UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

VIVIANE LUCENA MOTA

UMA ANÁLISE SOBRE A SEGURANÇA DOS USUÁRIOS NO MEIO DIGITAL APÓS A ENTRADA EM VIGOR DA LEI GERAL DE PROTEÇÃO DE DADOS

JUAZEIRO DO NORTE-CE
2023

VIVIANE LUCENA MOTA

UMA ANÁLISE SOBRE A SEGURANÇA DOS USUÁRIOS NO MEIO DIGITAL APÓS A ENTRADA EM VIGOR DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso – *Artigo Científico*, apresentado à Coordenação do Curso de Graduação em Direito do Centro Universitário Doutor Leão Sampaio, em cumprimento às exigências para a obtenção do grau de Bacharel.

Orientadora: Ma. Tamyris Madeira de Brito

JUAZEIRO DO NORTE-CE
2023

VIVIANE LUCENA MOTA

UMA ANÁLISE SOBRE A SEGURANÇA DOS USUÁRIOS NO MEIO DIGITAL APÓS A ENTRADA EM VIGOR DA LEI GERAL DE PROTEÇÃO DE DADOS

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de VIVIANE LUCENA MOTA.

Data da Apresentação 03/07/2023

BANCA EXAMINADORA

Orientador: Prof. Ma. Tamyris Madeira de Brito

Membro: Prof. Ma. Joseane de Queiroz Vieira

Membro: Prof. Esp. Alyne Leite de Oliveira

JUAZEIRO DO NORTE-CE
2023

UMA ANÁLISE SOBRE A SEGURANÇA DOS USUÁRIOS NO MEIO DIGITAL APÓS A ENTRADA EM VIGOR DA LEI GERAL DE PROTEÇÃO DE DADOS

Viviane Lucena Mota[1]
Tamyris Madeira de Brito[2]

RESUMO

O presente artigo retrata o tema da segurança no meio digital após a entrada em vigor da Lei n° 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados-LGPD, que trouxe relevantes contribuições para cada cidadão em uma sociedade tecnológica, digitalizada, que requer o amparo e proteção legal diante do amplo acesso à internet, seja nas redes sociais, aplicativos, entre outros. Tem como objetivo, analisar a segurança no meio digital após a entrada em vigor da LGPD, compreender sua efetivação legal e sua real finalidade por meio da ação de danos morais, proteção virtual e digital; identificar as formas viáveis e plausíveis da sua aplicação; analisar seus desafios e conquistas nos dias atuais junto à ação jurídica. A pesquisa foi baseada no teor legal e científico da própria LGPD, dos autores que retratam essa temática e do estudo de caso que oferece um novo olhar e agir nesse contexto, fundamentando o estudo e oferecendo credibilidade no decorrer desse trabalho, com abordagem descritiva e qualitativa enriquecendo a temática em estudo. Este artigo científico, torna-se fundamental ao demonstrar quão importante o estudo dos casos aqui mencionados com suas peculiaridades que requer ações jurídicas efetivas para assegurar e proteger cada sujeito que teve sua privacidade e direitos violados, daí a relevância do papel dos profissionais da justiça, para fazer valer a LGPD e através da judicialização de casos concretos que são tutelados por essa lei. Como resultado percebe-se que infringir pode levar a indenização e punição pecuniária em alguns casos onde o dano é demonstrado.

Palavras Chave: LGPD. Meio Digital. Segurança. Ação Jurídica.

ABSTRACT

This article portrays the issue of security in the digital environment after the entry into force of Law No. 13,709, of August 14, 2018, known as the General Data Protection Law-LGPD, which brought relevant contributions to each citizen in a society technological, digitized, which requires support and legal protection in view of the wide access to the internet, whether in social networks, applications, among others. Its objective is to analyze the level of security in the digital environment after the entry into force of the LGPD, to understand its legal effectiveness and its real purpose through the action of moral damages, virtual and digital protection; identify the viable and plausible ways of its application; analyze its challenges and achievements in the present day with the legal action. The research was based on the legal and scientific content of the LGPD itself, the authors who portray this theme and the case study that offers a new look and action in this context, supporting the study and offering credibility throughout this work, with a descriptive, investigative approach. and qualitative, enriching the theme under study. This scientific article (TCC) becomes fundamental in demonstrating how important the study of the cases mentioned here with their peculiarities that requires effective legal actions to ensure

[1] Viviane Lucena Mota, acadêmica, Graduando do Curso de Direito do Centro Universitário Doutor Leão Sampaio/Unileão-vivianemota11@hotmail.com

[2] Tamyris Madeira de Brito. Professora do Centro Universitário Doutor Leão Sampaio/UNILEÃO, Mestre em Desenvolvimento Regional Sustentável pela UFCA.

and protect each subject who had his privacy and rights violated, hence the relevance of the role of professionals of justice, to enforce the LGPD and through the judicialization of concrete cases that are protected by this law. As a result, it is clear that infringing can lead to compensation and pecuniary punishment in some cases where damage is demonstrated.

Keywords: LGPD. Medium Digital. Security. Legal Action.

1 INTRODUÇÃO

Com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) em setembro de 2020, houve uma mudança significativa na forma como as empresas e organizações lidam com informações pessoais. A LGPD tem como objetivo garantir uma maior segurança e privacidade aos dados pessoais, bem como o livre desenvolvimento dos cidadãos brasileiros. Nesse sentido, torna-se essencial avaliar como a segurança digital foi impactada pela implementação da nova legislação e como é realizado o tratamento dos dados pessoais diante desse novo cenário.

Alguns autores, como Granzotto et al. (2020) e Andrade e Campanile (2019), já realizaram estudos sobre o impacto da LGPD na segurança da informação. Esses estudos apontam para a necessidade de as empresas se adaptarem às novas exigências da legislação, a fim de garantir a proteção dos dados pessoais e evitar sanções. Além disso, Marques e Almeida (2020) destacam que a LGPD pode ser vista como um fator impulsionador para o aprimoramento da segurança da informação nas empresas.

