IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NA PRIVACIDADE DO CONSUMIDOR E A ADEQUAÇÃO DAS EMPRESAS

IMPACTS OF THE GENERAL DATA PROTECTION LAW (LGPD) ON CONSUMER PRIVACY AND THE SUITABILITY OF COMPANIES

Lucas Vinicius Martines[1]

Resumo: O estudo trata sobre os impactos das empresas e dos consumidores perante a chegada da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, que entrou em vigor em setembro de 2020 e estabeleceu novas regras para o tratamento de dados pessoais por empresas e entidades públicas. O objetivo da LGPD é proteger a privacidade dos cidadãos e garantir que seus dados pessoais sejam tratados de forma adequada e segura, equilibrando os interesses das empresas com o direito fundamental à privacidade. A LGPD estabelece os direitos dos titulares dos dados, incluindo o direito de acesso, correção, exclusão e portabilidade dos dados. A lei prevê sanções para empresas que violam suas disposições, incluindo multas, advertências e suspensão do tratamento de dados pessoais. A proteção da privacidade é essencial para a preservação da dignidade humana e da autonomia individual, valores fundamentais da democracia.
Palavras-chave: LGPD. Privacidade. Consumidor. Proteção. Empresas.

Abstract: The study examines the impacts of companies and consumers regarding the arrival of the General Data Protection Law (LGPD) in Brazil, which came into effect in September 2020 and established new rules for the processing of personal data by companies and public entities. The objective of the LGPD is to protect citizens' privacy and ensure that their personal data is handled appropriately and securely, balancing the interests of companies with the fundamental right to privacy. The LGPD establishes the rights of data subjects, including the right of access, correction, deletion, and portability of data. The law provides sanctions for companies that violate its provisions, including fines, warnings, and suspension of the processing of personal data. Privacy protection is essential for the preservation of human dignity and individual autonomy, fundamental values of democracy.
Keywords: LGPD. Privacy. Consumer. Protection. Companies.

1 INTRODUÇÃO

O objetivo deste estudo é apresentara LGPD e destacar a sua importância para a proteção da privacidade dos cidadãos brasileiros, também enfatizar a importância da privacidade como um direito fundamental e essencial para a preservação da dignidade humana e da autonomia individual, valores fundamentais

[1] Orientadora: Prof. Ma. Thaís Fernanda Botelho.

da democracia. Este é um artigo bibliográfico realizado no ano de 2023, trazendo informações de publicações acadêmicas dos últimos 10 anos, afim de melhor compreender as questões aqui levantadas.

Para o direito, uma empresa é uma entidade que exerce atividades econômicas com o objetivo de produzir bens ou prestar serviços em troca de lucro. É uma entidade jurídica que tem personalidade própria, separada da de seus proprietários, e que pode ser responsabilizada por seus atos e obrigações.No Brasil, a definição legal de empresa está prevista no Código Civil, em seu artigo 966 (BRASIL, 2002, art. 966).Já o consumidor, para o direito, é toda pessoa física ou jurídica que adquire ou utiliza produtos ou serviços como destinatário final. No Brasil, a definição de consumidor e suas relações com fornecedores estão previstas no Código de Defesa do Consumidor (CDC), Lei nº 8.078/1990 no artigo. 2º da lei (BRASIL, 1990).

Não há um número exato de países que possuem legislações de proteção de dados pessoais em todo o mundo, pois isso está em constante evolução e muitos países estão em processo de implementação de novas leis ou atualização de leis existentes. No entanto, segundo dados de 2021, da Organização para a Cooperação e Desenvolvimento Econômico (OCDE)mais de 130 países possuem alguma forma de lei ou regulamentação de proteção de dados pessoais. ("Em que pé estão as leis de proteção de dados no mundo?", 2021) Alguns exemplos incluem: União Europeia: Regulamento Geral sobre a Proteção de Dados (GDPR);Estados Unidos: Lei de Privacidade do Consumidor da Califórnia (CCPA);Canadá: Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA);Argentina: Lei de Proteção de Dados Pessoais (Ley de Protección de Datos Personales); Japão: Lei de Proteção de Informações Pessoais (Actonthe Protectionof PersonalInformation);Austrália: Lei de Privacidade (PrivacyAct).

De acordo com Danilo Doneda, especialista em Direito Digital e Proteção de Dados, a LGPD representa um marco importante na história da proteção de dados no Brasil e coloca o país em sintonia com os padrões internacionais de proteção de dados pessoais (DONEDA, 2020). Esta lei representa uma importante conquista para os cidadãos brasileiros, que passam a ter mais controle sobre seus dados pessoais e mais garantias em relação ao seu tratamento pelas empresas (ALVES e SILVA, 2020, p. 40).

