VAZAMENTO DE DADOS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: RESPONSABILIDADE CIVIL DOS FORNECEDORES DE SERVIÇOS DIGITAIS

JOSÉ VINICIUS PIRES ROCHA [1]
FERNANDO HENRIQUE DA SILVA HORITA[2]

RESUMO: Este trabalho tem como objetivo analisar o vazamento de dados à luz da Lei Geral de Proteção de Dados Pessoais (LGPD) e a responsabilidade civil dos fornecedores de serviços digitais. A LGPD foi instituída em 2018 e tem como objetivo garantir a proteção dos dados pessoais dos cidadãos brasileiros. O vazamento de dados é uma situação recorrente na era digital e pode causar prejuízos à privacidade e à segurança das pessoas afetadas. A responsabilidade civil dos fornecedores de serviços digitais é um tema importante a ser abordado, visto que estes são os responsáveis por armazenar e proteger os dados dos usuários. Para a estruturação deste trabalho foram utilizadas diversas doutrinas, como a teoria da responsabilidade civil, o direito digital e a segurança da informação. Será abordado o papel dos fornecedores de serviços digitais na proteção dos dados pessoais, as consequências do vazamento de dados e as medidas preventivas e reparatórias previstas pela LGPD. Conclui-se que os fornecedores de serviços digitais devem ser responsabilizados pelos danos causados em casos de vazamento de dados, e que a LGPD representa um importante avanço na proteção da privacidade e dos dados pessoais dos usuários.
Palavras chaves: Cibersegurança; Dados; LGPD.

DATA BREACH IN LIGHT OF THE GENERAL DATA PROTECTION LAW: CIVIL LIABILITY OF DIGITAL SERVICE PROVIDERS

ABSTRACT: The purpose of this study is to analyze the data breach in light of the General Data Protection Law (LGPD) and the civil liability of digital service providers. The LGPD was established in 2018 with the objective of ensuring the protection of Brazilian citizens' personal data. Data breaches are a recurring situation in the digital era and can cause harm to the privacy and security of affected individuals. The civil liability of digital service providers is an important issue to be addressed, as they are responsible for storing and protecting user data. Various doctrines, such as ivil liability theory, digital law, and information security, were employed to structure this study. The study will cover the role of digital service providers in safeguarding personal data, the consequences of data breaches, and the preventive and remedial measures envisaged by the LGPD. It is concluded that digital service providers must be held responsible for the damages caused by data breaches and that the LGPD represents a significant advance in protecting the privacy and personal data of users.
Key-words: Cybersecurity; Data; LGPD.

[1] Acadêmico de Direito. Curso de Direito. Faculdade Fasipe. Endereço eletrônico: direito@unifasipe.com,br
[2] Professor Doutor em Filosofia. Faculdade Fasipe. Endereço eletrônico: profhorita@outlook.com

1. INTRODUÇÃO

Nas últimas décadas, com o constante avanço da humanidade, pode-se perceber uma concentração de recursos em determinadas áreas, porém, com todas elas sempre se há foco na facilitação tecnológica, logo, o homem busca a resolução de seus problemas por meio de mecanismos, esta busca foi facilitada devido aos grandes avanços de pesquisa permitidos pela integração das nações, tornada ainda mais notória após a criação da Internet, que inicialmente, fora criada para facilitar a transmissão de informações entre pesquisadores.

Conectada a este salto de comunicação, a sociedade evolui e busca novos horizontes digitalmente, com isto a Internet que tinha o intuito de ser utilizada somente por governos e a princípio como ferramenta militar, se populariza entre os civis devido a facilitação de comunicabilidade, iniciando-se ao mundo digital e com isto a troca de informações pessoais e consequentemente os dados do usuário característico são transportados neste mundo digital, ainda mais visível na sociedade contemporânea por meio de aplicativos e sites que requerem a permissão, tanto em computadores, quanto em celulares de terem acesso aos dados do usuário interessado ao acesso daquele produto digital.

A respeito dos dados dos usuários se é notório que a sociedade brasileira de forma generalizada, mesmo com o grande avanço da Era da Informação, não possui entendimento que os dados digitais representam uma fonte de informação riquíssima para as empresas de produtos digitais, logo, tratam com banalidade o assunto já que não se há um interesse na funcionalidade do mundo digital e a utilização dos dados.

Os dados digitais são informações relevantes a serem debatidas devido a importância da privacidade e seguridade no mundo digital e que com o passar dos anos será ainda mais relevante, já que estas informações são uma extensão do usuário, criando assim um laço entre o digital e real, devido a exprimir as peculiaridades de cada um.

Diante destes fatores que levam a formação social atual e o constante avanço tecnológico, no Brasil criasse a Lei de nº 13.709/2018 com o intuito de proteger os dados pessoais do povo brasileiro e prevenir situações que levem a situações danosas aos usuários digitais.

A Lei de nº 13.709/2018, tendo como título Lei Geral de Proteção de Dados (LGPD) trata sobre os dados pessoais em geral dos usuários, de forma digital ou física mantida por empresas determinando as normas que devem ser seguidas e quais os direitos e deveres, tanto dos usuários, quanto das empresas prestadoras de serviço digital.

2. REVISÃO DE LITERATURA

2.1 A Lei Geral De Proteção De Dados

Com a popularização da internet nas últimas duas décadas vivenciadas no Brasil, é evidente a necessidade de o legislativo nacional buscar o estabelecimento de um marco legal digital, abrangendo tanto o aspecto penal quanto o cível. Isso se justifica pelo fato de que situações originadas na internet podem desencadear eventos no mundo real, com impactos positivos ou negativos, os quais requerem uma análise apropriada.

Os dados dos usuários que utilizam serviços online representam ativos valiosos para empresas atuantes no ambiente digital. A maneira como essas informações são utilizadas demonstra ser altamente eficaz na alocação de recursos econômicos e na criação de estratégias "personalizadas" baseadas nos dados coletados de cada usuário. Por exemplo, quando alguém

manifesta interesse por um determinado tópico e o pesquisa online, segue especialistas nesse assunto e interage em mídias sociais relacionadas, isso resulta na formação de um perfil. Observa-se que indivíduos que demonstram interesse em um assunto específico buscam informações na internet devido à facilidade de comunicação, e, como resultado, suas ações digitais geram dados que refletem seu comportamento online.

Diante desse cenário, a Lei Geral de Proteção de Dados (LGPD), promulgada em 2018, representou um avanço tardio. Essa legislação tinha como objetivo proteger os dados dos usuários que utilizam serviços online, estabelecendo diretrizes a serem seguidas pelas empresas e princípios gerais. O artigo 1° dessa lei, em particular, enfatiza a importância do princípio da privacidade.

