VI ENCONTRO VIRTUAL DO CONPEDI

DIREITOS E GARANTIAS FUNDAMENTAIS II

DANIELA MENENGOTI RIBEIRO

ELOY PEREIRA LEMOS JUNIOR

VIVIAN DE ALMEIDA GREGORI TORRES

D597

Direitos e garantias fundamentais II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Daniela Menengoti Ribeiro; Eloy Pereira Lemos Junior; Vivian de Almeida Gregori Torres – Florianópolis; CONPEDI, 2023.

Inclui bibliografia
ISBN: 978-65-5648-744-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito e Políticas Públicas na era digital

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direitos. 3. Garantias fundamentais. VI Encontro Virtual do CONPEDI (1; 2023; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VI ENCONTRO VIRTUAL DO CONPEDI

DIREITOS E GARANTIAS FUNDAMENTAIS II

Apresentação

Advindos de estudos aprovados para o VI Encontro Virtual do CONPEDI, realizado entre os dias 20 a 24 de junho de 2023, apresentamos à comunidade jurídica a presente obra voltada ao debate de temas contemporâneos cujo encontro teve como tema principal “Direito e Políticas Públicas na Era Digital”.

Na coordenação das apresentações do Grupo de Trabalho “Direitos e Garantias Fundamentais II” pudemos testemunhar relevante espaço voltado à disseminação do conhecimento produzido por pesquisadores das mais diversas regiões do Brasil, vinculados aos Programas de Mestrado e Doutorado em Direito. Os estudos que compõem esta obra reafirmam a necessidade do compartilhamento das pesquisas direcionadas aos direitos e garantias fundamentais, como também se traduzem em consolidação dos esforços para o aprimoramento da área e da própria Justiça.

Nossas saudações aos autores e ao CONPEDI pelo importante espaço franqueado a reflexão de qualidade voltada ao contínuo aprimoramento da cultura jurídica nacional.

Daniela Menengoti Ribeiro

Universidade Cesumar

Eloy Pereira Lemos Junior

Universidade de Itaúna - MG

Vivian de Almeida Gregori Torres

Universidade Federal do Mato Grosso do Sul

VAZAMENTO DE DADOS E A LEI GERAL DE PROTEÇÃO DE DADOS: DESAFIOS E MÁ APLICAÇÃO

DATA LEAKAGE AND THE GENERAL DATA PROTECTION LAW: CHALLENGES AND MISUSE

Marina Grothge de Lima [1]
Jéssica Amanda Fachin [2]

Resumo

O objetivo deste trabalho é compreender a proteção de dados no Brasil, em especial, a partir da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), a fim de discutir sua abrangência e entender sua aplicação. A presente pesquisa busca responder à seguinte pergunta (problema): os atuais dispositivos da referida lei são suficientes para proteger os indivíduos de vazamentos de dados pessoais? Nesse sentido, o artigo estuda as consequências da má aplicação da referida lei, suas consequências em casos concretos e como o tema pode ser aperfeiçoado. A pesquisa terá como método aplicado o teórico-dogmático, com a análise de axiomas de doutrinas, leis e análise de casos concretos para direcionar o conhecimento. Serão questionados conceitos, princípios e aplicações legais, de forma a objetivar seu melhoramento prático dentro da sociedade atual. O objetivo deste estudo é explorar o tema da lei de proteção de dados a fim de melhorar sua eficácia, buscando meio viáveis para sua aplicação.

Palavras-chave: Lgpd, Vazamento de dados, Direitos humanos, Informações pessoais, Proteção

Abstract/Resumen/Résumé

The objective of this work is to explore the concept and depth of the articles of the General Law for the Protection of Personal Data (Law nº 13.709/2018), in order to discuss its scope and understand its application. Throughout the research, the following question is faced: are the current provisions of the law sufficient to protect individuals from leaks of personal data? The article will study the consequences of the misapplication of that law, its consequences in concrete cases and how the theme can be improved. The research will have as applied the theoretical-dogmatic, with the analysis of axioms of doctrines, laws and analysis of methods of concrete cases to direct the knowledge. Concepts, principles and legal applications will be

[1] Graduada em Direito na Universidade Federal da Grande Dourados (UFGD). Mestranda no Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias das Faculdades Londrina.

[2] Doutora em Direito Constitucional (PUCSP). Mestre em Ciência Jurídica (UENP). Coordenadora de Pós-Graduação (IDCC). Professora no Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias das Faculdades Londrina.

questioned, in order to aim at their practical improvement within today's society. The aim of this study is to explore the subject of data protection law in order to improve its effectiveness, looking for viable means for its application.

