Revista Multidisciplinar do Nordeste Mineiro, v.03, 2024

ISSN 2178-6925

A IMPORTÂNCIA DA LEI Nº 13.709/2018 E A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

THE IMPORTANCE OF LAW Nº 13.709/2018 AND THE PROTECTION OF PERSONAL DATA IN BRAZIL

Adriana Carvalho Vieira

Graduanda do 7º Período do Curso de Direito do Centro Universitário AlfaUnipac de Teófilo Otoni – MG, Brasil

E-mail: driu.helio@yahoo.com.br

Janaina Ferreira Lopes

Graduanda do 7º Período do Curso de Direito do Centro Universitário AlfaUnipac de Teófilo Otoni – MG, Brasil

E-mail: Janainalopesrodrigues@hotmail.com

.

Igor do Vale Oliveira

Pós-Graduado em Direito e Processo do Trabalho pela Damásio Educacional, Graduado em Direito pela Faculdade Presidente Antônio Carlos de Teófilo Otoni - MG, Advogado e Docente no Curso de Direito na Faculdade AlfaUnipac de Teófilo Otoni - MG, Brasil

E-mail: igorvale.adv@gmail.com

RESUMO

Este estudo abordou a importância da Lei Geral de Proteção de Dados (LGPD) no contexto brasileiro e seu impacto na proteção de dados pessoais no Brasil. O objetivo principal foi analisar a importância da LGPD no que tange a proteção de dados pessoais no Brasil. Para tanto, realizou-se uma revisão bibliográfica, por meio da consulta em livros, artigos e materiais publicados e indexados nas bases de dados da SciELO, CAPES e Google Acadêmico. Os resultados obtidos evidenciaram que a LGPD representou um avanço significativo na proteção de dados pessoais no país, estabelecendo princípios claros e requisitos sólidos para o tratamento responsável dessas informações. No entanto, a efetiva implementação da lei tem enfrentado desafios devido à complexidade das relações entre as partes envolvidas e à falta de clareza na aplicação da legislação. Conclui-se que a LGPD desempenha um papel fundamental na proteção dos direitos fundamentais e dos dados pessoais dos cidadãos brasileiros, especialmente em um contexto de crescente digitalização. No entanto, o pleno sucesso da lei dependerá da superação dos desafios identificados e da conscientização ativa dos cidadãos sobre a importância da proteção de seus dados pessoais. A LGPD representa um marco importante na proteção de dados no Brasil e destaca a necessidade de colaboração entre os setores público e privado para garantir a segurança e privacidade das informações pessoais.

Palavras-chave: LGPD. Dados pessoais. Proteção.

ISSN 2178-6925

ABSTRACT

This study addresses the importance of the General Data Protection Law (LGPD) in the Brazilian context and its impact on the protection of personal data in Brazil. The main objective was to analyze the importance of the LGPD in terms of protecting people in Brazil. To this end, a bibliographical review was carried out, through consultation of books, articles and materials published and indexed in the SciELO, CAPES and Google Scholar databases. The results obtained show that the LGPD represents a significant advance in the protection of people in the country, establishing clear principles and solid requirements for the responsible treatment of information. However, the effective implementation of the law will face challenges due to the complexity of relationships between the parties involved and the lack of clarity in the application of the legislation. It is concluded that the LGPD plays a fundamental role in protecting two fundamental rights and assets of people in Brazilian cities, especially in a context of increasing digitalization. However, the full success of the law will depend on overcoming two identified challenges and actively raising awareness among citizens about the importance of protecting their people. The LGPD represents an important milestone in data protection in Brazil and highlights the need for collaboration between the public and private sectors to guarantee the security and privacy of personal information.

Keywords: LGPD. Personal data. Protection.

1. INTRODUÇÃO

A crescente digitalização da sociedade e a expansão do uso da internet têm transformado drasticamente a forma como os dados pessoais são coletados, armazenados e utilizados. Com essa evolução tecnológica, tornou-se imperativo garantir a proteção e a privacidade das informações dos indivíduos, bem como estabelecer mecanismos legais que regulem a manipulação desses dados.

Nesse contexto, a Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados (LGPD), representa um marco importante no Brasil, conferindo direitos e responsabilidades tanto a indivíduos quanto a empresas que tratam dados pessoais. Esta legislação visa assegurar que os cidadãos tenham controle sobre suas informações pessoais e que as organizações adotem práticas responsáveis de processamento de dados.

