigo 25, GDPR). Além disso, o princípio da responsabilidade (accountability) impôs aos controladores de dados o ônus de demonstrar o cumprimento das normas, e não apenas de segui-las de forma passiva (Artigo 5º, item 2, GDPR). Essa abordagem proativa transformou a proteção de dados de uma questão secundária em um componente central da estratégia de negócios (Kamara e Anaraki, 2020).

O chamado “efeito Bruxelas” do GDPR reverberou em todo o mundo. Para continuar a fazer negócios com a União Europeia, empresas globais tiveram que se adaptar aos seus rigorosos requisitos, o que levou à exportação de suas normas (Bradford, 2020). Essa influência serviu como catalisador para a criação de legislações em outras jurisdições, buscando alinhamento para garantir que suas economias pudessem interagir no comércio digital global sem entraves legais (Schwartz, 2018).

No Brasil, a resposta a esse cenário global veio com a aprovação da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018. A LGPD não surgiu no vácuo; foi um resultado direto da necessidade de o país se alinhar às melhores práticas internacionais e de conferir segurança jurídica ao ambiente digital (Doneda, 2020). Sua promulgação foi fundamental para posicionar o Brasil como um ator confiável no mercado global, demonstrando um compromisso com os direitos fundamentais de seus cidadãos (Mancuso, 2019).

Apesar de inspirada no GDPR, a LGPD possui suas próprias nuances. Uma das principais distinções reside nas bases legais para o tratamento de dados pessoais, sendo que a LGPD expandiu esse leque para dez, incluindo, por exemplo, a "proteção do crédito", inexistente no GDPR (Artigo 7º, inciso X, LGPD). Outra diferença significativa é que a LGPD não possui uma base legal específica para a autoridade pública, embora o tratamento de dados pelo Poder Público seja regulamentado por uma seção própria (Artigo 23, LGPD).

Um dos pontos mais notáveis de semelhança entre as leis é a criação de um órgão regulador. A Autoridade Nacional de Proteção de Dados (ANPD), no Brasil, tem a responsabilidade de zelar pela aplicação da lei e de fiscalizar seu cumprimento (Artigo 55-J, LGPD). No entanto, a ANPD, por ser uma entidade mais recente, enfrenta o desafio de construir sua estrutura e consolidar sua atuação, equilibrando sua função orientadora com o seu poder sancionatório, o que é importante para a efetividade da lei (Berti, 2021).

Ambas as leis conferem aos titulares de dados uma série de direitos que antes eram inexistentes ou de difícil aplicação. O direito de acesso, por exemplo, permite que o indivíduo solicite uma cópia de todos os seus dados mantidos por um

controlador (Artigo 18, inciso II, LGPD). Já o direito à portabilidade permite que o titular transfira seus dados para outro fornecedor de serviço, um direito que reforça a autonomia do indivíduo sobre suas informações (Artigo 20, GDPR).

A LGPD e o GDPR também estabelecem um regime de responsabilidade civil rigoroso. Em caso de vazamento de dados ou de tratamento indevido, a sanção pode ser severa, sendo que a LGPD prevê multas de até 2% do faturamento da empresa, com um limite de R$ 50 milhões por infração (Artigo 52, LGPD). A responsabilidade é objetiva, o que significa que o controlador de dados pode ser responsabilizado por danos mesmo sem culpa, um padrão de proteção elevado para o titular (Rodrigues, 2022).

A implementação dessas leis impôs um desafio significativo para as organizações. Pequenas, médias e grandes empresas tiveram que revisar seus processos, mapear o fluxo de dados e designar um Encarregado de Dados (DPO) para atuar como ponto de contato entre a organização, os titulares de dados e a ANPD (Artigo 41, LGPD). Esse esforço de adequação legal e técnica é um investimento na confiança dos clientes e na sustentabilidade do negócio a longo prazo (Doneda, 2021).

O cenário jurídico da proteção de dados é dinâmico e está em constante evolução. O surgimento de novas tecnologias, como a Inteligência Artificial e a Internet das Coisas (IoT), levanta novas questões sobre como essas leis serão aplicadas (Martins, 2023). O desafio do futuro é garantir que a legislação possa acompanhar o ritmo da inovação, evitando que a falta de regulamentação clara gere riscos à privacidade e aos direitos fundamentais (Cavalcanti, 2022).

