O VALOR FUNDAMENTAL DOS DADOS PESSOAIS: UMA ANÁLISE COMPARATIVA ENTRE A LGPD E GDPR SOB A ÓTICA DA ANÁLISE ECONÔMICA DO DIREITO | *THE FUNDAMENTAL VALUE OF PERSONAL DATA: A COMPARATIVE ANALYSIS BETWEEN LGPD AND GDPR FROM THE PERSPECTIVE OF ECONOMIC ANALYSIS OF LAW*

ANNELIESE REGINA FEILER
FELIPE GAZANIGA
THIAGO ANDRÉ MARQUES VIEIRA

RESUMO | Este artigo tem como objetivo realizar uma análise comparativa entre a Lei Geral de Proteção de Dados (LGPD) do Brasil e o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia sob a perspectiva da análise econômica do direito. A análise considera aspectos como os custos de conformidade, os incentivos para adoção de medidas de proteção de dados, as consequências para empresas que não cumprem as normas e os impactos sobre a inovação e a concorrência nos mercados. A abordagem interdisciplinar busca compreender o impacto das normas jurídicas sobre o comportamento humano e as interações econômicas. A comparação das legislações pode ajudar a entender as implicações no contexto empresarial e econômico. Perante o exposto, a metodologia utilizada na pesquisa é a comparativa e a técnica é bibliográfica.

PALAVRAS-CHAVE | Análise econômica do direito. Dados pessoais. Privacidade. Proteção de dados.

ABSTRACT | *This article aims to carry out a comparative analysis between Brazil's General Data Protection Law (LGPD) and the European Union's General Data Protection Regulation (GDPR) from the perspective of the economic analysis of law. The analysis considers aspects such as the costs of compliance, the incentives for adopting data protection measures, the consequences for companies that do not comply with the rules and the impacts on innovation and competition in the markets. The interdisciplinary approach seeks to understand the impact of legal norms on human behavior and economic interactions. Comparing legislation can help to understand the implications for the business and economic context. In view of the results, the methodology used in the research is comparative and the technique is bibliographical.*

KEYWORDS | *Data protection. Economic analysis of law. Personal data. Privacy.*

1. INTRODUÇÃO

A proteção de dados pessoais é um tema cada vez mais relevante na atualidade, especialmente com o advento de novas tecnologias e o crescente uso de dados digitais em diversas esferas da vida. Nesse contexto, a União Europeia e o Brasil adotaram legislações específicas para tratar da proteção de dados: o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) e a Lei Geral de Proteção de Dados (LGPD), respectivamente.

Embora tenham objetivos similares, as legislações apresentam diferenças importantes em relação aos seus escopos, regras e sanções. Além disso, a forma como as leis são aplicadas pode impactar diferentes setores econômicos, empresas e indivíduos.

Nesse sentido, uma análise comparativa entre a LGPD e o GDPR sob a ótica da análise econômica do direito pode ser de grande valia para compreender melhor as implicações dessas legislações no contexto empresarial e econômico. A análise econômica do direito é uma abordagem que busca entender o impacto das normas jurídicas sobre o comportamento humano e as interações econômicas, a partir de uma perspectiva interdisciplinar que combina elementos do direito, economia e outras ciências sociais.

Assim, o presente artigo tem como objetivo realizar, a partir de uma metodologia comparativa com técnica bibliográfica, uma análise entre a LGPD e o GDPR sob a ótica da análise econômica do direito, considerando aspectos como os custos de conformidade, os incentivos para adoção de medidas de proteção de dados, as consequências para empresas que não cumprem as normas e os impactos sobre a inovação e a concorrência nos mercados.

2. A PROTEÇÃO DE DADOS COMO ELEMENTO DO DIREITO A PRIVACIDADE

O direito à privacidade é elevado à qualidade de direito fundamental, conforme expõe o texto constitucional brasileiro em seu art. 5º, inc. X, no momento em que a norma constitucional afirma que é inviolável a vida privada. Ao considerar os avanços tecnológicos, em especial o mundo digital no qual a sociedade vive atualmente, verifica-se que o "surgimento da rede de internet, por exemplo, decididamente alargou as possibilidades de comunicação e fez emergir um grande número de questões ligadas à privacidade" (Doneda, 2020).

Doneda (2020) entende que o direito à privacidade, no atual contexto histórico da humanidade, assume uma posição de relevância enquanto elemento inerente à autonomia, à liberdade e ao exercício da cidadania, bem como dos direitos políticos. Com isso, a compreensão do autor é de que o direito à proteção da privacidade é pressuposto da sociedade democrática moderna.

A proteção do direito à privacidade ganha contornos ainda mais importantes no atual contexto tecnológico, em que Kosta *et al.* (2018) cunham na expressão em inglês como *Smart World Revolution*[1], em razão das diversas novas tecnologias, de forma que a proteção da privacidade não pode ser um entrave para o desenvolvimento tecnológico.

É inserido nesse contexto histórico contemporâneo da Revolução Industrial 4.0 que a informação é o principal fator de produção nessa quarta fase do capitalismo (Rodrigues; Santos; Gamba, 2021) e, deste modo, a proteção de dados pessoais tem se tornado cada vez mais importante em um mundo digital em constante evolução.

Nessa ideia de revolução industrial 4.0, sociedade da informação, sociedade em rede, capitalismos de vigilância, modernidade líquida (Rodrigues; Santos; Gamba, 2021) ou *Smart World Revolution* (Kosta *et al.*, 2018) é que Taylor e Schroeder (2015) cunham que "a privacidade é um valor fundamental que deve ser protegido em qualquer sociedade, e os dados pessoais são a base da privacidade em uma sociedade digital".

1 Em tradução livre significa "Revolução do Mundo Inteligente".

Debatin *et al.* (2014) destacam que a proteção de dados pessoais é essencial para garantir a segurança e a confiança dos usuários no uso de serviços e tecnologias digitais, e que a privacidade é um direito humano básico que deve ser respeitado tanto no mundo físico quanto no mundo digital.

Com base nas aduzidas premissas é que se pode inferir que a proteção de dados está intimamente conectada à ideia de privacidade, de modo que a proteção da privacidade possui relevância jurídica tanto ao indivíduo, quanto para a própria sociedade. Isto porque é a partir da proteção jurídica da privacidade, em especial com a proteção de dados, que é possível assegurar diversas garantias elementares à dignidade da pessoa humana, como, por exemplo, o direito a liberdade de opinião, liberdade de religião, garantia da livre pesquisa científica, lisura do processo eleitoral, dentre tantos outros bens jurídicos que devem gozar de proteção a partir da proteção da privacidade (Doneda, 2020).