O cenário atual de grandes transformações no mundo, sejam de ordem social, tecnológica, cultural, política, dentre outros, está diante de desafios diários quanto ao uso da internet, os quais precisam de um olhar atento, científico e legal da referida Lei de Proteção de Dados-LGPD.

A finalidade da Lei Geral de Proteção de Dados no cenário nacional (Brasil) é estabelecer regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção, privacidade e penalidades para o não cumprimento e violação dos Direitos básicos de cada indivíduo (cidadão).

Nesse sentido, a Lei Geral de Proteção de Dados pode impactar a estratégia, desenvolvimento de Marketing de uma determinada empresa, ou pessoa, a qual assegura a regulamentação da aquisição, armazenamento e uso de dados pessoais por terceiros. A mencionada lei estabelece regras sobre segurança e proteção de dados, tomando as medidas legais, zelando pelos Direitos Humanos e preceitos constitucionais de todos os cidadãos.

Os usuários de meios tecnológicos encontram-se, na maioria das vezes, em situação vulnerável, pois para um simples acesso às redes sociais, são necessários fornecimento de dados pessoais, os quais são armazenados por empresa competente, estando estes suscetíveis a invasões e vazamento de dados sensíveis.

É de suma importância destacar que a segurança dos usuários dos meios tecnológicos digitais vem a cada dia sendo invadida, usados indevidamente, motivo pelo qual tem afetado a vida das pessoas, organizações atuais através dos armazenamentos e vazamentos de dados sensíveis, informações, dados organizacionais, entre outros.

Porém, apenas as adoções de soluções tecnológicas não asseguram as devidas medidas de forma efetiva, buscando assim adequação e apoio à LGPD. Tendo em vista que os maiores impactos estão na necessidade de investimento em cibersegurança em parceria com a nova Lei de Proteção de Dados para implementar sistemas de proteção efetivos de prevenção, detecção e remediação de vazamento de dados. Frente a esses desafios se faz necessário ampliar conhecimentos técnicos, tecnológicos, midiáticos e principalmente jurídicos.

Assim, este artigo, tem como objetivo geral analisar sobre a segurança no meio digital após a entrada em vigor da LGPD, por meio de casos concretos em que essa lei foi aplicada. Como objetivos específicos busca apresentar a importância da Lei n° 13.709, de 14 de agosto de 2021, Lei Geral de Proteção de Dados-LGPD; discutir os avanços trazidos pela LGPD e as principais infrações cometidas pelo uso inadequado dos dados através da rede mundial de computadores e por fim apresentar casos em que empresas foram condenadas judicial ou administrativamente pelo uso inadequado dos dados de seus usuários.

Dessa forma, será abordado o impacto que a LGPD teve sobre as empresas, que agora necessitam adotar medidas mais eficazes para à proteção dos dados de seus clientes e usuários. Também serão discutidos os desafios enfrentados pelas empresas para se adequarem à nova legislação. A partir dessa análise, será possível compreender melhor como as empresas estão se adaptando à nova realidade e quais são as principais tendências em termos de segurança da informação no contexto da LGPD.

O estudo da presente temática justifica-se que é urgente e relevante entender a importância do assunto, sendo fundamental saber que a nova lei quer oferecer um cenário atualizado e eficaz de segurança, apoio e orientações jurídicas, através da padronização de normas e práticas que venham ajudar a compreender os seus direitos como cidadão, ou suas obrigações, caso seja responsável por base de dados de pessoas, para promover a proteção necessária e legal, de forma ética, igualitária e dentro do país, e no mundo, preservando e

zelando juridicamente aos dados pessoais de todo cidadão que reside no Brasil, assegurando sua integridade e dignidade.

Daí a importância de desenvolver este estudo, o qual busca aprimorar conhecimentos teóricos, jurídicos, contribuindo com a nova Lei Geral de Proteção de Dados-LGPD e obter com ela o suporte, as determinações legais para proporcionar a todos a segurança que necessitam, pois conforme a ilustríssima Miriam Wimmer em seu livro "Proteção de dados pessoais: a função e os limites do consentimento", afirma que "o consentimento deve ser visto como um instrumento de proteção do titular de dados, que deve estar informado sobre o tratamento de seus dados e ter o poder de decidir sobre o que será feito com eles" (WIMMER, 2020, p.40)

Portanto, é necessário analisar e conhecer a nova Lei (LGPD) na chamada globalização que conecta todos em todo o momento de qualquer lugar, onde não há fronteiras, para uma troca de informações instantâneas, seja através de uma tela de computador ou de um telefone celular, onde a sociedade está intimamente conectada com as novidades que aparecem a todo momento, com a globalização, a internet e vários outros aspectos que precisam ser encarados para obter os Direitos e ordenamentos legais capazes de garantir o mínimo exigido e determinado pela Constituição Federal e da própria LGPD.

2 CONCEPÇÕES E IMPORTÂNCIA DA NOVA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

As redes sociais e meios digitais são ferramentas poderosas que conectam pessoas em todo o mundo, permitindo a troca de informações e o compartilhamento de ideias. No entanto, há também riscos associados ao uso dessas plataformas, como a disseminação de informações falsas, a exposição excessiva de dados pessoais, bem como a possibilidade de cyberbullying e assédio online.

Estudos recentes têm mostrado que o uso das redes sociais afeta em muitos aspectos os sujeitos envolvidos, através da gravidade da exposição e das características individuais, dados e informações pessoais daqueles que são expostos, bem como de suas relações com os meios digitais, onde são impactados por agressões psicológicas e verbais por meio de invasões abusivas aos internautas.

Tal fenômeno foi destacado por Carlos Alberto Bittar, conforme se observa:

> "Esse direito vem assumindo, paulatinamente, maior relevo, com a contínua expansão das técnicas de virtualização do comércio, de comunicação, como defesa natural do homem contra as investidas tecnológicas e a ampliação, com a necessidade

> de locomoção, do círculo relacional do homem, obrigando-se à exposição permanente perante públicos os mais distintos, em seus diferentes trajetos sociais, negociais ou de lazer. É fato que as esferas de intimidade têm- se reduzido com a internet e meios eletrônicos."