Entretanto, a efetiva implementação da LGPD e a conscientização sobre a importância da proteção de dados pessoais no Brasil enfrentam desafios significativos. Diversos incidentes de violação de dados e o compartilhamento inadequado de informações sensíveis ainda ocorrem, levantando questões sobre a capacidade do país em garantir a eficácia da legislação e a proteção dos direitos fundamentais dos cidadãos. Além disso, a complexidade das relações entre as partes envolvidas na gestão de dados pessoais, juntamente com a falta de clareza sobre a aplicação da LGPD, requer uma análise mais aprofundada.

Nesse contexto, torna-se fundamental aprofundar o entendimento sobre a relevância da LGPD e a sua implementação efetiva no Brasil. Este estudo propõe uma análise abrangente das questões relacionadas à proteção de dados pessoais, explorando os desafios e oportunidades que surgem com a entrada em vigor da legislação.

Portanto, o objetivo principal traçado para este estudo foi o de analisar a importância da LGPD no que tange a proteção de dados pessoais no Brasil. No mesmo sentido foram estabelecidos os seguintes objetivos específicos: apresentar os principais conceitos acerca da LGPD; e descrever a punição para vazamentos de dados pessoais no Brasil, sob a perspectiva da LGPD.

Para alcançar esses objetivos, a pesquisa foi conduzida utilizando a metodologia de pesquisa bibliográfica e documental, com uma abordagem descritiva e exploratória de natureza qualitativa. Os recursos utilizados para a realização desta pesquisa incluíram livros, artigos e legislação como fontes de consulta publicados e indexados em bibliotecas físicas e virtuais, além de bases de dados eletrônicos da CAPES, SciELO e Google Acadêmico.

2 O ADVENTO DA LEI Nº 13.709/2018 – A LEI GERAL DE PROTEÇÃO DE DADOS

Segundo Souza (2018), antes da promulgação da Lei Geral de Proteção de Dados (LGPD), o Brasil estava em uma situação de grande vulnerabilidade em termos de regulamentação no que diz respeito à proteção de dados pessoais. No entanto, após vários escândalos de espionagem nos Estados Unidos, tornou-se evidente que o país não estava preparado para lidar com violações de dados pessoais. Embora houvesse avanços na jurisprudência nesse campo, as decisões eram frequentemente contraditórias e careciam de profundidade.

Devido à urgência em abordar a proteção de dados pessoais no país, a LGPD representa uma mudança significativa na proteção da privacidade na sociedade contemporânea, representando um passo fundamental na consolidação dos direitos individuais.

Conforme observado por Pinheiro (2021), a LGPD foi inspirada na Regulação Geral de Proteção de Dados (GDPR), que tem como objetivo principal proporcionar um maior controle sobre a coleta e o tratamento de dados pessoais dos usuários. Ela estabelece diretrizes e normas a serem seguidas, além de aplicar sanções para aqueles

que não as cumpram. A GDPR é aplicada na União Europeia, unificando esse regulamento entre seus 28 Estados-Membros para fortalecer a proteção dos dados e aumentar a eficiência por meio da padronização dos processos e diretrizes.

Mendes (2019) argumenta que a LGPD pressupõe um modelo de proteção de dados que se baseia em previsões, evitando suposições. Esse modelo é subjetivo e leva em consideração a importância dos dados na era da informação, considerando todos os dados como relevantes em certo grau.

Em relação à conceituação e aplicação da LGPD, Maciel (2020, p. 17) fornece uma explicação concisa:

> [...] dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade natural, inclusive por meio digital.

Portanto, é evidente que a LGPD tem como principal objetivo a proteção de dados coletados e processados de maneira a salvaguardar a privacidade de todos os cidadãos, independentemente de serem brasileiros ou estrangeiros, contanto que tais atividades ocorram no território nacional. Ela busca equilibrar a necessidade de lidar com os novos modelos de negócios e contratações que surgiram devido ao avanço tecnológico, ao mesmo tempo em que assegura a segurança dos usuários.

O artigo 2º da LGPD, aborda a importância da consolidação da utilização adequada de dados pessoais:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a 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. (BRASIL, 2018)

Considerando que os dados funcionam como uma representação eletrônica do cidadão no ambiente digital em que estão inseridos, qualquer atividade que envolva a manipulação de dados pessoais pode se tornar uma potencial ameaça aos direitos fundamentais. Essa preocupação fundamental serviu como uma das principais bases para a proteção legal dos dados pessoais sob a perspectiva da Lei Geral de Proteção

ISSN 2178-6925

de Dados (LGPD), que possui uma abrangência horizontal, ou seja, se aplica tanto ao setor econômico quanto ao setor público.