É evidente que, ao discutir a questão dos dados digitais, tratamos visivelmente da privacidade e segurança online. É possível observar, como destacado por Doneda em 2019, que a atual Constituição Federal garante aos cidadãos brasileiros proteção à sua vida privada, conforme estabelecido no artigo 5°, inciso IX. Além disso, o mesmo artigo aborda a inviolabilidade dos dados, como interceptações telefônicas, telegráficas, correspondências e outros, conforme indicado no inciso XII. Isso sugere que, através do princípio da analogia, pode-se afirmar que a Constituição vigente já demonstrava preocupação com a proteção de dados, mesmo que não existisse, naquela época, legislação específica regulamentando essa questão.

No processo de criação da LGPD, o legislativo brasileiro adotou normas estrangeiras como base para estabelecer um marco legal inicial. Inspirada na lei denominada "General Data Protection Regulation" (GDPR), criada pela União Europeia (UE) em 2016 e efetivada em 2018 após a preparação das empresas que oferecem serviços digitais, a LGPD se fundamenta na questão da privacidade. Vale ressaltar que tanto a lei europeia quanto a brasileira abrangem não apenas dados digitais, mas também quaisquer informações mantidas por empresas, independentemente de sua forma, devido à necessidade de proteção de ambos, como apontado por Pinheiro em 2020.

Outro motivo para a criação da LGPD, como observado por Pinheiro (2020), relaciona-se à necessidade de alinhar o Brasil com as práticas comerciais da União Europeia. Isso ocorre porque a nova lei afetaria empresas como um todo, criando, de certa forma, a necessidade de que os países que mantêm relações comerciais com a UE se adaptem a essa mudança.

À medida que exploramos a questão dos dados pessoais, é perceptível que, na sociedade contemporânea, o debate sobre dados, com ênfase nos digitais, está destinado a crescer de forma exponencial, não apenas no Brasil, mas em todo o mundo. Isso ocorre porque, até o momento, não existe regulamentação internacional abrangente sobre dados, como mencionado por Doneda em 2019.

2.2 Aplicabilidade da LGPD

Ao discutir legislações, é importante considerar como essas normas são aplicadas, e a contextualização da territorialidade desempenha um papel fundamental nesse processo, como destacado por Pinheiro em 2020. Esse conceito é embasado no artigo 3° da Lei Geral de Proteção de Dados (LGPD), que estabelece que a lei se aplica a qualquer operação de tratamento de dados, independentemente do local ou país da pessoa ou organização que a realiza, desde que se apliquem as seguintes condições: a operação de tratamento seja realizada no território nacional, a atividade de tratamento tenha por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos no território nacional ou os dados pessoais tenham sido coletados no território nacional (BRASIL, 2018).

Como mencionado, a LGPD aborda de maneira abrangente a quem a lei se aplica, considerando os indivíduos envolvidos no processo, a natureza do tratamento e a localização dos dados, tudo isso com o propósito de assegurar a proteção da privacidade de maneira abrangente. O legislador, durante a criação dessa legislação, formulou o caput de forma genérica, a fim de evitar brechas. Portanto, todos os dados, inclusive aqueles offline, em território brasileiro, independentemente de sua origem, devem estar em conformidade com os requisitos legais.

Além disso, conforme observado por Pinheiro (2020), a legislação não se concentra na nacionalidade do titular dos dados ou na origem dos dados, mas sim nos dados em si. Portanto, o critério é se, em algum ponto do processamento, armazenamento ou uso dos dados, ocorre em território brasileiro, a norma se aplica.

Nesse sentido, Menezes e Colaço (2020) abordam a proteção de estrangeiros em território brasileiro. Mesmo que um estrangeiro esteja apenas fazendo uma conexão em um aeroporto brasileiro, o regulamento legal brasileiro ainda será aplicado para proteger os dados dessa pessoa.

No que diz respeito à territorialidade, o Brasil adota uma abordagem diferente da União Europeia. Enquanto na União Europeia o tratamento de dados é baseado na localização física da empresa, no Brasil, como mencionado anteriormente, a LGPD tutela qualquer dado utilizado em qualquer parte do processo em território brasileiro, independentemente do titular dos dados, conforme explicado por Menezes e Colaço (2020, p. 187).

A LGPD, como sugerem Menezes e Colaço (2020), não se limita apenas a ela mesma para abordar questões jurídicas, mas se vale de outras legislações complementares, como o Marco Civil da Internet e, no caso em discussão, o Código Civil, que lida com o direito material em geral, e o Código do Consumidor, que se mostra mais detalhado na relação entre usuários e fornecedores de serviços digitais. Essas complementações desempenham um papel importante na garantia da proteção dos titulares dos dados.

Considerando as informações apresentadas anteriormente, é essencial analisar as situações em que a LGPD não é aplicável. O legislador, ao fundamentar esses aspectos, visa antecipar possíveis disputas judiciais no futuro, uma vez que os dados envolvem informações pessoais e podem potencialmente levar a conflitos na esfera cível. Nesse sentido, o artigo 4° da LGPD enumera os casos em que a lei não se aplica.

Conforme observam Menezes e Colaço (2020), o primeiro inciso do artigo 4°, que trata de finalidades puramente pessoais e não econômicas, não prejudica o sistema de dados nem cria desequilíbrio de informações. Um exemplo disso são as pesquisas realizadas por indivíduos por mera curiosidade, sem uma finalidade específica. No entanto, é importante destacar que, mesmo que o indivíduo esteja isento da regulamentação da LGPD, ainda pode ser responsabilizado na esfera cível e penal, dependendo do uso dos dados. O ordenamento jurídico específico continuará a ser aplicado, e o indivíduo deve ser responsabilizado de acordo com outras normas jurídicas brasileiras.

Mesmo em casos de violação de privacidade que não envolvem agentes econômicos ou o Estado, o impacto é geralmente menor, pois não há desproporção entre as partes envolvidas. Isso ocorre quando as informações são compartilhadas com outras pessoas físicas, criando uma situação paritária, conforme explicado por Menezes e Colaço (2020).

No segundo inciso, que se baseia em finalidades jornalísticas, artísticas e acadêmicas, há uma exceção para fins jornalísticos devido à necessidade de comunicação social. Conforme argumentado por Menezes e Colaço (2020), essa exceção promove a liberdade de expressão e

abre espaço para debates de interesse público, facilitando o acesso à informação e promovendo uma visão crítica.

Para os autores mencionados, a coleta de dados para fins acadêmicos tem o objetivo de promover a liberdade de pesquisa, com foco na educação. Além disso, a coleta de dados em trabalhos acadêmicos é frequentemente regulamentada por leis específicas, e o processo envolve comitês e bancas julgadoras que adotam abordagens jurídicas e mantêm padrões éticos ao longo do processo de elaboração.

