



UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS E HUMANAS
GRADUAÇÃO EM DE DIREITO

Rummening Júnior Alves Nunes

**Implicações da Lei Geral de Proteção de Dados no Enfrentamento às Vulnerabilidades
do Tratamento de Dados Pessoais no Comércio Eletrônico**

MOSSORÓ

2024

Rummening Júnior Alves Nunes

**Implicações da Lei Geral de Proteção de Dados no Enfrentamento às Vulnerabilidades
do Tratamento de Dados Pessoais no Comércio Eletrônico**

Artigo apresentado ao Centro de Ciências Sociais Aplicadas e Humanas como parte dos requisitos para a obtenção do grau de Bacharel em Direito, pela Universidade Federal Rural do Semi-Árido.

Orientador: Rodrigo Vieira Costa, Prof. Dr.

MOSSORÓ

2024

Rummening Júnior Alves Nunes

**Implicações da Lei Geral de Proteção de Dados no Enfrentamento às Vulnerabilidades
do Tratamento de Dados Pessoais no Comércio Eletrônico**

Artigo apresentado ao Centro de Ciências Sociais Aplicadas e Humanas
como parte dos requisitos para a obtenção do grau de Bacharel em
Direito, pela Universidade Federal Rural do Semi-Árido.

APROVADO EM: 19/03/2024

BANCA EXAMINADORA

Rodrigo Vieira Costa

Assinado de forma digital por Rodrigo
Vieira Costa
Dados: 2024.04.08 09:39:28 -03'00'

**Orientador: Rodrigo Vieira Costa, Prof. Dr. (UFERSA)
Presidente**



Documento assinado digitalmente
GIOVANNA MARTINS WANDERLEY
Data: 08/04/2024 12:49:55-0300
Verifique em <https://validar.iti.gov.br>

**Giovanna Martins Wanderley, Prof. Msc.
(Faculdade Católica do Rio Grande do Norte - FCRN)
Membro Examinador**

Assinado de forma digital por
FELIPE MEDEIROS MARIZ
Dados: 2024.04.08 09:14:51
-03'00'

**Felipe Medeiros Mariz, Prof. Esp.
(Faculdade caicoense Santa Terezinha)
Membro Examinador**

MOSSORÓ

2024

© Todos os direitos estão reservados a Universidade Federal Rural do Semi-Árido. O conteúdo desta obra é de inteira responsabilidade do (a) autor (a), sendo o mesmo, passível de sanções administrativas ou penais, caso sejam infringidas as leis que regulamentam a Propriedade Intelectual, respectivamente, Patentes: Lei nº 9.279/1996 e Direitos Autorais: Lei nº 9.610/1998. O conteúdo desta obra tomar-se-á de domínio público após a data de defesa e homologação da sua respectiva ata. A mesma poderá servir de base literária para novas pesquisas, desde que a obra e seu (a) respectivo (a) autor (a) sejam devidamente citados e mencionados os seus créditos bibliográficos

N972i Nunes, Rummening Júnior Alves.
Implicações da Lei Geral de Proteção de Dados no
Enfrentamento às Vulnerabilidades do Tratamento de
Dados Pessoais no Comércio Eletrônico / Rummening
Júnior Alves Nunes. - 2024.
41 f. : il.

Orientador: Rodrigo Vieira Costa.
Monografia (graduação) - Universidade Federal
Rural do Semi-árido, Curso de Direito, 2024.

1. LGPD. 2. vulnerabilidade. 3. proteção de
dados pessoais. 4. plataformas digitais. I.
Costa, Rodrigo Vieira, orient. II. Título.

Ficha catalográfica elaborada por sistema gerador automático em conformidade
com AACR2 e os dados fornecidos pelo(a) autor(a).

Biblioteca Campus Mossoró / Setor de Informação e Referência

Bibliotecária: Keina Cristina Santos Sousa e Silva

CRB: 15/120

O serviço de Geração Automática de Ficha Catalográfica para Trabalhos de Conclusão de Curso (TCC's) foi desenvolvido pelo Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (USP) e gentilmente cedido para o Sistema de Bibliotecas da Universidade Federal Rural do Semi-Árido (SISBI-UFERSA), sendo customizado pela Superintendência de Tecnologia da Informação e Comunicação (SUTIC) sob orientação dos bibliotecários da instituição para ser adaptado às necessidades dos alunos dos Cursos de Graduação e Programas de Pós-Graduação da Universidade.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, por estar presente em minha vida e ter me guiado através da minha fé. Dedico gratidão por me conceder forças, paciência e discernimento ao longo dessa árdua jornada.

Aos meus pais pelo dom da vida e sempre acreditarem que darei orgulho pelas minhas conquistas. Em especial, agradeço à minha querida tia, Lourdes Afonso, a qual a chamo carinhosamente de “Scharlô”. Sou-lhe imensamente grato por existir em minha vida e por permanecer nela com o seu apoio, sentimento de amor e carinho e por sempre chorar comigo e me fazer criar forças para prosseguir e sentir que eu não estou só. Aos meus queridos avós, Terezinha e Pedro, por terem me ensinado a nobreza e humildade nas minhas bases educacionais desde criança.

Aos amigos que a UFERSA me proporcionou durante a graduação, tenho imensa admiração por cada um e a certeza de que se tornarão exímios profissionais. E em especial as minhas amigas de longas datas, Luzia Cilene, Joseilda Cristian e Gabriella West de Magalhães, e ao meu amigo/irmão André das Chagas Silva, gratidão pelo companheirismo e mútuo apoio nessa jornada, meu coração se alegra por ter encontrado vocês.

A todos os mestres, por todo o conhecimento compartilhado nesses anos de graduação e, em especial, ao meu orientador, Rodrigo Vieira Costa, por toda assistência prestada e paciência empregados na orientação deste trabalho de conclusão de curso.

Por fim, a todos que, de alguma maneira, fizeram parte da minha formação. Meus mais sinceros sentimentos de gratidão!

IMPLICAÇÕES DA LEI GERAL DE PROTEÇÃO DE DADOS NO ENFRENTAMENTO ÀS VULNERABILIDADES DO TRATAMENTO DE DADOS PESSOAIS NO COMÉRCIO ELETRÔNICO

IMPLICATIONS OF THE GENERAL DATA PROTECTION LAW IN ADDRESSING VULNERABILITIES OF PERSONAL DATA PROCESSING IN E-COMMERCE

Rummening Júnior Alves Nunes¹

RESUMO

O presente artigo analisa as implicações da Lei Geral de Proteção de Dados Pessoais (LGPD), lei 13.709/2018, diante da vulnerabilidade no tratamento de dados pessoais pelas plataformas de compras online operando no Brasil. Discute, ainda, a relevância da proteção de dados pessoais e sua aplicabilidade jurídica, com o objetivo de garantir o exercício efetivo dos direitos e liberdades fundamentais do titular dos dados. A tecnologia está cada vez mais presente em nosso cotidiano, o que aumenta a exposição de nossos dados pessoais. Essa nova era traz muitos benefícios, como a facilidade de acesso a informações e serviços, a possibilidade de comunicação com pessoas de todo o mundo e a inovação em diversas áreas. No entanto, também traz riscos, como o vazamento de dados, a discriminação e o monopólio. Para os usuários, é difícil compreender como seus dados são coletados, armazenados e utilizados. Isso dificulta a identificação de práticas abusivas, que podem prejudicar a privacidade e a segurança das pessoas. No contexto brasileiro, a cultura de proteção de dados ainda está em desenvolvimento. Neste estudo, empregou-se artigos acadêmicos e se conduziu uma pesquisa bibliográfica e, como também, realizou-se uma pesquisa qualitativa, para proporcionar uma perspectiva abrangente sobre a proteção de dados pessoais em plataformas digitais. Por fim, discutir-se-á enquadramentos jurídicos não só de casos de e-commerce, mas também, de empresas de pequeno, médio e grande portes e de vários segmentos de atuação, que podem ser investigadas e penalizadas pela Autoridade se usarem indevidamente dados pessoais, sejam eles digitais ou não.

Palavras-chave: vulnerabilidade; proteção de dados pessoais; plataformas digitais.

ABSTRACT

This article analyzes the implications of the General Personal Data Protection Law (LGPD), Law 13.709/2018, in light of the vulnerability in the processing of personal data by online shopping platforms operating in Brazil. It also discusses the relevance of personal data protection and its legal applicability, aiming to guarantee the effective exercise of the fundamental rights and freedoms of the data subject. Technology is increasingly present in our daily lives, which increases the exposure of our personal data. This new era brings many benefits, such as easy access to information and services, the possibility of communication with people from all over the world, and innovation in various areas. However, it also brings risks, such as data leaks, discrimination, and monopoly. For users, it is difficult to understand how their data is collected, stored, and used. This makes it difficult to identify abusive practices that can harm people's privacy and security. In the Brazilian context, the data protection culture is still under development. This study used academic articles and conducted a bibliographic research and a qualitative research, in order to provide a comprehensive perspective on the protection of personal data in digital platforms. Finally, it will discuss legal frameworks not only for e-commerce cases, but also for small, medium and large companies and companies from various segments that can be investigated and penalized by the Authority if they misuse personal data, whether digital or not.

Keywords: vulnerability; personal data protection; digital platforms.

1 INTRODUÇÃO

A era digital inaugurou uma nova fase para a sociedade, demandando uma perspectiva renovada sobre a informação. Nesta conjuntura, a informação é percebida como um recurso precioso, e seus ativos têm importância significativa para a economia do país. Nesse sentido, de acordo com Castells (2002, p.119), “informação e conhecimentos sempre foram elementos cruciais no crescimento da economia, e a evolução da tecnologia determinou em grande parte a capacidade produtiva da sociedade e os padrões de vida, bem como formas sociais de

¹ Acadêmico do curso de Direito da Universidade Federal Rural do Semi-árido (UFERSA).
E-mail: rummeningjr@gmail.com

organização econômica”. Isso significa que as pessoas agora têm acesso a um enorme banco de dados de conhecimento, que pode ser usado para aprender, inovar e tomar decisões.

A partir dessa perspectiva, no contexto atual de compras no Brasil, os processos têm se tornado progressivamente mais automatizados com o auxílio de ferramentas tecnológicas capazes de processar dados de maneira mais ágil e dinâmica, promovendo uma transformação cultural voltada para a digitalização. Assim, com o surgimento de novos padrões de mercado, como, por exemplo, a expansão do setor de e-commerce no país, disponibilizou-se uma ampla gama de produtos em larga escala e distribuição.

Justifica-se, então, este trabalho pela relevância de proteção de informações como uma prioridade e necessidade de limitar o uso e tratamento de dados pessoais por parte das empresas e usuários que manuseiam dados pessoais, consequentemente, vinculá-las a regras de utilização através das implicações da vigência da Lei Geral de Proteção de Dados (LGPD) nas plataformas de compras *online* operando no Brasil, atuando na aplicabilidade jurídica na condição de proteção e garantia dos direitos dos usuários.

Quando nos deparamos com novas demandas, consequentemente, delas acarretará novas necessidades, problemas e complexidades na busca de uma resposta mais assertiva para as respectivas resoluções. Nesse sentido, o exímio avanço tecnológico tem trazido mudanças significativas para todas as esferas da sociedade.

A nova era digital tem tornado a tecnologia cada vez mais presente no cotidiano das pessoas. Isso tem levado a um aumento da exposição tecnológica e do tratamento de dados pessoais. No entanto, para os usuários, há pouca transparência sobre o funcionamento e a manipulação desses dados. Torna-se, assim, mais difícil identificar práticas abusivas, discriminatórias ou monopolistas, principalmente no contexto brasileiro, onde a cultura de proteção de dados ainda está no início.