Em suma, a transição do direito à privacidade para o direito à proteção de dados não é apenas uma questão técnica, mas uma mudança cultural e legal profunda. O alinhamento do Brasil com o padrão global do GDPR, por meio da LGPD, fortaleceu o ecossistema digital nacional, tornando-o mais seguro e confiável (Blum, 2021). Essa jornada jurídica demonstra que a proteção de dados é uma necessidade inegável para a construção de uma sociedade digital justa, ética e transparente (Doneda, 2019).

2. O PAPEL DAS TECNOLOGIAS NA PROTEÇÃO DE DADOS: CRIPTOGRAFIA, ANONIMIZAÇÃO E PRIVACIDADE POR DESIGN

A proteção de dados na era digital não se restringe à aplicação de normas jurídicas; ela é intrinsecamente ligada à adoção de tecnologias que permitem a efetivação dos direitos dos titulares. A Lei Geral de Proteção de Dados (LGPD) e o GDPR reconhecem essa simbiose ao preverem a necessidade de medidas técnicas e organizacionais adequadas para garantir a segurança da informação (Artigo 46, LGPD). A tecnologia, portanto, age como um pilar de sustentação para a segurança e a privacidade, complementando o arcabouço legal.

Nesse contexto, a filosofia da Privacidade por Design (Privacy by Design), cunhada por Ann Cavoukian, emerge como um princípio-chave. Cavoukian (2009) propôs sete princípios fundamentais, como a proatividade, a incorporação da privacidade no design e a visibilidade. A essência do conceito é que a privacidade não deve ser uma característica opcional ou um "remendo", mas sim uma condição padrão em todos os sistemas e processos, o que o torna um pilar central na implementação do GDPR e da LGPD (Doneda, 2019).

A LGPD, de fato, incorpora a privacidade por design como um princípio estruturante. O Artigo 6º, em seu inciso I, prevê o princípio da "finalidade", que exige que o tratamento de dados seja realizado com propósitos legítimos, específicos e informados ao titular. A adoção de tecnologias que garantam esse princípio, como a segmentação de dados, é um exemplo prático. Além disso, a LGPD estabelece a necessidade de avaliações de impacto à proteção de dados (DPIA), que são intrinsecamente ligadas ao conceito de privacidade por design, pois forçam as organizações a pensarem nos riscos de privacidade desde o início de seus projetos (Mancuso, 2021).

A criptografia é a ferramenta tecnológica mais fundamental para a segurança dos dados. Ela transforma informações legíveis em um formato ilegível, garantindo a confidencialidade tanto dos dados em repouso (armazenados em servidores) quanto em trânsito (durante a transmissão pela internet). A aplicação de algoritmos de

criptografia de ponta a ponta é uma medida técnica considerada robusta para proteger dados pessoais, conforme exigido pelas leis de proteção de dados (Blum, 2021).

O uso da criptografia não apenas previne o acesso não autorizado, mas também é um fator mitigador em caso de incidentes de segurança. Se um banco de dados for comprometido, mas os dados estiverem criptografados, o risco de exposição dos dados pessoais é significativamente reduzido, o que pode eximir a empresa de responsabilidade em algumas situações (Simeão, 2020). Por essa razão, as legislações incentivam e até exigem o uso de criptografia para proteger dados sensíveis.

No campo da privacidade, a anonimização e a pseudonimização são técnicas importantes para a minimização de dados. A anonimização visa remover a possibilidade de o dado ser vinculado a um indivíduo de forma irreversível. Segundo o GDPR e a LGPD, dados anonimizados deixam de ser considerados dados pessoais e, portanto, não estão sujeitos à maioria das regras das leis de proteção de dados (Artigo 12, LGPD). A anonimização, quando bem-sucedida, desvincula o dado da pessoa para sempre (Gatti, 2020).

A pseudonimização, por sua vez, é uma técnica mais flexível. Ela substitui os dados pessoais por um identificador artificial (pseudônimo), tornando a identificação indireta e reversível apenas com o uso de chaves adicionais. A LGPD, ao lado do GDPR, valoriza essa técnica, pois ela permite que as organizações utilizem os dados para análise sem expor a identidade dos indivíduos, ao mesmo tempo que mantém uma camada de segurança (Artigo 13, LGPD). A pseudonimização é considerada uma medida de segurança importante e é incentivada por ambas as leis.