2.3. O Tratamento Dos Dados Pessoais

Para compreender o tratamento de dados pessoais, é necessário começar por entender o que a Lei Geral de Proteção de Dados (LGPD) define como dados pessoais. No artigo 5° da LGPD, encontramos as definições essenciais: Dado pessoal: informação relacionada a pessoa natural identificada ou identificável; Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (BRASIL, 2018).

Conforme Doneda (2019), as definições legais presentes na legislação atual guardam semelhança com os conceitos utilizados pelo Conselho da Europa, em especial com a Convenção 108 de 1981. Dessa forma, os dados pessoais não apenas identificam os titulares, mas também permitem a integração com outros dados, contribuindo para a formação de perfis detalhados dos indivíduos interligados a esses dados, quer sejam titulares ou não.

O General Data Protection Regulation (GDPR) influencia diretamente a categorização de dados sensíveis, como explica Doneda (2020, p. 143), resultando da observação pragmática das diferenças no tratamento dessa categoria de dados em relação aos demais.

Seguindo esse raciocínio, Pinheiro (2020) afirma que os dados sensíveis estão relacionados com as escolhas pessoais dos titulares, podendo impactar significativamente a vida desses indivíduos, devido à natureza mais pessoal desses dados. Konder (2020) ainda destaca que os dados pessoais têm o potencial de ser lesivos, pois, durante o tratamento, podem revelar informações íntimas do titular. Por exemplo, informações de localização, hábitos de compra, preferências de filmes e histórico de pesquisa podem parecer inofensivas quando isoladas, mas, quando analisadas em conjunto, podem revelar a orientação religiosa, política e até sexual do titular (KONDER, 2020, p. 451).

Além disso, no artigo 5° da LGPD, no inciso III, é definido o que são dados anonimizados, ou seja, dados relativos a um titular que não podem ser diretamente identificados, desde que sejam utilizados meios técnicos razoáveis e disponíveis no momento do tratamento. Isso implica na perda do vínculo entre a informação e o indivíduo, conforme ressalta Doneda (2019). No mesmo artigo, no inciso XI, a anonimização é mais detalhadamente descrita como o uso de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação direta ou indireta a um indivíduo (BRASIL, 2018), corroborando o entendimento de Doneda (2019).

O General Data Protection Regulation (GDPR) tem influência direta na categorização dos dados sensíveis, como observado por Doneda (2020, p. 143), que menciona que a criação dessa categoria de dados sensíveis decorreu da observação pragmática das diferenças nos efeitos do tratamento desses dados em comparação com os demais.

De acordo com o entendimento de Pinheiro (2020), os dados sensíveis são informações relacionadas às escolhas pessoais dos titulares e têm o potencial de impactar diretamente a vida do indivíduo devido à sua natureza altamente pessoal. Além disso, conforme a compreensão de Konder (2020), os dados pessoais têm um potencial de ser lesivos, pois, durante o tratamento, é possível obter acesso a informações íntimas do titular. Konder (2020) ainda ilustra esse ponto ao afirmar que, por exemplo, informações de localização geográfica, hábitos de compras, preferências de filmes e histórico de pesquisa podem parecer inofensivas individualmente, mas um rápido tratamento em conjunto pode servir para identificar orientação religiosa, política e até orientação sexual.

Quanto à definição de dados anônimos, o artigo 5° da LGPD estipula que são dados relativos a um titular que não podem ser diretamente identificados, considerando o uso de meios técnicos razoáveis e disponíveis no momento do tratamento (BRASIL, 2018). Portanto, esses dados anônimos não podem ser diretamente associados ao titular quando utilizados, uma vez que, como enfatizado por Doneda (2019), ocorre a perda de vínculo entre a informação e o indivíduo, desvinculando-se de qualquer associação direta ou indireta com o titular.

Além disso, a anonimização é detalhada no mesmo artigo 5° da LGPD, no inciso XI, como o uso de meios técnicos razoáveis e disponíveis no momento do tratamento para que um dado perca a possibilidade de associação direta ou indireta a um indivíduo, o que confirma o entendimento de Doneda (2019).

Entretanto, de acordo com a LGPD, em seu artigo 12, é possível reverter esses casos de anonimato, desde que ocorram por meios apropriados ou mediante esforços razoáveis (BRASIL, 2018). Para garantir a titularidade dos dados em tratamento, a LGPD, em seu artigo 5°, inciso V, estipula que o titular deve ser uma pessoa natural, reforçando assim a proteção do bem jurídico (os dados coletados) prevista na legislação.

Além disso, a questão do consentimento do titular é abordada no mesmo artigo, no inciso XII, que define o consentimento como uma manifestação livre, informada e inequívoca do titular, concordando com o tratamento de seus dados pessoais (BRASIL, 2018). Portanto, além de o indivíduo estar ciente de que seus dados serão usados, ele deve estar informado sobre os fins desse uso.

O processo de armazenamento dos dados, conforme estipulado no artigo 5° da LGPD e detalhado no inciso IV, é definido como um conjunto estruturado de dados pessoais estabelecidos em um ou vários locais, em suporte eletrônico ou físico (BRASIL, 2018).

A LGPD também prevê a possibilidade de eliminação dos dados (ou bloqueio) durante o tratamento, como definido nos incisos XIII e XIV do artigo 5°. O bloqueio é a suspensão temporária de qualquer operação de tratamento, enquanto a eliminação envolve a exclusão de um dado ou conjunto de dados armazenados em um banco de dados, independentemente do procedimento empregado (BRASIL, 2018).

Quanto ao tratamento de dados, a LGPD, no artigo 5°, inciso X, estabelece que ele abrange todas as operações realizadas com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018). Vale destacar que os casos mencionados são exemplos e podem ser cumulativos, ou seja, a realização de qualquer uma das ações acima já se enquadra como tratamento de dados (COTS; OLIVEIRA, 2019). A LGPD também aborda a questão do compartilhamento de dados coletados, tanto em âmbito nacional quanto internacional, como definido no inciso XVI do artigo 5° da Constituição Federal (1988).

2.4. Agentes de tratamento

Como mencionado anteriormente, a LGPD no artigo 5° identifica os agentes envolvidos no tratamento de dados, ou seja, o controlador e o operador de dados. Além de conceituar esses agentes, a legislação estabelece condutas a serem seguidas, métodos de segurança e práticas relacionadas ao processamento e tratamento de dados.

A LGPD, em seu artigo 37, exige o registro das ações realizadas, com ênfase na necessidade de registro quando envolver interesses próprios (BRASIL, 2018). O registro pode ser feito tanto em meio físico quanto eletrônico, sendo o último o mais comum. Segundo Cots e Oliveira (2019, p. 171), a documentação gerada pelos agentes deve conter informações como a atividade desenvolvida, data, horário, identificação da pessoa que realizou o processo, meios tecnológicos utilizados, como sistemas e softwares, entre outras informações.