Um dos principais objetivos da LGPD é proteger a privacidade dos cidadãos e garantir que seus dados pessoais sejam tratados de forma adequada e segura. Conforme afirma Bruno Bioni, professor de Direito Digital e Proteção de Dados na FGV Direito SP, a LGPD foi criada para equilibrar os interesses das empresas que tratam dados pessoais com o direito fundamental à privacidade dos cidadãos (BIONI, 2021).

A privacidade é um direito fundamental reconhecido internacionalmente, que garante o controle sobre as informações pessoais e a proteção contra a sua divulgação não autorizada. Sendo reconhecido pela Constituição Federal brasileira de 1988 e por diversos tratados internacionais de direitos humanos. Segundo Fabrício da Mota Alves e Fernanda Marques da Silva, professores de Direito na Universidade de Brasília, "a proteção da privacidade é essencial para a preservação da dignidade humana e da autonomia individual, valores fundamentais da democracia" (ALVES e SILVA, 2020, p. 37).

De fato, a LGPD está relacionada à proteção de direitos fundamentais, não sendo considerada um direito fundamental pois a LGPD tem caráter infraconstitucional, ou seja, está abaixo da Constituição Federal na hierarquia das normas jurídicas. Porém com a chegada da emenda constitucional nº115, de 10 de fevereiro de 2022, a tornou uma garantia fundamental no artigo 5, inciso LXXIX da Constituição Federal do Brasil de 1988.

No contexto atual, em que a coleta e o tratamento de dados pessoais se tornaram cada vez mais comuns e abrangentes, a proteção da privacidade se tornou ainda mais relevante. “A privacidade é uma necessidade básica das pessoas e está intrinsecamente relacionada com a sua segurança e bem-estar" (DONEDA, 2020, p. 20).Além de estabelecer regras para o tratamento de dados pessoais, a LGPD também prevê sanções para empresas que violam suas disposições. Isso inclui multas, advertências e até mesmo a suspensão do tratamento de dados pessoais pela empresa infratora. Vale ressaltar que a criação da Autoridade Nacional de Proteção de Dados (ANPD) aumenta a eficácia da LGPD na fiscalização e aplicação das sanções.

2 IMPACTOS DA LGPD NA PRIVACIDADE DA CONSUMIDOR

A entrada em vigor da LGPD trouxe diversos impactos para a privacidade e segurança dos dados pessoais dos consumidores brasileiros. Segundo pesquisa realizada pela Confederação Nacional da Indústria (CNI), cerca de 91% das empresas afirmam ter implementado mudanças em suas políticas de privacidade em decorrência da LGPD (CNI, 2021).

As empresas que tratam dados pessoais dos consumidores agora têm obrigações e responsabilidades específicas em relação à proteção desses dados. De acordo com Alves e Silva, “As empresas devem informar aos titulares dos dados sobre as finalidades do tratamento, os tipos de dados coletados, a forma de armazenamento e compartilhamento, entre outras informações relevantes” (ALVES e SILVA, 2020).

Conforme explica Doneda (2020) a LGPD garante aos titulares dos dados o direito de acessar, corrigir, excluir e portar seus dados pessoais, o que significa mais controle sobre suas informações sendo que os principais impactos da LGPD na privacidade do consumidor estão em seus princípios.

3 PRINCÍPIOS E FUNDAMENTOS DA LGPD E A PROTEÇÃO DA PRIVACIDADE DOS CONSUMIDORES

A Lei Geral de Proteção de Dados (LGPD) estabelece uma série de princípios que devem ser observados no tratamento de dados pessoais. Esses princípios são fundamentais para garantir a proteção dos dados pessoais e a privacidade dos titulares desses dados. Os princípios estabelecidos pela LGPD estão em seu no artigo 6º. Como afirma Bioni (2021) a LGPD estabelece princípios como a finalidade, adequação, necessidade, transparência e segurança, que devem nortear o tratamento de dados pessoais pelas empresas. Os princípios e fundamentos estabelecidos pela LGPD são fundamentais para garantir a proteção da privacidade dos consumidores.

Princípio da finalidade

Estabelece que os dados pessoais só podem ser coletados e tratados para fins específicos e legítimos. A finalidade do tratamento é uma das principais limitações impostas pela LGPD, pois garante que as empresas não usem os dados pessoais para fins não autorizados ou não informados aos titulares (DONEDA, 2020).