Keywords/Palabras-claves/Mots-clés: Lgpd, Data leakage, Human rights, Personal information, Protection

INTRODUÇÃO

A internet se tornou parte indispensável da vida da humanidade, ocasionando uma revolução em questão de compartilhamento de informação e comunicação, gerando impacto em todos os setores sociais. Através dela, as pessoas começaram a expor sua vida, publicando em redes sociais fotos particulares de lugares que frequentam, amigos, interesses, dentre outras informações que antes eram consideradas parte da privacidade e intimidade de um indivíduo.

Esta grande mudança afeta diretamente as relações humanas. A comunicação entre duas pessoas se tornou muito mais rápida, por meio de mensagens instantâneas em plataformas digitais, bem como possibilitou que indivíduos que moram longe um do outro possam manter o contato constantemente.

Ocorre que, apesar das inúmeras vantagens, há de mesmo modo desvantagens advindas de toda esta exposição das frações de suas vidas. Os cidadãos ficam sujeitos a aplicação de golpes e roubo de informações pessoais, fatos que podem trazer consigo consequências muito graves, tanto patrimoniais quanto físicas e morais.

Deste modo, é necessário proteger tais informações pessoais, inclusive em relação ao acesso irrestrito e amplo por agentes de tratamento, tanto de iniciativa privada quanto de iniciativa pública. Os agentes de tratamento correspondem aos indivíduos que serão responsáveis por manipular os dados pessoais de outrem, o que inclui coletar, transmitir, armazenar, utilizar e até mesmo eliminar.

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), conhecida como LGPD, foi criada com este objetivo. Ela coloca em foco a proteção da privacidade e livre iniciativa, fixando princípios, diretrizes e fundamentos para garantir referidos direitos fundamentais, que muitas vezes acabam esquecidos por outros dispositivos legais. O presente trabalho busca explorar esta lei, realizando uma análise crítica em relação a seus pontos positivos e negativos.

Na primeira parte do artigo, busca-se estudar o conceito da LGPD e seus princípios, expondo os fundamentos de seus principais artigos. Na segunda parte do trabalho, dedica-se ao estudo dos direitos humanos, visto que, mesmo com a vigência desta lei, a ocorrência de vazamento de dados é constante, prejudicando profundamente a vida das pessoas. O que se observa muitas vezes é o não entendimento da importância da proteção de dados pessoais, e a ignorância em relação a suas consequências. Na terceira parte, o estudo se voltará à análise de um caso concreto, e responderá perguntas levantadas ao longo do estudo, como a eficácia da LGPD dentro da sociedade e como sua aplicação pode ser mais eficiente.

1. LGPD: CONCEITO E OBJETIVO

A Lei Geral de Proteção de Dados, mais conhecida como LGPD (Lei 13.709/2018), foi promulgada com o fim de proteger a liberdade, a privacidade e a personalidade da pessoa natural, todos como direitos fundamentais dos indivíduos. Embora haja relação com tais valores constitucionais, entendeu-se a proteção de dados como direito fundamental autônomo, que atualmente encontra assento da Constituição Federal.

Nesse sentido, a lei objetiva criar um cenário pautado na segurança jurídica, padronizando regulamentos e práticas a fim de resguardar os dados pessoais dos cidadãos presentes no Brasil, com base em parâmetros internacionais preexistentes (MPF, 2023).

Para que a LGPD tenha efeitos concretos, foi criada a Autoridade Nacional de Proteção de Dados (ANPD). Ela consiste em um órgão independente que faz parte do Poder Executivo, e é responsável pela fiscalização e divulgação dos dados pessoais utilizados pelas empresas. Assim, pode-se dizer que a criação da ANPD objetiva garantir o cumprimento da LGPD (ANPD, 2021).

Antes de iniciar-se o estudo mais aprofundado sobre esta lei, é imperioso destacar a nomenclatura da legislação. Apesar da menção à proteção de dados pessoais, não são eles que são propriamente protegidos, e sim a pessoa titular dos dados. Nesse sentido, Doneda aponta este aspecto da lei:

> A própria expressão proteção de dados não reflete fielmente seu âmago, pois é resultado de um processo de desenvolvimento do qual participaram diversos interesses em jogo- não são os dados que são protegidos, porém a pessoa à qual tais dados se referem (DONEDA, 2006, p. 118).

O referido texto legal foi aprovado em 2018. Porém, apenas entrou em vigência no ano de 2020, sendo que a Autoridade Nacional de Proteção de Dados (ANPD) foi autorizada a aplicar sanções a partir de agosto de 2021. Após entrar em vigor, o Brasil foi inserido no grupo de países que possuem regulamento específico para proteção de dados, inspirado em grande parte pelo Regulamento Geral sobre Proteção de Dados da Europa.