Essa situação implica que os indivíduos não têm conhecimento de seus direitos e estão incertos sobre como salvaguardar suas informações pessoais. Como resultado, elas são mais vulneráveis a esses abusos. A nova era digital traz muitos benefícios, mas também traz riscos. É importante que as pessoas estejam cientes desses riscos e que tomem medidas para se proteger.

Cumpre, assim, “investigar como e quando a informação passou a avocar tal papel de protagonismo, a ponto de imprimir uma completa alteração do padrão em que se estruturam as relações sociais.” (Bioni, 2021, p. 5).

Desta forma, faz-se necessário o presente artigo analisar as demandas imediatas geradas pelo vigor da LGPD no cenário brasileiro, bem como, investigar os desafios do futuro quanto à efetividade desta lei, especialmente nestes ambientes modernos como o *e-commerce*, de tal modo a abordagem das principais legislações pertinentes a proteção dos dados do consumidor neste mercado digital, visando demonstrar a evolução da legislação brasileira no quesito de regulação do uso, tratamento, sanções de mau uso e proteção de dados pessoais.

Entretanto, tem-se como o objetivo desta pesquisa analisar a relevância da proteção de dados pessoais oriundos da implementação da LGPD e da sua aplicabilidade jurídica frente aos deveres das plataformas de comércio eletrônico no tratamento de dados.

Em relação à metodologia, foi empregado o método bibliográfico com seu suporte teórico e normativo, bem como estudos de artigos científicos e outros textos selecionados, tornando, assim, esta pesquisa de natureza qualitativa. Assim, podemos citar alguns exemplos de livros de doutrinadores relevantes utilizados neste estudo como: "Proteção de Dados Pessoais: Fundamentos, Princípios e Aplicação" (de Gustavo Junqueira e Bruno Bioni); "A Lei Geral de Proteção de Dados Pessoais" (de Fabrício Copetti Ribeiro); "Direito Digital: Fundamentos, Princípios e Aplicações" (de Rafael Siqueira), dentre outros.

Assim, este artigo apresenta, em sua primeira seção, o contexto geral da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, e o avanço das discussões sobre a proteção de

dados pessoais no Brasil. A legislação brasileira, que antes carecia de uma lei específica sobre o tema, agora exige requisitos mais rigorosos para o tratamento de dados pessoais.

Contudo, na segunda seção, discutir-se-á sobre o comércio eletrônico no Brasil, os benefícios que ele trouxe para os consumidores virtuais e a necessidade de proteger a privacidade dos dados pessoais.

Posteriormente, a terceira seção discute as análises das implicações significativas oriundas da LGPD para as empresas e os usuários que lidam com dados pessoais. Essas implicações incluem mudanças no marketing, nos custos operacionais, nas restrições comerciais e em outros aspectos que serão debatidos no decorrer deste estudo.

E na quarta seção, será abordado o contexto da aplicabilidade jurídica da LGPD e da importância da criação do órgão da Autoridade Nacional de Proteção dos Dados, ANPD, que fiscaliza os dados pessoais de pessoas físicas, sejam eles digitais ou não, utilizados e acessados por empresas. Como também, dar-se-á ênfase às análises não só de casos de e-commerce já julgados sobre as penalidades e sanções administrativas, mas também, de empresas de pequeno, médio e grande portes e de vários segmentos de atuação, que podem ser investigadas e penalizadas pela ANPD se usarem indevidamente dados pessoais, sejam eles digitais ou não.

2 A LEI GERAL DE PROTEÇÃO DE DADOS

No atual panorama em que estamos inseridos, a proteção de dados assume um papel de importância no cenário brasileiro e mundial para os próximos anos. Logo, a Constituição Federal do Brasil de 1988 estabelece diversos direitos fundamentais. Nela, em seu art. 5º, XII, também, foram adotadas possíveis medidas de sigilo, com objetivo de preservar a inviolabilidade da privacidade, alcançada também pela classe de mensagens da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

No entanto, a proteção de dados pessoais não é tema novo na legislação brasileira, havendo menção em várias normas, a exemplo da Constituição Federal (art. 5º, X, XI, XII, LV e IX), do Código Civil (arts. 20 e 21), do Código de Processo Penal (art. 201, § 6º) e do Marco Civil da Internet (Lei n. 12.965/2014, arts. 3º, II, 7º, I, 8º, 21 e 23), cujos arts. 7º, X, e 16, II, foram alterados pelo art. 60 da Lei n. 13.709/2018 (LGPD – Lei Geral de Proteção de Dados).

Todavia, no ano de 2022, ocorreu uma alteração importante em nossa Constituição Federal. Foi introduzida a Emenda Constitucional (EC) nº 115, que acrescentou o inciso LXXIX ao artigo 5º. Essa emenda ampliou a proteção dos dados pessoais nos meios digitais e ela é considerada uma norma de eficácia limitada, ou seja, para sua aplicação e efetiva vigência dependerá de uma regulamentação por meio de uma lei infraconstitucional. Nesse contexto, primeiro, houve a edição da lei infraconstitucional (a Lei 13.709/18 - Lei Geral de Proteção de Dados) e posteriormente, foi promulgada a EC nº 115, que incorporou as mudanças ao artigo 5º da Constituição Federal (BRASIL, 1988), que cita: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Nesta perspectiva, podemos constatar que houve um grande avanço no ordenamento jurídico nacional no tocante ao tratamento de proteção de dados pessoais. Uma vez que esta se iniciou com a lei de Acesso à Informação (lei 12.527/11) e com o Marco Civil da Internet (lei 12.965/14) que versaram de forma tímida sobre o tema.

Depois, o Supremo Tribunal Federal já havia reconhecido, através da liminar da ADI 6.387, em maio de 2020, a proteção de dados pessoais como um direito fundamental implícito, passando a ser bem disciplinada pela lei 13.709/18, a lei geral de proteção de dados (LGPD). E, logo depois, com a promulgação da EC 115/2022 a proteção de dados passa a ser um direito

fundamental expresso e explícito no nosso ordenamento jurídico, consolidando-se tal direito como uma garantia constitucional.

Nesse intervalo, com o intuito de um melhor entendimento, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD) são duas leis brasileiras que regulam o uso da internet no país. Apesar de terem objetivos distintos, ambas se complementam na criação de um ambiente digital mais seguro e transparente para os usuários. De acordo com Gonçalves (2017, p. 1) cita que "O Marco Civil inicia-se com o comando legal de que nele se estabelecem os princípios, garantias, direitos e deveres para o uso da internet no Brasil." , a LGPD (Lei Geral de Proteção de Dados) visa regulamentar a captura e tratamento de dados pessoais em território nacional. Em resumo, o Marco Civil da Internet estabeleceu os princípios gerais para o uso da internet no Brasil, enquanto a LGPD trouxe exigências mais específicas para a proteção de dados pessoais, alinhando-se às melhores práticas internacionais.

Entretanto, cabe ressaltar que, a lei brasileira que tutela os dados pessoais, a LGPD, em grande parte, recebeu influência da legislação europeia. Assim, afirma Garcia *et al.* (2020, p. 16) que,

A Lei Geral de Proteção de Dados Pessoais (LGPD, Lei n. 13.709/2018), ainda em *vacatio legis*, tem causado tumulto. Afinal, para quê serve? Inspirada na lei europeia de proteção de dados, conhecida como *General Data Protection regulation (GDPR)*, a LGPD tem como objetivo proteger dados pessoais de pessoas naturais, ou seja, pessoas físicas. Este é o primeiro ponto: a LGPD não tem como escopo os dados das empresas (pessoas jurídicas), mas sim os dados que as empresas têm das pessoas físicas, sejam elas funcionárias, terceiras, clientes, acionistas etc. - ou seja, todo mundo. A lei, criada em 14 de agosto de 2018, tem 65 artigos e foi alterada pela Medida Provisória 869/2018 e pela Lei n. 13.853/2019. Embora seja a legislação mais recente e mais específica, não é a única lei que rege a privacidade. Esse tema já havia sido tratado em alguns outros lugares antes, como: a Constituição Federal, o Marco Civil da Internet, o Código de Defesa do Consumidor, a Lei de Acesso à Informação, a Lei do Habeas Data e o Decreto do Comércio Eletrônico. (Garcia *et al.*, 2020, p. 16)

Nesse sentido, devido às lacunas legislativas na seara protetiva de dados, tais leis e regulamentos publicados anteriormente, foram a mola propulsora para motivação de necessidades jurídicas na criação de novas leis que possam promover a regulação da rede de *internet*, contudo sem ferir a liberdade dos indivíduos que fazem o uso da mesma, contribuindo para o avanço tecnológico, e assim, para o surgimento da LGPD como apoio jurídico à proteção de dados pessoais na criação de novas regras e regulamentação desses novos mercados digitais para harmonizar o convívio em sociedade.

De acordo com Almeida e Soares (2022), destaca-se a regulamentação híbrida presente nas normativas da LGPD. Essa lei, aborda a proteção de dados pessoais em diversos contextos, incluindo a governança, o tratamento de dados e a segurança das informações. A multidisciplinaridade de conhecimentos é fundamental para compreender e aplicar a LGPD de maneira eficaz. Isso envolve a atualização documental e o assessoramento jurídico, garantindo que as respostas sejam definidas com a devida relevância e prioridade.

Assim, a Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção dos Dados, promulgada no Brasil em 14 de agosto de 2018, alterada pela Medida Provisória nº 869/2018 e, convertida na Lei 13.853/2019, entrou em vigor em 18 de setembro de 2020. É composta por 65 artigos, distribuídos em 10 capítulos e com a fiscalização pela Autoridade Nacional de Proteção de Dados, ANPD, iniciada em 1º de agosto de 2021.

Como principais quesitos da LGPD, podemos destacar em seu primeiro capítulo que dispõe sobre os objetivos da lei (art. 1º), seus fundamentos (art. 2º), sua aplicabilidade (art. 3º e 4º), definições (art. 5º), princípios (art. 6º) e dez tópicos de permissão do tratamento de dados pessoais (artigo 7º),

Deste modo, no art. 1º da LGPD, tem como principal “[...] objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.”. Nessa perspectiva, regulamentar o uso, a proteção e o tratamento de dados pessoais, garantindo a privacidade e a segurança dos indivíduos.

No artigo 2º desta lei, baseia-se como a disciplina da proteção de dados pessoais os fundamentos:

I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - à inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Segundo Garcia *et al.* (2020, p. 18) todos esses fundamentos estão “previstos constitucionalmente, e são repetidos aqui com o intuito de reforçar sua aplicabilidade”. No entanto, aplicar-se-ão a todas as empresas que realizam o tratamento de dados pessoais, seja no meio físico ou digital, que ocorra no Brasil ou que envolva dados de pessoas que estejam no Brasil. Em seu art. 3º, da LGPD:

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência. III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.[...];

Portanto, podemos afirmar que, não importa o modo de operação de tratamento de dados, o país de origem da empresa, a localização dos dados, a nacionalidade dos titulares dos dados. A LGPD se aplica às empresas que preenchem pelo menos um dos requisitos como ter estabelecimento no Brasil, oferecer serviço no mercado consumidor brasileiro, coletar e tratar dados de pessoas localizadas no Brasil.