Nesse contexto, limites e atenção devem ser tomados por todos na sociedade digital, que a cada dia se eleva o número de navegantes nas redes sociais. É evidente que se sabe de tudo isso, tanto sabe-se que se tem ampliado seus investimentos para se equipar com diferentes tecnologias. Contudo, cabe destacar que ter uma pluralidade de meios celulares avançados, computadores individuais, tablets, salas informatizadas, etc., à disposição de todos não significa, necessariamente, o aproveitamento, uso ético e adquirido desses meios. Não raro se depara com situações de violações, invasão de dados pessoais, constrangimentos psicológicos, onde assumem funções diferentes dos benefícios dessas ferramentas.

Conforme Soares (2018, p.59)

> (...) em lugar da exploração das possibilidades comunicativas desses meios, os usuários parecem assumir vários riscos, na tentativa de gerenciar, controlar seus usos, acaba por artificiá-los e de se expor a vários perigos, constrangimentos, reduzindo-os a meros acessórios destinados a tornar mais abrangente a interação, atraente, sem perceber o nível de perigos diante da exposição de dados pessoais e até organizacionais.

No entanto, pode-se observar que mais do que um acessório, os meios digitais, a concepção tem um potencial enorme de comunicação extraordinária. Contudo, não se pode desprezar o papel preponderante das redes sociais e seus meios digitais, midiáticos, o que se faz necessário é saber fazer o uso correto e ter o cuidado em preservar seus dados, informações pessoais principalmente.

Segundo Andrade (2013, p.44-45)

> (...) recentemente, com o aparecimento das facilidades e acessos dos recursos eletrônicos, tecnológicos digitais da rede mundial de computadores, celulares, internet, essa outra forma de pesquisa tornou o acesso muito mais amplo e praticamente sem fronteiras físicas (...), entretanto, devido à enorme quantidade e à especialidade do endereçamento, encontrar o que se procura, expor pensamentos, formas de agir, de ser, sentir, não tem sido fácil de controlar.

Nesse contexto, surgiu uma nova ciência, a informática e uma ferramenta de comunicação, a internet. Essa ferramenta tornou-se responsável por uma parte expressiva das informações que circulam no mundo, no armazenamento e ao mesmo tempo divulgação de Dados pessoais ou organizacionais, onde surgiu a necessidade da Proteção e segurança jurídica. Dessa forma, cabe questionar o seu efetivo papel, principalmente no meio acadêmico, jurídico, pois, do contrário, corre-se o risco de fazer uso das coisas secundárias, da privacidade pessoal e deixar de lado as essenciais, tornando-se muitas vezes afetadas até mesmo por pessoas desconhecidas, má intencionadas.

Para Velloso (2015, p.73)

> Foi a partir da década de 1980 que o uso da internet (meios digitais) tornou-se público e popular, deixando de ser exclusividade de especialistas e instituições governamentais, a internet vem popularmente com a implantação de laboratórios de informática nas diversas instituições de ensino, sobretudo após a utilização das ondas de rádio para essa finalidade, uma vez que, através de uma linha telefônica, seu uso era muito dispendioso e, por isso, restrito, atualmente ampliou-se através da telefonia celular móvel, tornando-se um perigo no vazamento e distorções de dados pessoais, organizacionais e informações em geral.

Dessa forma, ter noção das consequências dos atos é fundamental, preponderante no dia-a-dia em todos os aspectos e situações da realidade. O mau uso da internet requer orientações, cibersegurança e apoio jurídico que implica na capacitação dos profissionais jurídicos para efetivação da nova Lei Geral de Proteção de Dados, como parâmetro legal, constitucional e jurídico.

No panorama histórico, a nova Lei Geral da Proteção de Dados (Lei 13.709 de 2018) tornou-se um marco legal que regulamenta o uso a proteção e a transparência de dados pessoais no país (Brasil), assegurando amplo controle dos cidadãos sobre seus dados, informações pessoais, exigindo consentimento explicito legal para coleta e uso dos dados e determina, ordena e oferta opções para o usuário visualizar, corrigir e excluir esses dados.

Nesse contexto, a Lei Geral de Proteção de dados-LGPD originou-se no PLC 53/2018, aprovado por unanimidade e em regime de urgência pelo Plenário do Senado em julho de 2018. O texto é aplicável mesmo em empresas com sede no exterior, desde que a operação de tratamento de dados seja realizada no território nacional. Foi sancionada pelo então presidente da república Michel Temer em agosto de 2018.

O avanço tecnológico é elemento propulsor da evolução do direito como instrumento de garantia dos direitos fundamentais, que neste momento histórico se depara com a identificação de novos riscos (Cadernos Jurídicos, p.97-115, 2020). Segundo Levy (2015, p.68) “O acesso à informática deve ser visto como um direito e, portanto, o cidadão deve usufruir desses benefícios tecnológicos, porém de forma adequada, ética dentro dos limites e privacidade”.

Nessa perspectiva a relação entre segurança da informação e LGPD corresponde à privacidade e à proteção de dados pessoais. A lei traz muitos benefícios para a empresa quanto à prática de segurança como também dos dados pessoais por prever o uso de medidas administrativas e técnicas que aprimoram a cibersegurança. (Lei nº 13.709/2018- Lei Geral de Proteção de Dados)

Portanto, a Lei Geral de Proteção de Dados Lei 13709/2018 de 14 de agosto de 2018, é tida como uma lei que além de alterar o Marco Civil da internet, cria um sistema de regulamentação para o uso, a proteção e a transferência de dados pessoais no Brasil oferecendo

mais segurança e garantindo também, possibilidades de progresso para o país, tanto no aspecto privado, quanto no público. Atribui suas responsabilidades, agentes passíveis de sanção, condutas reprováveis e as penalidades no âmbito civil.