Ao analisar essa série de bens jurídicos a serem protegidos no contexto da privacidade, é possível identificar que a grande maioria desses bens jurídicos tuteláveis a partir da proteção da privacidade emerge do princípio da liberdade, ou seja, trata-se de postulados jurídicos que tem por natureza assegurar a proteção de direitos fundamentais de primeira dimensão (Sarlet, 2011).

É possível concluir que a importância da proteção de dados pessoais está no fato de que a privacidade é um valor essencial para a autonomia e a liberdade individual, e que a falta de proteção adequada pode levar a consequências negativas, como a discriminação e o uso indevido de informações sensíveis (Solove, 2013).

A guisa de conclusão acerca deste tópico inicial é importante, primeiramente, destacar o reconhecimento pelo Supremo Tribunal Federal de que o direito à proteção de dados está se tornando um direito fundamental autônomo em relação ao direito fundamental à privacidade. Ainda, em um momento mais atual, a Emenda Constitucional n° 115/2022 reconheceu, de forma definitiva, a proteção de dados como um direito fundamental autônomo,

havendo proporcionado a inserção do inciso LXXXIX ao *caput* do artigo 5° da Constituição Federal.

2.1. História da proteção de dados no mundo

A proteção de dados é uma questão que tem sido discutida e regulamentada há décadas em todo o mundo. O início da regulação da proteção de dados surge como uma reação a determinados impulsos tecnocráticos ocorridos no bojo da administração pública no cenário pós-guerra e é com base nisso que a ideia de proteção de dados nasceu como algo em relação à atuação do Estado na esfera jurídica individual (Doneda, 2020). Bernal (2017) e Schwartz (2011) destacam que as primeiras legislações a respeito de proteção de dados pessoais surgiram na década de 1970, na Europa e nos Estados Unidos, respectivamente.

Na Europa, a primeira legislação surgiu na Alemanha, em 1970; posteriormente, é possível verificar a criação de uma legislação na Suécia, em 1973, a qual é considerada a primeira lei nacional de proteção de dados. Já nos Estados Unidos, surge o *Privacy Act*, em 1974. Estas legislações tinham por objetivo proteger direitos e liberdades fundamentais ameaçados pela coleta de dados pessoais de maneira ilimitada pelo Estado. Essas legislações surgem, portanto, como ferramenta de anteparo ao exercício do poder estatal no manejo de dados pessoais. Por essa razão, essas legislações são conhecidas como a primeira geração de leis que visam a proteção de dados pessoais (Doneda, 2020).

Na Europa, a primeira legislação abrangente sobre proteção de dados foi a Diretiva 95/46/CE, em 24 de abril de 1995, que estabeleceu um conjunto de princípios para coleta, processamento e armazenamento de dados pessoais. Posteriormente, com o Regulamento (UE) n° 2016/679, do Parcelamento Europeu e do Conselho, de 27 de abril de 2016, foi instituído o Regulamento Geral de Proteção de Dados (GDPR), que passou a ter vigência

a partir de 2018, substituindo a Diretiva e fortalecendo ainda mais as regras de proteção de dados pessoais na União Europeia.

Nos Estados Unidos, a proteção de dados pessoais é regulamentada por uma série de leis, incluindo a Lei de Proteção à Privacidade Online das Crianças (COPPA) e a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA).

Todavia, como afirmam Bernal (2017) e Schwartz (2011), a legislação americana é mais focada em setores específicos, como saúde e finanças, e não tem uma abordagem abrangente como o GDPR.

No contexto global, a discussão sobre proteção de dados também tem sido impulsionada por eventos como as revelações de Edward Snowden sobre a vigilância em massa realizada pela Agência de Segurança Nacional (NSA) dos Estados Unidos e o escândalo envolvendo a empresa Cambridge Analytica, que coletou dados pessoais de milhões de usuários do Facebook sem o consentimento adequado.

3. LEGISLAÇÃO EUROPÉIA (GDPR)

O Regulamento Geral de Proteção de Dados, que entrou em vigor na União Europeia em maio de 2018, é uma das legislações mais abrangentes e importantes sobre proteção de dados pessoais em todo o mundo. Como afirmam Kierkegaard e Székely (2019), o GDPR estabeleceu uma série de direitos e obrigações para as empresas e organizações que lidam com dados pessoais, incluindo o direito à portabilidade de dados, o direito ao esquecimento e a obrigação de notificar as autoridades em caso de violação de dados.

Além disso, a legislação tem uma abordagem mais rigorosa em relação ao consentimento do titular dos dados, como destacam Lievens *et al.* (2020). De acordo com os autores, o GDPR exige que o consentimento seja obtido de

forma clara e específica, e que seja possível revogar o consentimento a qualquer momento.

Entretanto, o GDPR também tem sido criticado por sua complexidade e por gerar custos significativos para as empresas, especialmente para as de pequeno e médio porte. Como afirmam Balkin e Zittrain (2018), embora o GDPR seja uma importante iniciativa de proteção de dados, é necessário continuar a monitorar e avaliar seus impactos.

3.1. Bases legais e princípios

O Regulamento Geral de Proteção de Dados estabelece uma série de bases legais e princípios que devem ser seguidos pelas empresas e organizações que lidam com dados pessoais. Como destacam Röck e Wiese (2019), as bases legais incluem o consentimento do titular dos dados, a execução de um contrato ou medidas pré-contratuais, o cumprimento de uma obrigação legal, a proteção de interesses vitais do titular dos dados, a realização de uma tarefa de interesse público ou o interesse legítimo da empresa ou organização.

Ainda, estabelece uma série de princípios que devem ser observados na coleta, processamento e armazenamento de dados pessoais, como destacam Wachter e Mittelstadt (2019). Entre esses princípios, estão a transparência, a minimização de dados, a precisão dos dados, a limitação de finalidade, a integridade e confidencialidade, e a responsabilidade.

Porém, como afirmam Röck e Wiese (2019), a aplicação dessas bases legais e princípios pode ser complexa e pode variar de acordo com o contexto e o tipo de dados pessoais envolvidos. Por isso, é importante que as empresas e organizações busquem orientação especializada e estejam sempre atualizadas em relação às mudanças e atualizações na legislação de proteção de dados.

3.2. Direitos do titular dos dados

O Regulamento Geral de Proteção de Dados estabelece uma série de direitos para os titulares de dados pessoais, como destacam Mola *et al.* (2020). Entre esses direitos, estão o direito de acesso aos dados, o direito de retificação, o direito de apagamento (ou "direito ao esquecimento"), o direito à limitação de processamento, o direito à portabilidade dos dados e o direito de oposição.

Como afirmam Mola *et al.* (2020), esses direitos são fundamentais para garantir que os titulares de dados tenham controle sobre seus dados pessoais e possam exercer sua privacidade de forma eficaz. Além disso, o GDPR também exige que as empresas e organizações forneçam informações claras e transparentes sobre o processamento de dados pessoais, como destacam Röck e Wiese (2019).