A LGPD busca proteger os dados pessoais tratados por pessoa natural ou jurídica de direito público ou privado, e não apenas nos meios físicos, mas também nos meios digitais (de acordo com o expresso em seu artigo 1º). Desse modo, sua grande inovação se encontra no fato de possibilitar ao cidadão o acesso a informações essenciais relacionadas ao modo que

seus dados são coletados, processados e armazenados, assegurando à Autoridade Nacional de Proteção de Dados a competência necessária para fiscalização das organizações.

Entender o conceito de dado pessoal é fundamental para conseguir compreender a importância desta lei. O artigo 5º, inciso I, descreve os dados pessoais como informações ligadas a pessoa natural identificada ou identificável. Isso significa que o dado pessoal pode gerar a identificação sozinho ou pode gerá-la combinado com outros dados, ampliando assim o leque de proteção para os indivíduos (SAAD, 2021, p. 24-25).

Como o objetivo da lei é a proteção de dados pessoais, as pessoas jurídicas não são incluídas pela LGPD. Outras situações também não são inclusas pelo dispositivo, como afirma o seu artigo 4º, destacando-se alguns tratamentos específicos, como o jornalístico e a segurança pública[1].

Apesar da exclusão das situações acima mencionadas, a aplicação material da lei é ampla. Em seu artigo 3º, fica expresso que ela resguarda operações de tratamento ocorridas no Brasil ou que ofereçam bens e serviços a pessoas presentes em território nacional, independentemente do país onde estejam localizados a sede ou os dados.

Caso haja descumprimento do estabelecido na LGPD, os agentes responsáveis pelos danos estarão sujeitos a sanções, de acordo com o estabelecido nos artigos 52 a 54 da referida lei. As principais sanções consistem em advertência, multas, publicização da infração após confirmada sua ocorrência, e até mesmo bloqueio e eliminação dos dados pessoais a que se refere a infração, dentre outras.

As operações de tratamento de dados possuem três grandes figuras, introduzidas na legislação pela LGPD. Cada uma delas possui um papel específico e importante dentro desta nova lei, visando sempre o respeito aos direitos humanos. Tem-se assim os agentes de tratamento de dados, chamados de controlador e operador, e o encarregado.

---

[1] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II - realizado para fins exclusivamente:
a) jornalístico e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou
IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

O controlador pode ser definido como “pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais” (BRASIL, 2018), de acordo com o inciso VI do mesmo artigo. Assim, esta figura representa a empresa que demanda o tratamento dos dados, sendo possível a própria empresa realizar esta função ou contratar um operador para realizá-la.

O controlador tem a obrigação de seguir o disposto na LGPD, respeitando seus princípios e orientando o operador para tal, a fim de trabalhar dentro dos limites da lei. Ele responderá por danos materiais, morais, individuais e coletivos que resultem de suas ações, respondendo inclusive solidariamente por danos causados pelo operador, quando estiver envolvido diretamente no tratamento de dados (QUEIROZ, 2022, p. 71-73).

O operador, como mencionado anteriormente, é uma figura que cumpre ordens, sempre respeitando os dispositivos legais. Ele se refere a um terceiro, contratado pelo controlador, para realizar o tratamento de dados. O operador seria como um subcontratante, que deve respeitar as diretrizes estabelecidas pelo controlador, bem como as políticas de privacidade e ordenamento jurídico.

A diferença entre o operador e o controlador está no poder de decisão, já que o operador só age dentro dos limites e finalidades determinadas pelo controlador. Responde pelos danos causados, assim como o controlador, possuindo dever de repará-los. A responsabilidade solidária também está presente, caso descumpra a legislação e não siga as instruções do controlador (QUEIROZ, 2022, p. 74-75).

Por fim, tem-se o encarregado. Nas palavras do inciso VIII do artigo 5º da LGPD, esta figura refere-se à “pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)” (BRASIL, 2018...). Isso significa que possui a responsabilidade legal de estabelecer a comunicação entre os titulares de dados e a autoridade nacional, sendo necessariamente indicado pelo controlador, e não pelo operador, sem previsão expressa neste sentido.

O encarregado deve esclarecer fatos, direitos, tomar providências e fornecer orientações internas. Importante ressaltar, porém, que não há previsão sobre o encarregado responder legalmente. Logo, a responsabilidade será do controlador ou operador, dependendo do caso concreto, cabendo ao controlador sua devida fiscalização, já que é de seu próprio interesse que o encarregado exerça sua função de acordo com a lei. Para que o encarregado

seja responsabilizado, há necessidade de comprovar o nexo causal e a culpa do mesmo, com sua responsabilidade sendo assim subjetiva (QUEIROZ, 2022. P. 71 e 77).