A Autoridade Nacional de Proteção de Dados pode determinar que o controlador desenvolva um relatório sobre o impacto na proteção de dados pessoais. O artigo 38 da LGPD fornece um formato exemplificativo desse relatório, que deve incluir, no mínimo, a descrição dos tipos de dados coletados, a metodologia usada para a coleta e garantia da segurança das informações, bem como a análise do controlador em relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (BRASIL, 2018).

No que diz respeito à descrição dos dados pessoais, Cots e Oliveira (2019, p. 172) compreendem que esses dados englobam informações como nome, números de documentos (CPF, RG, PIS, CNH etc.), endereço físico e eletrônico, e assim por diante.

Os autores também apontam que o uso do termo "coleta" no artigo 38 da LGPD pode gerar algumas divergências, uma vez que sugere que os agentes obtêm os dados ao entrar em contato com o titular. No entanto, as informações podem ser obtidas por meio de comunicação necessária entre as partes, compartilhamento ou transferência, não necessariamente exigindo um ato ativo de coleta por parte dos agentes.

Em relação ao operador, a LGPD estabelece, no artigo 39, que este deve tratar os dados de acordo com as instruções fornecidas pelo controlador, que por sua vez verifica a conformidade com suas próprias instruções e as normas da LGPD (BRASIL, 2018). Isso reflete a relação essencial entre o controlador e o operador no processo de tratamento de dados.

A ANPD, com o objetivo de cumprir suas funções, pode definir padrões para a comunicação e a colaboração entre os agentes (operadores e controladores) em relação aos dados, bem como a segurança e a retenção de registros. No entanto, é importante observar os princípios da necessidade e transparência, que possibilitam essa padronização pela ANPD (BRASIL, 2018). De acordo com Pinheiro (2020), a padronização facilita o trabalho das agências encarregadas de fiscalizar o cumprimento das normas da LGPD.

Dado o constante avanço no mundo digital, a LGPD enfatiza a necessidade de manter a segurança dos dados, dada a crescente incidência de violações de dados que resultam na exploração de informações sigilosas, potencialmente levando a crimes como estelionato e falsa identidade (SOUZA, 2020). Em virtude dessas crescentes violações de segurança, o artigo 46 da LGPD estabelece que o controlador e o operador devem adotar medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas que possam resultar em destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018).

Conforme apontado por Cots e Oliveira (2019), o artigo mencionado não é uma aspiração, mas uma obrigação legal que pode resultar em sanções administrativas para os envolvidos. Pinheiro (2020) argumenta que, por meio da formalização e adoção desses

procedimentos pelos agentes, deve-se garantir a integridade, disponibilidade e confidencialidade dos dados ao longo de toda a cadeia de tratamento.

Para assegurar efetivamente a segurança dos dados, Cots e Oliveira (2019) sugerem que isso pode ser alcançado por meio de várias abordagens, abrangendo aspectos computacionais, sistêmicos e físicos. A adoção dessas abordagens visa preservar o princípio da preservação e mitigar riscos futuros. Os autores também argumentam que os padrões técnicos e as medidas de segurança e sigilo adotados pelos agentes de tratamento devem impedir o acesso não autorizado de terceiros, como o uso indevido de credenciais ou a invasão de sistemas de armazenamento, tanto físicos quanto digitais. Essas referências recorrentes na LGPD refletem a preocupação em preservar a integridade dos titulares de dados e garantir a segurança daqueles que detêm esses dados.

Após se entender de forma inicial os conceitos aduzidos pela Lei Geral de Proteção de Dados a respeito da forma de tratamento de dados pessoais, as atribuições que a legislação prevê para os responsáveis pelo tratamento de dados e os interesses legais defendidos pelos dispositivos com um ensejo em gerar a proteção digital, deve-se entender do que se trata os dados pessoais e os pessoais sensíveis.

Após se entender de forma inicial os conceitos aduzidos pela Lei Geral de Proteção de Dados a respeito da forma de tratamento de dados pessoais, as atribuições que a legislação prevê para os responsáveis pelo tratamento de dados e os interesses legais defendidos pelos dispositivos com um ensejo em gerar a proteção digital, deve-se entender do que se trata os dados pessoais e os pessoais sensíveis.

Para abordar os dados pessoais e seu tratamento, devemos considerar o regulamento presente durante o processamento, com foco nos princípios da LGPD. Além disso, o artigo 7° apresenta as possibilidades de autorização para o tratamento de dados, podendo, de acordo com Cots e Oliveira (2019), ser fundadas em várias bases legais, permitindo a cumulação de motivos para o tratamento.

2.4.1 O tratamento dos dados pessoais

A primeira possibilidade para o tratamento de dados é o consentimento do titular, que se manifesta de forma livre, inequívoca e informada, autorizando o uso de seus dados para um propósito específico (BRASIL, 2018). Esse consentimento pode ser dado por escrito ou, como observado por Cots e Oliveira (2019), em ambientes digitais, como autenticação por e-mail, tokens, SMS e outros meios. Essa forma de consentimento precisa ser clara, compreensível e vinculada aos termos do tratamento de dados (COTS; OLIVEIRA, 2019, p. 92).

Portanto, o controlador é responsável por comprovar que possui o consentimento adequado para o tratamento de dados, e o tratamento de dados com consentimento irregular é proibido no Brasil (BRASIL, 2018). O consentimento é válido apenas se estiver em conformidade com os requisitos da LGPD e se a finalidade for claramente informada ao titular, o que implica que o uso de termos genéricos em aplicativos não tem base legal e não deve ser levado a sério (COTS; OLIVEIRA, 2019, p. 95-96). Isso dá ao titular o direito de recusar o consentimento.

O processamento de dados não pode ser interrompido até que o titular solicite a interrupção. O titular pode solicitar que seus dados não sejam mais usados, o que deve ser um processo gratuito e simples, conforme estabelecido no artigo 18 da LGPD (BRASIL, 2018).

O §5º do artigo 7º da LGPD destaca que, para compartilhar os dados do titular entre diferentes controladores, é necessário obter o consentimento específico do titular, conforme já mencionado anteriormente. Embora a lei não forneça detalhes sobre a forma desse

consentimento, é razoável supor que ele deva ser obtido por meio do contrato em que o usuário autoriza o compartilhamento. Esse contrato deve incluir o nome dos outros controladores que terão acesso aos dados, seguindo o princípio da transparência.

A segunda situação envolve o tratamento de dados pessoais relacionados às funções regulatórias do controlador. Como observado por Cots e Oliveira (2019, p. 83), isso inclui o tratamento de dados de funcionários, como registros de pagamento e obrigações acessórias, bem como o tratamento de dados de consumidores, como emissão de notas fiscais para transporte de mercadorias e serviços logísticos.

A terceira hipótese refere-se ao compartilhamento de dados pela administração pública para fins de políticas públicas, como regulamentações, convênios e leis, como é o caso das políticas relacionadas ao saneamento básico.