No entanto, como apontam Mola *et al.* (2020), a aplicação desses direitos pode ser desafiadora para as empresas e organizações, especialmente em relação à implementação de procedimentos para garantir a segurança dos dados pessoais e a resposta a solicitações de exercício desses direitos. É importante, portanto, que as empresas e organizações estejam sempre atualizadas em relação às mudanças e atualizações na legislação de proteção de dados e busquem orientação especializada para garantir a conformidade.

3.3. *Data protection officer* (DPO)

A legislação europeia estabelece a figura do Encarregado de Proteção de Dados (DPO, na sigla em inglês) como um elemento fundamental para garantir a conformidade das empresas e organizações com a legislação de proteção de dados, como destacam Wachter e Mittelstadt (2019).

Segundo o GDPR, o DPO deve ser um especialista em proteção de dados pessoais e deve ser designado para todas as empresas e organizações que realizam o processamento de dados pessoais em grande escala, bem como para aquelas que realizam o processamento de categorias especiais de dados pessoais ou dados pessoais relativos a condenações criminais e infrações.

De acordo com Wachter e Mittelstadt (2019), o papel do DPO inclui aconselhar e informar a empresa ou organização sobre as suas obrigações no âmbito do GDPR, monitorizar a conformidade com a legislação de proteção de dados, cooperar com as autoridades de proteção de dados e ser um ponto de contato para os titulares de dados que desejam exercer seus direitos.

Contudo, como apontam Wachter e Mittelstadt (2019), a implementação do DPO pode ser desafiadora para as empresas e organizações, especialmente em relação à identificação das situações em que a designação do DPO é obrigatória e à busca de profissionais especializados em proteção de dados. É importante, portanto, que as empresas e organizações busquem orientação especializada para garantir a conformidade com a legislação de proteção de dados.

3.4. Penalidades

As penalidades previstas no GDPR encontram-se no artigo 84 do regulamento, que prevê que podem ser aplicadas multas pela violação de regras nacionais, multas administrativas e multas aplicadas pelos Estados Membros.

Ainda, na União Europeia, empresas podem ser penalizadas com multa de 20 milhões de euros ou até 4% do faturamento, aquilo que for maior. Um exemplo disso é a British Airways, que teve um prejuízo de 183 milhões de euros pelo mau uso de dados.

4. LEGISLAÇÃO BRASILEIRA (LGPD)

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que entrou em vigor em setembro de 2020 e que tem como objetivo proteger a privacidade e os dados pessoais dos cidadãos brasileiros. A LGPD é inspirada e tem por base a Regulamento Geral de Proteção de Dados da União Europeia. Com a lei, são trazidas diversas obrigações para empresas e organizações que coletam, armazenam, processam e compartilham dados pessoais.

Uma das principais obrigações trazidas pela LGPD é a necessidade de consentimento explícito para o tratamento de dados pessoais. Segundo a lei, as empresas devem obter o consentimento dos titulares dos dados de forma clara e específica, informando para quais finalidades os dados serão utilizados.

Além disso, a LGPD traz diversas outras obrigações para as empresas, como a necessidade de implementar medidas de segurança adequadas para proteger os dados pessoais, a obrigação de notificar os titulares em caso de vazamentos de dados, e a necessidade de designar um Encarregado de Proteção de Dados (DPO) responsável por garantir a conformidade com a lei.

4.1. Bases legais e princípios

A legislação brasileira estabelece uma série de princípios e bases legais para o tratamento de dados pessoais. Segundo Barbosa e Fuchshuber (2020), a LGPD se baseia em 10 princípios, incluindo transparência, finalidade, adequação, necessidade, livre acesso, qualidade, segurança, prevenção, não discriminação e responsabilização. Esses princípios visam garantir que o tratamento de dados pessoais seja realizado de forma ética, responsável e compatível com os direitos dos titulares de dados.

Em relação às bases legais para o tratamento de dados pessoais, a LGPD estabelece 10 possibilidades, incluindo o consentimento do titular, o cumprimento de obrigação legal ou regulatória pelo controlador, a proteção da vida ou da integridade física do titular, a execução de contrato ou procedimentos preliminares, a tutela da saúde, a legítima defesa, o interesse público, o exercício regular de direitos em processos judiciais, administrativos ou arbitrais, a proteção do crédito e a proteção do patrimônio do titular.

Segundo Araújo (2020), a LGPD adota uma abordagem semelhante ao do GDPR em relação aos princípios e bases legais para o tratamento de dados pessoais. No entanto, existem diferenças significativas em relação à definição de dados pessoais sensíveis, fiscalização e aplicação da lei, direitos dos titulares de dados, papel do DPO e sanções e penalidades.

Portanto, a LGPD estabelece um conjunto de princípios e bases legais para o tratamento de dados pessoais que visam garantir a proteção dos direitos dos titulares de dados. A adoção desses princípios e bases legais pode ajudar as empresas e organizações a realizarem o tratamento de dados pessoais de forma ética e responsável, contribuindo para o desenvolvimento de uma economia digital mais sustentável e justa.

4.2. Anonimização x pseudonimização

A anonimização e a pseudonimização são técnicas utilizadas para garantir a proteção da privacidade e dos dados pessoais dos titulares de dados. De acordo com a LGPD, a anonimização é o processo pelo qual um dado pessoal perde a possibilidade de associação, direta ou indireta, a um indivíduo, enquanto a pseudonimização é o processo pelo qual um dado pessoal é substituído por um identificador que não permite a identificação direta do titular do dado.

Segundo Moreira *et al.* (2020), a anonimização é uma técnica mais eficaz do que a pseudonimização para garantir a privacidade dos titulares de

dados, uma vez que torna impossível a identificação do indivíduo a partir dos dados tratados. No entanto, a pseudonimização pode ser uma alternativa útil em situações em que a anonimização é impraticável ou desnecessária.

Já para Melo (2021), a pseudonimização é uma técnica mais adequada para a LGPD, uma vez que permite a utilização dos dados pessoais para finalidades específicas, como pesquisas científicas e estatísticas, sem comprometer a privacidade dos titulares de dados. Além disso, a pseudonimização pode ser mais fácil de implementar do que a anonimização, especialmente em casos em que os dados já foram coletados e armazenados sem a garantia da proteção de dados.

Com isso, tanto a anonimização quanto a pseudonimização são técnicas importantes para a proteção da privacidade e dos dados pessoais dos titulares de dados. A escolha entre uma ou outra depende das finalidades do tratamento de dados e das características dos dados a serem tratados.