Vale ressaltar a posição de Mendes (2019, p. 02-03) em relação à LGPD:

> Por a LGPD se basear em um conceito amplo de dado pessoal, a princípio todo tratamento de dados – realizado tanto pelo setor público quanto pelo privado – está submetido a ela. Seu âmbito de aplicação abrange também a Internet. As exceções são justificadas de forma particular, seja pelo respaldo em um direito fundamental (por exemplo, a liberdade de informação, no caso da exceção à atividade jornalística) ou no interesse público relevante (como nas exceções à segurança pública e defesa nacional).

Uma novidade significativa na legislação em questão é a exigência de que o tratamento de dados pessoais seja fundamentado em pelo menos uma das bases legais estabelecidas no regulamento. Essas bases legais, de acordo com a síntese fornecida por Barbosa (2021, p. 25-26), são: O consentimento, onde há a autorização livre do uso de seus dados para uma finalidade específica, com total conhecimento de como eles serão utilizados. O Legítimo Interesse, onde os dados poderão ser utilizados para fins legítimos da empresa ou de terceiros, desde que não prejudiquem seus direitos e liberdades; O Cumprimento de Obrigação Legal, onde a empresa precisa tratar seus dados para cumprir leis ou regulamentações. Os dados poderão ainda serem tratados pela Administração Pública, para executar políticas públicas, desde que previsto em lei ou contrato, ou para Estudos e Pesquisas, realizadas através de Entidades públicas e privadas, desde que sigam as regras da LGPD; Ademais, será permitido ainda o uso em face de Execução Contratual, onde os dados são utilizados para cumprir os termos de um contrato firmado com a empresa ou para o Exercício Regular de Direitos, onde os dados podem ser utilizados em processos judiciais, administrativos ou arbitrais.

Além disso, os dados poderão ser utilizados para resguardar o Direito à Vida, à saúde ou a proteção de crédito, podendo ser utilizados para proteger sua vida ou a de terceiros em situações emergenciais, por profissionais de saúde, serviços de saúde ou autoridades sanitárias para realizar procedimentos e garantir sua saúde, sem a necessidade de seu consentimento ou para proteger o crédito em transações financeiras, sem a necessidade de seu consentimento. (BARBOSA, 2021, p. 25-26)

A legitimidade do tratamento de dados pessoais está condicionada à observância de, pelo menos, uma das hipóteses previstas nas disposições do artigo 7 da LGPD. Estas hipóteses estão diretamente relacionadas à necessidade de obter ou não o consentimento do titular dos dados pessoais.

No processo de avaliação da legitimidade do tratamento de dados, é imprescindível considerar os princípios que orientam a LGPD, tais como a boa-fé, a finalidade, o livre acesso, a segurança, a transparência e a qualidade.

A LGPD aborda aspectos contemporâneos e relevantes na proteção de dados em nosso atual contexto social. No que se refere à responsabilidade, a LGPD inova ao estabelecer diversas sanções administrativas em caso de violação de seus preceitos legais. A Autoridade Nacional de Proteção de Dados, com competência nacional na proteção de dados e fiscalização, é responsável por aplicar essas sanções. Elas variam desde advertências até multas e, em casos extremos, a proibição total ou parcial das atividades relacionadas ao tratamento de dados. As multas podem atingir valores consideráveis, variando de 2% do faturamento anual anterior até R$ 50 milhões, além da possibilidade de penalidades diárias.

A LGPD representa um avanço significativo na busca por um sistema eficaz de proteção de dados no Brasil, visando a fortalecer a confiança dos indivíduos na utilização de sites, aplicativos e outras plataformas digitais que dependem da coleta de dados pessoais para seu funcionamento, em um cenário em que a sociedade se encontra cada vez mais imersa no ambiente digital.

Em relação à aplicação da LGPD, ela abrange todas as entidades que realizam o tratamento de dados pessoais, sejam elas de direito público ou privado, pessoas físicas ou jurídicas. A aplicabilidade da lei independe do setor de atuação e da localização da sede da entidade, desde que a operação de tratamento de dados ocorra no território brasileiro e tenha como finalidade a oferta de bens, serviços ou o tratamento de dados de indivíduos localizados no Brasil, conforme disposto no artigo 3º e seus incisos da LGPD.