A quarta hipótese envolve o uso de dados em estudos conduzidos por órgãos de pesquisa, como universidades e instituições de pesquisa, como mencionado anteriormente. Isso inclui órgãos da administração pública direta ou indireta e entidades sem fins lucrativos envolvidas em pesquisas científicas, históricas, estatísticas ou tecnológicas. A LGPD busca, na maioria dos casos, anonimizar os usuários sempre que possível, reduzindo a quantidade de informações pessoais coletadas, como e-mails, números de telefone e dados do governo. Isso envolve a desconexão dos dados coletados e os usuários.

A quinta hipótese da LGPD relaciona-se à execução de contratos ou procedimentos pré-contratuais. O tratamento de dados nesse contexto só é permitido se o titular concordar legalmente, o que implica que o titular deve fornecer seu consentimento de forma específica para o tratamento durante a fase pré-contratual ou na formação do contrato. Isso deve ser feito por meio de um pedido específico do titular. (BRASIL, 2018; COTS; OLIVEIRA, 2019).

A sexta hipótese envolve o tratamento de dados pessoais em processos judiciais, administrativos ou arbitrais. Nesse contexto, o tratamento de dados deve estar em conformidade com as leis e regulamentos aplicáveis, garantindo que os direitos dos titulares sejam respeitados. Para processos arbitrais, é importante seguir as leis de arbitragem para assegurar o tratamento formal dos dados.

O legislador procurou equilibrar as necessidades dos titulares dos dados com outros interesses, evitando que o tratamento de dados prejudique outros direitos. Por exemplo, obter o consentimento do devedor para processar seus dados prejudicaria o direito do credor de cobrar a dívida.

A sétima hipótese permite o tratamento de dados pessoais para proteger a vida ou integridade física do titular dos dados ou de terceiros. A proteção de dados pessoais é um direito fundamental, mas em situações de conflito entre a proteção de dados e a proteção da vida, o direito à proteção da vida prevalece, independentemente de o titular dos dados ser a pessoa afetada ou um terceiro. Esse tratamento de dados só é permitido em situações de necessidade real e imediata, não como medida preventiva ou sem motivo legítimo.

A oitava hipótese envolve a tutela da saúde, aplicável a procedimentos realizados por profissionais de saúde, serviços de saúde e autoridades sanitárias. Profissionais de saúde, que são profissionais liberais, e serviços de saúde, públicos ou privados, podem realizar o tratamento de dados ao desempenhar suas funções. As autoridades sanitárias são entidades governamentais dedicadas à saúde pública.

A nona hipótese aborda situações em que o controlador precisa atender a interesses legítimos, desde que não prejudiquem os direitos e liberdades fundamentais dos titulares. O tratamento de dados deve ter finalidade legítima em situações concretas e não se limitar apenas

ao apoio ou promoção das atividades do controlador, mas deve respeitar as expectativas legítimas dos titulares e seus direitos e liberdades fundamentais.

Conforme a LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) tem a autoridade para solicitar que o controlador elabore um relatório de impacto à proteção de dados, permitindo a supervisão do tratamento de dados, seja pelo controlador ou por terceiros com base em interesses legítimos. Essa medida assegura que o tratamento de dados esteja em conformidade com a LGPD e respeite os direitos dos titulares, garantindo sua correta aplicação (BRASIL, 2018).

A concessão de crédito é uma das hipóteses previstas na LGPD para o tratamento de dados pessoais. O crédito é considerado fundamental para o desenvolvimento pessoal e empresarial e o funcionamento do mercado nacional (COTS; OLIVEIRA, 2019). O Código de Defesa do Consumidor (CDC) possibilita a criação de bancos de dados por serviços de proteção ao crédito, dada a relevância dos dados pessoais no mercado de crédito, como evidenciado na regulamentação dos cadastros positivos e no cadastro de inadimplentes (OLIVA; VIÉGAS, 2020).

Contudo, é importante observar que a oferta de crédito envolve riscos, como a inadimplência e a deterioração de garantias, resultando em custos mais altos de crédito conforme o aumento do risco (COTS; OLIVEIRA, 2019). A LGPD reconhece a importância da oferta de crédito e busca proteger os direitos dos titulares de dados pessoais envolvidos nesse processo. Portanto, a regulamentação da LGPD contribui para a proteção dos direitos dos titulares, incentivando comportamentos responsáveis em relação ao tratamento de informações e promovendo a participação ativa do titular na gestão de seus dados (COTS; OLIVEIRA, 2019).

2.4.2 Dados pessoais sensíveis

O tratamento de dados pessoais sensíveis requer regras específicas para proteger essa categoria, conforme a LGPD. O artigo 11 da lei, como mencionado por Konder (2020), estabelece condições para o tratamento desses dados, incluindo hipóteses restritas. Além disso, ele contém regras adaptadas aos dados sensíveis.

Tanto o tratamento de dados pessoais comuns quanto o de dados sensíveis são baseados no consentimento do titular. No entanto, no caso dos dados sensíveis, o consentimento precisa ser específico e destacado (COTS; OLIVEIRA, 2019), com limitações formais definidas pelo legislador (KONDER, 2020).

As hipóteses para o tratamento de dados pessoais incluem o cumprimento de obrigações legais ou regulatórias, estudos de órgãos de pesquisa, proteção da vida e saúde e contratos na execução de políticas públicas. No entanto, no tratamento de dados pessoais sensíveis, esse último caso é restrito às políticas públicas previstas em leis ou regulamentos, dispensando o consentimento (KONDER, 2020).

A LGPD faz uma distinção no que diz respeito ao "exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral" (BRASIL, 2018). Em relação aos contratos, essa disposição difere do artigo 7º, que permite o tratamento de dados pessoais apenas na fase de execução dos contratos.

Cots e Oliveira (2019) salientam a necessidade de restringir o uso de dados pessoais sensíveis, sugerindo que o tratamento sem o consentimento do titular seja permitido apenas na fase de execução dos contratos.

O artigo 11 da LGPD introduz uma inovação ao permitir o tratamento de dados sensíveis para garantir a prevenção de fraudes e a segurança do titular, especialmente nos

processos de identificação e autenticação de cadastro em sistemas eletrônicos, como a utilização de impressão biométrica em instituições financeiras. No entanto, essa alternativa não será aplicada quando os direitos e liberdades fundamentais dos titulares precisarem ser protegidos (KONDER, 2020).

A isenção do consentimento para o tratamento de dados sensíveis deve ser divulgada publicamente para cumprir obrigações legais, regulatórias ou para a execução de políticas públicas estabelecidas em lei ou regulamentos (BRASIL, 2018).

A LGPD proíbe a comercialização de dados pessoais sensíveis relacionados à saúde, com exceção dos casos de prestação de serviços de saúde, assistência farmacêutica e assistência. O tratamento desses dados deve ser benéfico para o titular e não deve ser utilizado para fins de seleção de riscos ou exclusão do titular, mesmo que haja vantagens econômicas para os controladores (COTS; OLIVEIRA, 2019).