Nessa seara, Lima (2020, p. 41) aponta que, “No Brasil, a recente lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD) é um importante instrumento de regulação do poder da empresa no trato de dados pessoais para garantia da liberdade, privacidade e desenvolvimento dos seres humanos”. Essa lei deve ser entendida como um sistema, pois ela define os princípios que orientam os direitos essenciais dos titulares dos dados pessoais, bem como os fundamentos e as obrigações dos que tratam esses dados. Além dos fundamentos, a lei traz conceituações importantes. De acordo com Garcia *et al.* (2020, p. 18-19),

Para a lei, dado pessoal é uma “informação relacionada à pessoa natural identificada ou identificável”, ou seja, dados como nome, endereço, sexo, RG e CPF. A lei define ainda o conceito de dado pessoal sensível como um “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (Garcia *et al.*, 2020, p. 18-19)

Outro ponto-chave da LGPD é o consentimento dos indivíduos para a coleta e uso de seus dados. Isso implica que as empresas precisarão informar claramente aos indivíduos qual será a finalidade da coleta dos dados e como eles serão utilizados.

Ainda, os autores mencionados acima, Garcia et al. (2020, p. 19), mostram que a LGPD estabelece, no artigo 5º, quem são os principais envolvidos no tratamento de dados pessoais:

- **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- **Encarregado de dados:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **Autoridade Nacional de Proteção de Dados (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei em todo o território nacional. (Garcia *et al.*, 2020, p. 19)

Isto posto, a proteção que a LGPD garante é voltada para as pessoas físicas, não alcançando os dados das pessoas jurídicas. Protege os dados pessoais de qualquer pessoa que tenha seus dados pessoais tratados para fins econômicos, seja por órgãos públicos, empresas ou outras pessoas. Sobre o titular da lei LGPD supracitado, Teixeira & Guerreiro (2022, p. 31) afirmam que, “a lei fala em titularidade dos dados pessoais e não propriedade, uma vez que os dados pessoais não constituem algo de que se possa dispor, pelo contrário, os dados pessoais passaram a ser considerados uma nova variante da categoria dos direitos de personalidade”.

Já referente aos agentes de tratamento de dados pessoais, estão presentes com melhor detalhamento no capítulo VI da lei LGPD em que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. Sobre estes, Teixeira e Guerreiro (2022, p. 40) confirmam que,

É obrigação legal do controlador e do operador manter o registro de operações de tratamento de dados que realiza, materializando-se o princípio da prestação de contas (accountability). Segundo o princípio da accountability, é necessário documentar tudo o que foi feito para dar cumprimento à lei, inclusive as negativas. Assim, deve-se registrar tudo com relatórios e evidências, que serão de suma importância para se demonstrar o cumprimento da lei. Identificam-se nesse artigo os princípios da transparência e o da responsabilização e prestação de contas, em que não basta cumprir a lei, é necessário que se deixe registrado que a lei foi cumprida. Não houve determinação pelo legislador de qual seria o conteúdo mínimo ou mesmo quais seriam as suas exceções, entretanto a LGPD traz em seu bojo elementos que servem como guia para orientar as organizações de como fazer esse registro, dos quais podem-se citar: identificação do responsável pelo preenchimento; finalidade, forma e duração do tratamento; identificação do controlador com informações de contato; informações acerca do uso compartilhado de dados; base legal atribuída a cada operação; informações relacionadas à transferência internacional quando houver; descrição da natureza dos dados pessoais tratados e informações sobre os titulares envolvidos. (Teixeira e Guerreiro, 2022, p. 40)

Nessa seara, para que haja um compartilhamento de dados resguardados de perigos e em conformidade com a lei, a LGPD busca um equilíbrio entre o desenvolvimento econômico e o respeito à privacidade dos indivíduos, garantindo que seus dados pessoais sejam coletados, armazenados, utilizados e compartilhados de forma segura.

A LGPD exige que as empresas atuem em diferentes frentes de trabalho, criando uma cultura de proteção e de privacidade de dados. Diante de tais constatações, faz-se indispensável a aplicação de princípios, que conduzam a aplicação da lei na lacuna legal.

Através do seu art. 6º, a LGPD determina que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os dez seguintes princípios: I – finalidades; II – adequação;

III – necessidade; IV – livre acesso; V – qualidade dos dados; VI – transparência; VII – segurança; VIII – prevenção; IX – não discriminação; X – responsabilização e prestação de contas.

Portanto, são estes os princípios que têm como objetivos norteadores do tratamento de dados pessoais, com intuito de ajudar a garantir que as empresas estejam em conformidade e adequação à LGPD. Assim, Teixeira e Guerreiro, (2022, p.19) afirmam que traz “os princípios dentre os seus artigos destacando que eles devem ser considerados em toda atividade de tratamento de dados, independentemente das mudanças que virão com o decorrer do tempo”.

Há, também, os dez requisitos elencadas no artigo 7º da LGPD para a permissão do tratamento de dados pessoais:

I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Nessa seara, através da análise dos objetivos deste estudo, a LGPD pode ser vista como uma lei baseada em princípios, que oferece um conjunto de orientações preventivas de possíveis incidentes ou práticas ilegais. Se tais incidentes ocorrerem, os agentes encarregados serão responsabilizados por meio de decisões jurídicas.

Assim, Fornasier e Knebel (2021) comentam que a LGPD tende a permitir a criação de maiores condições para implementação de um mercado de dados no Brasil, sendo o consentimento do titular o instrumento de regulação e legitimidade que a lei entrega a esse novo mercado, tornando a exploração de dados nada além de uma contratação.

O comércio eletrônico brasileiro, em franca expansão, impõe a necessidade de uma regulamentação robusta para a proteção dos dados pessoais dos consumidores em plataformas digitais. Assim, a LGPD assume um papel crucial no e-commerce, definindo regras claras para o tratamento de dados por parte das empresas. O consentimento livre, específico e com o poder de revogação a qualquer momento, é um elemento fundamental na relação entre a LGPD e o comércio eletrônico.

3 REGULAMENTAÇÃO DO COMÉRCIO ELETRÔNICO NO BRASIL

O comércio eletrônico, também conhecido como *e-commerce*, é frequentemente usado para a descrição de venda, troca de produtos ou serviços diretamente aos consumidores de forma virtual. Ressalta-se aqui que este estudo inclui vendas de produtos e serviços por meio de quaisquer canais de forma virtual como computadores, celulares, aplicativos e lojas virtuais próprias.

De acordo com Stival (2013) o *e-commerce* surge como uma ferramenta de revolução para o mercado *online* e a forma de realização de negócios por meio do ambiente virtual é ágil, interativa e simples de implantação para as entidades, que estão adaptando-se nas situações de

comunicação com o cliente, nas formas de recebimento e pagamento e outras facilidades promovidas pela tecnologia contemporânea que são ditadas pelo consumidor e não pelo produtor. Campos e Goulart (2021) afirmam que, até então, esse novo mercado digital era totalmente desconhecido e

não existiam pressupostos teóricos para essa nova realidade e muitos conceitos do varejo tradicional não se aplicavam ao varejo on-line. O jeito era colocar a mão na massa e aprender o mais rápido possível com a própria experiência, ou seja, o foco era fazer, validar e corrigir de forma contínua. (Campos e Goulart, 2021, p. 15)

Assim, a partir da discussão sobre a necessidade de uma norma específica para o *e-commerce*, entrou em vigor no Brasil o Decreto n. 7.962, de 15 de março de 2013, que regulamenta o Código de Defesa do Consumidor para dispor sobre a contratação no comércio eletrônico. Este Decreto, que regulamenta a Lei nº 8.078 de 1990, estabelece regras para a contratação no comércio eletrônico. Ele enfatiza a necessidade de informações claras sobre o produto, serviço e fornecedor, facilita o atendimento ao consumidor e respeita o direito de arrependimento.

Assim, o *e-commerce* começou a despertar uma série de interesses por parte dos empreendedores, pelo motivo de uma prospecção de atingir esse novo nicho de compras e por ser algo irreversível e de forte crescimento de lucratividade e de baixo custo no mundo dos negócios. Nesse sentido, “O *e-commerce* é um dos sistemas que mais cresce na economia digital e está fazendo parte das estratégias de vendas das empresas.” (Campos e Goulart, 2021, p. 14). Essa regulamentação trata de pontos fundamentais para que consumidores e lojistas do comércio eletrônico tenham mais segurança em suas relações.

Segundo Andrade e Silva (2017) o comércio eletrônico trouxe uma verdadeira revolução, tornando a compra e venda mais fácil, confortável, rápida e de baixo custo. A flexibilidade na compra é maior, pois não é necessário ir até a loja física, há a facilidade de comprar de qualquer lugar. Sendo assim, com cuidado e atenção, o comércio eletrônico pode ser uma ótima maneira de fazer compras de forma conveniente e segura, visto que, a literatura salienta que é necessário pesquisar, buscar informações sobre a empresa vendedora e procurar ler comentários sobre as experiências de compras.

Conforme afirmam Gimenez, Montanhas e Silva (2023) que no ano de 2020, a humanidade enfrentou um desafio sem precedentes,

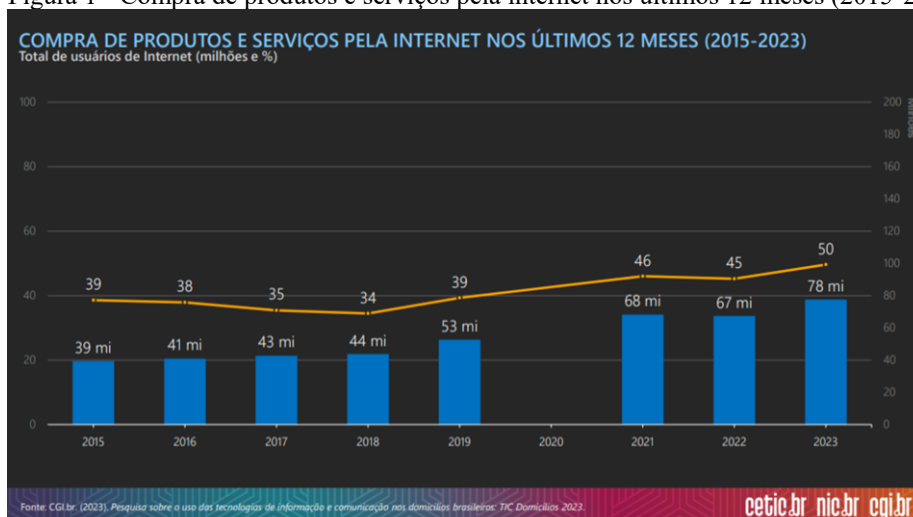
na pandemia de Covid-19, que alterou profundamente a forma como vivemos, trabalhamos e consumimos. Diante desse cenário, o comércio eletrônico emergiu como uma solução vital para a sobrevivência e o crescimento dos negócios, que tiveram que se adaptar às novas exigências e oportunidades do mercado digital. [...] O comércio no geral teve que se adaptar às novas regras, e ao mesmo tempo, conseguir de alguma maneira uma forma de continuar lucrando para não ir à falência. [...] Foram criadas diversas estratégias de vender mesmo em quarentena, o principal foi o comércio eletrônico e de seus produtos. [...] Portanto, o e-commerce se consolidou como uma tendência irreversível no mundo dos negócios [...]. (Gimenez; Montanhas; Silva, 2023)

A era digital é uma realidade inegável. O mundo online se tornou um mercado crucial para o sucesso de qualquer empresa, e Gimenez, Montanhas e Silva (2023) ainda ressaltam que as empresas físicas que até este momento não ingressaram nesse universo precisam se adaptar rapidamente. A pandemia serviu como um grande acelerador dessa mudança, evidenciando a importância da presença digital para a sobrevivência dos negócios. Mais do que uma tendência, a transformação digital é uma necessidade. As empresas que ignoram essa realidade correm o risco de ficar para trás, perdendo competitividade e relevância no mercado. Acompanhar o ritmo

acelerado das mudanças é fundamental para criar estratégias eficazes e se manter à frente da concorrência.