4.3. Compartilhamento de dados

O compartilhamento de dados pessoais é uma prática comum no contexto atual, especialmente com a expansão das tecnologias da informação e comunicação. No entanto, com a entrada em vigor da LGPD, o compartilhamento de dados pessoais passou a ser regulado, sendo necessário atender a certos requisitos para garantir a proteção dos dados e a privacidade dos titulares.

De acordo com Andrade e Santos (2020), o compartilhamento de dados pessoais na LGPD deve ser realizado com base em uma das hipóteses legais previstas na lei, como o consentimento do titular ou o cumprimento de obrigação legal ou regulatória pelo controlador. Além disso, o compartilhamento deve ser realizado de forma clara e transparente, informando aos titulares quais dados serão compartilhados, com quem e com quais finalidades.

De outro modo, para Lunardi *et al.* (2020), a LGPD estabelece limites para o compartilhamento de dados pessoais, proibindo-o em algumas situações, como nos casos em que os dados são sensíveis e não há autorização expressa do titular. Além disso, a LGPD prevê a responsabilização solidária dos controladores e operadores envolvidos no compartilhamento de dados, o que reforça a importância de garantir a conformidade com a lei.

Com base no exposto, compreende-se que o compartilhamento de dados pessoais na LGPD deve ser realizado com base em hipóteses legais e de forma transparente, garantindo a proteção dos dados e da privacidade dos titulares. A lei estabelece limites para o compartilhamento, proibindo-o em algumas situações, e prevê a responsabilização solidária dos controladores e operadores envolvidos.

4.4. Direitos dos titulares

A Lei Geral de Proteção de Dados visa garantir a toda pessoa natural a titularidade de seus dados pessoais, além de assegurar os direitos fundamentais de privacidade, intimidade e liberdade. Também, há diversos direitos especificados ao longo dos artigos 18 e 20 da LGPD, que tratam da revisão de decisões automatizadas, como a possibilidade de requisição dos dados tratados pelo controlador visando a confirmação de tratamento, o acesso aos dados, a correção, a anonimização, bloqueio ou eliminação de dados desnecessários, a portabilidade, a eliminação de dados pessoais, a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, informações importantes sobre o tratamento e a revogação do consentimento, bem como solicitar a revisão de decisões baseadas no tratamento automatizado (Brasil, 2018).

Portanto, estes direitos podem ser invocados quando há a necessidade de restringir a publicidade de algum fato para a defesa de sua intimidade.

A lei traz mecanismos que viabilizam a proteção ao direito do titular de dados, sendo o consentimento o critério mais importante para o tratamento de seus dados. Com isso, o “objetivo das legislações relativas ao tratamento de dados pessoais é justamente assegurar o respeito dos direitos e liberdades fundamentais, nomeadamente do direito à vida privada” (Martini; Bergstein, 2021).

4.5. Hipóteses de exclusão de dados

A exclusão de dados pessoais é um direito fundamental garantido pela Lei Geral de Proteção de Dados e está diretamente relacionado ao direito à privacidade dos titulares. Nesse sentido, a LGPD estabelece algumas hipóteses em que os dados pessoais devem ser excluídos, como a revogação do consentimento, a finalidade da coleta ter sido alcançada e a eliminação de dados desnecessários.

De acordo com Souza *et al.* (2020), a revogação do consentimento é uma das principais hipóteses de exclusão de dados na LGPD. Isso significa que o titular dos dados pode, a qualquer momento, solicitar a exclusão das informações que foram coletadas a partir do seu consentimento. Essa exclusão deve ser feita de forma definitiva e segura, garantindo que os dados não possam ser recuperados ou acessados indevidamente.

Além disso, a lei prevê a exclusão de dados quando a finalidade para a qual eles foram coletados foi alcançada. Segundo Dias e Nardi (2020), essa hipótese é importante para evitar a manutenção de dados pessoais por tempo desnecessário, garantindo a proteção da privacidade e dos direitos dos titulares.

Outra hipótese de exclusão de dados prevista pela LGPD é a eliminação dos dados desnecessários. Conforme destaca Costa (2021), a LGPD estabelece o princípio da minimização dos dados, que orienta as empresas e organizações a coletarem somente as informações que são

realmente necessárias para a finalidade específica da coleta. Assim, quando os dados não são mais necessários, é necessário eliminá-los de forma definitiva e segura.

Ainda, é importante destacar que a LGPD prevê a possibilidade de exclusão de dados de forma anonimizada ou pseudonimizada. Segundo Barbosa e Alves (2020), a anonimização e a pseudonimização são técnicas que visam proteger a privacidade dos titulares, tornando os dados irreversivelmente anonimizados ou substituindo as informações que permitam identificar o titular por um código.

Em síntese, a exclusão de dados pessoais é um direito fundamental garantido pela LGPD e está diretamente relacionado ao direito à privacidade dos titulares. A revogação do consentimento, a finalidade da coleta ter sido alcançada, a eliminação de dados desnecessários e a anonimização ou pseudonimização são algumas das hipóteses previstas pela LGPD para a exclusão de dados. É importante que as empresas e organizações cumpram as exigências legais para garantir a proteção dos dados pessoais e da privacidade dos titulares.

4.6. Sanções

A Lei Geral de Proteção de Dados estabelece sanções para empresas e organizações que não cumprirem com as normas de proteção de dados pessoais. As sanções previstas na LGPD têm o objetivo de garantir o cumprimento das normas estabelecidas e proteger a privacidade e a autonomia dos titulares de dados pessoais.

Segundo a LGPD, as sanções podem variar desde uma simples advertência até multas que podem chegar a 2% do faturamento da empresa, limitadas a um total de 50 milhões de reais por infração. Além disso, as empresas também podem ser obrigadas a realizar a suspensão temporária ou

definitiva do tratamento dos dados, ou até mesmo a exclusão dos dados pessoais que foram coletados sem a devida autorização do titular.

De acordo com Rezende e Azevedo (2019), “as sanções administrativas previstas na LGPD são mecanismos que visam incentivar o cumprimento das normas estabelecidas e coibir o uso indevido de dados pessoais”. Os autores destacam ainda que “as sanções aplicáveis em caso de descumprimento da lei devem ser proporcionais à gravidade da infração e ao porte econômico da empresa ou organização infratora” (Rezende; Azevedo, 2019).

Portanto, as empresas e organizações devem estar atentas às normas estabelecidas pela LGPD e tomar as medidas necessárias para garantir a proteção dos dados pessoais de seus clientes e usuários. Caso contrário, poderão ser penalizadas com sanções que podem afetar significativamente seu faturamento e sua reputação no mercado.

4.7. Autoridade Nacional de Proteção de Dados (ANPD)

A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão regulador criado pela Lei Geral de Proteção de Dados para fiscalizar e regulamentar o tratamento de dados pessoais no Brasil. A ANPD tem como objetivo principal garantir a proteção dos dados pessoais dos cidadãos brasileiros, promover a transparência nas práticas de tratamento de dados e orientar as empresas e organizações em relação ao cumprimento das normas estabelecidas pela LGPD.