Em situações específicas, o tratamento de dados pessoais sensíveis pode ser necessário para estudos de saúde pública, desde que os princípios da finalidade e o Código de Ética sejam respeitados. Nesse contexto, o processamento deve ocorrer em órgãos de pesquisa que priorizem a anonimização dos dados sempre que possível (COTS; OLIVEIRA, 2019). Portanto, a abordagem especial para dados pessoais sensíveis é relevante, mas é fundamental garantir a proteção dos direitos e liberdades fundamentais do titular por meio de precauções e medidas de segurança adequadas.

2.5 Da Responsabilidade Civil Na Lei Geral De Proteção De Dados Pessoais

Tratar-se-á neste capítulo a respeito do foco desta pesquisa, sendo a questão da responsabilidade civil, tanto objetiva, quanto subjetiva visíveis no ordenamento jurídico até o atual momento para se utilizar como um alicerce jurídico para se adentrar em tópico futuro sobre as responsabilidades do controlador e operador, introduzidos anteriormente, ao ocorrer o vazamento de dados. Será analisado também a respeito das sanções administrativas (trabalhando com a ideia de responsabilidade de pessoas jurídicas) e das hipóteses de isenções de responsabilidade do indivíduo.

2.5.1 Responsabilidade civil subjetiva

Conforme o Código Civil, especificamente nos artigos 186 e 927, caput, a responsabilidade civil é delineada:

O ato ilícito, conforme Figueiredo (2020), está relacionado a ações ou omissões voluntárias, negligência ou imprudência que violem os direitos de outrem e causem dano, mesmo que seja exclusivamente moral.

Figueiredo (2020) também destaca que, para configurar a responsabilidade civil subjetiva, é necessário evidenciar a voluntariedade do ato ou omissão. Sem a presença de dolo ou culpa, a responsabilidade civil não é estabelecida. Em outras palavras, "cada um responde por sua própria culpa."

No contexto do dolo, esse pode se manifestar por ações ou omissões, e sua comprovação requer a demonstração da intenção do responsável. Já a culpa está relacionada aos erros do agente, que podem ocorrer devido à sua imprudência, negligência ou imperícia.

No que diz respeito ao dano, é fundamental que ele tenha afetado a parte, independentemente de como tenha causado infortúnios. O dano representa uma lesão a um interesse jurídico tutelado, seja ele de natureza patrimonial ou extrapatrimonial. Esse dano decorre de ações ou omissões do responsável (GAGLIANO; PAMPLONA FILHO, 2021).

De acordo com Gagliano e Pamplona Filho (2021), para que um dano seja passível de indenização, é necessário observar três requisitos: a violação de um interesse jurídico, seja patrimonial ou extrapatrimonial, pertencente a uma pessoa física ou jurídica; a comprovação do dano; e a permanência do dano.

Assim, torna-se evidente que um dano, para ser indenizável, deve ser causado a um bem jurídico tutelado, independentemente de ser material ou não. Além disso, o dano deve ser visível para a parte afetada, a fim de mensurar seu impacto real, evitando especulações hipotéticas (GAGLIANO; PAMPLONA FILHO, 2021).

2.5.2 Responsabilidade civil objetiva

Na responsabilidade civil objetiva, a comprovação de dolo ou culpa do agente é dispensada, conforme Figueiredo (2020) (p. 385). Isso é estabelecido no parágrafo único do artigo 927 (BRASIL, 2002), que prevê que a obrigação de reparar o dano existe independentemente de culpa, nos casos previstos em lei ou quando a atividade normalmente desenvolvida pelo autor do dano, por sua natureza, implica risco para os direitos de terceiros.

No contexto da responsabilidade civil, o elemento crucial é o nexo de causalidade entre o dano e a conduta do agente responsável, o que configura a responsabilidade do agente causador do dano (GAGLIANO; PAMPLONA FILHO, 2021).

Em situações envolvendo vazamento de dados, onde os dados são vazados por um terceiro, não diretamente responsável pelos dados, pode ocorrer o que se chama de responsabilidade solidária. Isso significa que, embora o dano seja causado por outra pessoa, o indivíduo legalmente responsável pela situação responde pelo dano. Os artigos 932 e 933 do Código Civil (BRASIL, 2002) detalham as pessoas que são responsáveis pela reparação civil, independentemente de culpa, por atos praticados por terceiros mencionados nos incisos I a V do artigo 932.

O artigo 942 complementa a questão da responsabilidade, estabelecendo que "os coautores e as pessoas designadas no art. 932" também são solidariamente responsáveis com os autores. Isso significa que, em casos em que a vítima sofre algum dano, ela pode buscar diretamente o responsável legal pelo agente causador do dano para obter compensação pelo dano sofrido (GAGLIANO; PAMPLONA FILHO, 2021).

Em resumo, na responsabilidade civil objetiva, o nexo de causalidade entre o dano e a conduta do agente é o fator determinante que gera a obrigação de reparação, que pode ser realizada por meio de indenização. Além disso, essa responsabilidade pode ser solidária, envolvendo o agente responsável pelo dano e o indivíduo legalmente responsável por ele (GAGLIANO; PAMPLONA FILHO, 2021).

2.5.3 Responsabilidade prevista da lei geral de proteção de dados aos agentes de tratamento

Os vazamentos de dados, também conhecidos como data breach, são situações em que ocorre a exposição não autorizada de informações (ARAÚJO; FIGUEREDO, 2020). A LGPD busca a transparência nas relações relacionadas a esses vazamentos. O artigo 48 exige que o controlador informe à autoridade nacional e ao titular sobre incidentes de segurança que possam resultar em riscos ou danos relevantes aos titulares. No entanto, os casos que se enquadram como incidentes de segurança não são especificados (BRASIL, 2018).

Vazamentos de dados podem acontecer de duas maneiras principais: intencionalmente, quando alguém invade o sistema para obter vantagens econômicas, e por negligência, quando

ocorrem falhas de segurança devido a erros no tratamento de dados (ARAÚJO; FIGUEREDO, 2020).

A avaliação da extensão dos danos causados por um vazamento de dados considera vários fatores, incluindo a natureza da violação, o número de titulares de dados afetados, a duração da exposição dos dados, as medidas tomadas para mitigar os danos, a intencionalidade ou negligência envolvida e as medidas de segurança adotadas (ARAÚJO; FIGUEREDO, 2020).