Princípio da adequação e da necessidade

Estão relacionados em estabelecer que o tratamento de dados pessoais deve ser adequado, relevante e limitado ao mínimo necessário para a finalidade que se propõe. Isso significa que a empresa ou organização responsável pelo tratamento de dados pessoais deve definir claramente a finalidade para a qual os dados serão utilizados e garantir que o tratamento desses dados seja adequado e relevante para essa finalidade. Estes Princípios evitam o tratamento excessivo ou inadequado de informações sensíveis e contribuindo para a transparência e confiança nas relações entre empresas e consumidores.

Princípio do livre acesso

Estabelece que o titular dos dados tem o direito de obter do controlador, em relação aos seus dados pessoais, informações claras, precisas e facilmente acessíveis sobre a existência de tratamento, a forma como foram coletados, a finalidade do tratamento, os dados pessoais tratados, os destinatários ou categorias de destinatários dos dados, a possibilidade de compartilhamento dos dados, a existência de tratamento automatizado, o prazo de conservação dos dados e a identificação do controlador. Com o livre acesso, o titular dos dados pode monitorar o tratamento de seus dados pessoais e verificar se as empresas ou organizações estão cumprindo as obrigações previstas na LGPD. Permite que as pessoas possam tomar decisões informadas sobre como suas informações pessoais são tratadas e como podem ser utilizadas.

Princípio da qualidade dos dados

Tem como objetivo garantir a exatidão e a integridade das informações pessoais, além de evitar que dados incorretos, incompletos ou desatualizados sejam tratados. Dessa forma, as empresas e organizações que tratam dados pessoais devem adotar medidas para garantir que as informações coletadas sejam precisas e atualizadas, e que sejam mantidas dessa forma ao longo do tempo. A qualidade dos dados é importante para garantir a proteção dos direitos dos titulares dos dados, pois informações imprecisas ou desatualizadas podem afetar negativamente a sua privacidade e os seus direitos. A qualidade dos dados é fundamental para a tomada de decisões empresariais, pois a utilização de informações incorretas ou incompletas pode prejudicar a eficácia das decisões tomadas e até mesmo causar prejuízos financeiros. Para garantir a qualidade dos dados, as empresas e

organizações devem implementar medidas de controle de qualidade e realizar periodicamente verificações e atualizações dos dados coletados, além de garantir a veracidade e a correção das informações obtidas. A LGPD estabelece que os titulares dos dados têm o direito de solicitar a correção, atualização ou eliminação dos seus dados pessoais que não estejam corretos ou que não estejam atualizados.

Princípio da transparência

Estabelece que os titulares dos dados devem ser informados de forma clara e acessível sobre a coleta, o tratamento, o armazenamento e o compartilhamento dos seus dados pessoais. Isso significa que as empresas e organizações que tratam dados pessoais devem ser transparentes em relação às suas práticas de proteção de dados, tornando as informações acessíveis e compreensíveis aos titulares dos dados. Conforme destaca Bioni, "a transparência é um princípio fundamental para a confiança dos consumidores nas empresas que tratam seus dados pessoais" (BIONI, 2021, p. 27) o que ajuda a contribuir para a construção de relacionamentos de confiança. Além disso, a transparência pode ajudar as empresas e organizações a construir uma imagem positiva perante o público, demonstrando que estão comprometidas com a proteção dos direitos dos titulares dos dados. Para garantir a transparência, as empresas e organizações devem implementar medidas para garantir a divulgação clara e acessível das informações sobre a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais, utilizando linguagem simples e compreensível para os titulares dos dados.

Princípio da segurança

É um dos pilares fundamentais da LGPD também é essencial para a proteção da privacidade dos consumidores e estabelece que as empresas e organizações que coletam e tratam dados pessoais devem implementar medidas de segurança adequadas para garantir a proteção desses dados contra acessos não autorizados, uso indevido, perda, alteração ou destruição No entendimento de Alves e Silva (2020) .O princípio da segurança exige que as empresas e organizações avaliem os riscos associados ao tratamento de dados pessoais e implementem medidas técnicas e organizacionais adequadas para proteger esses dados contra ameaças internas e externas. As medidas de segurança podem incluir criptografia de dados, controle de acesso, monitoramento de atividades, backups regulares, políticas de senha, treinamento de funcionários e outras ações que visem garantir a

confidencialidade, integridade e disponibilidade dos dados pessoais. As medidas de segurança adotadas pelas empresas e organizações devem ser proporcionais aos riscos envolvidos no tratamento de dados pessoais. Por exemplo, uma empresa que trata dados sensíveis, como informações médicas ou financeiras, deve implementar medidas de segurança mais rigorosas do que uma empresa que coleta apenas dados básicos de contato. As empresas e organizações devem monitorar continuamente suas medidas de segurança e realizem auditorias regulares para identificar e corrigir falhas de segurança.