Partindo dessa premissa, podemos destacar a pesquisa TIC Domicílios (Tecnologias da Informação e Comunicação nos Domicílios) do ano de 2023, que recentemente foi divulgada pelo Comitê Gestor da Internet no Brasil (CGI.br) em 16 de novembro, que confirma esses fatos e apresenta informações interessantes sobre o *e-commerce* no Brasil. Na edição de 2023, a coleta de dados foi realizada entre março e julho de 2023, abrangendo amostra de 23.975 domicílios respondentes e 21.271 indivíduos respondentes. Desde 2005, a pesquisa TIC Domicílios é realizada anualmente com o propósito de rastrear o acesso e uso das tecnologias de informação e comunicação em residências permanentes no país, por pessoas com 10 anos de idade ou mais. A pesquisa aborda diversos temas, como acesso às TIC nos domicílios, uso do computador, uso da internet, habilidades digitais, uso do telefone celular, serviços públicos *online*, comércio eletrônico e atividades culturais na internet.

Figura 1 - Compra de produtos e serviços pela internet nos últimos 12 meses (2015-2023) no Brasil



Fonte: CGI.br (2023). Pesquisa sobre o uso das Tecnologias da Informação e Comunicação nos domicílios brasileiros: TIC Domicílios 2023.

Assim, a referida pesquisa revelou que o *e-commerce* no Brasil está em ascensão e, logo, 84% dos domicílios brasileiros têm acesso à *internet*, o que equivale a cerca de 156 milhões de usuários de internet e destes, cerca de 78 milhões, o que equivale a 50% dos internautas, que realizaram compras de produtos e serviços pela internet em 2023, um aumento de 5 pontos percentuais em relação a 2022. A pesquisa também revelou que 16% dos domicílios compartilham a conexão com vizinhos. O uso de smartphones para compras feitas *online* é predominante com 82%, consolidando o domínio do *mobile* no *e-commerce* e a confiança do consumidor está aumentando, pois a pesquisa indica que 74% dos consumidores se sentem seguros ao comprar *online*, pois estes adotaram medidas de segurança para proteger dispositivos e contas. Os principais fatores que contribuem para essa segurança são a reputação do *site*, a política de troca e devolução e a proteção de dados.

No entanto, desafios como logísticas de entrega e confiança em sites desconhecidos persistem. O estudo destaca a oportunidade de crescimento no *e-commerce* brasileiro, especialmente nas classes C e D/E com aumento de 16% nas compras online e a necessidade de as empresas investirem em segurança, logística eficiente e experiência do cliente.

A interpretação desses dados da pesquisa mencionada mostra que o crescimento digital nos últimos anos permitiu que um maior número de indivíduos e empresas se conectassem e efetuassem transações pela internet, um elemento crucial para o estímulo do *e-commerce* em todo o mundo e, de maneira significativa, no Brasil. Essa expansão digital proporcionou

diversos benefícios para os consumidores, as empresas e a economia brasileira como um todo. Isso resultou em implicações como a ampliação da base de consumidores, uma vez que a internet democratizou o acesso ao comércio, possibilitando que indivíduos de diversas classes sociais e regiões do país pudessem realizar compras online.

Além disso, proporcionou a expansão da oferta de produtos e serviços de pequenas e médias empresas que criaram suas próprias lojas virtuais, atingindo um público mais amplo e aumentando a variedade de produtos e serviços disponíveis na internet. O *e-commerce* é um segmento que proporciona a criação de milhares de novos postos de trabalho e aumenta a renda das pessoas anualmente, tanto em empresas de varejo online quanto em empresas que oferecem serviços relacionados ao *e-commerce*. Esse fato oportunizou uma conveniência e acessibilidade aos consumidores, permitindo que realizassem compras de qualquer lugar e a qualquer momento através do comércio eletrônico, sem a necessidade de se deslocarem até lojas físicas.

Contudo, com a maior exposição de nossos dados pessoais por meio dessas transações *online*, surgem também riscos associados, como vazamento de dados, discriminação e monopólio. Para os usuários, é complexo entender como seus dados são coletados, armazenados e usados. Um dos riscos mais significativos da coleta de dados online é o vazamento. Hackers e criminosos digitais podem violar sistemas e servidores, roubando informações sensíveis que podem ser empregadas para atividades fraudulentas, como roubo de identidade e fraudes financeiras. A acumulação de dados por grandes empresas pode resultar na formação de monopólios e na redução da concorrência. Essas empresas podem exercer seu poder de mercado para influenciar preços, controlar o acesso à informação e prejudicar os consumidores. Termos de serviço longos e linguagem complicada tornam difícil a identificação de práticas prejudiciais que podem comprometer a privacidade e a segurança das pessoas.

Esses dados são fundamentais para tomar medidas para mitigar os riscos da coleta de dados online, para entender a propagação e o uso das TICs nos domicílios brasileiros, e poder orientar políticas governamentais e iniciativas do setor privado para expandir o acesso e o uso eficiente dessas tecnologias.

4 IMPLICAÇÕES DA LGPD NO COMÉRCIO ELETRÔNICO

Em relação ao comércio eletrônico, considerando o aumento significativo de dados em várias operações *online*, a LGPD foi estabelecida para garantir que novas demandas de manejo de dados pessoais estejam em conformidade com as leis, através de um ambiente jurídico que ofereça uma proteção de dados mais robusta.

O surgimento desta lei específica sobre proteção dos dados pessoais decorreu das novas necessidades do mundo digital em que vivemos, o qual exige mais transparência nas relações perante o modelo atual de negócios, tendo em vista que a informação é a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências. (Pinheiro, 2019)

Sob essa ótica, a partir desta pesquisa, conseguiu-se identificar diversas implicações importantes que surgiram com a implementação da LGPD para empresas e usuários que manuseiam dados pessoais, tais como:

Quadro 1 - Implicações que surgiram com a implementação da LGPD

<i>Áreas de Impactos</i>	<i>Descrição</i>	<i>Artigos Relevantes da LGPD</i>
<i>Implicações no Marketing</i>	A LGPD exige que as empresas que coletam dados pessoais para fins de marketing obtenham o consentimento dos titulares dos dados antes que sejam coletados.	· 5º define dados pessoais e dados pessoais sensíveis; · 6º estabelece princípios e em observância à boa-fé para as atividades de tratamento de dados pessoais; · 10 obrigações das empresas que coletam dados pessoais; · 18 direitos dos titulares dos dados pessoais; · 52 sanções para as empresas que não cumprem a LGPD.
<i>Implicações nos Custos Operacionais</i>	Investimento em medidas e procedimentos para garantir conformidade com a LGPD.	Inclui treinamentos de funcionários, implementação de sistemas de segurança e privacidade, auditorias de conformidade e outras ações relacionadas, “utilizando-se de estratégias e instrumentos de prevenção, às penalidades poderão ser evitadas, [...]”. (Teixeira, 2021, p. 95)
<i>Implicações nas Restrições Comerciais</i>	Empresas podem enfrentar restrições para operar em mercados ou setores por não conformidade com a LGPD.	6º elenca uma série de princípios a serem observados pelas empresas no tratamento de dados. Um exemplo específico de restrições comerciais: a empresa de e-commerce que não tenha um sistema de segurança adequado para proteger os dados de seus clientes pode ser multada e até mesmo ter seu site suspenso.
<i>Implicações no Gerenciamento de Consentimento</i>	As empresas de comércio eletrônico precisam garantir que obtenham consentimento explícito para dados confidenciais, como informações financeiras ou de saúde	8º o consentimento previsto no inciso I do art. 7º desta lei que deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular
<i>Implicações no Direitos do Usuário e Transparência</i>	Diversos direitos aos usuários em relação aos seus dados.	· 17 os direitos dos titulares; · podemos destacar alguns artigos relevantes da LGPD que tratam dos direitos do usuário e da transparência, o art. 18, art. 19, art. 20, art. 21 e o art. 22
<i>Implicações nas Transferências de Dados Internacionais</i>	Transferência de dados para outros países com medidas de segurança.	· 5º, inciso XV “[...] transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro”; · 33 a transferência internacional de dados pode ocorrer desde que seja compatível com seu rol de situações.

<i>Implicações no Manuseio e Armazenamento de Dados</i>	A LGPD exige que as empresas manipulem e armazenem dados pessoais com medidas de segurança	46 os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
<i>Implicações nos Litígios e Processos judiciais</i>	Notificação de violação de dados às autoridades e usuários.	48 caso haja vazamento ou uma violação de dados que possa afetar negativamente os indivíduos, as empresas de comércio eletrônico são obrigadas a notificar as autoridades e os usuários afetados imediatamente. Isso pode acarretar de a empresa poder enfrentar ações judiciais por parte dos clientes ou das autoridades de proteção de dados.
<i>Implicações em Potenciais multas e penalidades</i>	Multas e penalidades por não conformidade.	52 trata das sanções administrativas aplicáveis àqueles que descumprirem as suas disposições. Essas multas podem ser baseadas em percentual da receita da empresa ou em valor fixo. De advertências e multas simples, até a proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados, as sanções previstas objetivam coibir más práticas e ações contrárias à lei tomadas por agentes de tratamento de dados;
<i>Implicações na Vantagem Competitiva</i>	Vantagem competitiva para empresas em conformidade com a LGPD.	clientes estão cada vez mais preocupados com a privacidade de seus dados e tendem a escolher empresas que demonstram um compromisso sólido com a proteção de dados. Conforme enfatiza Teixeira (2021, p.95) que será preciso “implementar ferramentas que gerem segurança jurídica, informática e administrativa, que, uma vez adotadas, poderão resultar no aumento da credibilidade e boa imagem da sua empresa, resultando mais tarde no volume de clientes e negócios”

Fonte: Autoria própria (2024).

Logo, a Lei Geral de Proteção de Dados Pessoais alterou a forma como o mercado e as organizações lidam com dados pessoais, assim, trouxe impactos significativos para usuários, empresas e instituições, que vivenciam um aumento da exposição tecnológica e da fragilidade do tratamento de dados pessoais em plataformas digitais.

De acordo com Almeida e Soares (2022) O legítimo interesse do controlador, nesse caso identificado aqui como a empresa, deve se apresentar revestida pela adoção de medidas, cuja finalidade se resume na transparência quando da utilização de dados específicos, úteis

necessários, possibilitando a “autoridade nacional solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial” (Art. 5º, § 3º da Lei nº 13.709/18).

Dados pessoais ficam em uma posição vulnerável e exposta por falta de conhecimento sobre direitos e mecanismos de proteção. A população precisa ser educada sobre seus direitos e métodos de proteção de dados para assegurar a privacidade deles. Assim, conforme descrito no Art. 55-J, VI da LGPD, "Compete à ANPD [...] promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança".

Nesse sentido, Nascimento e Silva (2023) afirmam que, dentre alguns fatores, é possível destacar a praticidade e a ampla oferta de serviços digitais disponíveis atualmente. Esses serviços abrangem desde a solicitação de benefícios governamentais até a realização de transações bancárias, compras on-line e consultas a produtos. No entanto, ao utilizar esses diversos serviços oferecidos pelas empresas, o cidadão se encontra em um cenário de exposição de dados pessoais e informações de sua vida privada. Essa exposição se torna ainda mais intensa à medida que o usuário faz uso frequente desses serviços. Segundo Andrade e Silva (2017) "há ainda grandes desafios a serem superados pelas empresas, as quais precisam realizar os investimentos necessários, pois precisam estar inseridas nesse novo modelo de negócios [...]"