Em casos de vazamento de dados decorrentes de não conformidade com as regulamentações legais, os agentes de tratamento de dados são responsáveis e podem ser sancionados administrativamente. A LGPD, nos artigos 42 a 45, estabelece a responsabilidade civil dos agentes de tratamento, exigindo que o responsável pelo controle ou operação de dados pessoais indenize qualquer pessoa que sofra danos patrimoniais, morais, individuais ou coletivos devido ao tratamento de dados, não especificando a necessidade de culpa (BRASIL, 2018). Em resumo, a LGPD regulamenta a transparência nos vazamentos de dados, e os agentes de tratamento de dados são responsáveis por indenizar terceiros afetados por violações, independentemente da questão da culpa (ARAÚJO; FIGUEREDO, 2020; BRASIL, 2018).

A Lei Geral de Proteção de Dados (LGPD) estabelece padrões rigorosos de conduta que devem ser integralmente seguidos, pois o tratamento de dados é uma obrigação de resultado e não de meio (TASSO, 2020). Com a responsabilidade civil objetiva, a imposição de deveres específicos relacionados às bases de dados torna-se desnecessária, já que o agente é obrigado a reparar danos independentemente dos resultados (TASSO, 2020).

O artigo 44 da LGPD estabelece que o tratamento de dados será irregular se não obedecer à legislação ou não fornecer a segurança esperada pelo titular dos dados (BRASIL, 2018). De acordo com Tasso (2020), o tratamento de dados não é considerado irregular se a LGPD for seguida adequadamente para garantir a segurança dos titulares de dados. A responsabilidade civil objetiva exige a expressa previsão na legislação para que a reparação de danos decorrentes de ilicitudes ocorra (TASSO, 2020).

A LGPD estabelece que o operador responde solidariamente ao controlador em duas situações: quando viola a LGPD ou quando não segue as instruções de tratamento fornecidas pelo controlador (COTS; OLIVEIRA, 2019). Essas hipóteses não são cumulativas, e a solidariedade é uma exceção à regra, de acordo com o artigo 42 da LGPD (COTS; OLIVEIRA, 2019).

Logo, em base de tais entendimentos, pode-se alegar que para que o titular possa ter direito a uma prestação pecuniária ou que algo seja feito com o intuito de reparar o dano sofrido por este ao ter informações pessoais difundidas de forma ilegal, se é necessário que este faça o recolhimento de elementos comprobatórios que o vazamento é de responsabilidade dos envolvidos no tratamento de dados (controlador e operador), podendo ainda efetivamente atuar na fiscalização da ação desses responsáveis, podendo realizar denúncias a respeito diretamente para órgãos responsáveis fiscalizadores.

2.5.3 A Autoridade Nacional de Proteção de Dados.

A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão criado pela LGPD para fiscalizar empresas e as práticas de tratamento de dados, bem como investigar denúncias. Suas competências incluem a proteção de dados pessoais, a garantia da privacidade, a supervisão de informações protegidas por lei e a aplicação de sanções em casos de descumprimento da legislação. Além disso, a ANPD é responsável por conscientizar o público sobre as normas de proteção de dados, conduzir estudos sobre práticas nacionais e internacionais nesse campo, promover a adoção de padrões que facilitem o controle dos titulares

sobre seus dados e cooperar com autoridades de proteção de dados estrangeiras. A ANPD também pode solicitar informações específicas sobre o tratamento de dados realizado por entidades públicas e emitir pareceres técnicos para garantir o cumprimento da lei.

O artigo 55-J da LGPD estabelece as competências da ANPD, que incluem zelar pela proteção dos dados pessoais, garantir o cumprimento dos segredos comercial e industrial, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, fiscalizar e aplicar sanções em caso de tratamento de dados em desacordo com a lei, apreciar petições de titulares, promover o conhecimento das normas de proteção de dados na população, realizar estudos sobre práticas nacionais e internacionais de proteção de dados, estimular a adoção de padrões para facilitar o controle dos titulares sobre seus dados, promover a cooperação internacional com autoridades de proteção de dados e estabelecer as formas de publicidade das operações de tratamento de dados.

No que diz respeito às funções do controlador, em caso de vazamento de dados, as etapas incluem a notificação imediata ao titular, explicando as circunstâncias e medidas corretivas adotadas. A investigação sobre o vazamento é fundamental para identificar a fonte, compreender a exposição de dados e implementar medidas de proteção apropriadas para prevenir futuros vazamentos, de acordo com o artigo 17 da LGPD.

O artigo 17 da LGPD estabelece medidas para a proteção de dados vazados, exigindo que o controlador tome ações rápidas para proteger os dados, incluindo a remoção ou tornando-os inacessíveis a terceiros. Além disso, é necessário monitorar regularmente os dados vazados para evitar exposições adicionais.

De acordo com o artigo 33 da LGPD, em certos casos, o controlador pode ser obrigado a notificar as autoridades, como a Autoridade Nacional de Proteção de Dados, sobre vazamentos de dados, seguindo as leis e regulamentos locais.

A prevenção de futuros vazamentos, conforme o artigo 17 da LGPD, requer uma avaliação das causas do vazamento e a implementação de medidas para evitar recorrências, como o reforço da segurança da informação e o treinamento dos funcionários. O objetivo é minimizar o risco de futuros incidentes e cumprir as obrigações da LGPD.

Em casos de vazamentos de dados, a ação rápida e eficiente do controlador é fundamental para proteger os titulares de dados e evitar sanções graves e danos à reputação da empresa.

A Agência Nacional de Proteção de Dados (ANPD) tem como missão auxiliar os titulares de dados na proteção de sua privacidade e na prevenção de vazamentos de informações pessoais. Ela fornece materiais informativos, dicas e orientações sobre como manter os dados seguros e o que fazer em caso de vazamento.

A ANPD se compromete a garantir a privacidade e segurança dos dados pessoais dos cidadãos, aplicando as leis de proteção de dados de maneira rigorosa. Em casos de violação das leis, a ANPD pode impor sanções administrativas e, em situações mais graves, iniciar ações judiciais contra a empresa ou entidade responsável. No entanto, a ação judicial por parte do titular não depende da atuação da ANPD.

Em resumo, é crucial que os titulares de dados conheçam seus direitos e obrigações conforme as leis de proteção de dados e sigam as recomendações da ANPD para garantir a segurança de suas informações pessoais.

No caso de um vazamento de dados pessoais, a vítima pode registrar um boletim de ocorrência na polícia. Isso é fundamental para iniciar uma investigação e proteger a privacidade. A vítima deve fornecer documentos comprobatórios, como printscreens ou e-mails, e estar

ciente de seus direitos e obrigações conforme as leis de proteção de dados. A ANPD está disponível para orientação na proteção dos dados pessoais.

Para abrir um processo civil relacionado a um vazamento de dados, a vítima pode basear-se no boletim de ocorrência, desde que ele contenha informações suficientes e identifique os responsáveis pelo vazamento. É importante que o boletim de ocorrência seja elaborado como um registro de um crime informático.