É importante ressaltar que o princípio da segurança é uma obrigação não apenas das empresas e organizações que coletam e tratam dados pessoais, mas também de seus fornecedores de serviços e terceiros que possam ter acesso a esses dados.

Princípio da não discriminação

Estabelece que o tratamento de dados pessoais deve ser realizado sem qualquer tipo de discriminação, direta ou indireta, com base em raça, etnia, cor, religião, orientação sexual, identidade de gênero, idade, deficiência, entre outros. Isso significa que as empresas e organizações que coletam e tratam dados pessoais devem tratar todos os titulares de dados de forma igualitária, sem fazer distinção ou discriminação com base em características pessoais ou sensíveis. A LGPD proíbe ainda o tratamento de dados pessoais sensíveis com o objetivo de obter vantagem econômica, sem o consentimento do titular dos dados ou sem uma base legal específica. Isso significa que as empresas e organizações não podem tratar dados pessoais sensíveis, como informações sobre saúde, orientação sexual ou crenças religiosas, de forma discriminatória ou para fins comerciais sem uma base legal adequada.

Além desses princípios, a LGPD estabelece fundamentos importantes para a proteção da privacidade dos consumidores, como o consentimento, a necessidade do tratamento para o cumprimento de obrigação legal e a tutela da saúde e da vida do titular ou de terceiros. Como ressalta Doneda (2020) os fundamentos da LGPD visam garantir que o tratamento de dados pessoais seja adequado e necessário, e que os titulares dos dados tenham seus direitos protegidos.

Assim os princípios e fundamentos estabelecidos pela LGPD são fundamentais para garantir a proteção da privacidade dos consumidores e

estabelecer limites claros para o tratamento de dados pessoais pelas empresas e entidades públicas. Sua implementação adequada pode contribuir para a construção de uma sociedade mais justa e democrática, em que a privacidade e a segurança dos dados pessoais são respeitadas e protegidas (DONEDA, 2020).

A base legal para o tratamento de dados pessoais está prevista em seu artigo 7º. Esse artigo lista as dez hipóteses legais para o tratamento de dados pessoais, sendo elas: Consentimento do titular; Cumprimento de obrigação legal ou regulatória pelo controlador; Execução de políticas públicas; Estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular; Exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);Proteção da vida ou da incolumidade física do titular ou de terceiros; Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; Interesse legítimo do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A base legal da LGPD é o fundamento jurídico que autoriza o tratamento de dados pessoais, enquanto os princípios são as orientações gerais que devem ser seguidas pelas organizações no tratamento de dados pessoais. Ambos são importantes e devem ser observados para garantir a conformidade com a LGPD.

4 DIREITOS DOS TITULARES DOS DADOS PREVISTOS NA LGPD

A Lei Geral de Proteção de Dados garante uma série de direitos aos titulares dos dados pessoais, com o objetivo de assegurar o controle e a transparência no tratamento dessas informações pelas empresas. Um desses direitos é o acesso aos dados, conforme estabelecido no artigo 18 da LGPD (BRASIL,2018). Segundo Lopes (2021), os titulares dos dados têm o direito de obter informações claras e completas sobre o tratamento de seus dados pessoais pelas empresas, incluindo a finalidade do tratamento, a forma de coleta e as medidas de segurança adotadas.

Além disso, a LGPD prevê o direito de retificação e correção dos dados pessoais. De acordo com Azevedo e Mourão (2020), os titulares dos dados têm o direito de solicitar a correção, atualização ou exclusão de informações incorretas,

incompletas ou desatualizadas. Isso garante que os titulares dos dados tenham controle sobre suas informações pessoais e possam mantê-las precisas e atualizadas.

Outro direito importante previsto na LGPD é o direito à portabilidade dos dados conforme estabelecido no artigo 18-A da LGPD, onde os titulares dos dados têm o direito de receber seus dados pessoais em formato estruturado e interoperável, permitindo a transferência para outros serviços ou empresas (BRASIL, 2018).

A LGPD também garante o direito de exclusão dos dados pessoais. Segundo Guimarães e Leal (2020), os titulares dos dados podem solicitar a exclusão de seus dados pessoais das bases de dados das empresas, desde que a exclusão não prejudique interesses legítimos das empresas ou obrigações legais.