É importante destacar o princípio da extraterritorialidade da lei, que significa que a LGPD possui alcance internacional. Mesmo que uma organização colete dados pessoais no território brasileiro, mas tenha sua sede em outro país, ela estará sujeita aos termos da LGPD.

Quanto à inaplicabilidade da referida lei, o artigo 4º estabelece as seguintes condições:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

ISSN 2178-6925

> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

É evidente que a LGPD também incorporou restrições em relação à sua aplicabilidade no que se refere aos tipos de dados sujeitos à regulamentação da lei. Conforme observado por Pinheiro (2021), o tratamento de dados pessoais deve estar alinhado com propósitos específicos e funcionais, sem ultrapassar os limites da liberdade de informação e expressão, bem como sem comprometer a soberania, segurança e defesa do Estado. Essas limitações têm como objetivo principal reforçar a segurança em questões críticas para a sociedade.

Essas restrições têm como finalidade estabelecer um equilíbrio entre a proteção da privacidade individual e a segurança pública. Isso significa que essas limitações buscam ser benéficas tanto para os indivíduos, que não devem ter seus dados pessoais divulgados sem seu consentimento, quanto para o Estado, no que diz respeito à manutenção da ordem pública e da segurança para toda a sociedade.

Além disso, é importante ressaltar que a LGPD não se limita apenas aos casos relacionados à busca de produtos ou contratação de serviços, mas se aplica a todas as situações que envolvem a coleta e o tratamento de dados pessoais. Isso ocorre porque a natureza da LGPD visa, em essência, proteger os dados pessoais coletados, independentemente do contexto específico em que são utilizados.

3 A PUNIÇÃO DA VIOLAÇÃO DE DIREITOS E A SUBTRAÇÃO DE DADOS PESSOAS EM MEIOS ELETRÔNICOS

Os direitos de personalidade estão sujeitos a crescentes violações no ambiente digital. A internet se tornou um cenário onde uma variedade de delitos pode ser cometida, resultando na violação de direitos fundamentais. Esses atos podem ser perpetrados por uma ampla gama de agentes, incluindo pessoas jurídicas, indivíduos e até mesmo o próprio Estado. Portanto, é essencial examinar as diferentes formas de violação que ocorrem nesse contexto, bem como as sanções correspondentes.

ISSN 2178-6925

3.1 A SUBTRAÇÃO DE DADOS PESSOAS E A VIOLAÇÃO DE DIREITOS EM MEIO ELETRÔNICOS POR PARTE DO ESTADO

Embora seja o dever do Estado garantir os direitos fundamentais de todos os cidadãos, coibindo e punindo atos contrários a esses direitos, em alguns casos, o próprio Estado se mostra como um violador desses direitos. (MIRAGAIA; BELMUDES, 2008)

Um exemplo notório de violação de direitos fundamentais por meio da apropriação de dados pessoais são os casos de espionagem eletrônica. Em 2013, Edward Snowden, um analista de sistemas norte-americano e ex-administrador de sistemas da Central Intelligence Agency (CIA) e da National Security Agency (NSA), revelou documentos confidenciais que indicavam que essas agências estavam utilizando a internet para espionar informações pertencentes a pessoas físicas e jurídicas (PORTAL G1, 2013). Essas atividades de espionagem eram realizadas por meio de um programa de computador que concedia à NSA acesso a e-mails, mensagens de texto, salas de chat de serviços como Facebook, Google, Microsoft, Apple e outros, em colaboração com uma empresa de telecomunicações dos EUA que também tinha parcerias com o Brasil e outras empresas do setor. (PORTAL G1, 2013)

No Brasil, um caso semelhante envolveu servidores da Agência Brasileira de Inteligência (ABIN) e ficou conhecido como Operação Satiagraha. Essa operação investigou corrupção e lavagem de dinheiro envolvendo banqueiros e executivos, com destaque para Daniel Dantas, proprietário do Banco Opportunity, que foi preso em 2008 (CONJUR, 2015). Durante a investigação de Dantas, chefiada por Protógenes Queiroz, ocorreu outra série de ilegalidades, incluindo a contratação de um investigador particular para obter informações sobre atividades clandestinas da ABIN. Essas atividades clandestinas envolviam a manipulação de informações confidenciais, monitoramento de e-mails por escritórios jurídicos, acesso ilegal a discos rígidos, obtenção de fotos e filmagens sem consentimento. (CONJUR, 2015)

É notável que, embora o Estado deva ser o principal defensor dos direitos fundamentais dos cidadãos, ele próprio, por meio de seus agentes, pode violá-los, prejudicando a honra, a privacidade e a intimidade de seus próprios cidadãos.