Essas questões enfatizaram a necessidade de medidas de proteção que garantam um equilíbrio entre os interesses individuais e coletivos, bem como, que fortaleçam a confiança da sociedade nas instituições responsáveis pelo tratamento de dados.

5 ENQUADRAMENTOS JURÍDICOS PELO TRATAMENTO INADEQUADO DE DADOS PESSOAIS

Discutir-se-á nesta seção não só casos de e-commerce, mas também, de empresas de pequeno, médio e grande portes e de vários segmentos de atuação, que podem ser investigadas e penalizadas pela ANPD se usarem indevidamente dados pessoais, sejam eles digitais ou não. O objetivo é a aplicabilidade jurídica da LGPD na condição de proteção e garantia dos direitos dos usuários.

A nova era digital traz muitos benefícios, mas também traz riscos. É importante que as pessoas estejam cientes desses riscos e que tomem medidas para se proteger. Assim, por se tratar de uma lei recente, a LGPD assume um papel ainda mais relevante, impactando diretamente a forma como as empresas operam e se relacionam com seus consumidores nesses novos padrões de manuseio e tratamento de dados pessoais em mercados digitais.

O mundo jurídico tem buscado maneiras de proteger e garantir a integridade das informações disponibilizadas na internet. Para isso, a legislação tem se adaptado à nova Lei Geral de Proteção de Dados, que traz regras específicas para o tratamento de dados pessoais no Brasil.

Segundo Fornasier e Knebel (2021), os dados comportamentais são tratados como mercadorias. No entanto, existe uma desigualdade nessa relação: os usuários só podem fornecer seus dados, enquanto aqueles que os gerenciam possuem um aparato técnico (humano e não humano) abrangente para sua gestão. Portanto, esses dados não têm valor significativo quando estão apenas nas mãos de seus proprietários. Sua verdadeira rentabilidade surge após o processamento por sistemas complexos e privados.

Não obstante, Bioni (2021, p. 5) ressalta que, “A ciência jurídica como um fato social deve adequar, ou, pelo menos, repensar as suas categorias para encarar os novos desafios regulatórios emergentes deste novo quadro.” Nessa seara, de acordo com o art. Art. 55-A da LGPD, criou-se a Autoridade Nacional de Proteção de Dados (ANPD), como uma autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. Ou seja, foi o órgão criado para fiscalizar o cumprimento da lei, zelar

pela proteção de dados pessoais, elaborar diretrizes e aplicar as sanções em casos de irregularidades.

Assim, Garcia *et al.* (2020, p. 22) afirmam que, “Caberá à ANPD a responsabilidade de fiscalizar eventuais abusos ou desvios do Poder Público com relação ao uso dos dados, assim como cabe a ela eventuais pareceres técnicos sobre dúvidas não endereçadas pela lei”. Portanto, a ANPD fiscaliza os dados pessoais de pessoas físicas, sejam eles digitais ou não, utilizados e acessados por empresas. Essa fiscalização ocorre independentemente da finalidade do uso dos dados, seja para cadastro, personalização de serviços, propagandas ou qualquer outra.

Em razão das infrações cometidas às normas previstas na LGPD, de acordo com o seu artigo 52, ficam sujeitos a sanções administrativas aplicáveis pela autoridade nacional, que podem variar desde advertências até gerar multas de até 2% do faturamento anual da organização no Brasil, limitado a R\$50 milhões por infração.

A aplicabilidade civil da Lei Geral de Proteção de Dados (LGPD) no Brasil, ditada pelo seu art. 52, diz respeito às ações cíveis que podem ser tomadas em decorrência do tratamento inadequado de dados pessoais por parte de empresas e órgãos públicos. A LGPD prevê a possibilidade de ações judiciais movidas por titulares de dados pessoais que se sentirem prejudicados pelo não cumprimento da lei ou pelo tratamento indevido de suas informações.

Contudo, Teixeira (2021) afirma que o Decreto n. 7.962, de 15 de março de 2013, que dispõe sobre contratação no comércio eletrônico no Brasil, citado anteriormente na seção 2 desta pesquisa, não cuida com precisão da extensão da responsabilidade civil nas compras pela internet, cujo tema está pautado fundamentalmente pelo Código Civil, arts. 927 e 931, e pelo Código de Defesa do Consumidor (CDC), especialmente os arts. 12 e 13. No entanto, a doutrina não apresenta divergências quanto à aplicação do ordenamento jurídico brasileiro às relações estabelecidas no comércio eletrônico.

Para os agentes de tratamento de dados que não se adequarem a normativa da lei 13.709/18, indo contra a regulação prevista, a LGPD estabelece em seu artigo 52 uma série de sanções administrativas para quem descumprir suas regras, são elas:

- I - advertência, com indicação de prazo para adoção de medidas corretivas;
- II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- III - multa diária, observado o limite total a que se refere o inciso II;
- IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- VI - eliminação dos dados pessoais a que se refere a infração;
- [...]
- X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
- XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
- XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019) [...]

Importante destacar que as sanções previstas na LGPD têm caráter preventivo e repressivo, ou seja, elas visam a garantir o cumprimento da lei e a proteção dos dados pessoais dos titulares. Além das sanções administrativas previstas na mencionada LGPD, o responsável

pelo tratamento de dados pessoais também pode ser responsabilizado civilmente por danos causados aos titulares dos dados. Esses danos podem ser patrimoniais, morais ou individuais ou coletivos.

Destarte, Mattos (2023) ressalta que, com o aumento do conhecimento dos cidadãos a respeito da lei, estima-se que as ações envolvendo a LGPD se tornem cada vez mais comuns e expressivas nos tribunais brasileiros, o que demanda a necessidade dos agentes de tratamento atuarem em consonância com a lei, sob pena de também serem acionados judicialmente.

Entretanto, é importante mencionar a primeira decisão que tratou a respeito da responsabilização civil em razão de tratamento indevido de dados pessoais através de plataformas digitais. Foi a primeira decisão judicial noticiada no Brasil, tornando-se pioneira na aplicação da Lei Geral de Proteção de Dados em caso concreto. Essa decisão foi expressa pelo Tribunal de Justiça do Estado de São Paulo, publicada em 29 de setembro do ano de 2020, proferida pela Juíza Tonia Yuka Koroku da 13ª Vara Cível, no processo nº 1080233-94.2019.8.26.0100. A decisão, em síntese, destaca:

[...] Isto posto, a responsabilidade da ré é objetiva (arts. 14, caput, CDC e 45, LGPD). Inexiste suporte para a exclusão de responsabilidade (art. 14, § 3º, I a III, CDC), de sorte que caracterizado o ato ilícito relativo a violação a direitos de personalidade do autor, especialmente por permitir e tolerar (conduta omissiva) ou mesmo promover (conduta comissiva) o acesso indevido a dados pessoais do requerente por terceiros. Irrelevante se a ré possui mecanismos eficazes para a proteção de dados, seja porque se sujeita às normas consumeristas em relação à sua responsabilidade, bem como pelo fato de que houve utilização indevida dos dados do requerente em decorrência do contrato firmado entre as partes. Sendo a responsabilidade objetiva, não há suporte para se inquirir a existência de culpa ou a presença de suas modalidades (imperícia, negligência ou imprudência). Tampouco desnecessário aferir se outras pessoas físicas ou jurídicas participaram da ilicitude (como no caso de corretores de imóveis), porquanto todos que participam da cadeia produtiva respondem de forma solidária pelos danos causados (arts. 7º, parágrafo único, e 25, I, CDC). [...]. (São Paulo, 2020).

A discussão da demanda refere-se a uma ação judicial de natureza consumerista em que, um cidadão foi indenizado por danos extrapatrimoniais após uma empresa de imóveis compartilhar seus dados cadastrais com terceiros sem seu consentimento através de plataformas digitais. O autor da ação contratou a empresa para a compra de um imóvel. No contrato, foram informados seus dados pessoais, como nome, endereço, e-mail e telefone. A empresa, no entanto, utilizou essas informações para enviar ofertas de outros imóveis e serviços a terceiros, sem a autorização do autor. O autor da ação alegou que, em decorrência do vazamento de seus dados, foi assediado por instituições financeiras, consórcios, empresas de arquitetura e de construção e fornecimento de mobiliário planejado pelo fato de ter adquirido imóvel junto a empresa ré.

A Justiça aplicou conjuntamente ao caso a LGPD e o CDC, constatou-se que a empresa de imóveis violou a Lei Geral de Proteção de Dados Pessoais ao compartilhar os dados do autor sem seu consentimento. A empresa foi condenada a pagar indenização de R\$ 10 mil ao autor, a título de danos morais.

Desse modo, em face de todo o conjunto probatório a Magistrada entendeu que independentemente de os dados serem sensíveis ou pessoais (art. 5º, inciso I e II, da LGPD), foram tratados em violação aos fundamentos de sua proteção, previstas no art. 2º, da LGPD, bem como desvirtuada a finalidade específica, explícita e informada ao seu titular (art. 6º, inciso I, da LGPD). Dessa forma, a juíza entendeu que a responsabilidade da ré é objetiva, com base nos artigos 14, caput do CDC e art. 45 da LGPD, e que é irrelevante se a construtora possui mecanismos eficazes para a proteção de dados, “seja porque se sujeita às normas consumeristas em relação à sua responsabilidade, bem como pelo fato de que houve utilização indevida dos dados do requerente em decorrência do contrato firmado entre as partes”.

Em sua decisão, a juíza do caso destacou que a informação adequada e clara dos conteúdos do serviço e a proteção à saúde e segurança do consumidor são direitos previstos em lei, mesmo antes da LGPD.

Porém, três anos após esta primeira decisão judicial noticiada no Brasil, houve um novo entendimento jurisprudencial sobre indenização a título de danos morais pelo vazamento de dados pessoais. De acordo com o Agravo em Recurso Especial Nº 2130619 - SP (2022/0152262-2), do então Relator Ministro Francisco Falcão, julgado na data 07 de março de 2023, decide a Segunda Turma do Superior Tribunal de Justiça do estado de São Paulo que, o dano moral pelo vazamento de dados não é presumido, pois o vazamento de dados não tem a capacidade, por si só, de gerar dano moral indenizável, sendo necessário que o titular dos dados demonstre ter havido efetivo dano com o vazamento e o acesso de terceiros. Ou seja, o titular de dados vazados deve comprovar dano efetivo ao buscar indenização gerado pela exposição dessas informações.

Assim, os dados vazados são de natureza comum, e não classificados como sensíveis. Assim ementado:

EMENTA: PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO.

I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais.

II - A sentença julgou os pedidos improcedentes, tendo a Corte Estadual reformulada para condenar a concessionária ao pagamento da indenização, ao fundamento de que se trata de dados pessoais de pessoa idosa.

III - A tese de culpa exclusiva de terceiro não foi, em nenhum momento, abordada pelo Tribunal Estadual, mesmo após a oposição de embargos de declaração apontando a suposta omissão. Nesse contexto, incide, na hipótese, a Súmula n. 211/STJ. In casu, não há falar em prequestionamento ficto, previsão do art. 1.025 do CPC/2015, isso porque, em conformidade com a jurisprudência do STJ, para sua incidência deve a parte ter alegado devidamente em suas razões recursais ofensa ao art. 1022 do CPC/2015, de modo a permitir sanar eventual omissão através de novo julgamento dos embargos de declaração, ou a análise da matéria tida por omissa diretamente por esta Corte. Tal não se verificou no presente feito. Precedente: AgInt no REsp 1737467/SC, Rel. Ministro Napoleão Nunes Maia Filho, Primeira Turma, julgado em 8/6/2020, DJe 17/6/2020.