Segundo Santos e Rocha (2021), “a ANPD tem um papel fundamental na implementação da LGPD no Brasil, uma vez que é responsável por regular e fiscalizar o tratamento de dados pessoais pelas empresas e organizações”. Os autores destacam ainda que “a ANPD deve atuar de forma independente e imparcial, garantindo a proteção dos direitos dos titulares de dados pessoais e o cumprimento das normas estabelecidas pela LGPD”.

Além disso, a ANPD também tem como responsabilidade promover a educação e a conscientização da população sobre a importância da proteção de dados pessoais e das normas estabelecidas pela LGPD. Para isso, a ANPD deve realizar campanhas de conscientização e divulgação de informações sobre a proteção de dados, além de orientar as empresas e organizações sobre as melhores práticas de tratamento de dados pessoais.

Portanto, a ANPD desempenha um papel crucial na implementação da LGPD no Brasil e na garantia da proteção dos dados pessoais dos cidadãos brasileiros. É importante que as empresas e organizações estejam em conformidade com as normas estabelecidas pela ANPD e cumpram com suas responsabilidades em relação ao tratamento de dados pessoais.

5. ANÁLISE COMPARATIVA ENTRE A LEGISLAÇÃO BRASILEIRA E EUROPEIA SOB A ÓTICA DA ANÁLISE ECONÔMICA DO DIREITO

A proteção de dados pessoais se tornou uma preocupação global nos últimos anos, e a implementação de regulamentações específicas para esse fim tem sido uma tendência crescente em todo o mundo. No Brasil, a Lei Geral de Proteção de Dados entrou em vigor em 2020, enquanto na União Europeia, o Regulamento Geral de Proteção de Dados está em vigor desde 2018. Uma análise econômica do direito pode ajudar a comparar as duas regulamentações, destacando semelhanças e diferenças.

De acordo com Cruz e Henrique (2020), a LGPD e o GDPR compartilham muitos princípios e requisitos comuns, como a necessidade de consentimento dos titulares de dados para o processamento de dados pessoais, a obrigatoriedade de notificação em caso de violação de dados, a garantia dos direitos dos titulares de dados e a exigência de segurança dos dados pessoais. Ambas as regulamentações visam proteger a privacidade dos titulares de dados e estabelecem um conjunto de direitos para os titulares de dados, incluindo o direito de acesso, correção, exclusão e portabilidade de seus dados pessoais.

No entanto, como destacam Cruz e Henrique (2020), existem diferenças significativas entre as duas regulamentações. Por exemplo, enquanto o GDPR prevê multas mais altas em caso de violação da lei, a LGPD prevê multas mais baixas, mas ainda significativas. O GDPR prevê multas de até 20 milhões de euros ou 4% do faturamento global anual da empresa, enquanto a LGPD prevê multas de até 2% do faturamento da empresa no Brasil, limitado a 50 milhões de reais por infração.

Outra diferença importante entre as duas regulamentações é a definição de dados pessoais sensíveis. Enquanto o GDPR define dados pessoais sensíveis de forma ampla, incluindo informações como orientação sexual e convicções religiosas, a LGPD inclui apenas algumas categorias específicas de dados pessoais, como informações sobre saúde e dados biométricos. A definição de dados pessoais sensíveis é importante porque o processamento desses dados é restrito e exige uma base legal específica.

Além disso, como apontam Cruz e Henrique (2020), a LGPD tem como objetivo incentivar a economia digital no Brasil, enquanto o GDPR tem um objetivo mais amplo de proteger a privacidade dos titulares de dados em toda a União Europeia. A LGPD foi projetada para promover o uso de dados pessoais de forma responsável e aumentar a confiança dos consumidores na economia digital brasileira. A regulamentação incentiva a inovação e o desenvolvimento de novos modelos de negócios baseados em dados, desde que esses modelos sejam compatíveis com a privacidade e a proteção de dados pessoais.

Em relação à aplicação da lei, a LGPD é fiscalizada pela Autoridade Nacional de Proteção de Dados, enquanto o GDPR é fiscalizado pelas autoridades de proteção de dados de cada país da União Europeia. A ANPD é responsável por fiscalizar e aplicar a LGPD em todo o território brasileiro, garantindo que as empresas e organizações estejam em conformidade com a lei. Porém, como a ANPD ainda está em fase de estruturação, a fiscalização e a aplicação da LGPD têm sido mais limitadas em comparação ao GDPR.

Quanto às bases legais para o processamento de dados pessoais, ambas as regulamentações têm uma abordagem semelhante, exigindo uma

base legal específica para o processamento de dados pessoais. Na LGPD, as bases legais incluem o consentimento do titular dos dados, a necessidade para cumprir obrigações contratuais ou legais, a execução de políticas públicas, a proteção da vida ou da integridade física, entre outras. No GDPR, as bases legais incluem o consentimento do titular dos dados, o cumprimento de obrigações legais, a proteção de interesses vitais, entre outras.

Embora ambas as regulamentações tenham como objetivo principal proteger a privacidade e os direitos dos titulares de dados, as diferenças em suas abordagens refletem contextos jurídicos, culturais e econômicos distintos. No entanto, compreender essas diferenças é crucial para empresas que operam em ambientes regulatórios globais, permitindo-lhes adotar estratégias eficazes de conformidade e gestão de riscos (Cruz; Henrique, 2020).

5.1. Análise econômica do direito: uma breve definição conceitual e um paralelo com a teoria de justificação e aplicação das normas jurídicas de Klaus Günther

Antes de se realizar minimamente a análise de eventuais implicações jurídico-econômicas da aplicação e adoção da Lei Geral de Proteção de Dados, Lei Federal n. 13.079/2018, é necessário definir o que é análise econômica do direito e por que ela é relevante para o mundo jurídico.

Inicialmente, cumpre destacar que o fenômeno da análise econômica do direito tem por objetivo realizar uma reanálise dos institutos jurídicos, ou seja, retomar a razão de ser dos institutos jurídicos, o porquê da proteção jurídica de determinados bens (Mackaay; Rousseau, 2015).

A ideia da análise econômica do direito não se consubstancia especificamente em levar em consideração estritamente aspectos econômicos, mas sim com a finalidade de ser instrumento de interpretação para a tomada de decisão com o intuito de levar em consideração os demais aspectos não

jurídicos que possam influir na melhor compreensão dos juristas sobre os conceitos e a razão de ser dos institutos jurídicos (Mackaay; Rousseau, 2015).