As sanções para tais casos foram aplicadas de acordo com as leis de cada nação, e essas questões repercutiram internacionalmente, levando à criação de várias normas para proteção de dados pessoais no ambiente digital. No Brasil, foi instaurada a Comissão de Investigação Parlamentar (CPI), conhecida como a "CPI da

Espionagem," que durou sete meses. O relatório final produzido pela CPI apontou a necessidade de implementar legislação que regulasse áreas de inteligência, a fim de garantir segurança jurídica à sociedade em relação aos dados pessoais na internet.

Em âmbito internacional, países como China, Rússia, Irã e nações africanas e do Oriente Médio propuseram à Organização das Nações Unidas a responsabilidade pela governança no ambiente digital, desencadeando um esforço global para promulgar leis e regulamentações para o uso de dados pessoais pelo Estado no meio digital. (SIMON, 2014)

O Superior Tribunal de Justiça reconheceu, no Habeas Corpus impetrado por Daniel Dantas, que o Estado, representado por Protógenes Queiroz, atuou como violador de um direito fundamental ao coletar informações de forma clandestina. O caso culminou com a subsequente prisão de Dantas e aproximadamente 15 outros indivíduos, além da condenação de Protógenes Queiroz por violação de sigilo profissional e fraude processual, bem como seu afastamento das investigações e demissão de seu cargo de delegado. (SIMON, 2014)

3.2 A SUBTRAÇÃO DE DADOS PESSOAS E A VIOLAÇÃO DE DIREITOS EM MEIO ELETRÔNICOS POR PARTE DE PESSOAS JURÍDICAS

As pessoas jurídicas de interesse para esta discussão englobam associações, sociedades e fundações, sejam elas com ou sem fins lucrativos. Com a expansão da internet e a crescente adoção de modelos de consumo digital, as pessoas jurídicas passaram a ter um papel cada vez mais proeminente no cenário online. No entanto, essa evolução digital também trouxe consigo desafios, visto que casos frequentes de compartilhamento não autorizado de dados pessoais na internet começaram a surgir.

Um exemplo notório envolve a violação de direitos fundamentais relacionada à divulgação de informações provenientes de órgãos de proteção ao crédito, como a Serasa Experian e o SPC. Essas empresas mantêm extensos registros dos cidadãos, contendo informações como nomes, números de documentos de identificação, renda, gênero, dados bancários, e muito mais. O vazamento de tais informações nas mãos erradas facilita ações fraudulentas. Em resposta a relatos crescentes de fraudes ligadas a esses dados, os termos de uso foram revisados, permitindo a divulgação apenas de informações relacionadas a registros negativos e inadimplência. O diretor do Procon do Estado de São Paulo chegou a afirmar, em 2012, que a consulta ao SCPC e ao Serasa

constituía uma violação da Constituição Federal, expondo os cidadãos a riscos de violações de privacidade, honra, imagem e intimidade. (LUZ, 2012)

Outro caso de destaque, a nível mundial, envolveu o armazenamento inadequado de dados bancários dos usuários pelo Google, por meio do aplicativo Google Wallet. A juíza que presidiu o caso determinou que o Google violou sua política de privacidade, uma vez que, ao acessar a loja virtual de aplicativos, automaticamente transferia os dados pessoais dos usuários para desenvolvedores de outros aplicativos. Essa exposição facilitada de dados pessoais colocou em risco a ocorrência de futros casos de roubo de identidade. (CONVERGÊNCIA DIGITAL, 2015)

Em 2011, a empresa Facebook enfrentou pressões do governo irlandês para reforçar os serviços de proteção de privacidade dos usuários, após acusações do governo australiano de que a rede social estava rastreando os usuários. Alegava-se que o uso do botão "Curtir" permitia tal rastreamento. A empresa negou essa possibilidade e aumentou as medidas de segurança para o armazenamento dos dados pessoais dos usuários. (BARROS, 2011)