Por fim, a LGPD prevê o direito à informação sobre o compartilhamento dos dados pessoais. De acordo com Santos e Pereira (2020), as empresas devem informar aos titulares dos dados sobre o compartilhamento de suas informações pessoais com terceiros, incluindo os motivos e as condições do compartilhamento.

5 DESAFIOS E OPORTUNIDADES DA IMPLANTAÇÃO DA LGPD PARA EMPRESAS E PARA OS CONSUMIDORES

A LGPD também tem impactos significativos para as empresas que coletam e tratam dados pessoais. Alguns desses impactos são:

Investimentos em segurança; as empresas precisam investir em tecnologias e medidas de segurança adequadas para proteger os dados pessoais dos consumidores. Isso pode envolver a contratação de especialistas em segurança da informação, a implementação de políticas de segurança e a utilização de softwares de proteção de dados.

Mudança de cultura organizacional; as empresas precisam mudar a cultura organizacional para garantir que todos os funcionários estejam cientes das regras da LGPD e que sigam as políticas de proteção de dados pessoais.

Custos adicionais; as empresas podem ter que arcar com custos adicionais para implementar as medidas de segurança necessárias e cumprir as regras da LGPD. Isso pode envolver a contratação de pessoal especializado, a aquisição de

softwares e tecnologias de proteção de dados, e a realização de treinamentos para os funcionários.

Reputação; A LGPD exige que as empresas sejam transparentes sobre o tratamento de dados pessoais dos consumidores. Isso pode impactar a reputação da empresa, caso ocorram incidentes de segurança ou vazamentos de dados.

Multas e sanções; as empresas que não cumprem as regras da LGPD podem ser multadas em até 2% do faturamento anual, limitado a R$ 50 milhões por infração. Essas multas podem representar um custo significativo para as empresas.

A implantação da LGPD traz desafios e oportunidades tanto para as empresas quanto para os consumidores. Um dos principais desafios é a necessidade de investimentos significativos em infraestrutura e treinamento para garantir a implementação adequada da lei (BIONI, 2021). As empresas que se adaptarem à LGPD e implementarem práticas de proteção de dados poderão ganhar vantagem competitiva, uma vez que a privacidade e segurança são fatores cada vez mais relevantes para os consumidores (ALVES e SILVA, 2020).

Conforme podemos destacar a LGPD exige que as empresas implementem medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais, o que pode exigir investimentos em tecnologia e recursos humanos (BIONI, 2021).

O custo de implementação da LGPD em uma empresa pode variar bastante dependendo de diversos fatores, como o tamanho e o setor da empresa, a complexidade de suas operações, a quantidade e o tipo de dados pessoais que a empresa manipula, o estágio atual de conformidade com a LGPD. Devido à complexidade e à personalização do processo de implementação da LGPD, não é possível determinar um custo fixo para todas as empresas. Recomenda-se que as empresas consultem especialistas em privacidade e proteção de dados para avaliar suas necessidades específicas e determinar um plano de ação adequado.

Outro desafio é a necessidade de adaptação cultural e mudança de paradigma, já que a LGPD exige uma postura mais proativa das empresas em relação à proteção dos dados pessoais dos consumidores. Conforme afirma Alves e Silva (2020) a LGPD exige uma mudança cultural nas empresas, que precisam passar a tratar a proteção de dados pessoais como um valor fundamental e adotar uma postura proativa na prevenção de violações.

Também Está previsto a obrigatoriedade de prestação de contas (Accountability) que se refere à responsabilidade das empresas e organizações no tratamento de dados pessoais. O princípio da accountability está previsto no artigo 6º, inciso IX da LGPD, que estabelece que é dever do controlador adotar medidas que assegurem a responsabilidade dos agentes que realizarem o tratamento de dados pessoais em seu nome. Implica ainda na necessidade de as empresas e organizações criarem uma cultura de proteção de dados, promovendo a conscientização e a capacitação dos seus colaboradores e parceiros sobre as melhores práticas para a proteção da privacidade e segurança dos dados pessoais.

Além disso, o artigo 42 da LGPD prevê a obrigação de as empresas e organizações indicarem um encarregado de proteção de dados (Data Protection Officer/DPO). O DPO é o responsável por orientar a empresa em relação às melhores práticas de proteção de dados pessoais, além de atuar como canal de comunicação entre a organização, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). A figura do DPO é obrigatória para as empresas que realizam tratamento de dados pessoais em grande escala ou que realizam tratamento de dados sensíveis, conforme disposto no artigo 41 da LGPD. O DPO deve ter conhecimentos técnicos e jurídicos sobre a LGPD, além de ter autonomia e independência para exercer suas funções.