O bom trabalho das três figuras anteriormente conceituadas é essencial para garantir a proteção do direito à privacidade dos cidadãos. Mas para entender a importância desta função, é necessário compreender quais os tipos de dados existentes, e o próprio tratamento que estes devem receber.

Importante registrar que os dados sensíveis correspondem aos dados de "origem racial ou ética, 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", de acordo com os dizeres do inciso II do artigo 5º da LGPD. Eles possuem maior potencial de prejudicar o titular, pois se relacionam a questões sensíveis que podem gerar alguma discriminação.

Estes dados possuem um tratamento especial, que só pode ocorrer em algumas hipóteses, listadas pelo artigo 11: no caso de o titular consentir de forma específica, para finalidades específicas, ou se for informação indispensável para certas ações, descritas no segundo inciso do referido artigo. Algumas dessas ações incluem cumprimento de obrigação legal, exercício regular de direitos, proteção da vida do titular ou de terceiro e tutela da saúde em procedimento realizado por profissionais da saúde, autoridade sanitária ou serviços de saúde (FERRACIOLI, 2022, p. 15-16).

Já os dados anônimos são definidos no inciso II do artigo 5º da LGPD como aqueles relativos à titulares que não possam ser identificados. Essa ocultação de informações sensíveis ocorre antes da disponibilização das informações para uso, impossibilitando a identificação do perfil do titular de dados antes do processo (FERRACIOLI, 2022, p. 16).

Dados relacionados a crianças e adolescentes também ganharam uma atenção especial na LGPD, sendo classificados como dados especiais. Afinal, estes possuem uma condição vulnerável e merecem proteção específica. A lei afirma que o tratamento dos dados pessoais de menores de idade sempre deverá ser realizado "em seu melhor interesse, ou seja, de acordo com as diretrizes das normas protetivas legais e constitucionais preexistentes.

O artigo 14 da LGPD expõe que o tratamento dos dados de crianças (até 12 anos incompletos) depende do consentimento específico de pelo menos um dos pais ou responsável legal. Se ocorrer divergência entre as opiniões dos pais em relação ao assunto, entende-se que

a ação mais segura se tomar é suspender o tratamento até que exista maior clareza jurídica de vontades (COTS; OLIVEIRA: 2019, p.115-116).

O elevado grau de transparência é um elemento de extrema importância no tratamento de dados pessoais, não somente de crianças, mas de indivíduos em geral. Apesar de ter uma exigência maior quando relacionado às crianças, a transparência é um dos princípios que norteiam a LGPD. Desse modo, deve ser disponibilizado aos titulares, pelo controlador, a qualquer momento, acesso irrestrito e livre aos dados objetos de tratamento (BOTELHO, 2020, p. 217-218). Feigelson e Siqueira também destacam a importância da transparência:

> Na perspectiva do princípio da transparência, o art. 9º, § 1º, da LGPD estabelece que o consentimento será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca (FEIGELSON; SIQUEIRA: 2019, p. 38)

Qualquer dado que tenha o potencial de identificar uma pessoa são importantes para o Estado, e consequentemente, merece proteção constitucional. Este foi o entendimento jurisprudencial estabelecido em acórdão pelo Supremo Tribunal Federal. Seguindo este entendimento, todos os dados merecem serem protegidos por tutela constitucional, tendo uma maior abertura e flexibilidade em relação ao tema (CORREA, 2020, p. 65).

Outros princípios norteadores da Lei nº 13.709/2018 incluem o princípio da boa-fé, da finalidade (o propósito do tratamento de dados deve ser legítimo, específico e explícito, compatível com sua finalidade), da adequação (não adianta esclarecer a finalidade, e na prática atuar de modo diferente do expresso ao titular) e da necessidade. Este último tem a função de limitar o tratamento de dados ao mínimo necessário para cumprir com sua finalidade, envolvendo a extração de dados pertinentes, não excessivos e proporcionais (QUEIROZ, 2022. p. 64-66).

O princípio do livre acesso tem como função garantir ao titular uma consulta facilitada e gratuita em relação a forma e duração do tratamento, assim como sobre a integralidade dos dados analisados. Isso permite que o titular acompanhe toda a utilização de seus dados pessoais, e possibilita que este avalie eventuais inexatidões a serem corrigidas (QUEIROZ, 2022. p. 67).