Está claro que os cidadãos se encontram vulneráveis ao fornecerem dados pessoais para redes sociais, aplicativos e sites. No entanto, a questão da responsabilização penal de pessoas jurídicas em casos de violação de direitos fundamentais é complexa. A exceção à responsabilização penal de pessoas jurídicas ocorre nos casos de violações ambientais, onde a punição abrange as esferas administrativa, civil e penal, sem excluir a responsabilidade das pessoas físicas envolvidas como autores, coautores ou partícipes. (CORREA, 2013)

Sobre essa questão, Gonçalves (2018, p. 10-11) oferece a seguinte perspectiva:

> No Brasil, existem três correntes diversas quando tratado deste tema: na primeira, os argumentos são em torno de que a pessoa jurídica não pode praticar determinada conduta criminosa porquê não possui consciência e, tão pouco sabe discernir quão ilícito é a conduta praticada e, sua punição geraria uma responsabilidade penal objetiva, visto que ela não possui culpa, portanto uma pessoa jurídica nunca entenderia a finalidade e a gravidade de uma pena. Numa segunda corrente, o STJ entende que a pessoa jurídica pode ser passível de punição, desde que seja denunciada em conjunto com a pessoa física. Em uma terceira corrente, o STF asseverou que a pessoa jurídica poderá ser penalizada criminalmente independentemente de estar vinculada a uma pessoa física, ou seja, sem uma pessoa física concreta, pois haveria certa dificuldade na identificação do sujeito para ser responsabilizado o ilícito.

É evidente que a sanção destinada às pessoas jurídicas deve ser administrativa, uma vez que o domínio penal é voltado para a responsabilização das pessoas físicas, devido às complexidades inerentes à jurisdição penal. No entanto, é importante notar

ISSN 2178-6925

que a LGPD aborda a imposição de penalidades para as infrações cometidas, as quais também se estendem às pessoas jurídicas.

Neste sentido, o art. 52 da LGPD estabelece uma série de medidas para garantir a segurança e o uso adequado de seus dados pessoais. Caso as empresas ou órgãos públicos não sigam essas regras, podem ser penalizadas pela Autoridade Nacional de Proteção de Dados (ANPD) com as seguintes sanções: Advertência, onde a empresa ou órgão público recebe um aviso por escrito, com um prazo para corrigir o problema. Além disso, pode haver a aplicação de Multa de até 2% do faturamento anual da empresa, limitada a R$ 50 milhões, além de aplicação de Multa diária

A ANPD poderá, nos termos do art. 52 da LGPD, inciso IV, divulgar a infração no seu site e em outros canais de comunicação, bloqueio dos dados pessoais envolvidos na infração pode ser bloqueados até que o problema seja corrigido, ou eliminar os dados pessoais envolvidos na infração podem ser excluídos definitivamente. Ademais, poderá haver ainda a suspensão parcial do banco de dados, onde os dados pessoais estão armazenados pode ser suspenso por até 6 meses, podendo ser prorrogado por mais 6 meses. A empresa ou órgão público pode ser proibido de tratar os dados pessoais por até 6 meses, podendo ser prorrogado por mais 6 meses ou até mesmo de forma definitiva.

Assim, dada a complexidade de aplicar sanções penais às pessoas jurídicas, é compreensível que essa abordagem seja considerada como uma medida de último recurso nesses cenários.

2.3 A SUBTRAÇÃO DE DADOS PESSOAS E A VIOLAÇÃO DE DIREITOS EM MEIO ELETRÔNICOS POR PARTE DE PESSOAS FÍSICAS

A pessoa física frequentemente figura como uma das principais perpetradoras de violações de direitos fundamentais e da prática de crimes envolvendo dados pessoais. Tais condutas ilícitas resultam na violação de aspectos como a honra, liberdade, intimidade e, em alguns casos, no patrimônio, abrangendo uma ampla variedade de delitos, conforme mencionado anteriormente neste estudo.