Inserido nessa perspectiva, pode-se afirmar que a análise econômica do direito é a retomada do realismo jurídico em contraposição ao positivismo jurídico, bem como ao jusnaturalismo. O objetivo da análise econômica do direito é reaproximar o direito do mundo real, é buscar dar aderência social às normas jurídicas, ao levar em consideração aspectos econômicos (Azevedo, 2018).

Nesse contexto, é possível aferir que o fenômeno da análise econômica do direito deve ser utilizado enquanto ferramenta para o jurista interpretar o direito, em especial os julgadores quando submetidos a casos complexos, nos quais a análise de questões não puramente jurídicas podem auxiliar para a tomada de uma decisão a qual pode ser melhor socialmente aceita.

Numa concepção de interpretação e aplicação do direito, é possível fazer um paralelo com o pensamento do jurista alemão Klaus Günther, que cunha a ideia de que a tomada de decisão deve levar em consideração todos os aspectos que influenciem num determinado caso, de modo que esses aspectos não precisariam ser necessariamente jurídicos, para assim se tomar a decisão jurídica mais viável para um determinado caso. Isto é o que o jurista alemão chama de “norma U” (Günther, 2011).

A respeito do paralelo da análise econômica do direito e a teoria de Klaus Günther, pode-se concluir que ambas são uma alternativa à rigidez do positivismo jurídico, de modo que ambas são visões do direito de caráter instrumental, ou seja, com a missão de aplicar o direito ao caso concreto ao levar em considerações todas as questões que possam implicar a aplicação de determinada norma jurídica. Em suma, tem por missão não apenas considerar as normas jurídicas positivas a serem aplicáveis, mas as demais causas que possam interferir naquilo que seria a melhor aplicação do direito.

Nesse ponto, pode-se afirmar que a análise econômica do direito avança em relação à teoria de justificação e aplicação das normas de Klaus

Günther, no que diz respeito aos elementos que possam ser considerados influenciadores. Isso porque a análise econômica do direito propõe uma interdisciplinaridade entre as demais ciências (Azevedo, 2018), enquanto a teoria de Klaus Günther visa desconsiderar um positivismo jurídico puro de aplicação exclusiva de normas legais, de tal forma que, na teoria de justificação e aplicação da norma, o objetivo é utilizar enquanto elementos influenciadores os demais conteúdos normativos, como por exemplo os principiológicos, para a tomada de decisão (Günther, 2011).

Ao considerar o atual momento histórico que a humanidade vive, nesse ambiente digital da sociedade da informação, revolução industrial 4.0, dentre outros sinônimos já abordados neste artigo, pode-se concluir que a aplicação da análise econômica do direito faz mais sentido. Isso porque a análise econômica do direito compreende que é impossível chegar a uma ciência pura do direito, pois a análise econômica do direito aceita que o ordenamento jurídico não é autossuficiente e que existirão lacunas e, portanto, busca a interdisciplinaridade com a economia para o preenchimento de tais lacunas jurídicas. Isso é o que se pode denominar de reconstrutivismo realista (Azevedo, 2018).

A partir dessa premissa de uso da análise econômica do direito, conclui-se que é necessário analisar os impactos econômicos que uma determinada norma jurídica causa ao plano fático e, para isso, é impossível desconsiderar os elementos influenciadores de caráter econômico que são levados em consideração por qualquer pessoa em relação à lei.

5.2. Análise econômica do direito na delimitação da responsabilidade civil no âmbito da Lei Geral de Proteção de Dados no Brasil

Realizadas as comparações entre a legislação brasileira de proteção de dados com a lei geral de proteção de dados europeia, bem como a definição do que é a análise econômica do direito e a que se propõe tal visão de aplicação e instrumentalização do direito, verifica-se que o uso da análise

econômica do direito deve ser uma ferramenta a ser adotada pelo jurista no âmbito do direito brasileiro como instrumento para solução de litígios que envolvam a proteção de dados.

Como a legislação brasileira de proteção de dados é inspirada em outras legislações estrangeiras, verifica-se que a análise econômica do direito também pode ajudar a comparar as implicações econômicas da LGPD e do GDPR.

É inegável que a implementação da LGPD no Brasil pode aumentar os custos das empresas para cumprir com as novas obrigações de privacidade de dados, como a contratação de DPOs (Encarregados de Proteção de Dados) e investimentos em segurança da informação. Por outro lado, a regulamentação também pode levar a benefícios econômicos a longo prazo, como maior confiança dos consumidores na economia digital e incentivos à inovação baseada em dados (Borba; Radaelli, 2020).

Para traçar um paralelo, quando da implementação do GDPR na União Europeia, foi possível verificar um impacto significativo nas empresas e organizações que processam dados pessoais. A implementação do GDPR levou a um aumento nos custos de conformidade, mas também levou a uma maior conscientização sobre a privacidade de dados e uma maior transparência no processamento de dados pessoais. Além disso, o GDPR teve um impacto positivo na economia digital da União Europeia, incentivando a inovação e o desenvolvimento de novos modelos de negócios baseados em dados (Deloitte, 2019).

De fato, é inegável que a proteção de dados é algo essencial ao atual contexto histórico que a humanidade se encontra, de modo que o uso dos dados pessoais é algo corriqueiro e que nem sempre significará malefícios. Para evitar, portanto, situações prejudiciais de uso e má-fé dos dados pessoais, é necessário que o ordenamento jurídico preveja proporcionalmente critérios de proteção de dados, bem como no que se refere à responsabilidade pela inobservância dos critérios estabelecidos proporcionalmente a serem observados para a proteção de dados (Doneda, 2020).

A definição da responsabilidade pelo uso inadequado de dados pessoais ganha contornos mais relevantes a partir do contexto econômico brasileiro, pois a Lei Geral de Proteção de Dados (Lei n. 13.079/2018) define enquanto agente de tratamento qualquer pessoa física ou jurídica que controle, ou seja, exerça poder de decisão sobre o tratamento de dados pessoais, ou que realize o tratamento de tais dados.

Nessa conceituação, verifica-se que a Lei Geral de Proteção de Dados impactará também nas micro e pequenas empresas. Isso porque, conforme dados de 2022 do Ministério da Economia do Brasil, as micro e pequenas empresas representam 99% das empresas brasileiras, ou seja, são empresas que faturam até o limite de um milhão e duzentos mil reais, nos termos da Lei n. 9.841/1999, que define o conceito de microempresa e empresa de pequeno porte.

O cerne do problema se encontra justamente no fato de que o legislador infraconstitucional não definiu, ao estabelecer a Lei Geral de Proteção de Dados, o tipo de responsabilidade civil à qual estão sujeitos os agentes de tratamento de dados (Santos; Leitão; Wolkart, 2022).