O princípio da segurança fornece ao titular embasamento para utilizar medidas técnicas e administrativas aptas a resguardarem dados pessoais não autorizados e ligados à situações acidentais ou ilícitas envolvendo perda, alteração, destruição, comunicação ou difusão. Sua base legal se encontra no capítulo VII da LGPD, voltado à segurança e boas práticas (QUEIROZ, 2022. p. 69).

Esta grande preocupação é justificada, visto que há um alto risco de violação dos direitos dos titulares. Os vazamentos de dados são constantes, e geram grandes consequências negativas na vida das pessoas. Muitas vezes, eles poderiam ser evitados, se houvesse uma aplicação mais efetiva da lei, bem como aprimoramento de seus dispositivos legais, como veremos nos próximos tópicos.

2. VAZAMENTOS DE DADOS E A LGPD

A proteção à privacidade e à intimidade está presente na Constituição Federal, em seu artigo 5º, inciso X e XI, com este declarando serem invioláveis a vida privada, a honra, a imagem e a casa das pessoas, assegurando o direito a indenização por dano material ou moral decorrente de sua violação.

Destaca-se que não são apenas tais dispositivos que se relacionam com a proteção de dados, visto que os incisos XIV, IX e LXXII correspondem, respectivamente, a direito à informação, liberdade de expressão e proteção contra interceptação das comunicações telefônicas, telegráficas ou de dados. O instituto *habeas data* (artigo 5º, inciso LXXII) foi o primeiro remédio constitucional adequado para tutelar a proteção de dados perante o Estado, visto que inclui acesso e retificação dos mesmos (DONEDA, 2021, p. 13).

Em 20 de outubro de 2021, o Senado aprovou a Emenda Constitucional (PEC) 17/2019. Esta PEC tornou a proteção de dados pessoais um direito fundamental, inclusive nos meios digitais, e conferiu à União competência privativa para legislar sobre o tema. Foi aprovada de forma unânime, e marcou a cristalização deste direito como direito fundamental e cláusula pétrea, avançando significativamente a garantia dos direitos de privacidade dos titulares de dados (SENADO, 2021).

Doneda destaca a importância da privacidade crescendo cada vez mais dentro da sociedade moderna, e como ela é uma figura importante para a democracia:

> A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Neste papel, a vemos como pressuposto de uma sociedade democrática moderna (DONEDA, 2006, p. 99-100)

Além da proteção constitucional, antes da criação da LGPD, haviam outros institutos que continham em seus dizeres princípios de proteção contra vazamento de dados. O Código de Defesa do Consumidor é um deles, já que exige que os registros, cadastros, e dados dos consumidores sejam objetivos, claros e autênticos, bem como que sejam fáceis de compreender (em seu artigo 43). A correção de dados sempre poderá ser exigida pelo consumidor, buscando proteger o mesmo de eventuais bancos de dados que possam atingir sua personalidade (CUEVA, 2019, p. 88).

Percebe-se assim que o direito à privacidade, liberdade e intimidade é considerado um direito fundamental dos indivíduos, que já se encontrava amparado dentro da Constituição e outros dispositivos legais, mas não possuía uma lei específica para proteção. Com a LGPD, a proteção de dados ganhou contornos próprios, considerado como direito fundamental autônomo, além de proporcionar fiscalização de sua aplicação se tornou mais eficiente. Entretanto, mesmo com esta lei específica, a aplicação prática ainda possui muito espaço para evoluir, visto que a ocorrência de vazamentos de dados é muito constante dentro da sociedade.

A quantidade de dados circulando na sociedade é imensa. A transferência deles ocorre de modo dinâmico, muitas vezes sem as pessoas perceberem. Qualquer cadastro em lojas que é efetuado a fim de conseguir descontos ou benefícios exige que os indivíduos passem o número de seu CPF, telefone, RG, e-mail, dentre outros documentos. Se ocorrer uma violação ou falha na segurança, alguém deverá ser responsabilizado por essa falta de mecanismos de segurança, e precisará reparar os dados causados ao titular dos dados.

Utiliza-se a internet para inúmeras funções, incluindo armazenamento, pesquisas, compras, mensagens e transferências bancárias. Toda vez que o indivíduo utiliza algum desses serviços, as informações pessoais que ele ali deposita são gravadas. Mesmo que imperceptível ao usuário, essas informações podem ser combinadas com outros rastros e formar um perfil específico, vulnerabilizando a pessoa a atos ilícitos (SAAD, 2021, p. 28-29).