IV - O art. 5º, II, da LGPD, dispõe de forma expressa quais dados podem ser considerados sensíveis e, devido a essa condição, exigir tratamento diferenciado, previsto em artigos específicos. Os dados de natureza comum, pessoais mas não íntimos, passíveis apenas de identificação da pessoa natural não podem ser classificados como sensíveis.

V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.

VI - Agravo conhecido e recurso especial parcialmente conhecido e, nessa parte, provido. (São Paulo, 2023)

Sendo assim, o entendimento foi estabelecido pela Segunda Turma, ao dar provimento ao recurso especial da Eletropaulo e, por unanimidade, reformar acórdão do Tribunal de Justiça de São Paulo (TJSP) que havia condenado a concessionária a pagar indenização por danos morais de R\$ 5 mil, em virtude do vazamento dos dados de uma cliente. De acordo com o ministro, o TJSP entendeu que os dados vazados da cliente deveriam ser classificados como sensíveis, porém foram indicados apenas dados de natureza comum, não de índole íntima.

Podemos, também, verificar mais um julgado bastante interessante. Recentemente, a empresa de comércio eletrônico, Serasa Experian, enfrentou um processo judicial por uso indevido de dados pessoais através de suas plataformas digitais. O caso se refere a uma Apelação civil pública de Processo nº 0736634-81.2020.8.07.0001, Acórdão Nº 1397176 pelo Órgão Julgador pela 2ª Turma Cível de Brasília, em 09 de Fevereiro de 2022. Assim ementado:

EMENTA: APELAÇÃO. AÇÃO CIVIL PÚBLICA. PRELIMINAR DE NEGATIVA DE PRESTAÇÃO JURISDICIONAL. REJEITADA. COMERCIALIZAÇÃO DE PRODUTOS E FERRAMENTAS DE TRATAMENTO DE DADOS PESSOAIS. PROTEÇÃO DOS DIREITOS DO CONSUMIDOR. INOBSERVÂNCIA DA LEGISLAÇÃO DE REGÊNCIA.

1. Apelação interposta contra sentença que, em sede de ação civil pública, julgou procedente a pretensão formulada pelo Ministério Público para condenar a requerida a se abster de comercializar dados pessoais de consumidores, por meio de duas específicas ferramentas de tratamento de dados, sob pena de imposição das medidas indutivas, coercitivas, mandamentais ou sub-rogatórias necessárias para assegurar o cumprimento de ordem judicial, conforme legislação processual civil.

2. A eventual discrepância entre as teses defendidas pelos litigantes e a interpretação conferida pelo julgador às disposições normativas que disciplinam determinada matéria posta em debate não se confunde com a negativa de prestação jurisdicional.

3. Se o que está em pauta é a comercialização de dados tratados, resta evidente que as condições do tratamento – em todas as dimensões do conceito legal – devem ser examinadas, respeitadas a legítima expectativa do titular das informações tratadas e os direitos e liberdades fundamentais. E somente em uma relação de efetiva transparência é possível conceber a existência de legítima expectativa.

5. Mesmo que o produto final dos serviços impugnados garanta ao contratante um apanhado de informações de natureza meramente cadastral, é inafastável a conclusão de que a segmentação e o direcionamento de mercado – prometidos pela requerida – depende de tratamento de informações outras, de natureza socioeconômica e comportamental, elementos intrinsecamente vinculados à esfera da privacidade. Assim, não havendo transparência sobre os trâmites de coleta e tratamento, é impositivo o acolhimento da pretensão autoral.

6. Recurso conhecido e desprovido. (Brasília, 2022)

O processo foi movido pelo Instituto Brasileiro de Defesa da Proteção de Dados Pessoais, Compliance e Segurança da Informação (Instituto Sigilo), em conjunto com o Ministério Público Federal (MPF). A acusação é de que a Serasa Experian teria comercializado os dados de mais de 150 milhões de cidadãos, incluindo brasileiros vivos e falecidos, junto a terceiros. As partes acusatórias alegam que a empresa contrariou regras e princípios da Lei Geral de Proteção de Dados, da Lei do Marco Civil da Internet e do Código de Defesa do Consumidor. As investigações apontaram para a possível divulgação de informações pessoais dos consumidores na internet, incluindo históricos de compras, endereços de e-mail, dados da Previdência Social, renda, Receita Federal e até acesso a dados de cartões de crédito e débito. Segundo o MPF, esse tipo de vazamento expõe os cidadãos de forma pública e ilegal, atraindo graves riscos de possíveis fraudes envolvendo suas identidades e vida privada.

Dessa forma, o magistrado baseou sua decisão em princípios caros à LGPD, como o da privacidade, consentimento e a inviolabilidade do sigilo de dados, uma vez que as pessoas naturais eram identificáveis e o uso compartilhado de dados foi feito irregularmente. O juiz substituto da 5ª Vara Cível de Brasília confirmou decisão liminar da 2ª Turma Cível do TJDF que determinou que a Serasa Experian pare de comercializar dados pessoais dos titulares por meio dos produtos “Lista Online e Prospecção de Clientes”, oferecidos pelo site da ré, sob pena de imposição das medidas para assegurar o cumprimento da ordem judicial, conforme legislação vigente. Logo, apesar deste processo não ter tido sentença de mérito, ainda assim a liminar já demonstra, na prática, uma das diversas aplicações da Lei Geral de Proteção de Dados. Em 17 de março de 2022, a ação civil pública nº 0736634-81.2020.8.07.0001 transitou

em julgado e a decisão desfavorável à Serasa S.A. se tornou final. O caso ainda está em tramitação na 2ª Turma Cível do TJDF, e até o momento, não há decisão judicial determinando o pagamento de indenizações.

Podemos, também, verificar mais um outro julgado nos autos do Agravo de Instrumento nº 0702702-37.2022.8.07.0000 - Res. 65 CNJ. Relator: Diaulas Costa Ribeiro. Data de Julgamento: 07/04/2022, do TJDF - Poder Judiciário da União, assim ementado:

EMENTA: AGRAVO DE INSTRUMENTO. AÇÃO DE OBRIGAÇÃO DE FAZER. CONTRATO DE PRESTAÇÃO DE SERVIÇOS. EMPRESAS. HOSPITAL E PLANO DE SAÚDE. AUDITORIA. CONTAS. PROVAS. JUNTADA DE DOCUMENTOS MÉDICO-HOSPITALARES. PACIENTES. SIGILO. LEI GERAL DE PROTEÇÃO DE DADOS. INFORMAÇÕES PESSOAIS. INTIMIDADE. PRIVACIDADE. DADOS SENSÍVEIS. PROTEÇÃO. NECESSIDADE. 1. O relator poderá deferir, em antecipação de tutela, total ou parcialmente, a pretensão recursal quando estiverem presentes os requisitos relativos ao perigo de dano grave, de difícil ou de impossível reparação, bem como a demonstração da probabilidade do provimento do recurso (art. 995, parágrafo único, do CPC). Não sendo o caso, indefere-se o pedido de antecipação de tutela. 2. A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, tanto de direito público quanto privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade. 3. A lei exige o consentimento expresso do titular para o tratamento dos dados ou, sendo crianças e adolescentes, o consentimento específico realizado por um dos pais ou representante legal (LGPD, art. 7º, I e art. 14, §1º). 4. A documentação anexada aos autos originários, assinalada com sigilo, refere-se aos beneficiários do plano de saúde agravado, na qual constam nomes, idades e os procedimentos médico-hospitalares resumidos e simplificados realizados. É obrigatório preservar o sigilo anotado nos documentos médicos dos pacientes que, inclusive, não integram a demanda, como mecanismo de proteção dos direitos à privacidade e à intimidade, assim como do sigilo profissional correspondente. 5. Recurso conhecido e provido. (Brasília, 2022)

No caso em destaque, refere-se a decisão antecipatória de tutela que determinou a inclusão de sigilo em documentos e prontuários médicos que contenham dados pessoais sensíveis de pacientes referentes à saúde e protegidos pela Lei Geral de Proteção de Dados – LGPD, Constituição Federal e legislação esparsa. *In casu*, a empresa agravante requer a inclusão de sigilo na documentação anexada aos autos originários, na qual consta o nome completo, a idade e o procedimento médico-hospitalar resumido realizado nos beneficiários do plano de saúde agravado. O agravante argumenta que a manutenção do sigilo é necessária, pois os documentos anexados ao processo incluem prontuários e fichas médicas com dados sensíveis pessoais de pacientes, inclusive menores. Esses dados são protegidos pela Lei Geral de Proteção de Dados (LGPD), pela Constituição Federal e por outras leis. O agravante defende que o processo inteiro deve ser mantido em segredo de justiça, e não apenas os documentos. Deu provimento ao recurso para manter o sigilo dos documentos médico-hospitalares que contenham o nome dos pacientes, idade e procedimentos realizados. Essa decisão foi tomada com base no art. 7º, I e art. 14, §1º, da LGPD, que exigem o consentimento específico dos pais ou representantes legais para o tratamento de dados pessoais de menores. O objetivo da decisão é proteger os direitos fundamentais à liberdade e à privacidade.

Isto posto, sendo a proteção de dados pessoais um desafio a ser enfrentado pelo Poder Judiciário, foi através da fiscalização do cumprimento da lei 13.709/18, que já temos a primeira sanção aplicada pela ANPD na data de 6 de julho de 2023, contra uma microempresa de telemarketing pelo motivo de irregularidades e não adequação da Lei Geral de Proteção de Dados (LGPD). A Telekall Infoservice SA, é a microempresa que atua no setor privado como provedora de serviços de telefonia como telemarketing e autoatendimento via serviço de

mensagens pela plataforma digital WhatsApp. O despacho vinculado ao Processo Administrativo Sancionador nº 00261.000489/2022-62, que autua a empresa Telekall InforService SA, do Espírito Santo, está disponível no site da ANPD² e a Multa foi publicado no D.O.U³ na data 06/07/2023.

Nesse ínterim, pode-se afirmar que, com essa aplicação da primeira sanção pela ANPD, tornou-se um marco importante para a proteção de dados pessoais no Brasil. Ela mostra que a ANPD está comprometida em fazer cumprir a LGPD e que as empresas que não se adequarem à lei poderão sofrer sanções.

Conforme afirma Blum (2023), de acordo com o relatório que fundamentou a decisão, a microempresa oferecia uma lista de contatos de WhatsApp de eleitores de Ubatuba/SP para candidatos às eleições municipais de 2020. A ANPD foi notificada pelo Ministério Público de São Paulo, que recebeu denúncia de que a empresa estaria comercializando a lista para fins de disparo de material eleitoral. Assim, foi instaurado um processo administrativo para apurar o caso. A ANPD intimou a empresa autuada para que fornecesse informações sobre o encarregado de dados, a origem dos dados de contatos comercializados, como a base de dados foi criada, a categoria dos dados pessoais disponibilizados aos clientes e o volume de registros existentes. A empresa não respondeu à intimação, mesmo após ela ser renovada. Por isso, a ANPD instaurou o Processo Administrativo Sancionador e lavrou o auto de infração.

Neste contexto, notou-se que a empresa autuada teria tratado dados pessoais sem fundamento em uma das hipóteses legais previstas na LGPD (art. 7º da referida lei) e sem nomear um encarregado (art. 41 da LGPD), bem como não teria atendido a uma requisição de envio de documentos para a ANPD no curso do processo administrativo que incorreu na decisão sancionatória (art. 5º do Regulamento de Fiscalização). Teve como consequência, as sanções de uma advertência, sem imposição de medidas corretivas, por infração ao art. 41 da LGPD; e uma multa simples, nos valores de R\$ 7.200,00 (sete mil e duzentos reais) por infração ao art. 7º da LGPD e de R\$ 7.200,00 (sete mil e duzentos reais) por infração ao art. 5º do Regulamento de Fiscalização, totalizando R\$ 14.400,00 (catorze mil e quatrocentos reais).