Conforme relata Laura Schertel Mendes (2019), divide-se em três grandes frentes. Tem na base de sua estrutura, as condições de legitimidade para o tratamento de dados pessoais, ao comtemplar sua base principiológica e as bases legais autorizadas do tratamento de dados pessoais.

A Lei Geral de Proteção de Dados e o Marco Civil da internet são leis complementares, onde ambas visam resguardar dados pessoais dos usuários na internet. O Marco Civil da internet aprovado em 2014, estabeleceu princípios, garantias, direitos e deveres para o uso do meio digital no Brasil. A LGPD, por sua vez, estabelece regras específicas para o tratamento de dados pessoais no país, incluindo consentimento para o uso desses dados, a transparência no tratamento e o direito dos usuários de solicitar a exclusão de seus dados.

Tendo como base que antes era apenas regulado pela esfera do Direito Penal com suas condutas típicas e suas sanções caso fosse praticado o fato típico e devidamente descrito nas linhas do Código Penal, a Lei Geral de Proteção de Dados e transferências, estabelecendo limites de uso e o que não é permitido. Assim, o papel do Direito na era digital e como tecnologia, impacta no cotidiano dos seres humanos (cidadãos) analisando juridicamente como a Lei Geral de Proteção de Dados assegura e protege os direitos fundamentais guardados e exigidos pela Carta Magna (Constituição Federal 1988) vigente no país (Brasil) onde em seu artigo 5º estabelece um rol de direitos e garantias fundamentais dentre às quais à liberdade dos indivíduos e a privacidade são resguardar pelas linhas da Carta Magna.

Contudo, para fortalecer o sistema de proteção iniciado na própria Constituição a LGPD desenvolve-se sob os fundamentos do respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, informação, comunicação e opinião, a inviolabilidade da intimidade da honra e da imagem; o desenvolvimento econômico, tecnológico e da inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, bem como os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas físicas, conforme o que consta em seu artigo segundo.

A Lei Geral de Proteção de Dados foi aprimorada pela Lei nº13.853 de oito de julho de 2019, que providenciou criar uma autoridade nacional de proteção de dados para que os quais a LGPD foi estabelecida possa ser realmente cumprido. A Autoridade Nacional de Proteção de Dados (ANPD) tem o objetivo de zelar sobre os dados, elaborar políticas adequadas para Proteção de Dados, fiscalizar e aplicar as sanções quanto ao uso incorreto de dados. Dessa

forma, tornando o sistema de proteção cada vez mais seguro, sólido, ético e eficaz.

3 AVANÇOS TRAZIDOS PELA LGPD E PRINCIPAIS INFRAÇÕES COMETIDAS PELO USO INADEQUADO DA REDE

A LGPD busca a proteção e regulamentação de dados que aparentemente são inofensivos, porém, estes são relevantes e podem trazer grandes consequências pessoais para àqueles que os forneceram. Esta é a principal ideia da teoria do mosaico apresentada por Conesa, qual seja:

> Existem dados a priori irrelevantes do ponto de vista do direito à privacidade e que, no entanto, em relação a outros, talvez também irrelevantes, podem servir para tornar a personalidade de um cidadão totalmente transparente, tal como acontece com as pedrinhas. Que em si mesmos nada dizem, mas que juntos podem formar conjuntos completos de significados. (CONESA, 1984, traduzido)

A Lei Geral de Proteção de Dados trouxe diversas alterações para o meio digital da sociedade brasileira. Algumas das principais mudanças incluem: maior proteção aos dados pessoais, direito dos titulares dos dados, sanções e multas, consentimento no tratamento de dados, responsabilidade compartilhada entre empresas, órgãos públicos e os próprios titulares dos dados, o que incentiva a colaboração e o comprometimento com a segurança dos dados pessoais.

Ademais, outros pontos de grande relevância, são a adequação do tratamento de dados, para que não sejam recolhidos dados desnecessários ou até mesmos excessivos, a transferência internacional de dados, a qual estabelece regras claras para a transferência de dados internacionais, bem como regras para a utilização de dados sensíveis. (BRASIL, 2021)

Nos tempos de enormes mudanças, se faz necessário que se crie regras, normas de conduta, penalidades e Leis, com o uso da política on-line e termos de uso, em relação a utilização de meios digitais, ferramentas como redes sociais, internet (blogs, chats, e-mails, espaço virtual, facebook, instagram), entre tantos outros.

A Lei Geral de Proteção de Dados-LGPD e demais leis geram responsabilidade não apenas por ação, mas também por omissão e negligência, violação de direitos de privacidade e outras formas de agressão pessoal, e é nesse ponto que se ressalta a atuação jurídica, e Direito Humano, proporcionando segurança, apoio e respaldo legal nas infrações cometidas na internet, nos meios digitais.

Principais infrações cometidas com o uso da internet:

Tabela 1 — Crimes Digitais

Ação	Crime	Legislação	Pena
Dizer em um chat, blog ou comunidade que alguém deve matar-se ou sugerir como fazê-lo.	Instigação ou auxílio ao suicídio.	Art.122 do Código Penal.	Reclusão de 2 a 6 anos, se o suicídio for consumado; reclusão de 1 a 3 anos, se da tentativa de suicídio resultar lesão corporal de natureza grave.
Dizer em um chat que alguém cometeu algum crime (p.ex.: "Ele é ladrão).	Calúnia.	Art. 138 do Código Penal.	Detenção de 6 meses a 2 anos e multa.
Encaminhar um boato eletrônico para várias pessoas.	Difamação.	Art.139 do Código Penal.	Detenção de 3 meses a 1 ano de multa.
Enviar um e-mail para terceiros com informação considerada confidencial pela instituição.	Divulgação de segredo.	Art.153 do Código Penal.	Detenção de 1 a 6 meses ou multa.
Enviar um vírus que destrua equipamento ou conteúdo.	Dano.	Art.163 do Código Penal.	Detenção de 3 meses a 1 ano ou multa.
Copiar um conteúdo e não mencionar a fonte ou entregá-lo ao professor como se fosse seu; baixar arquivos mp3.	Violação ao direito autoral.	Art.184 do Código Penal.	Detenção de 3 meses a 1 ano ou multa.
Criar uma comunidade on-line que fale mal sobre a religião de um colega de classe.	Escárnio por motivo religioso.	Art.208 do Código Penal.	Detenção de 1 mês a 1 ano de multa.
Criar uma comunidade para ensinar como fazer "um gato"	Apologia ao crime ou ato criminoso.	Art.287 do Código Penal.	Detenção de 3 a 6 meses ou multa.
Devolver um spam com um vírus ou com mais spam.	Exercício arbitrário das próprias razões.	Art.345 do Código Penal.	Detenção de 15 dias a 1 mês ou multa, além da pena correspondente à violência.
Participar de cassinos on-line	Jogo de azar.	Art.50 da Lei das Contraversões Penais.	Prisão de 3 meses a 1 ano de multa.
Falar mal de alguém em um chat por sua ascendência ou etnia.	Preconceito ou discriminação por raça-cor-etnia.	Art.20 da Lei nº 7.716/89.	Reclusão de 1 a 3 anos e multa.
Enviar ou encaminhar fotos de crianças nuas on-line (cuidado com as fotos de seus filhos).	Pedofilia.	Art.247 da Lei nº8.069/90.	Multa de 3 a 20 salários de referência, aplicando-se o dobro em caso de reincidência.
Usar, sem autorização no todo ou em parte, logomarca da escola em um link em página da internet, comunidade virtual ou algum tipo de material.	Crime contra a propriedade industrial.	Art.195 da Lei nº9.279/96.	Detenção de 3 meses a 1 ano ou multa.
Usar cópia de software sem ter licença para isso.	Crime contra a propriedade intelectual; "pirataria".	Art.12 da Lei nº 9.609/98.	Detenção de 6 meses a 2 anos ou multa.

Fonte: Autoria Própria.

Portanto, se faz necessário que esse projeto valorize a pesquisa de casos práticos do

direito digital, que é o ramo do direito que cuida dessas questões, se estruturando adequadamente na documentação, legislação, de forma jurídica, orientando sobre o que é correto e errado no uso das ferramentas tecnológicas digitais, tornando-se essencial preparar o terreno para evitar responsabilidade legal, seja ela civil, criminal ou administrativa, contando quando necessário dos profissionais de Direito na forma da Lei.

Ademais, a Lei Geral de Proteção de Dados, prevê uma série de penalidades administrativas para empresas que descumprirem as normas estabelecidas em seu texto. As sanções podem ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por fiscalizar o cumprimento da LGPD no Brasil.

A advertência é a primeira medida que a ANPD pode aplicar em caso de violação da LGPD. Consiste em uma notificação formal (advertência) por escrito, para a empresa ou organização, informando sobre a violação e orientando sobre as medidas necessárias pra a correção do problema apontado em um prazo determinado. (LGPD BRASIL,2021)

Outra medida, em caso de infração de menor gravidade, é a aplicação da multa simples, como no caso de não fornecimento de informações solicitadas pelo titular dos dados ou o não atendimento aos pedidos de correção ou exclusão de dados pessoais. O valor da multa é de até 2% (dois por cento) do faturamento bruto anual, em sede brasileira, estando limitada a R$ 50.000.000,00 (cinquenta milhões) por infração.

Além disso, poderá ser aplicada a multa diária, desde que esta observe os limites supramencionados, estando estes previstos no dispositivo 52, II e III da Lei 13.709/2018-LGPD, qual seja:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> 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;
>
> (BRASIL 2018)

A LGDP, também prevê que a ANPD pode determinar a publicização da infração cometida pela empresa ou organização, penalidade esta que consiste em divulgar publicamente a irregularidade e seus detalhes, com o intuito de informar ao público em geral sobre o ocorrido. A publicização pode ser efetivada de diferentes maneiras, como nos casos de comunicação à imprensa e publicações em redes sociais. (BRASIL, 2018)

A publicização da infração tem como objetivo conscientizar a sociedade sobre a importância da proteção de dados pessoais e alertar os indivíduos sobre possíveis riscos envolvidos no tratamento inadequado de seus dados por parte das empresas e organizações. Ademais, a publicidade da infração pode causar danos à imagem e reputação da empresa ou organização, tornando-se um incentivo para o cumprimento efetivo da LGPD. (BRASIL, 2018)

Vale ressaltar que a publicização da infração não é aplicada de forma automática, mas sim após análise de cada caso específico pela ANPD. A decisão de publicizar ou não a infração depende das circunstâncias envolvidas, podendo ser aplicada de forma isolada ou em conjunto com outras penalidades previstas pela LGPD.

Do mesmo modo, existe previsão legal para a aplicação da penalidade de bloqueio ou eliminação dos dados pessoais tratados pela empresa ou organização que não esteja cumprindo com as disposições da lei. A referida medida, impede o acesso a esses dados sem que haja a sua eliminação. Isso significa que os dados ficam indisponíveis para o acesso e tratamento, mas ainda são mantidos pela empresa ou organização. O bloqueio pode ser temporário ou definitivo, variando de acordo com a gravidade da violação.

Já a eliminação de dados pessoais é uma medida que implica a sua exclusão definitiva, tornando-os irrecuperáveis. A empresa ou organização deve garantir que os dados sejam apagados de forma segura e irreversível, de modo a evitar a sua recuperação por terceiros não autorizados. (BRASIL, 2018)

A aplicação da penalidade de bloqueio ou eliminação de dados pessoais podem ser bastante prejudiciais para a empresa ou organização, especialmente se esses dados são essenciais para a sua atividade ou para a prestação de serviços aos seus clientes. Além disso, a penalidade pode gerar danos à reputação da empresa ou organização, uma vez que indica que ela não está cumprindo com as obrigações previstas na LGPD.