Contudo, é importante entender que a anonimização não é um processo trivial e pode ser desafiador. Pesquisas demonstram que, mesmo com a remoção de informações de identificação direta, é possível re-identificar indivíduos a partir de dados anonimizados cruzando-os com outras bases de dados (Ohm, 2010). O famoso caso da re-identificação de usuários do Netflix a partir de um conjunto de dados "anonimizado" serve como um alerta sobre a complexidade e os riscos dessa técnica, reforçando a necessidade de abordagens robustas e cuidadosas (Narayanan & Shmatikov, 2008).

Além das técnicas de anonimização e criptografia, a governança de dados envolve a implementação de políticas internas e a adoção de tecnologias para o mapeamento e a gestão do ciclo de vida dos dados. Ferramentas de Data Loss Prevention (DLP) e de gerenciamento de consentimento são exemplos de como a tecnologia pode ajudar as empresas a cumprirem suas obrigações legais, automatizando processos e monitorando o fluxo de informações para evitar vazamentos (Rodrigues, 2022).

A automação do gerenciamento do ciclo de vida dos dados, desde a coleta até a exclusão, é um requisito das leis de proteção de dados. Soluções tecnológicas permitem que as empresas rastreiem o consentimento dos titulares, gerenciem os pedidos de acesso e exclusão de dados e garantam que as informações sejam descartadas de forma segura quando não forem mais necessárias para o propósito original (Doneda, 2021). Isso não apenas aumenta a eficiência, mas também demonstra a conformidade com o princípio da minimização de dados.

O futuro da proteção de dados reside na evolução de tecnologias emergentes, como a Computação Multipartidária Segura (Secure Multi-Party Computation) e a Criptografia Homomórfica. Tais tecnologias permitem que os dados sejam processados e analisados sem que a informação seja revelada a terceiros, ou mesmo ao próprio provedor de serviço, o que pode revolucionar o tratamento de dados em setores como o de saúde e finanças (Cavalcanti, 2022). A aplicação dessas tecnologias promove a colaboração e a inovação sem comprometer a privacidade dos dados.

A sinergia entre o direito e a tecnologia é inegável. A legislação de proteção de dados, ao impor a necessidade de medidas técnicas adequadas, impulsiona a inovação tecnológica no campo da segurança e da privacidade. Por outro lado, a evolução tecnológica oferece novas ferramentas para a implementação e a efetivação dos direitos previstos em lei, promovendo um ciclo virtuoso em que a tecnologia serve como um pilar fundamental para a proteção dos direitos dos indivíduos (Opice Blum, 2021).

Em suma, a criptografia, a anonimização, a pseudonimização e o princípio de privacidade por design não são meros acessórios; eles são elementos essenciais da

conformidade legal e da responsabilidade corporativa. A tecnologia, nesse contexto, deixa de ser uma ameaça em potencial e se torna a principal aliada na construção de um ecossistema digital mais seguro, ético e confiável, onde os dados são tratados com o respeito e a proteção que as leis e a sociedade exigem.

3. OS DIREITOS DO TITULAR DE DADOS E OS DESAFIOS DE SUA EFETIVAÇÃO

O direito digital, por meio de leis como a LGPD, inaugurou uma era de empoderamento do cidadão, que agora tem um papel ativo na gestão de suas informações pessoais. Essa mudança de paradigma se alicerça no conceito de autodeterminação informativa, que eleva o controle sobre os próprios dados a um direito fundamental (Doneda, 2019). A LGPD reforça essa visão em seu Artigo 18, ao enumerar de forma explícita os direitos do titular, que formam o núcleo da lei e conferem a ele o poder de exigir ações de empresas e do setor público (Mancuso, 2021).

O primeiro pilar desse empoderamento é o Direito de Acesso. O titular pode solicitar a qualquer momento e de forma gratuita que a empresa informe se trata seus dados, e caso a resposta seja positiva, quais dados são esses. O Artigo 18, inciso II, da LGPD, e o Artigo 15 do GDPR, garantem esse direito, permitindo que o indivíduo saiba quais informações a organização detém sobre ele e a finalidade de seu uso (BRASIL, 2018; European Union, 2016). Essa transparência é vital para que o titular possa exercer os demais direitos, como a correção ou a exclusão.

Intimamente ligado ao direito de acesso, o Direito de Retificação permite ao titular corrigir dados incompletos, inexatos ou desatualizados. A LGPD, em seu Artigo 18, inciso III, e o GDPR, em seu Artigo 16, asseguram que as organizações tenham a obrigação de manter os dados precisos e atualizados (Bioni, 2020). Este direito é fundamental para a integridade dos dados, especialmente em sistemas que

dependem de informações corretas, como bancos de dados de crédito e registros governamentais.