Após a elaboração do boletim de ocorrência, é aconselhável contratar um advogado especializado para representar a vítima na ação civil. O advogado analisará o caso e iniciará uma ação na Justiça para buscar a reparação de possíveis danos causados pelo vazamento.

Em alguns casos, o processo pode ser resolvido por meio de negociações extrajudiciais com base no boletim de ocorrência. Contudo, é essencial contar com a assistência de um advogado especializado para conduzir essas negociações de maneira adequada.

Resumidamente, o boletim de ocorrência é uma ferramenta crucial para iniciar um processo civil relacionado a um vazamento de dados, fornecendo informações relevantes e identificando os responsáveis. No entanto, contar com um advogado é essencial para orientar o processo judicial.

3. CONSIDERAÇÕES FINAIS

O presente trabalho teve o intuito geral de fazer uma análise a respeito sobre a responsabilidade civil disposta aos agentes operadores de dados em casos que envolvam o vazamento de informações pessoais de titulares. Para que se fosse realizado tal objetivo fora realizado uma pesquisa qualitativa, buscando-se informações a respeito em diversos entendimentos doutrinários. Conforme explicitado em tópicos anteriores, a pesquisa foi baseada em bibliografias e documentos gerais, tendo como grande alicerce a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14 de agosto de 2018, e a Lei nº 12.965, de 23 de abril de 2014. Para garantias de princípios gerais também se fora utilizado a Constituição Federal de 1988 e doutrinas de autores jurídicos.

Devido ao rápido avanço e tecnologias vindouras da internet, formou-se novos entendimentos a respeito sobre o "mundo virtual", gerando assim uma importância relevante a todos os envolvidos. Logo, para que se evitasse problemas a respeito sobre os dados, desde o início fora pensado em como estes deveriam ser protegidos, tendo a União Europeia responsável por se tornar uma das pioneiras do movimento voltado a proteção de dados com o General Data Protection Regulation¸ influenciando desta forma nações ao geral para se atualizarem a respeito da segurança de dados devido a necessidades de manterem relações econômicas.

Um dos exemplos de países que se necessitou adaptar foi o Brasil, que até o momento possuía somente a proteção a vida privada como objeto jurídico disposto em sua Constituição, porém, com o avanço tecnológico e do globalismo econômico se foi aos poucos inserido a respeito da privacidade de dados por meio de legislações ordinária, como o Código de Defesa do Consumidor, o Marco civil da Internet e a LGPD, esta que é o cerne jurídico atual a respeito de dados.

A LGPD que foi promulgada em 14 de agosto de 2018 no Brasil trouxe influências extremamente perceptíveis com a GDPR, devido a necessidade de manter conexões econômicas com a Europa. A influência fora baseada na finalidade da boa-fé das partes, transparência, livre acesso, do tratamento de dados e principalmente a segurança destes, que dia após dias se tornam mais cruciais para a globalização.

Os titulares de dados possuem uma importante garantia por meio das legislações vigentes, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, que visam proteger seus direitos e privacidade no que diz respeito ao tratamento de suas informações pessoais. Essas leis estabelecem que as informações sobre como os dados serão tratados devem ser comunicadas de maneira clara, transparente e acessível aos titulares, garantindo seu consentimento informado e consciente.

Além disso, a LGPD também determina que os titulares de dados têm o direito de conhecer quais dados estão sendo coletados, para que finalidades são utilizados, com quem são compartilhados e por quanto tempo são armazenados. Essas informações devem ser disponibilizadas de forma objetiva, utilizando linguagem clara e de fácil compreensão, de modo que os titulares possam exercer efetivamente seu controle sobre seus próprios dados.

A legislação também estabelece os direitos e deveres tanto dos titulares quanto dos agentes de tratamento de dados. Os titulares possuem direitos, como o acesso aos seus dados, a correção de informações incorretas, a exclusão de dados desnecessários ou excessivos, a portabilidade dos dados para outros serviços, entre outros. Por sua vez, os agentes de tratamento têm o dever de garantir a segurança e a confidencialidade dos dados, adotar medidas técnicas e organizacionais adequadas para protegê-los e cumprir todas as normas estabelecidas na legislação.

No contexto da LGPD, os agentes de tratamento referem-se às empresas, organizações ou indivíduos que coletam, armazenam, utilizam ou compartilham dados pessoais. Esses agentes podem ser tanto controladores (responsáveis pelas decisões sobre o tratamento dos dados) quanto operadores (encarregados de realizar o tratamento dos dados em nome dos controladores).

É importante ressaltar que a LGPD estabelece a responsabilidade civil dos agentes de tratamento em caso de descumprimento das normas previstas na legislação. Isso significa que, em situações de violação da privacidade ou danos causados aos titulares de dados, os agentes de tratamento podem ser responsabilizados e estar sujeitos a sanções, como multas e indenizações.

Dessa forma, a LGPD busca estabelecer um equilíbrio entre a proteção dos direitos dos titulares de dados e a promoção de boas práticas no tratamento dessas informações, incentivando a transparência, a segurança e a responsabilidade por parte dos agentes de tratamento.

REFERÊNCIAS

ARAÚJO, Vitor Eduardo Lacerda; FIGUEREDO, Douglas Dias Vieira de. Análise jurídica dos incidentes de segurança e a responsabilidade civil no Brasil. In: GROSSI, Bernardo Menicucci (org.). **Lei Geral de Proteção de Dados**: uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Fi, 2020.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil. Brasília**, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 28 de dezembro de 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidente da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 28 de dezembro de 2022

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidente da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 30 de dezembro de 2022

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 28 de dezembro de 2022

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 3. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo**. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FIGUEIREDO, Luciano Lima; FIGUEIREDO, Roberto Lima. **Direito civil: obrigações e responsabilidade civil**. 11. ed. Salvador: Juspodivm, 2020.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil: responsabilidade civil**. 23. ed. São Paulo: Saraiva Educação, 2021.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2020.

OLIVA, Milena Donato; VIÉGAS, Francisco de Assis. Tratamento de dados para a concessão de crédito. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord**.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 6, p. 555-594.

OLIVEIRA; Marco Aurélio Belizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2020.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018** (LGPD). São Paulo: Saraiva Educação, 2020.

SOUZA, Carlos Affonso Pereira de. Segurança e sigilo dos dados pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 15, p. 413-437.

QUINTILIANO, Leonardo. Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD). *In*: TEIXEIRA, Clever Marcos. **Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD)**. [*S. l.*], 17 mar. 2021. Disponível em: https://iapd.org.br/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/#:~:text=A%20LGPD%20%C3%A9%20fruto%20da,proemin%C3%AAncia%20no%20texto%20final%20aprovado.

TASSO, Fernando Antonio. **A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor**. **Cadernos Jurídicos**, São Paulo, v. 53, n. 1, p. 97-115, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_1_interface_entre_a_lgpd.pdf?d=637250344175953621. Acesso em: 02 de janeiro de 2023.