Outrossim, a suspensão parcial do funcionamento do banco de dados utilizado para o tratamento de dados pessoais é uma das penalidades previstas na Lei Geral de Proteção de Dados (LGPD), apresentando sua aplicação em empresas que descumprem as suas disposições. Desta feita a suspensão parcial do funcionamento do banco de dados utilizados para o tratamento de dados pessoais pode durar até 6 meses, prorrogável por igual período. (LGPD BRASIL, 2018)

Destaca-se que, durante o período de suspensão, a empresa não poderá realizar o tratamento de dados pessoais que estejam contidos no banco de dados suspenso, sob pena de aplicação de multa diária. Todavia, a suspensão parcial do funcionamento do banco de dados deve ser precedida de um processo administrativo, no qual a empresa terá a oportunidade de apresentar defesa e produzir provas. (LGPD BRASIL,2018)

Por fim, conforme previsto na Lei Geral de Proteção de Dados (LGPD), a Autoridade Nacional de Proteção de Dados (ANPD) pode proibir parcial ou totalmente o exercício de atividades relacionadas ao tratamento de dados pessoais em caso de infração grave ou reiterada. A medida tem caráter temporário e pode ser revogada caso a empresa ou organização comprove que implementou as medidas necessárias para sanar as infrações cometidas.

É importante trazer à baila, que as penalidades previstas na LGPD podem ser cumulativas, ou seja, a empresa ou organização pode ser penalizada com mais de uma sanção em caso de violação da lei. Além disso, a LGPD também prevê a possibilidade de responsabilização penal nos casos mais graves de violação da lei.

As referidas sanções previstas na LGPD têm como objetivo garantir a proteção dos dados pessoais dos cidadãos brasileiros e incentivar às empresas adotarem boas práticas de segurança e privacidade, deixando-as cientes de suas obrigações legais.

3 METODOLOGIA

A presente pesquisa desse artigo caracteriza-se através de uma pesquisa documental com análise de casos concretos, tendo em vista a estratégia de buscar conhecimento teórico, prático, jurídico, em profundidade de uma realidade ou de um fenômeno social, sendo conduzido em detalhes e, com frequência, baseado em várias fontes de dados, com abordagem descritiva, participativa e qualitativa.

De acordo com Gil (2017, p.36) “a principal vantagem da pesquisa qualitativa, descritiva e exploratória é o conhecimento direto da realidade, pois o estudo de caso por si só fornece às informações fundamentais”.

Optou-se pela análise etnográfica e analise de casos concretos, selecionados por meio de websites, onde se obtém as informações através da fala e pensamentos dos participantes e fundamenta-se na pesquisa documental para sustentação teórica.

“Analisar significa investigar, estudar, decompor, analisar, interpretar. Através da análise podem-se observar os componentes de um conjunto e perceber suas possíveis relações, ou seja, de uma ideia-chave geral, passar-se para um conjunto de ideias mais específicas” (MARCONI e LAKATOS, 2013, p.39).

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

4.1 DA APLICAÇÃO EM CASOS CONCRETOS

O trabalho, através da análise, discussões e os relevantes pontos essenciais a esse estudo, aponta que todas as empresas de todos os setores enfrentam grandes desafios quanto a segurança, proteção e gestão de dados pessoais, desde a identificação e classificação de dados até o cumprimento de regulamentações no que se refere à privacidade. Dessa forma, esses desafios podem resultar em multas pela Lei Geral de Proteção de Dados (LGPD) e danos à imagem da (s) empresa (s).

Constatou-se que surge assim que as empresas no mercado atual requerem serviços e produtos, para conseguir auxiliar na sua organização à Lei Geral de Proteção de Dados (LGPD). Contudo, com um modelo desenvolvido, há o auxílio à (s) empresa (s) na preparação, aplicação de controles de segurança, no estabelecimento de estruturas de governança, gestão, bem como na identificação e efetivação de melhorias e seus respectivos ajustes.

Daí a relevância desse estudo de casos, tendo como parâmetro que a Lei Geral de Proteção de Dados (LGPD), a qual traz as devidas regulamentações e tratamento de dados pessoais de usuários titulares de dados em território brasileiro. A Lei impacta em todos os segmentos de negócios, inclusive os entes públicos. Nesse contexto, toda e qualquer empresa que utilize dados pessoais encontra-se obrigada a observar os procedimentos previstos na Lei nº 13.709/2018, a Lei Geral de Proteção de Dados.

Foi observado nas empresas em que se deu a pesquisa de estudos de casos que a LGPD deve ser aplicada aos dados pessoais tratados tanto em ambientes digitais quanto aos ambientes físicos. Porém, se faz necessário repensar seus procedimentos e governança para melhor adequação com a nova Lei (LGPD) e conformidade com a legislação, onde se orienta o trabalho de consultoria digital, para que de forma especialista proporcione segurança e proteção para as empresas.

Portanto, pode-se assegurar a eficiência da LGPD, essa nova Lei brasileira de proteção de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, no território

nacional ou em países onde estejam localizados os dados, transformando drasticamente a maneira como empresas e órgãos públicos tratam a privacidade e a segurança das informações de usuários, clientes, efetivando-se como lei que se tornou relevante nesse contexto globalizado, tecnológico, midiático, digital, no mundo da comunicação e informação tão necessária mas que requer o devido amparo legal no país.

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que tem como objetivo regulamentar o tratamento de dados pessoais por empresas e instituições, visando proteger os direitos fundamentais de privacidade e intimidade dos indivíduos. Abaixo, descreve-se três casos concretos em que a LGPD foi aplicada no meio digital.

4.2 APLICAÇÃO DA LGPD- CASO NUBANK

O caso Nubank refere-se a uma multa aplicada pela Autoridade Nacional de Proteção de Dados (ANPD), a qual é o órgão responsável pela fiscalização e aplicação das sanções previstas na Lei Geral de Proteção de Dados (LGPD), à instituição financeira Nubank, banco digital, por não ter fornecido informações suficientes a um cliente que havia solicitado acesso a seus dados pessoais.