O Direito de Exclusão, frequentemente chamado de "direito ao esquecimento", é um dos mais complexos e controversos. Ele permite que o titular solicite a eliminação de seus dados, por exemplo, quando o consentimento é retirado ou quando os dados não são mais necessários para a finalidade original (Artigo 18, IV, LGPD). O GDPR, em seu Artigo 17, detalha as condições sob as quais esse direito pode ser exercido, como quando o tratamento é ilícito ou os dados foram coletados de um menor (Rodrigues, 2022).

Apesar de sua importância, o direito de exclusão não é absoluto. A própria legislação prevê exceções que permitem que os dados sejam mantidos, como para o cumprimento de uma obrigação legal ou regulatória, ou para o exercício regular de direitos em processo judicial, administrativo ou arbitral (Artigo 16, LGPD). Essa ponderação visa a equilibrar a privacidade do indivíduo com o interesse público e a segurança jurídica (Doneda, 2020).

Outro direito fundamental é o Direito à Portabilidade, que permite ao titular obter os dados pessoais em um formato estruturado, de uso comum e legível por máquina, para transferi-los a outro fornecedor de serviço. O Artigo 18, inciso V, da LGPD e o Artigo 20 do GDPR, conferem esse direito, visando a fomentar a competição no mercado e a liberdade de escolha do consumidor (Opice Blum, 2021). Este direito tem implicações profundas para setores como o de telecomunicações, finanças e serviços de nuvem.

A efetivação da portabilidade, contudo, não é trivial. Os desafios práticos incluem a falta de padronização de formatos de dados entre diferentes empresas, a complexidade técnica para desenvolver sistemas de interoperabilidade e a garantia de que a transferência ocorra de forma segura (Cavalcanti, 2022). A Autoridade Nacional de Proteção de Dados (ANPD) tem um papel importante na definição de regulamentos e na fiscalização para garantir que as empresas cumpram com essa

obrigação de forma eficiente e segura, como previsto em suas atribuições (Artigo 55-J, inciso VIII, LGPD).

Apesar da clareza legal dos direitos, a sua efetivação enfrenta desafios práticos no dia a dia. A falta de canais de comunicação acessíveis e claros para o titular de dados, a complexidade no tratamento de informações por grandes empresas com sistemas fragmentados, e a dificuldade de o cidadão comum comprovar o tratamento indevido de seus dados são barreiras significativas (Berti, 2021). A ausência de um mecanismo de fácil acesso para o titular de dados acionar seus direitos é um ponto de vulnerabilidade no sistema de proteção.

É nesse ponto que a atuação da Autoridade Nacional de Proteção de Dados (ANPD) se torna fundamental. Ela é a principal responsável por fiscalizar e garantir que os direitos dos titulares sejam respeitados. De acordo com o Artigo 55-J da LGPD, a ANPD tem o poder de "aplicar sanções administrativas" em caso de descumprimento, além de "receber e apurar reclamações" dos titulares (BRASIL, 2018). Sua existência é a garantia de que as leis não serão apenas letra morta.

O titular de dados que se sentir lesado pode, primeiramente, contatar o Encarregado de Dados (DPO) da organização. Se a empresa não responder ou se a resposta for insatisfatória, o titular pode formalizar uma reclamação junto à ANPD. A LGPD prevê um procedimento administrativo para apurar a infração, que pode resultar em sanções severas, como multas de até 2% do faturamento da empresa, com um limite de R$ 50 milhões por infração (Artigo 52, LGPD).

A existência de um regime sancionatório robusto é um dos elementos que fortalece a LGPD e garante que os direitos do titular sejam levados a sério. A aplicação efetiva dessas penalidades, por sua vez, depende da capacidade da ANPD de investigar e de processar as reclamações de forma célere e justa (Doneda, 2021). O monitoramento da ANPD sobre o cumprimento das leis, portanto, serve como um incentivo para que as empresas invistam em governança de dados e em sistemas que facilitem o exercício dos direitos dos titulares.

Em suma, os direitos do titular de dados são o cerne da LGPD, transferindo o poder sobre as informações do controlador para o indivíduo. Embora a legislação seja detalhada, sua efetivação enfrenta obstáculos práticos e técnicos que exigem a mediação de uma autoridade competente. A atuação da ANPD e o engajamento das empresas na criação de mecanismos claros para o exercício desses direitos são de grande importância para que a promessa da proteção de dados se torne uma realidade no cotidiano do cidadão.