Para os consumidores, a LGPD traz a garantia de que seus dados pessoais serão tratados de forma adequada e segura pelas empresas e entidades públicas. Além disso, a LGPD garante aos titulares dos dados o direito de acessar, corrigir, excluir e portar seus dados pessoais, o que significa mais controle sobre suas informações (DONEDA, 2020).

6 SANÇÕES PREVISTAS NA LGPD PARA EMPRESAS QUE VIOLAM AS DISPOSIÇÕES DA LEI

A LGPD prevê sanções para as empresas que violam as disposições da lei, como forma de garantir a sua implementação e efetividade (BRASIL, 2018). As sanções incluem advertência, multa simples ou diária, publicização da infração, bloqueio ou eliminação dos dados pessoais relacionados à infração, suspensão parcial ou total do funcionamento do banco de dados ou da atividade empresarial e

até mesmo a proibição total ou parcial do exercício de atividades relacionadas ao tratamento de dados pessoais (BIONI, 2021).

A aplicação das sanções é feita pela Autoridade Nacional de Proteção de Dados (ANPD), criada pela LGPD como órgão responsável por garantir a proteção dos dados pessoais no Brasil, criada pela Lei nº 13.853/2019, que instituiu a LGPD, e está prevista no artigo 55-J da referida lei.

A ANPD é uma peça fundamental para a implementação efetiva da LGPD, pois tem o papel de fiscalizar e aplicar as sanções previstas na lei (BIONI, 2021). Através de sua atuação fiscalizatória, ela pode aplicar sanções em caso de violação da lei, o que aumenta a responsabilização e accountability das empresas e organizações. Além disso, a orientação que a ANPD pode fornecer pode ajudar a esclarecer dúvidas e a estabelecer boas práticas para o tratamento de dados pessoais.

As sanções previstas na LGPD têm o objetivo de garantir que as empresas tratem os dados pessoais dos consumidores de forma adequada e segura, respeitando seus direitos e garantindo a privacidade das informações. Cabe destacar que a aplicação das sanções não é automática, mas depende de um processo administrativo que garante o direito à ampla defesa e ao contraditório, pois o este processo é importante para garantir que as sanções sejam aplicadas de forma justa e proporcional, levando em consideração as circunstâncias de cada caso (ALVES e SILVA, 2020).

O não cumprimento do princípio da accountability também pode levar a sanções e penalidades, como multas e proibição de realizar o tratamento de dados pessoais. Além disso, o descumprimento desse princípio pode resultar em danos à reputação da empresa e perda de confiança dos consumidores e parceiros

7 CASOS DE VIOLAÇÃO DE DADOS PESSOAIS

A violação de dados pessoais é uma preocupação crescente em todo o mundo. Como destacado por Tene e Polonetsky (2019), as violações de dados podem causar danos significativos aos indivíduos, como perda de privacidade, roubo de identidade e discriminação. Alguns casos notórios de violação de dados pessoais incluem a *Cambridge Analytica, Yahoo e Equifax.*

A Cambridge Analytica foi uma empresa britânica de consultoria política que usou dados de usuários do Facebook para influenciar as eleições nos EUA em 2016. A empresa coletou dados pessoais de mais de 50 milhões de usuários do Facebook sem o seu consentimento, através de um aplicativo de teste de personalidade. Esses dados foram usados para criar perfis psicológicos e políticos dos usuários, que foram usados para criar anúncios políticos personalizados e influenciar as eleições. O escândalo levou a uma grande crise de privacidade para o Facebook e para a própria Cambridge Analytica, que fechou suas portas após o escândalo.

Em 2013 e 2014, a Yahoo sofreu uma grande violação de dados que afetou todas as suas contas de usuários, totalizando mais de três bilhões de contas. Os hackers roubaram informações pessoais, como nomes, endereços de e-mail, senhas e datas de nascimento. Além disso, em 2017, a Yahoo descobriu uma nova violação de dados que afetou cerca de 32 milhões de contas. As violações de dados da Yahoo levaram a uma série de processos judiciais e a empresa concordou em pagar US $ 117,5 milhões em acordos legais.