O cliente, que havia solicitado a portabilidade de sua conta para outra instituição financeira, teve sua solicitação negada pelo Nubank. Ao pedir informações sobre os motivos da negativa, o cliente não recebeu informações claras e completas. Porém, a LGPD estabelece princípios, regras e direitos relacionados à proteção de dados pessoais, incluindo o direito de acesso, retificação e exclusão de dados pessoais.

Diante das circunstâncias, o Nubank foi multado por não ter cumprido o direito de acesso do cliente aos seus dados pessoais, e a sanção aplicada pela ANPD foi de R$ 6,5 milhões de reais, sendo a primeira penalidade aplicada pela ANPD desde a entrada em vigor da LGPD.

O caso Nubank é um exemplo de como a Lei Geral de Proteção de Dados (LGPD) está sendo aplicada no Brasil, a qual foi criada para proteger os dados pessoais dos cidadãos brasileiros e garantir que as empresas que lidam com esses dados estejam em conformidade com os preceitos legais.

O direito de acesso aos dados pessoais é um dos direitos fundamentais previstos na LGPD, e a falta de resposta clara e completa viola esse direito. A multa aplicada mostra que a ANPD está levando a sério a referida lei e que as empresas que não estiverem em conformidade com a LGPD podem enfrentar consequências financeiras significativas.

O caso do Nubank também destaca a importância da transparência no tratamento de

dados pessoais. As empresas precisam ser claras e precisas em relação ao uso dos dados pessoais dos clientes e fornecer informações completas e precisas quando solicitadas pelos titulares dos dados. Isso é fundamental para garantir a confiança dos clientes e proteger seus direitos fundamentais de privacidade e proteção de dados.

4.3 CASO GRUPO FLEURY

Em dezembro de 2020, o Grupo Fleury, uma das maiores redes de laboratórios de análises clínicas do Brasil, sofreu um vazamento de dados pessoais de seus clientes, incluindo informações como nome completo, CPF, data de nascimento e resultados de exames. O vazamento teria ocorrido por meio de um ataque cibernético ao sistema da empresa.

A Autoridade Nacional de Proteção de Dados (ANPD) abriu um processo administrativo para investigar o caso e solicitou esclarecimentos ao Grupo Fleury sobre as medidas adotadas para proteger os dados pessoais de seus clientes. O Grupo Fleury informou que tomou medidas para conter o vazamento e proteger os dados de seus clientes, incluindo a contratação de uma empresa especializada em segurança da informação para investigar o incidente.

O caso do Grupo Fleury destaca a importância de as empresas adotarem medidas de segurança cibernética adequadas para proteger os dados pessoais de seus clientes. A LGPD estabelece a responsabilidade das empresas em proteger os dados pessoais de seus clientes e as sanções para casos de vazamento de dados. Empresas que não adotarem medidas adequadas para proteger os dados pessoais de seus clientes podem enfrentar consequências financeiras e de reputação significativas. O referido caso ainda está em andamento e pode resultar em sanções à empresa.

Destaca-se também a importância de a ANPD atuar de forma rápida e eficaz para investigar casos de vazamento de dados e aplicar sanções quando necessário. A ANPD é responsável por fiscalizar e aplicar as sanções previstas na LGPD e seu papel é fundamental para garantir que as empresas estejam em conformidade com a lei e protejam os dados pessoais de seus clientes.

4.4 CASO TIKTOK

A multa aplicada pela ANPD foi resultado de uma investigação iniciada em julho de 2020, após denúncias de que o TikTok estava coletando ilegalmente dados de crianças e

adolescentes. A empresa foi acusada de não obter o consentimento prévio e expresso dos pais ou responsáveis legais dos usuários com menos de 13 anos de idade, além de não fornecer informações claras e precisas sobre como os dados seriam usados.

A LGPD (Lei Geral de Proteção de Dados) tem como objetivo proteger a privacidade e os dados pessoais dos usuários, incluindo crianças e adolescentes. O Estatuto da Criança e do Adolescente, por sua vez, estabelece direitos e garantias para esse público, incluindo o direito à privacidade.

Como resultado da multa, o TikTok foi obrigado a implementar medidas para garantir a privacidade e proteção de dados de crianças e adolescentes em conformidade com a legislação brasileira. Isso incluiu a criação de uma política de privacidade específica para menores de idade, a implementação de medidas técnicas para impedir a coleta de dados de crianças e adolescentes sem o consentimento dos pais ou responsáveis legais, e a designação de um encarregado de proteção de dados para lidar com questões relacionadas à privacidade e proteção de dados.

A multa aplicada pelo ANPD serve como um alerta para outras empresas que lidam com dados pessoais, especialmente aquelas que lidam com dados de crianças e adolescentes. É importante que as empresas sigam as leis e regulamentos de privacidade e proteção de dados para garantir a segurança e privacidade dos usuários, especialmente os mais vulneráveis.

A multa aplicada pelo ANPD ao TikTok por violação de privacidade de crianças e adolescentes é um exemplo de como a legislação de proteção de dados está sendo aplicada no Brasil. A LGPD, que entrou em vigor em setembro de 2020, estabelece regras claras para a coleta, uso, armazenamento e compartilhamento de dados pessoais, incluindo dados de crianças e adolescentes.

A Lei nº 13.709/2018, que instituiu a LGPD, define dados pessoais como "informação relacionada a pessoa natural identificada ou identificável", o que inclui informações como nome, endereço, e-mail e localização. A lei estabelece que o tratamento desses dados deve ser feito de forma transparente e com o consentimento do titular dos dados ou de seu representante legal, no caso de crianças e adolescentes.

No caso do TikTok, a ANPD identificou que a empresa estava coletando dados de crianças e adolescentes sem o consentimento dos pais ou responsáveis legais, o que viola tanto a LGPD quanto o Estatuto da Criança e do Adolescente. Como resultado, o TikTok foi multado em R$ 9,4 milhões e obrigado a implementar medidas para garantir a privacidade e proteção de dados de crianças e adolescentes em conformidade com a legislação brasileira.