Um dos primeiros casos notórios de violação de direitos fundamentais no contexto digital no Brasil remonta a 1997 e envolveu a apresentadora de TV Maria Cristina Poli, que foi vítima de assédio por um analista de sistemas que descreveu cenas

de sexo que desejava praticar com ela. Graças ao rastreamento do provedor de internet, o agressor foi identificado e punido. (DA COSTA, 2011)

Com a expansão das redes sociais, houve um aumento significativo na prática de crimes contra a honra, imagem e intimidade das pessoas. No Twitter, por exemplo, hashtags frequentemente são usadas de maneira indevida, resultando em ataques contra indivíduos. Em 2010, durante a Copa do Mundo, a hashtag "Cala boca Galvão" rapidamente se espalhou pela internet, difamando o locutor de futebol Galvão Bueno. (DA COSTA, 2011)

O anonimato na internet também tem sido objeto de debate, com aplicativos como o Secret, que permitiam a publicação anônima de mensagens e imagens. Em 2014, decisões judiciais determinaram a remoção do aplicativo de lojas virtuais e a proibição de seu uso, com base na Constituição, que permite a liberdade de expressão e pensamento desde que não haja anonimato. A exposição de imagens de terceiros sem consentimento foi vista como uma violação da privacidade e intimidade. (GONZAGA, 2014)

Além dos crimes contra a intimidade e privacidade, a expansão da internet levou a um aumento nos crimes contra o patrimônio, à medida que mais transações ocorrem online. Isso resultou em casos frequentes de envio de mensagens e e-mails fraudulentos, oferecendo promoções falsas, negativações e bloqueios. Essas táticas enganosas levaram indivíduos a compartilhar informações de contas bancárias e cartões de crédito. (DA COSTA, 2011)

Os crimes sexuais também proliferaram, especialmente relacionados à divulgação não autorizada de imagens e vídeos, muitas vezes envolvendo menores, configurando delitos já tipificados na legislação penal.

Conforme mencionado anteriormente, a violação de direitos, princípios e garantias encontra respaldo na Constituição Federal e em legislações específicas. No contexto da pessoa física cometendo crimes envolvendo a apropriação indevida de dados pessoais na internet, muitos dos delitos mais comuns já são devidamente abordados pela legislação penal, garantindo a aplicação de penas correspondentes a cada caso.

É crucial destacar que a punição de qualquer crime deve estar em estrita conformidade com o princípio da legalidade, como estabelecido no artigo 5º, inciso XXXIX, da Constituição Federal, que determina que não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Portanto, mesmo que uma conduta seja

imoral ou prejudicial, o infrator somente deve ser punido quando houver previsão legal que aborde tal comportamento.

Portanto, percebe-se que apesar das inovações no âmbito da proteção de dados pessoais no meio eletrônico, fica evidente que o Estado ainda enfrenta desafios significativos nessa área, demandando aprimoramentos, especialmente no que diz respeito à criação de órgãos mais eficazes para fiscalizar as atividades relacionadas ao compartilhamento e armazenamento de dados pessoais. Isso se alinha com a obrigação do Estado de salvaguardar os direitos de seus cidadãos, essencial para a manutenção dos princípios democráticos.

CONSIDERAÇÕES FINAIS

O presente estudo teve como foco a análise da importância da LGPD enquanto ferramenta na proteção de dados pessoais em meio eletrônico no Brasil. Para atingir esse propósito, foram investigados os principais conceitos e o advento da LGPD, as principais disposições da lei e as principais sanções quando da violação de direitos e vazamento de dados pessoais pelo Estado, pessoas jurídicas e pessoas físicas.

Os resultados obtidos demonstram que a LGPD representa um marco fundamental na legislação brasileira no que tange à proteção de dados pessoais. Essa legislação estabeleceu princípios sólidos e requisitos claros para o tratamento responsável das informações pessoais, proporcionando aos cidadãos maior controle sobre seus dados e incentivando práticas éticas por parte das organizações.

Contudo, a efetiva implementação da LGPD enfrenta desafios significativos, decorrentes da complexidade das relações entre as partes envolvidas na gestão de dados pessoais e da falta de clareza na interpretação e aplicação da lei. Incidentes de violação de dados pessoais ainda ocorrem, questionando a capacidade do Brasil em assegurar a eficácia da legislação.

Conclui-se que a LGPD desempenha um papel crucial na proteção dos direitos fundamentais dos cidadãos brasileiros, particularmente em um ambiente de crescente digitalização e uso da internet. No entanto, para que a lei alcance seu pleno potencial, é essencial superar os desafios identificados e garantir uma aplicação rigorosa das sanções em caso de violações. Além disso, é importante promover a conscientização dos cidadãos sobre a importância da proteção de seus dados pessoais e seus direitos relacionados a essas informações.

A LGPD representa um avanço significativo na proteção de dados no Brasil e, para garantir seu sucesso, é fundamental a colaboração entre os setores público e privado, bem como a participação ativa dos cidadãos na defesa de seus direitos de privacidade e segurança de dados.