Já em 2017, a Equifax, uma das maiores agências de relatórios de crédito do mundo, sofreu uma grande violação de dados que afetou 147 milhões de pessoas. Os hackers acessaram informações pessoais, como nomes, endereços, datas de nascimento e números de Segurança Social. Além disso, os hackers roubaram números de cartões de crédito de cerca de 209.000 consumidores. O incidente gerou grande preocupação em relação à segurança dos dados pessoais e levou a uma série de ações legais contra a empresa, incluindo uma multa de US $ 700 milhões da Comissão Federal de Comércio dos Estados Unidos.

Esses são alguns exemplos de grandes violações de dados que afetaram milhões de usuários e causaram danos significativos à privacidade e segurança das informações pessoais. As consequências dessas violações destacam a importância de se ter medidas robustas de segurança de dados e a necessidade de proteger adequadamente as informações pessoais dos usuários.

Infelizmente, o Brasil é um país que já enfrentou diversos casos de vazamento de dados, que poderiam ter sido evitados ou minimizados com a implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil.

De acordo com a Agência Brasil, em 2018, o Facebook sofreu um vazamento de dados que afetou cerca de 87 milhões de usuários em todo o mundo. No Brasil, estima-se que mais de 443 mil usuários tiveram suas informações pessoais expostas. Com a LGPD em vigor, o Facebook poderia ter sido responsabilizado e multado pelas autoridades brasileiras.

Segundo o G1 em 2018, a Netshoes, uma das maiores empresas de comércio eletrônico do Brasil, sofreu um vazamento de dados que afetou mais de 2 milhões de clientes. As informações vazadas incluíam nomes, CPFs, endereços, telefones e e-mails. Com a LGPD, O Ministério Público solicitou que a Netshoes tome providências após o vazamento de 2 milhões de contas.

Conforme reportagem da Exame, em 2021, a Serasa Experian sofreu um vazamento de dados que afetou mais de 220 milhões de brasileiros. As informações vazadas incluíam nomes, CPFs, datas de nascimento, telefones e e-mails. Com a LGPD em vigor, a Serasa poderá ser responsabilizada e multada pelas autoridades brasileiras.

No caso da Serasa Experian, a empresa foi criticada por ter deixado os dados pessoais dos brasileiros expostos em um servidor desprotegido, sem senha, e acessível publicamente pela internet. De acordo com a LGPD, as empresas devem adotar medidas de segurança adequadas para proteger os dados pessoais que coletam e armazenam, como criptografia, firewalls, senhas seguras, entre outras. Além disso, as empresas também devem ter políticas claras de segurança da informação e treinamentos para os seus funcionários sobre como lidar com dados pessoais e prevenir vazamentos. Com a LGPD em vigor, a Serasa poderá ser responsabilizada por esse vazamento e poderá receber uma multa de até 2% do seu faturamento anual, limitado a R$ 50 milhões por infração.

8 CONSIDERAÇÕES FINAIS

A proteção de dados pessoais é um direito fundamental garantido pela Constituição Federal, e a LGPD tem como objetivo garantir esse direito e proteger os indivíduos de violações de dados pessoais. Sendo importante que tanto as empresas quanto os indivíduos estejam cientes da importância da proteção de dados pessoais e tomem medidas para garantir essa proteção.

A violação de dados pessoais é uma preocupação crescente em todo o mundo, com casos notórios como a Cambridge Analytica, Yahoo e Equifax. Para combater essa violação, a Lei Geral de Proteção de Dados foi implementada no Brasil em 2020. O que representa uma importante conquista para os cidadãos brasileiros, que passam a ter mais controle sobre seus dados pessoais e mais garantias em relação ao seu tratamento pelas empresas. Empresas precisam adotar medidas de segurança e mudar a cultura organizacional para garantir a conformidade com as regras da lei. Além disso, as multas e sanções previstas na lei representam um risco financeiro para as empresas que não cumprem as regras da LGPD uma vez que estabelece regras mais rigorosas para a coleta, tratamento e armazenamento de dados pessoais pelas empresas. Essas medidas visam proteger os direitos dos consumidores e garantir a segurança de suas informações pessoais.

A LGPD estabelece medidas importantes para prevenir e punir a violação de dados pessoais, incluindo a obtenção do consentimento dos titulares dos dados, medidas de segurança obrigatórias e notificação imediata em caso de violação de dados. As empresas que violam a LGPD estão sujeitas a diversas sanções, incluindo multas, advertências, suspensão temporária ou proibição total do tratamento de dados pessoais. Essas sanções são importantes para incentivar o cumprimento da lei e proteger os dados pessoais dos indivíduos. Além disso, a LGPD pode ajudar a aumentar a conscientização sobre a importância da privacidade e proteção de dados, incentivando uma cultura de privacidade e proteção de dados nas empresas e na sociedade em geral. Vale ressaltar que a LGPD não se aplica apenas às empresas, mas também a órgãos públicos e outras instituições.