CONCLUSÃO

A transição do direito à privacidade para o direito à proteção de dados não é apenas uma questão técnica, mas uma profunda mudança cultural e legal. O alinhamento do Brasil com o padrão global do GDPR, por meio da LGPD, fortaleceu o ecossistema digital nacional, tornando-o mais seguro e confiável. Essa jornada jurídica demonstra que a proteção de dados é uma necessidade inegável para a construção de uma sociedade digital justa, ética e transparente.

A sinergia entre o direito e a tecnologia é inegável, com a legislação de proteção de dados impulsionando a inovação tecnológica no campo da segurança e da privacidade. A tecnologia, por sua vez, oferece novas ferramentas para a implementação e a efetivação dos direitos previstos em lei. Nesse contexto, a criptografia, a anonimização, a pseudonimização e o princípio de privacidade por design não são meros acessórios, mas elementos essenciais da conformidade legal e da responsabilidade corporativa. A tecnologia deixa de ser uma ameaça em potencial e se torna a principal aliada na construção de um ecossistema digital mais seguro, ético e confiável, onde os dados são tratados com o respeito e a proteção que as leis e a sociedade exigem.

Os direitos do titular de dados são o cerne da LGPD, transferindo o poder sobre as informações do controlador para o indivíduo. Embora a legislação seja detalhada, sua efetivação enfrenta obstáculos práticos e técnicos que exigem a mediação de uma autoridade competente. A atuação da Autoridade Nacional de Proteção de Dados

(ANPD) e o engajamento das empresas na criação de mecanismos claros para o exercício desses direitos são essenciais para que a promessa da proteção de dados se torne uma realidade no cotidiano do cidadão.

REFERÊNCIAS BIBLIOGRÁFICAS

BERTI, Flávia. **ANPD: Desafios e Perspectivas da Autoridade Nacional de Proteção de Dados**. Revista Brasileira de Direito Civil, v. 2, n. 4, 2021.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A Revisão da Privacidade e o Direito à Autodeterminação Informativa**. Rio de Janeiro: Forense, 2020.

BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados Pessoais Comentada.** São Paulo: Revista dos Tribunais, 2021.

BRADFORD, Anu. **The Brussels Effect: How the European Union Rules the World**. New York: Oxford University Press, 2020.

BRASIL**. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet**). Brasília, DF: Diário Oficial da União, 2018.

CAVALCANTI, Thiago Amorim**. Desafios Regulatórios da Inteligência Artificial**. Revista de Direito Internacional e Econômico, v. 18, n. 1, 2022.

CAVOUKIAN, Ann. **Privacy by Design: The 7 Foundational Principles**. Information and Privacy Commissioner of Ontario, 2009.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. **A Lei Geral de Proteção de Dados: O que muda e por quê.** Revista da Associação Nacional dos Procuradores Federais, v. 12, n. 2, 2020.

DONEDA, Danilo. **LGPD: Guia de Implementação para as Empresas**. 2021.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data**. Official Journal of the European Union, 2016.

GATTI, Eduardo. **Anonimização e Pseudonimização na LGPD: Conceitos e Aplicações**, 2020.

KAMARA, H.; ANARAKI, N. **The GDPR: A Catalyst for a Global Change. International Journal of Law and Information Technology**, v. 28, n. 4, 2020.

MANCUSO, Rodolfo. **LGPD e GDPR: o que são e quais as principais particularidades**. JOTA, 2019.

MARTINS, Lucas. **Os Desafios da Proteção de Dados no Contexto da Inteligência Artificial**. Revista do Direito Digital, v. 1, n. 1, 2023.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **De-anonymizing Social Networks.** In: 29th IEEE Symposium on Security and Privacy. 2008.

OHM, Paul. **Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization**. UCLA Law Review, v. 57, 2010.

PÉREZ, Jorge A. **The GDPR: The New Global Standard for Privacy**. Journal of Data Privacy and Regulation, v. 1, n. 1, 2018.

RODRIGUES, Rafael. **Responsabilidade Civil e a Lei Geral de Proteção de Dados.** Revista Jurídica da CVM, v. 2, n. 3, 2022.

SCHWARTZ, Paul M. **The Pervasive Global Power of the GDPR**. International Data Privacy Law, v. 8, n. 2, 2018.

SIMEÃO, Fernanda. **Criptografia e a LGPD: Como a tecnologia pode garantir a segurança dos dados**, 2020.

.