A recente decisão da ANPD, além de manifestar que as violações à LGPD serão combatidas com rigor, demonstra que as empresas devem ficar atentas aos seus processos comerciais, principalmente no que diz respeito ao tratamento de dados pessoais relacionados ao marketing nas plataformas digitais. Além disso, transmite uma mensagem crucial para todas as organizações de que, independentemente do seu tamanho, estão sujeitas à supervisão e à aplicação de sanções em caso de violação da lei.

Podemos citar, também, um outro julgado importante do Processo nº: 0812915-60.2021.8.10.0001 do Tribunal de Justiça do Estado do Maranhão - 1º Grau, que se trata de uma Ação Civil Coletiva com pedido de obrigação de fazer proposta pelo Instituto Brasileiro de Defesa das Relações de Consumo – IBEDEC/MA em face de Facebook Serviços Online do Brasil Ltda, assim ementado:

EMENTA: AÇÃO CIVIL COLETIVA (63). INSTITUTO BRASILEIRO DE ESTUDO E DEFESA DAS RELAÇÕES DE CONSUMO - IBEDEC - FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA. – VAZAMENTO DE DADOS – FALHA DE SEGURANÇA – FALHA NA PRESTAÇÃO DE SERVIÇOS, COM FULCRO NA LEI GERAL DE PROTEÇÃO DE DADOS – RESPONSABILIDADE DE REPARAR - DANO MORAL IN RE IPSA - DANO MORAL COLETIVO. (Maranhão, 2023)

² Disponível em: <<https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao>> Acesso em: 07 de Setembro de 2023

³ Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/2022-62-dou-imprensa-nacional.pdf>> Acesso em: 03 de Setembro de 2023

O caso se refere ao uso de dados pessoais de clientes pelo Facebook sem o seu consentimento. Em 2021, o Facebook sofreu um vazamento de dados pessoais de 533 milhões de usuários de 106 países, incluindo 8,06 milhões de brasileiros. O vazamento incluiu dados como nome, e-mail, número de telefone, data de nascimento, local de trabalho, como gênero, localidade, idioma, status de relacionamento, religião, cidade natal, dispositivos usados para acessar o Facebook, educação, trabalho e os últimos dez locais onde estiveram ou nos quais foram marcados.

Assim, em 2023, o Instituto Brasileiro de Defesa das Relações de Consumo (Ibedec) entrou com uma ação civil coletiva contra o Facebook, pedindo indenização por danos morais coletivos. Foi proferida sentença, pela 29ª Vara Cível de Belo Horizonte/MG, condenando notória Rede Social ao pagamento de R\$ 20 milhões ao Fundo Estadual de Proteção e Defesa do Consumidor ("FEPDC/MG"), a título de indenização por dano moral coletivo, em razão do vazamento de dados dos usuários da plataforma.

O juiz levantou a proteção especial à intimidade, à vida privada, à honra e à imagem conferida pela Constituição Federal, configurando como invioláveis os direitos fundamentais da personalidade e assegurando o direito à indenização pelo dano moral ou material decorrente de sua violação. De acordo com Mendes (2023) os dados pessoais ganharam maior proteção após a promulgação da Emenda Constitucional nº 115/2022, que alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais do cidadão, assegurando o direito à proteção nos meios digitais.

A sentença destacou ainda as normas da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), que enuncia como fundamentos o respeito à privacidade e a autodeterminação informativa, estipulando que o tratamento de dados pessoais somente pode se dar mediante consentimento do titular. Citou, também, o Marco Civil da Internet (Lei Nº 12.695/2014), que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e a defesa do consumidor, entre os quais a proteção da privacidade e dos dados pessoais, assegurada a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; além de informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.

O juiz entendeu que o Facebook agiu de forma ilegal ao permitir que os dados pessoais de seus usuários fossem vazados. Ele também considerou que o vazamento atingiu uma gama relevante de usuários, o que aumenta a gravidade do caso. Nessa seara, a condenação do Facebook é um importante precedente na jurisprudência brasileira sobre a proteção de dados pessoais. Ela demonstra que as empresas que tratam dados pessoais de consumidores brasileiros devem adotar medidas de segurança adequadas para proteger esses dados.

A evolução das decisões judiciais em casos de violação à LGPD é um passo importante para a proteção dos dados pessoais no Brasil. Essa progressão demonstra o compromisso dos tribunais em garantir os direitos dos consumidores e promover a segurança da informação, com condenações a título de danos coletivos e individuais.

6 CONSIDERAÇÕES FINAIS

Como verificado, diante do cenário de lacunas legislativas acerca da proteção de dados pessoais, houve a necessidade de estipular limites para o exercício dessa atividade, e assim, tornou-se evidente a garantia de direitos fundamentais ao titular dos dados.

Nesse sentido, ao refletir sobre as implicações da Lei de Proteção de Dados Pessoais

nos cenários brasileiro e mundial, foi possível identificar o seu papel de importância na proteção de dados pessoais, justamente pelo motivo de estabelecer princípios, conceitos, procedimentos, normas e sanções pelo descumprimento da lei.

Assim, este artigo buscou fomentar o debate sobre a LGPD, com o claro objetivo de garantir ao cidadão o exercício efetivo de seus direitos e liberdades fundamentais, analisando a relevância da proteção de dados pessoais oriundos da implementação da lei geral de proteção de dados, LGPD, e da sua aplicabilidade jurídica frente aos deveres das plataformas eletrônicas no tratamento de dados pessoais, trazendo uma possível interpretação que visa garantir o exercício efetivo dos direitos e liberdades fundamentais do cidadão.

Com o intuito de entender e interpretar o novo fenômeno de proteção de dados pessoais, como uma prioridade e necessidade de limitar o uso e tratamento de dados pessoais por parte das empresas e usuários que manuseiam esses dados nas plataformas de ofertas dos mais diversos serviços e produtos operando no Brasil, constatou-se que o surgimento da LGPD foi uma resposta às novas necessidades oriundas de novos modelos de mercados no cenário digital, justamente por exigir mais transparência nas relações comerciais de produtos ou serviços, e que não se limitavam somente em *e-commerce*, mas também por meio de quaisquer canais de forma virtual ou não, e assim, a proteção de dados pessoais conquistou um papel de destaque como um bem valioso para o aspecto econômico do país nas tomadas de decisões.

Entretanto, através deste estudo, confirmou-se várias implicações significativas oriundas da LGPD para as empresas e os usuários que lidam com tratamento de dados pessoais, tais como: implicações no marketing, nos custos operacionais, nas restrições comerciais, implicações no gerenciamento de consentimento, nos direitos do usuário e transparência, implicações nas transferências de dados internacionais, implicações de manuseio e armazenamento de dados, em litígios e processos judiciais, em potenciais multas e penalidades e na Vantagem competitiva.

Nessa perspectiva, é crucial que todas as empresas e entidades que lidam com dados pessoais se adaptem à LGPD. A conformidade com suas obrigações e regras não só evitam multas e outras sanções, mas também aumenta a confiança de clientes, parceiros de negócios e do público em geral.

Constatou-se, também, que além da implementação de medidas de segurança padronizadas para proteção dos dados pessoais, a LGPD também exige que as empresas nomeiem um responsável de proteção de dados para assegurar a conformidade com as normas protegidas pela LGPD.

Portanto, com base nas informações fornecidas nas primeiras decisões, trazidas neste estudo, no contexto do processo de fiscalização e sanção pela ANPD, ocorre independentemente da finalidade do uso dos dados, seja para cadastro, personalização de serviços, propagandas ou qualquer outra,

Nesse ínterim, podemos concluir que, independentemente do tamanho da empresa ou do seu segmento comercial, ela está sujeita a investigação e penalidades pela Autoridade Nacional de Proteção de Dados, com relação ao mau uso dos dados pessoais, sejam eles digitais ou não, utilizados e acessados por empresas. E a tendência é que as jurisprudências sejam cada vez mais favoráveis à proteção dos dados pessoais, garantindo os direitos dos titulares e responsabilizando os agentes de tratamento por eventuais danos causados.

Assim, é essencial que as empresas se adequem à LGPD, não apenas para proteger os direitos dos usuários, mas também porque isso impacta diretamente a maneira como operam e se relacionam com seus consumidores, uma vez que a coleta e o armazenamento de dados são práticas comuns não apenas no contexto do *e-commerce*, que se caracteriza pela constante interação com dados de clientes, mas também para todos os usuários que manipulam dados pessoais em diferentes cenários de comercialização de produtos ou serviços no território brasileiro.

REFERÊNCIAS

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. (2022). **Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital**. Periódico Perspectivas Em Ciência Da Informação, 27 (3), 26–45. Centro Universitário Internacional Uninter, PR, Brasil. São Paulo, Jul-Sep 2022. Disponível em: <<https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/?lang=pt#>>. Acesso em: 01 de Mar. de 2024

ANDRADE, Marta Cleia Ferreira de; SILVA, Naiara Taiz Gonçalves da. **O comércio eletrônico (e-commerce): Um estudo com consumidores**. Revista Perspectivas em Gestão & Conhecimento, João Pessoa, v. 7, n. 1, p. 98-111, jan./jun. João Pessoa, 2017. Disponível em: <<https://dialnet.unirioja.es/servlet/articulo?codigo=6049990>> ou <<https://periodicos.ufpb.br/index.php/pgc/article/view/26895/17910>> Acesso em: 03 de mar. de 2024.

BATISTA, Peterson. **A Vantagem Competitiva em estar adequado à LGPD**. LINKEDIN. Publicado em 23 de mar. de 2023. Disponível em: <<https://pt.linkedin.com/pulse/vantagem-competitiva-em-estar-adequado-%C3%A0-lgpd-peterson-batista>> Acesso em: 04 de ago. de 2023

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021.

BLUM, Renato Opice. ANPD aplica 1ª sanção administrativa e confirma que adequação à LGPD também deve ser prioridade dos pequenos negócios. **FEBRABANTECH**. Publicado em: 03/08/2023. Disponível em: <<https://febrabantech.febraban.org.br/especialista/renato-opice-blum/anpd-aplica-1-sancao-administrativa-e-confirma-que-adequacao-a-lgpd-tambem-deve-ser-prioridade-dos-pequenos-negocios>> Acesso em: 03 de Set. de 2023

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ Acesso em: 24 de jan. 2024.

BRASIL, **Medida Provisória Nº 2.200-1, de 27 de Julho de 2001**. Disponível em: <https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-1.htm#:~:text=MEDIDA%20PROVIS%C3%A9RIA%20N%C2%BA%202.200%2D1,Brasil%2C%20e%20d%C3%A1%20outras%20provid%C3%AAs.&text=O%20PRESIDENTE%20DA%20REP%C3%A9BLICA%20no,que%20lhe%20confere%20o%20art.> Acesso em: 12 de Jul. de 2023, às 12h21.

BRASIL, **Lei Nº 11.419, de 19 de dezembro de 2006**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/11419.htm> Acesso em: 13 de Jul. de 2023, às 10h49.

BRASIL, **Decreto Nº 7.962, de 15 de Março de 2013**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm> Acesso em: 27 de jul. de 2023.

BRASIL, **Lei Nº 12.965, de 23 de Abril de 2014**. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm> Acesso em: 13 de Jul. de 2023, às 10h49.