REFERÊNCIAS

ALVES, Juliana, SILVA, Aline. **A Lei Geral de Proteção de Dados no Brasil e seu impacto no marketing digital.** Revista de Administração Mackenzie, v. 21, n. 3, 2020.

BIONI, Bruno. **Privacidade e Proteção de Dados: A perspectiva brasileira.** Rio de Janeiro: Forense, 2021.

CÂMARA, Rafael. **Proteção de dados pessoais: comentários à Lei Geral de Proteção de Dados.** São Paulo: Thomson Reuters Brasil, 2020.

CNI. **LGPD e as empresas: avaliação da adequação e dos desafios da nova legislação.** Disponível em: https://www.portaldaindustria.com.br/cni/ Acesso em: 08. Mar. 2023

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** In: MACHADO, João Paulo; BARROS, Flaviane de Magalhães. (Org.). Lei Geral de Proteção de Dados: Comentários Artigo por Artigo. São Paulo: Thomson Reuters Brasil, 2020. p. 13-26.

MACHADO, **Fabrício. Lei Geral de Proteção de Dados Pessoais: LGPD. São Paulo.** Editora Revista dos Tribunais, 2020.

SOUSA, **Rodrigo. Lei Geral de Proteção de Dados: principais aspectos e desafios.** Revista Eletrônica do Curso de Direito da UFSM, v. 15, n. 2, 2021.

TENE, Omer, POLONETSKY, Jules. **A. Big Data for All: Privacy and usercontrol in the age of analytics.** NorthwesternJournalof Technology and Intellectual Property, v. 17, n. 3, p. 239-273, 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 mar. 2023.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 12 set. 1990.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 15 abr.2023

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da República Federativa do Brasil, Brasília, DF, 11 jan. 2002.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 15 abr.2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988. Diário Oficial da República Federativa do Brasil, Brasília, DF, 5 out. 1988.** Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2023.

PROCON SÃO PAULO. **Serasa complementa resposta sobre vazamento de dados, 2021.**Disponível em: https://www.procon.sp.gov.br/serasa-complementa-resposta-sobre-vazamento-de-dados/. Acesso em: 15 abr. 2023.

CNN BRASIL**. Em 2021, o Brasil ficou no topo de vazamento de informação no mundo, diz especialista.** Disponível em: https://www.cnnbrasil.com.br/tecnologia/em-2021-brasil-ficou-no-topo-de-vazamento-de-informacao-no-mundo-diz especialista/#:~:text=Tivemos%20nesse%20ano%20de%202021,ainda%E2%80%9D%2C%20disse%20o%20especialista. Acesso em: 25 mar. 2023.

PLANALTO. **Emenda 115 Constituição federal de 1988.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 08. Mar. 2023.

FLOWTI. **LGPD o que muda na pratica com a nova lei geral de proteção de dados** Disponível em: https://flowti.com.br/blog/lgpd-o-que-muda-na-pratica-com-a-nova-lei-geral-de-protecao-de-dados. Acesso em: 15. abr. 2023.

Consumidor Moderno. **EM que pé estão as leis de proteção de dados no mundo?** Disponível em: https://consumidormoderno.com.br/2021/02/08/em-que-pe-estao-as-leis-de-protecao-de-dados-no-mundo/. Acesso em: 22 abr. 2023.

[1] AGÊNCIA BRASIL. **Facebook notifica usuários que tiveram dados vazados; 443 mil são no Brasil. Brasília: Agência Brasil, 2018.** Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2018-04/facebook-notifica-usuarios-que-tiveram-dados-vazados-443-mil-sao-no-brasil. Acesso em: 22abr. 2023.

[1] G1. **MP pede que Netshoes tome providência após vazamento de 2 milhões de contas. Brasília: G1, 2018.** Disponível em: https://g1.globo.com/df/distrito-federal/noticia/mp-pede-que-netshoes-tome-providencia-apos-vazamento-de-2-milhoes-de-contas.ghtml. Acesso em: 22 abr. 2023.

EXAME. **Vazamento de dados de 220 milhões de brasileiros não aconteceu da noite para o dia. São Paulo: Exame, 2021.** Disponível em:

https://exame.com/tecnologia/vazamento-de-dados-de-220-milhoes-de-brasileiros-nao-aconteceu-da-noite-para-o-dia/. Acesso em: 22abr. 2023.