É perceptível que a Lei Geral de Proteção de Dados guarda certa similitude com o Código de Defesa do Consumidor no que se refere aos deveres dos agentes de tratamento. No entanto, o art. 42 da Lei Geral de Proteção de Dados estabeleceu de maneira genérica a responsabilidade civil dos agentes de tratamento (Porto; Silva, 2020). Nesse contexto, o uso da análise econômica do direito como ferramenta para resolver eventuais conflitos ganha relevância (Azevedo, 2018), pois esta é uma ferramenta que possibilitará assegurar maior aderência social da proteção dos dados pessoais.

Em resumo, para se aferir a responsabilidade civil dos agentes de tratamento, sob a ótica da análise econômica do direito, é necessário integrar a realidade das pessoas sujeitas à imputação de responsabilidade civil pela proteção de dados pessoais com os ditames normativos ensejadores de tal responsabilidade.

A aplicação da análise econômica do direito envolverá, portanto, a análise dos custos de transação que envolvem a questão (Mackaay; Rousseau, 2015), de tal sorte que é necessário analisar com base em critérios econômicos se determinada conduta se configura enquanto ato ilícito sob a ótica da responsabilidade dos agentes de tratamento na Lei Geral de Proteção de Dados (Porto; Silva, 2020).

Como forma de analisar os custos de produção em relação à responsabilidade civil, uma proposta que se pode adotar é o uso da regra de Hand, a qual leva em consideração os custos e os benefícios de determinada conduta a fim de se aferir o nível de negligência praticado por determinado agente, de modo a lhe imputar a responsabilidade civil e o consequente dever de indenizar (Santos; Leitão; Wolkart, 2022).

Em conclusão, a análise econômica do direito pode ajudar a comparar a LGPD e o GDPR, destacando semelhanças e diferenças entre as duas regulamentações e suas implicações econômicas. Embora as regulamentações compartilhem muitos princípios e requisitos comuns, como a necessidade de consentimento dos titulares de dados e a garantia dos direitos dos titulares de dados, existem diferenças significativas, como a definição de dados pessoais sensíveis e a abordagem à fiscalização e à aplicação da lei. A implementação da LGPD e do GDPR pode ter impactos econômicos a curto e longo prazo, mas ambas as regulamentações têm como objetivo proteger a privacidade dos titulares de dados e incentivar a economia digital responsável.

6. CONSIDERAÇÕES FINAIS

Em conclusão, a análise econômica do direito é uma ferramenta importante para avaliar as implicações da LGPD e do GDPR em relação à privacidade dos dados e à economia digital. Embora ambas as regulamentações compartilhem muitos princípios e requisitos comuns, existem diferenças significativas em relação à definição de dados pessoais sensíveis,

bases legais para o processamento de dados, fiscalização e aplicação da lei, direitos dos titulares de dados, papel do DPO e sanções e penalidades.

A LGPD é uma legislação importante para o Brasil, que se alinha com os padrões internacionais de proteção de dados pessoais e pode ajudar a promover a economia digital responsável no país. A análise econômica do direito pode ajudar a identificar oportunidades e desafios para a implementação da LGPD, bem como para o desenvolvimento de políticas públicas que apoiem a inovação e a competitividade no setor de tecnologia.

O GDPR, por sua vez, estabeleceu um marco regulatório importante para a proteção de dados pessoais na Europa e influenciou a adoção de regulamentações semelhantes em outros países ao redor do mundo. Um ano após a entrada em vigor do GDPR, já foi possível observar um impacto significativo na maneira como as empresas coletam, processam e utilizam dados pessoais. A análise econômica do direito pode ajudar a avaliar os efeitos do GDPR na economia europeia e identificar oportunidades para aprimorar a proteção dos dados pessoais.

Em suma, a proteção de dados pessoais é um desafio global que exige a cooperação de governos, empresas e sociedade civil. A análise econômica do direito pode ajudar a promover o diálogo e a colaboração entre esses atores, contribuindo para o desenvolvimento de políticas públicas que garantam a privacidade dos dados e incentivem a inovação e o crescimento econômico sustentável.

REFERÊNCIAS

ANDRADE, B. M.; SANTOS, P. C. Compartilhamento de dados pessoais sob a ótica da Lei Geral de Proteção de Dados. **Revista de Direito da Informação e Comunicação**, v. 1, n. 2, 2020.

ARAÚJO, T. S. **LGPD: lei geral de proteção de dados comentada**. São Paulo: Thomson Reuters Brasil, 2020.

AZEVEDO, Lyza Anzanello de. A análise econômica do direito e o realismo jurídico norte-americano. **Revista Internacional de História, Política e Cultura Jurídica**. Rio de Janeiro: vol. 10, n. 2, maio-agosto, 2018, p. 256-273.

BALKIN, Jack M.; ZITTRAIN, Jonathan. **A grand bargain to make tech platforms safe**. Washington Post, 15 mai 2018.

BARBOSA, E.; FUCHSHUBER, C. M. C. **Comentários à Lei Geral de Proteção de Dados Pessoais: aspectos gerais e princípios**. São Paulo: Quartier Latin, 2020.

BARBOSA, R. F., & Alves, T. R. M. A Lei Geral de Proteção de Dados (LGPD): um novo marco regulatório para a proteção de dados pessoais no Brasil. **Revista Eletrônica do Curso de Direito da UFSM**, 2020, 15(3).

BARBOSA, R. S. C.; ALVES, R. A. O direito ao esquecimento na LGPD: uma análise da possibilidade de exclusão de dados pessoais. **Revista Brasileira de Direito das Tecnologias da Informação e da Comunicação**, v. 2, n. 2, 2020.

BERNAL, Paul. **The end of data protection? Constitutional identity in the age of surveillance**. International Data Privacy Law, v. 7, n. 4, 2017.

BORBA, G., & Radaelli, M. O impacto da LGPD na economia brasileira: Uma análise da perspectiva econômica. **Revista de Direito, Tecnologia e Inovação**, 2020, 7 (1).

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Brasília, 2018.

COSTA, Danielle Nunes da. LGPD: Princípios e Bases Legais. *In*: MENKE, Fabiano. **Direito Digital Aplicado: Proteção de Dados e Privacidade**. 1. ed. São Paulo: Atlas, 2021.

COSTA, V. S. **LGPD e o direito fundamental à proteção de dados pessoais no Brasil**. Revista de Direito Digital e Compliance, 2021, 2 (2).

CRUZ, I. S. da, & Henrique, R. S. **LGPD e GDPR: Uma análise comparativa**. Revista da Faculdade de Direito da Universidade de São Paulo, 2020, 115 (2).

DEBATIN, Bernhard *et al.* **Facebook and online privacy: Attitudes, behaviors, and unintended consequences**. Journal of Computer-Mediated Communication, v. 18, n. 1, 2014.

DELOITTE. (2019). The impact of the GDPR after one year. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-rr-impact-of-gdpr-after-one-year.pdf. Acesso em: 1 out. 2023.