REFERÊNCIAS

BARBOSA, Igor Gabriell Siqueira. **A proteção de dados pessoais como um direito fundamental à luz da Constituição Federal de 1988**. 43f. 2021. Monografia (Bacharelado em Direito), Pontifícia Universidade Católica de Goiás, Escola de Direito e Relações Internacionais, Goiânia, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1474/1/TCC%20II%20-%20TURMA%20B12%20-%20IGOR%20GABRIELL%20-%20ARTIGO-2021-1%29.pdf. Acesso em: 01 ago. 2023.

BARROS, Thiago. **Facebook diz que não há violação de segurança ou privacidade de dados dos usuários**. 2011. Disponível em: https://www.techtudo.com.br/noticias/noticia/2011/09/facebook-confirma-que-botao-curtir-repassa-dados-dos-usuarios-e-promete-correcao-dos-cookies.html. Acesso em: 31 ago. 2023.

CONJUR. Protógenes Queiroz é demitido da PF por uso indevido do cargo. **Revista Consultor Jurídico**, 14 de outubro de 2015. Disponível em: https://www.conjur.com.br/2015-out-14/protogenes-queiroz-demitido-pf-uso-indevido-cargo. Acesso em: 02 set. 2023.

CONVERGÊNCIA DIGITAL. **Justiça não poupa Google e mantém processo por venda de dados pessoais**. 2015. Disponível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=39306&sid=17#.VSKAPfzF_EU. Acesso em: 31 ago. 2023.

DA COSTA, Fernando José**. Locus delicti nos crimes informáticos**. 2011. 355f. Tese (Doutorado em Direito Penal) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/pt-br.php. Acesso em: 02 set. 2023.

GONÇALVES, Andressa Ferraz. Análise dos Direitos Fundamentais no Âmbito Digital e a Punição Estatal. In: **Revista Aporia Jurídica**, vol. I, p. 8-25, 2018. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiT-5O565LyAhWtILkGHfYODgIQFjAAegQIAxAD&url=http%3A%2F%2Fcescage.com.br%2Frevistas%2Findex.php%2Faporiajuridica%2Farticle%2Fdownload%2F136%2F135&usg=AOvVaw3c3aI-iAPUgrxVzd-bZmIo. Acesso em: 01 set. 2023.

GONZAGA, Yuri. **Justiça suspende decisão de remover Secret no Brasil após pedido do Google**. Folha de São Paulo, 2014. Disponível em: https://m.folha.uol.com.br/tec/2014/09/1515215-justica-suspende-decisao-de-remover-secret-no-brasil-apos-pedido-do-google.shtml. Acesso em: 30 set. 2023.

LUZ, Saulo. **ESTADÃO:** Cuidado, seus dados pessoais estão à venda. São Paulo, fev. 2012. Disponível em: https://www.estadao.com.br/blogs/jt-seu-bolso/2012/02/12/cuidado-seus-dados-pessoais-estao-a-venda/. Acesso em: 30 set. 2023.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)**. 2. ed. Goiânia: RM Digital Education, 2020.

MENDES, Laura Schertel. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. **Panorama setorial da Internet**, Brasília, n. 2, jun. 2019.

ISSN 2178-6925

MIRAGAIA, Bruno Ricardo; BELMUDES, Eduardo. Com o dever de proteger direitos humanos, Estado é o maior violador. **Consultor Jurídico**, São Paulo, 2008. Disponível em: https://www.conjur.com.br/2008-dez-26/estado_maior_violador_direitos_humanos. Acesso em: 30 ago. 2023.

PINHEIRO, Patrícia P. **Proteção de Dados Pessoais:** comentários à lei n. 13.709/2018 (LGPD). São Paulo: Editora Saraiva, 2021.

PORTAL G1. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA**. 2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 30 set. 2023.

SIMON, Joel. **Como a espionagem dos Estados Unidos fortalece o controle da China**. Committee to Protect Journalists, 2014. Disponível em: https://cpj.org/pt/2014/02/ataque-a-imprensa-em-2013-como-a-espionagem/. Acesso em: 30 set. 2023.

SOUZA, Luíza Ribeiro De Menezes. Proteção de Dados Pessoais: Estudo Comparado do Regulamento 2016/679 do Parlamento Europeu e Conselho e o Projeto de Lei Brasileiro N. 5.276/2016. **Caderno Virtual**, v. 1, n. 41, 2018.