De acordo com Menke e Goulart, há quatro atributos de uma informação inerentes a sua segurança: confidencialidade, integridade, disponibilidade e resiliência (MENKE, 2020,

p. 1181). A confidencialidade diz respeito à característica que deve ser protegida contra acesso não autorizado. A integralidade tem como objetivo garantir que a informação não seja alterada durante seu ciclo de vida, apenas se houver autorização expressa. Já a disponibilidade afirma que a informação deve estar disponível quando for necessário (BEAL, 2005, p. 01). Por último, tem-se a resiliência: um atributo essencial que explica que, muitas vezes, erros ou incidentes acontecem, mas o importante é preparar os sistemas para preverem e recomporem suas funções de modo rápido e eficiente (HANSEN, 2019, p. 824).

Esses quatro atributos são passíveis de serem ameaçados por determinadas situações. A vulnerabilidade do sistema, ou seja, sua fragilidade, pode ser atingida por diversos tipos de ameaças, podendo estas serem físicas, pessoais, técnicas ou ambientais. Quando o incidente acontece, é importante desenvolver medidas capazes de impedir que o mesmo incidente ocorra novamente, ou pelo menos diminuir essa probabilidade (SMEDINGHOFF, 2008, p. 15-16).

Mesmo com o desenvolvimento das medidas acima mencionadas, há casos em que a ocorrência do incidente não consegue ser impedida, assim como os danos decorrentes do mesmo. Quando ocorre o vazamento dos dados, se torna muito difícil amenizar os prejuízos causados ao titular, uma vez que dificilmente consegue-se apagá-los dos diversos registros de pessoas e organizações que os captaram. Uma vez afetada, a confidencialidade fica comprometida como um todo, pois o poder de compartilhamento de informações pela internet é extremamente vasto (GOBEO, 2018, p. 2059).

Este vazamento pode acontecer através de várias formas. A maioria acontece por meio de ataques cibernéticos, sequestro de contas de usuários, os quais têm suas senhas vazadas, repasse incorreto de dados por funcionários de empresas, furto de equipamentos, ações de *hackers* que exploram vulnerabilidades em sistemas, bem como erros e negligências humanas, como por exemplo se desfazer um pen drive que contém dados pessoais sem tomar as medidas necessárias (CERT, 2021, p. 02).

Em uma pesquisa anual da IBM, feita em parceria com o Instituto Ponemon de 2019 (*Cost of a Data Breach*, traduzida em português como “o custo da violação de dados”), houve a avaliação de mais de 500 empresas de 16 regiões e países, com 35 delas ocorrendo no Brasil. No final da pesquisa, concluiu-se que o Brasil era o quarto país que mais possuía informações vazadas, sendo que em 2018 era o quinto. Percebe-se que o número de informações vazadas aumentou em um ano, ao invés de diminuir (HERNANDEZ, 2019).

Em 2021, o Brasil ainda continuava sendo um país caracterizado por constantes vazamentos. Castilho destaca este aspecto, explicando o fato segundo dados levantados pela empresa *Surfshark*, atuante na área de privacidade e segurança online:

> Em 2021, o Brasil foi o sexto país mais atingido por vazamentos de dados, de acordo com um levantamento da empresa Surfshark, que atua na área de ferramentas de privacidade e segurança online. No âmbito empresarial não foi diferente. Só no primeiro semestre de 2021, pelo menos 69 instituições brasileiras foram alvo de ataques de vazamento e sequestro de dados, conforme dados da Apura Cyber Intelligence (CASTILHO, online, 2022).

Quando um vazamento ocorre, é preciso primeiramente buscar sua fonte de origem. Muitas vezes, os funcionários da empresa têm seus direitos de acesso roubados por hackers, os quais se disfarçam dentro da empresa para conseguirem dados corporativos. Porém, não se pode descartar a possibilidade de que o próprio colaborador possa estar agindo de má-fé, passando dados a terceiros não autorizados. Os Tribunais de Justiça brasileiros se encontram com um aumento significativo no número de processos envolvendo vazamento de dados, como por exemplo este caso, em que a pessoa ganhou indenização por danos morais:

> DANO MORAL – VAZAMENTO DE DADOS – CÓDIGO DE DEFESA DO CONSUMIDOR – DEVER DE SEGURANÇA. 1 – Reconhecida a falha no sistema, ante a invasão por terceiros, ocasionando o vazamento de dados pessoais do consumidor, patente o dever de indenizar pelos danos morais sofridos; 2 – Indenização por danos morais fixada no montante pleiteado, ou seja, em R$ 10.000,00, corrigidos do arbitramento e acrescido de juros de mora de 1% ao mês, a partir da citação. RECURSO PROVIDO
>
> (TJ-SP - AC: XXXXX20218260405 SP XXXXX-71.2021.8.26.0405, Relator: Maria Lúcia Pizzotti, Data de Julgamento: 25/08/2021, 30ª Câmara de Direito Privado, Data de Publicação: 13/09/2021)

Se torna de extrema importância, deste modo, o desenvolvimento de soluções que diminuam consideravelmente os riscos de vazamento de dados, conscientizando as pessoas e empresas dos perigos que essas situações podem apresentar. Apenas assim será possível aumentar a diligência em relação aos mecanismos de proteção.