BRASIL, **Código de Processo Civil, 16 de março de 2015**. Código de Processo Civil

Brasileiro. Brasília, DF: Senado, 2015. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113105.htm>. Acesso em: 13 de Jul. de 2023, às 12h19.

BRASIL, **Lei Nº 13.185, de 6 de Novembro de 2015**. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113185.htm> Acesso em: 13 de Jul. de 2023, às 12h19.

BRASIL, **Lei Nº 13.476, de 28 de Agosto de 2017**. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/113467.htm> Acesso em: 13 de Jul. de 2023, às 12h19.

BRASIL, **Lei Nº 13.709, de 14 de Agosto de 2018**. Dispõe sobre a lei geral de proteção de dados pessoais. Brasília, DF: Presidência da República, 2018.. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm> Acesso em: 13 de Jul. de 2023, às 12h19.

BRASÍLIA, Tribunal de Justiça do Distrito Federal e dos Territórios. (2ª turma cível) Classe judicial: Apelação Cível. **Processo Número 0736634-81.2020.8.07.0001 / Acórdão Nº 1397176**. Ementa: Apelação. Ação Civil Pública. Preliminar de Negativa de Prestação Jurisdicional. Rejeitada. Comercialização de produtos e ferramentas de Tratamento de dados pessoais. Proteção dos direitos do consumidor. Inobservância da Legislação De Regência. Apelante: Serasa S.A. Apelado: Ministerio Publico Do Distrito Federal E Dos Territórios. Relator: Desembargador Sandoval Oliveira, Brasília, 09 de Fevereiro de 2022. Disponível em: <<https://pje2i-consultapublica.tjdft.jus.br/consultapublica/ConsultaPublica/listView.seam>> Acesso em: 01 de Mar. de 2024, às 19h10.

BRASÍLIA, Tribunal de Justiça do Distrito Federal e dos Territórios (8ª Turma Cível).

Agravo de Instrumento n. 0702702-37.2022.8.07.0000 - Res. 65 CNJ. Acórdão 1414740.

Agravo De Instrumento. Ação De Obrigação De Fazer. Contrato De Prestação De Serviços. Empresas. Hospital E Plano De Saúde. Auditoria. Contas. Provas. Juntada De Documentos Médico-Hospitalares. Pacientes. Sigilo. Lei Geral De Proteção De Dados. Informações Pessoais. Intimidade. Privacidade. Dados Sensíveis. Proteção. Necessidade. Agravante(S) Servicos Hospitalares Yuge S.A. Agravado(S) Santa Luzia Assistência Medica S/A. Relator Desembargador Diaulas Costa Ribeiro, Brasília, 07 de abril de 2022. Disponível em:

<https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&controladorId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.ControladorBuscaAcordao&visaoAnterior=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&nomeDaPagina=resultado&comando=abrirDadosDoAcordao&enderecoDoServlet=sistj&historicoDePaginas=buscaLivre&quantidadeDeRegistros=20&baseSelecionada=BASE_ACORDAOS&numeroDaUltimaPagina=1&buscaIndexada=1&mostrarPaginaSelecaoTipoResultado=false&totalHits=1&internet=1&numeroDoDocumento=1414740> Acesso em: 04 de dez de 2023

CAMPOS, Alexandre de; GOULART, Douglas Garcia. **Técnicas de vendas e e-commerce**. São Paulo: Érica, 2021.

CASTELLS, Manuel. **A sociedade em rede**. tradução: Roneide Venâncio Majer. Atualização para 6ª ed.: Jussara Simões. São Paulo: Paz e Terra, 2002. (A era da informação: economia, sociedade e cultura; v.1. São Paulo: Paz e Terra, 1999) Disponível em: <<https://globalizacaointegracaoregionalufabc.files.wordpress.com/2014/10/castells-m-a-sociedade-em-rede.pdf>> Acesso em: 15 de Nov. de 2023, às 16h09

CONSTRUTORA É CONDENADA COM BASE NA LGPD. **AGF Advice Consultoria Legislativa, Tributária e Empresarial**. Atualizado em 06 de outubro de 2020 às 11:11 pm. Disponível em: <<https://www.agfadvice.com.br/construtora-e-condenada-com-base-na-lgpd/>> Acesso em: 03 de Ago. de 2023.

FORNASIER, Mateus de Oliveira e KNEBEL, Norberto Milton Paiva. **O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados**. Revista Direito e Práxis [online]. 2021, v. 12, n.2. Universidade do Estado do Rio de Janeiro. Rio de Janeiro, 2021. Disponível em: <<https://www.scielo.br/j/rdp/a/hTqmGJVy7FP5PWq4Z7RsbCG/?lang=pt#>>. Acesso em: 02 de Mar de 2024.

GARCIA, Lara Rocha; AGUILERA-FERNANDES, Edson; GONÇALVES, Rafael Augusto Moreno; PEREIRA-BARRETO, Marcos Ribeiro. **Lei Geral de Proteção de Dados Pessoais (LGPD): guia de implantação**. São Paulo : Blucher, 2020. 128 p.

GIMENEZ, Carina Alves; MONTANHAS, Leticia Santos das; SILVA, Micheli da. **Aumento do Comércio Eletrônico no Brasil durante e Pós Período Pandêmico**. 2023. fol. 17. Administração - Bacharelado (CPNA). Fundação Universidade Federal de Mato Grosso do Sul - UFMS. Mato Grosso do Sul, 2023. Disponível em: <<https://repositorio.ufms.br/handle/123456789/6743>> Acesso em: 03 de Mar. de 2024.

GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado**. 1. ed. – São Paulo: Atlas, 2017.

HENRIQUES, Antonio; MEDEIROS, João Bosco. **Metodologia científica na pesquisa jurídica**. 9. ed., rev. e reform. São Paulo: Atlas, 2017.

LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados: Lei nº 13.709/18, com alteração da Lei n. 13.853/2019**. Coordenadora Cíntia Rosa Pereira de Lima. São Paulo: Almedina, 2020.

LOZADA, Gisele; NUNES, Karina da Silva. **Metodologia científica [recurso eletrônico]**. revisão técnica: Ane Lise Pereira da Costa Dalcul]. – Porto Alegre: SAGAH, 2018.

MARANHÃO. Tribunal de Justiça do Estado do Maranhão (1. grau). **Processo Nº: 0812915-60.2021.8.10.0001 Classe Processual: Ação Civil Coletiva**. Instituto Brasileiro De Estudo E Defesa Das Relações De Consumo - Ibedec - Facebook Serviços Online Do Brasil Ltda. – Vazamento De Dados – Falha De Segurança – Falha Na Prestação De Serviços, Com Fulcro Na Lei Geral De Proteção De Dados – Responsabilidade De Reparar - Dano Moral In Re Ipsa

- Dano Moral Coletivo”. Autor: Instituto Brasileiro De Estudo E Defesa Das Relacoes De Consumo. Reu: Facebook Servicos Online Do Brasil Ltda. Relator: Dr. Douglas De Melo Martins, São Luís, 23 de março de 2023. Disponível em: <<https://www.conjur.com.br/wp-content/uploads/2023/09/facebook-multa-indenizacao-maranhao.pdf>> Acesso em: 04 de dez. de 2023.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia científica. Fundamentos de metodologia científica.** atualização da edição João Bosco Medeiros - 9. ed. – [2. Reimpr.]. São Paulo: Atlas, 2023.

MATTOS, Jenifer. LGPD e Marketing Digital: Qual o impacto da lei?. **Jusbrasil.** Data de publicação: 24/04/2023. Disponível em: <<https://www.jusbrasil.com.br/artigos/lgpd-e-marketing-digital-qual-o-impacto-da-lei/1818923038>> Acesso em: 03 de ago. de 2023.

MENDES, Juliana. Justiça condena Facebook a indenizar oito milhões de brasileiros por vazamento de dados. **Portal do poder Judiciario do Maranhão.** Publicado em: 23/03/2023. Disponível em: <<https://www.tjma.jus.br/midia/cgj/noticia/509573/justica-condena-facebook-a-indenizar-oito-milhoes-de-brasileiros-por-vazamento-de-dados>> Acesso em: 04 de dez. de 2023.

MONTENEGRO FILHO. Misael. **Curso de Direito Processual Civil:** teoria geral do processo e processo de conhecimento. 4. ed. São Paulo: Atlas, 2007. v.l.

MORAES, Helio Ferreira. O que nos diz a 1ª multa da ANPD sobre as vendas de base de dados. **CONJUR.COM.BR.** Publicado em: 18 de julho de 2023, 17h22. Disponível em: <<https://www.conjur.com.br/2023-jul-18/helio-moraes-multa-anpd-vendas-base-dados>> Acesso em: 01 de set. de 2023

NASCIMENTO, Bruna Lais Campos do; SILVA, Edilene Maria da. (2023). **Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais: reflexões e adequações. Em Questão**, 29, e–127314. Disponível em: <<https://www.scielo.br/j/emquestao/a/w3xQNY4bnytwK6MxzgyKggy/?lang=pt#>> Acesso em: 01 de Mar. de 2024.

Núcleo de Informação e Coordenação do Ponto BR (NIC.br). (2023). **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: pesquisa TIC Domicílios, ano 2023.** Disponível em: <<https://cetic.br/pt/arquivos/domicilios/2023/individuos/>>. Acesso em: 17 de fev de 2024.

OLIVEIRA, Damião. A primeira empresa a ser multada pela ANPD é uma microempresa. **Techcompliance.** Disponível em: <<https://techcompliance.org/multa-da-lgpd/>> Acesso em: 03 de Setembro de 2023.

PINHEIRO, Patricia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. **Revista dos Tribunais**, v. 1000, p. 309-323, fev. 2019.

SÃO PAULO, Superior Tribunal de Justiça de São Paulo (2. turma). **Agravo em Recurso Especial Nº 2130619 - SP (2022/0152262-2).** Processual Civil e Administrativo. Indenização

por dano moral. Vazamento de dados Pessoais. Dados Comuns E Sensíveis. Dano Moral Presumido. Impossibilidade. Necessidade de comprovação do dano. Agravante: Eletropaulo Metropolitana Eletricidade de Sao Paulo S.A. Agravado: Maria Edite de Souza. Relator Exmo. Sr. Ministro Francisco Falcão. São Paulo, 03 de março de 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023 Acesso em: 01 de mar. de 2024.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (13ª Vara Cível). **Processo n. 1080233-94.2019.8.26.0100**. Sentença. Requerente: Fabricio Vilela Coelho. Requerido: Cyrela Brazil Realty S/A Empreendimentos e Participações. Relatora: Tonia Yuka Koroku. São Paulo, 29 de setembro de 2020. Disponível em: <https://www.conjur.com.br/dl/compartilhar-dados-consumidor-terceiros.pdf> Acesso em: 03 de Setembro de 2023.

STIVAL, Mariane Morato. Relação De Consumo Na Internet: Responsabilidade Civil Dos Fornecedores De Produtos E Serviços No Comércio Eletrônico. **Revista Jurídica**, V. 1, P. 80-101, 2013. Disponível em: <http://revistas.unievangelica.com.br/index.php/revistajuridica/article/view/651> Acesso em: 27 de julho de 2023.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil Conteúdo E Tecnologia Ltda, 2019.

TEIXEIRA, Tarcisio. **Comércio eletrônico: conforme o Marco Civil da Internet e a regulamentação do e-commerce no Brasil**. São Paulo : Saraiva, 2015.

TEIXEIRA, Tarcisio. **LGPD e E-commerce**. - 2. ed. - São Paulo: Saraiva Educação, 2021.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo / 4. ed.** - São Paulo : SaraivaJur, 2022.