DIAS, C. V., & Nardi, H. C. A LGPD e seus desafios para a proteção de dados pessoais no Brasil. **Revista de Direito, Estado e Telecomunicações**, 2020, 12 (1).

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados.** 2. ed. São Paulo: Thomson Reuters, 2020.

DONEDA, Danilo *et al.* **Tratado de proteção de dados pessoais.** Rio de Janeiro: Editora Forense, 2021.

GÜNTHER, Klaus. **Teoria da Argumentação no Direito e na Moral: Justificação e aplicação.** Tradução: Claudio Molz; coordenação, revisão técnica e introdução à edição brasileira: Luiz Moreira. 2. ed. Rio de Janeiro: Forense, 2011.

KIERKEGAARD, Sylvia; SZÉKELY, Erika. **The GDPR: Challenges and opportunities**. Journal of Business Research, v. 98, 2019.

KOSTA, Eleni; FOVINO, Igor Nai; FISCHER-HUBNER, Simone; HANSEN, Marit; RAAB, Charles; SANCHEZ, Ignácio; WHITEHOUSE, Diane. **The Smart Revolution:** Privacy and Identity 2017, IFIP AICT 526, pp. 3–12, 2018.

LIEVENS, Eva *et al.* Data protection law: In search of a better balance. **Computer Law & Security Review**, v. 36, 2020.
LUNARDI, F. D. *et al.* LGPD: a importância do compartilhamento de dados pessoais. **Revista do Instituto Brasileiro de Direito da Informática**, v. 12, n. 1, 2020.

MACKAAY, Ejan; ROUSSEAU, Stéphane. **Análise Econômica do Direito.** Tradução: Rachel Sztajn. 2. ed. São Paulo: Atlas, 2015.

MELO, A. J. **A pseudonimização como alternativa para o tratamento de dados pessoais sensíveis**. *In*: IX Congresso Consad de Gestão Pública, 2021.

AGÊNCIA Brasil. Micro e pequenas empresas se destacam nos empregos gerados em 2022. [*S. l.*], 5 out. 2022. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2022-10/micro-e-pequenas-empresas-se-destacam-nos-empregos-gerados-em-2022#:~:text=No%20Brasil%2C%2099%25%20de%20todas,os%20microempreendedores%20individuais%20(MEI).%3E,. Acesso em: 1 out. 2023.

MOLA, Lorenzo *et al.* The General Data Protection Regulation (GDPR): A practical guide. **International Journal of Information Management**, v. 50, 2020.

MOREIRA, R. G. *et al.* Proteção de dados pessoais no Brasil e na Europa: análise comparativa da LGPD e da GDPR. *In*: **Anais do 15º Congresso Brasileiro de Gestão de Tecnologia e Sistemas de Informação**, 2020.

PORTO, Antônio José Maristrello; SILVA, Maria Eduarda Vianna. Lei Geral de Proteção de Dados Pessoais: Uma Análise Econômica sobre seu Regime de Responsabilidade. **Economic Analysis of Law Review**, v. 11, n. 2, mai-ago 2020, p. 283-300.

REZENDE, Fernanda Nunes Barbosa; AZEVEDO, Paulo Furquim de. A LGPD e o Direito do Consumidor: um enfoque na tutela dos dados pessoais. **Revista Direito, Estado e Sociedade**, v. 1, n. 55, 2019.

RÖCK, Daniel; WIESE, Andreas. General Data Protection Regulation (GDPR): A practical guide. **Computer Law & Security Review**, v. 35, n. 2, 2019.

RODRIGUES, Cristina Barbosa; SANTOS, Jéssica Mequilaine Correia dos; GAMBA, João Roberto Gorini. Dados pessoais na economia digital: análise dos impactos da proteção dos dados no uso de *big data* pelo GAFA. **Revista Direito Internacional e Globalização Econômica**, v. 8, n. 8, 2021, p. 179-197.

SANTOS, R. P.; ROCHA, E. G. A Autoridade Nacional de Proteção de Dados e a implementação da LGPD no Brasil. **Revista Direito e Liberdade**, v. 21, n. 1, 2021.

SANTOS, Rômulo Marcel Souto dos; LEITÃO, André Studart; WOLKART, Eric Navarro. A responsabilidade civil na Lei Geral de Proteção de Dados e a Regra de Hand. **Revista Opinião Jurídica**, ano 20, n. 34, maio/ago 2022, p. 60-84.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 11. ed. Porto Alegre: Editora do Advogado, 2010.

SCHWARTZ, Paul M. **Privacy and American business**. Chapel Hill, NC: University of North Carolina Press, 2011.

SOLOVE, Daniel J. **Understanding privacy**. Cambridge, MA: Harvard University Press, 2013.

SOUZA, A. R. F., Gomes, R. V.; Costa, E. S. A Lei Geral de Proteção de Dados (LGPD) e seus impactos na sociedade brasileira. **Revista Tema Livre**, 2020,15 (2).

TAYLOR, Linnet; SCHROEDER, Ralph. Is bigger better? The emergence of big data as a tool for international development policy. **GeoJournal**, v. 80, n. 4, 2015.

WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. **Columbia Business Law Review**, v. 2019, n. 2, 2019.

SUBMETIDO | *SUBMITTED* | *SOMETIDO* | 29/10/2023
APROVADO | *APPROVED* | *APROBADO* | 10/06/2024

REVISÃO DE LÍNGUA | *LANGUAGE REVIEW* | *REVISIÓN DE LENGUAJE*
Andreia Regina da Silveira Evaristo

SOBRE OS AUTORES | *ABOUT THE AUTHORS* | *SOBRE LOS AUTORES*

ANNELIESE REGINA FEILER
Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, Rio Grande do Sul, Brasil.
Pós-graduanda em Direito Empresarial pela Pontifícia Universidade Católica do Rio Grande do Sul. Advogada. E-mail: anneliesefeiler@outlook.com.

FELIPE GAZANIGA
Universidade Regional de Blumenau, Blumenau, Santa Catarina, Brasil.
Mestrando em Direito pela Universidade Regional de Blumenau. Pós-graduando em Direito Tributário pelo Instituto Brasileiro de Estudos Tributários. Pós-Graduado em Contabilidade Tributária pela Faculdade Brasileira de Tributação. Advogado. E-mail: felipe.gaza.dir@gmail.com.

THIAGO ANDRÉ MARQUES VIEIRA
Centro Universitário Católica de Santa Catarina, Joinville, Santa Catarina, Brasil.
Mestre em Direito pela Universidade Federal de Santa Catarina. Professor Universitário. Advogado. E-mail: thiago.vieira@catolicasc.org.br. ORCID: https://orcid.org/0009-0002-2778-125X.