3. CONTORNOS E SOLUÇÕES DE VAZAMENTO DE DADOS DO BRASIL: UM CASO BRASILEIRO

Em 2021, ocorreu um grande vazamento de dados no Brasil, o qual comprometeu informações de 223 milhões de brasileiros[2]. Essas informações apareceram em fóruns utilizados por criminosos digitais, e estavam separadas por número de CPF e acompanhadas por informações relacionadas a veículos cadastrados no país.

Em realidade, o que aconteceu foi que existiram dois vazamentos diferentes. Um deles continha os dados acima mencionados, estando em livre circulação dentro da internet e até mesmo disponível para download. Já o outro era muito mais abrangente, e se referia a dados de escolaridade, renda, programas sociais, benefícios do INSS, dentre outras informações, com uma distribuição bem mais limitada.

Ao analisar o número de brasileiros expostos, observa-se que quantia é maior que a população brasileira em si. Isso ocorre porque o vazamento incluía CPF de pessoas falecidas. Um terceiro vazamento ocorreu logo depois, disponibilizando informações sobre empresas atreladas aos CPFs. Neste caso específico, os criminosos não disponibilizaram a fonte da informação, como por exemplo um banco ou uma seguradora. Desse modo, há possibilidade que tal pacote de dados tenha sido resultado de diversas fontes, até mesmo de vazamentos anteriores (G1, online, 2021).

O objetivo dos criminosos é vender os referidos dados, sendo possível apenas a comprar de trechos dos mesmos, com a oferta não cobrindo sua integralidade. O problema se agrava ainda mais com a existência da *Dark Web*, a "parte obscura da internet", que não possui fiscalização do governo e é atrelada à atividades ilícitas. A maioria dos infratores acaba vendendo as informações vazadas para a *Dark Web*, caindo nas mãos de indivíduos com más intenções que tem o poder de prejudicar muito as vítimas do vazamento (SANTOS, 2022, p. 08).

Grande parte das informações vazadas não eram públicas. Porém, algumas podem facilmente ser obtidas em portais governamentais ou serviços privados. Apesar dos dados já serem públicos, criminosos ou empresas podem copiá-los e organizá-los com o objetivo de facilitar operações de marketing e crédito, no caso de empresas, ou utilizá-los para cometer fraudes, no caso de criminosos. Perfis em redes sociais também fornecem muitos dados das pessoas, incluindo fotos. Ao se apropriarem da foto de perfil de um indivíduo, os criminosos

[2]Nesse sentido, ver: Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. G1. Economia. 28/01/2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em 10/04/2023.

conseguem se passar por ele a fim de aplicarem golpes, na maioria das vezes pedindo dinheiro aos contatos da vítima.

O vazamento de dados além de prejudicar imensamente as vítimas, gera prejuízos financeiros enormes. Em 2023, o custo de recuperação ultrapassou vinte e seis milhões de reais. O número foi fornecido pela empresa de segurança digital *Acronis*, que, em seu relatório, aponta o aumento de 60% em incidentes de *phishing* (técnica de engenharia social que utiliza fraude eletrônica para furtar informações confidenciais) e engenharia social em 2022. Na pesquisa, o Brasil aparece como sendo um dos países mais atingidos, ao lado da Alemanha e dos Estados Unidos (CANALTECH, online, 2023).

No entanto, o Brasil não é o único atingido por esses incidentes. Uma instituição de crédito norte-americana chamada *Equifax* foi vítima de um vazamento de documentos privados em 2017. Os dados vazados pertenciam à 147 milhões de clientes, de diversos países. Neste caso, a causa do vazamento foi mais clara: os invasores conseguiram identificar falhas de segurança no sistema da empresa, que incluía os processos de encriptação, e procederam a coleta de informações, que durou meses. Foi assinado um acordo global entre a empresa, a agência americana responsável pelo caso (*Federal Trade Commission*), o *Consumer Financial Protection Bureau* e 50 estados e territórios dos Estados Unidos, a fim de auxiliar as vítimas afetadas pela violação de dados (FRUHLINGER, online, 2020).