Essas medidas incluem a criação de uma política de privacidade específica para menores

de idade, a implementação de medidas técnicas para impedir a coleta de dados de crianças e adolescentes sem o consentimento dos pais ou responsáveis legais, e a designação de um encarregado de proteção de dados para lidar com questões relacionadas à privacidade e proteção de dados.

É importante notar que a LGPD não se aplica apenas a empresas de tecnologia e redes sociais, mas a qualquer empresa que lida com dados pessoais, incluindo escolas, hospitais, bancos e empresas de varejo. Todas essas empresas devem estar em conformidade com a legislação de proteção de dados para garantir a privacidade e proteção dos dados pessoais de seus clientes e usuários.

5 CONSIDERAÇÕES FINAIS

O presente estudo (pesquisa) traz em suas configurações finais, os mais relevantes pontos ressaltados no decorrer desse trabalho, com base em estudos de casos e fundamentado em pesquisa bibliográfica, retratando sua relevância legal e social.

Nesse sentido, o estudo assegura que todos os dados cujos titulares são pessoas naturais, estejam eles em formato físico ou digital. Dessa forma, a LGPD não alcança os dados titularizados por pessoas jurídicas, os quais não são considerados dados pessoais para os efeitos da Lei, pautado nos três pilares da LGPD: pessoas, processos e tecnologias; nos cinco (5) tipos de tratamentos de dados seguindo a Lei: transmissão, transferência e difusão. Para garantir a conformidade na era digital, as organizações precisam compreender as obrigatoriedades determinadas pela lei, além de entender como elas podem impactar nas operações e estratégias de marketing.

A partir disso, é possível implementar as adequações necessárias e evitar qualquer tipo de penalidade pelo descumprimento das normas, daí é fundamental compreender em sua essência todo o teor da Lei Geral de Proteção de Dados (LGPD) e como ela se aplica dentro da vigência da Lei no Brasil.

Portanto, é uma temática que mesmo se tratando há décadas da Proteção de Dados, somente a partir de 2018 e das recentes ocorrências de graves incidentes de segurança que veio entrar em vigor a LGPD promulgada com leis específicas voltadas para assegurar, salvaguarda e proteção legal da privacidade, onde as empresas iniciaram suas manifestações, preocupações e intervenções referentes à questão, mais pressionadas pelas duras penalidades impostas pela legislação do que pela pura preocupação com a privacidade individual e todos os direitos

assegurado à pessoa jurídica. É preciso e urgente, independente da motivação, o processo de adequação e efetivação à legislação de Proteção de Dados, indo além, requer um conjunto multidisciplinar de competências para que possa ser levado a sério e de fato concreto com êxito, daí a relevância da abordagem jurídica para a correta compreensão e interpretação de legislação e suas implicações dentro de um processo técnico relacionados à tecnologia e segurança da informação.

REFERÊNCIAS

ANDRADE, M, M. de. **Introdução à tecnologia digital e uso ético**. São Paulo: Atlas, 2013.

BRASIL. **Constituição Federativa do Brasil 1988**. Brasília DF, 1988.

BRASIL. **Lei Geral de Proteção de Dados Pessoais**. São Paulo: Revista dos Tribunais, 2019.

GIL. A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2017.

Grupo Fleury sofre vazamento de dados de clientes. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/grupo-fleury-sofrevazamento-de-dados-de-clientes.ghtml . Acesso em: 27 maio. 2023.

Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais): http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm- Estatuto da Criança e do Adolescente: http://www.planalto.gov.br/ccivil_03/leis/L8069.htm

LÉVY, P. **Cibercultura**. Rio de Janeiro: Editora 34, 2015.

MARCONI, M. de A; LAKATOS, E. M. **Fundamentos de metodologia científica**. São Paulo, 2013.

Nubank é multado em R$ 6,5 milhões pela ANPD por violação da LGPD. Disponível em: https://tecnoblog.net/381961/nubank-e-multado-em-r-65-milhoes-pela-anpd-por-violacaoda-lgpd/ . Acesso em: 27 de maio de 2023.

Portal da ANPD: https://www.gov.br/anpd/pt-br/assuntos/penalidades
Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados): http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

SOARES, L.O**. Comunicação e tecnologia digital: a emergência de um novo campo e o perfil de seus profissionais e áreas**. Brasília: contato, 2018.

TikTok é multado em quase R$ 10 milhões por coletar dados de crianças sem consentimento. Disponível em: https://www.tecmundo.com.br/seguranca/210244-tiktok-multado-r-9-4-milhoes-coletar-dados-criancas-sem-consentimento.htm . Acesso em: 27 de maio de 2023.

VELLOSO, F.C. **Informática: conceitos básicos**. Rio de Janeiro: Elsevier, 2015.

WIMMER, M. **Proteção de dados pessoais: a função e os limites do consentimento**, Cadernos Jurídicos, São Paulo, ano 21, nº53, p.97-115, janeiro-março/2020.

Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), artigo 52. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

ANPD, Autoridade Nacional de Proteção de Dados, disponível em: <https://www.gov.br/anpd/pt-br>, acesso em: 11 de março 2023.

ANPD. Resolução nº 01/2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/resolucoes-e-normas/resolucoes-e-normas/resolucao-no-01-de-29-de-abril-de-2021.pdf. Acesso em: 27 maio 2023.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. São Paulo. Saraiva. 8 ed. 2015. Pág.173.

CONESA,F. Derecho a la intimidad, informática y Estado de Derecho. Valencia: Universidad, 1984, pp.44-45.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Lei geral de proteção de dados pessoais. Salvador. Juspodivm. 2019. Pág. 26.

BRASIL. Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor. Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, DF, 6 jan. 1989. Seção 1, p. 809.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 31 dez. 1940. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 14 de fevereiro de 2023.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, DF, 16 jul. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/L8069.htm>. Acesso em: 19 de abril de 2023.

BRASIL. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, DF, 15 maio 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9279.htm>. Acesso em: 12 de maio de 2023.

BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, DF, 20 fev. 1998.

Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9609.htm>. Acesso em: 19 de abril de 2023.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. São Paulo: Revistas dos Tribunais, 2019.