Percebe-se assim que a implementação da Lei Geral de Proteção de Dados nas empresas é de extrema necessidade, mas ela deve ser realizada atendendo-se a todos os requisitos de adequação. Deve-se respeitar os processos de governança corporativa e implementar programas de compliance digital consistentes. Para isso, é necessário investir e atualizar ferramentas de segurança de dados, bem como revisar documentos e aprimorar os procedimentos e fluxos internos e externos dos dados, sempre com a presença de mecanismos de controle (PINHEIRO, 2021, p. 25).

A definição da equipe responsável pelo acompanhamento do tratamento dos dados, ou seja, o comitê de privacidade, é um passo muito importante. Logo após, se torna essencial mapear o fluxo dos dados. Entender o ciclo de vida dos dados é uma ferramenta indispensável para protegê-los. Nesta etapa, a empresa deve deixar claro determinados fatores, como por exemplo quais dados são coletados, quais canais realizam a coleta, onde eles são armazenados, quem os manipula e quais deles são compartilhados com parceiros externos.

Mapeado o fluxo de dados, analisa-se o panorama completo do ciclo de vida dos dados e verifica-se o embasamento legal. Afinal, é preciso verificar se existe necessidade de coletar tais dados e se há enquadramento do tratamento dos dados nos princípios da LGPD, e para fazer isso, é imprescindível haver transparência e comunicação com o titular dos dados, como já discutido no tópico anterior, assim como estabelecer uma pessoa para exercer o cargo de encarregado de dados. Com exceção de pequenas empresas e startups, o cargo é obrigatório, e vem sendo ocupado por advogados, consultores e profissionais de segurança da informação (FERRACIOLI, 2022, p. 19-20).

Há medidas administrativas e técnicas a serem tomadas, tanto por organizações como pelas pessoas, a fim de garantir que as ações estejam em conformidade com a lei. As administrativas se referem às medidas que focam na instituição como um todo, corroborando para atuações de acordo com a LGPD.

O Recital 78 do Regulamento Geral de Proteção de Dados Pessoais (GPDR) diz respeito a textos que acrescentam informações explicativas sobre o sentido dos artigos do regulamento, e expressa a importância de adotar orientações internas que respeitem a proteção de dados e medidas que destaquem o uso minimizado dos mesmos. Isso significa que, na prática, deve-se permitir o acesso apenas para os indivíduos da área que realmente os utilizem para realizar suas tarefas (SAAD, 2021, p. 38).

As medidas técnicas incluem o uso de *firewalls*, *antimalware*, *tokens* (identificadores ou palavras-chave), antivírus, criptografia, entre outras, sempre visando proteger o sistema de ataques cibernéticos. O firewall é um tipo de proteção responsável pela análise do tráfego da rede. Apenas assim é possível determinar a execução de operações de recepção ou transmissão de dados, e consequentemente aprovar somente os que estão em conformidade com as regras estabelecidas. O *antimalware* é um recurso de proteção contra vírus, impedindo arquivos de serem infectados e deletados. Tais medidas são essenciais para a proteção dos dados dos titulares e para a eficácia da LGPD (SAAD, 2021, p. 39).

Em 2021, foi lançado pela Autoridade Nacional de Proteção de Dados Pessoais um Guia Orientativo sobre Segurança de Informação para Agentes de Tratamento de Pequeno Porte. No guia, reconhece-se que todas as implementações e medidas são um elevado investimento, e podem excessivamente onerar agentes de tratamento de empresas de pequeno porte. Por este motivo, apresenta algumas medidas de segurança com capacidade de promover um aumento na segurança do ambiente institucional (ANPD, online, 2021).

Todas essas ações e medidas auxiliam para uma melhor aplicação da LGPD, evitando fraudes e vazamentos de dados. Porém, deve-se também estudar como agir caso haja o descumprimento da lei. Afinal, mesmo com medidas preventivas, é impossível evitar totalmente que acidentes aconteçam. A fiscalização é feita pela Autoridade Nacional de Proteção de Dados, e o não cumprimento das obrigatoriedades legais pode levar a multa de 2% sobre o faturamento da empresa (mas com limite de até 50 milhões) por infração cometida, bem como suspender parcialmente o direito de funcionamento e suspender o alvará de funcionamento por tempo indeterminado.

A LGPD, entretanto, traz em seu texto somente as sanções administrativas. Apesar de incentivarem a aplicação das medidas mencionadas anteriormente, elas muitas vezes não possuem força suficiente para punirem os infratores e desincentivarem o descumprimento da lei. Por este motivo, é preciso aplicar o Código Penal subsidiariamente à LGPD e outros dispositivos legais. Com ele, se torna possível imputar crimes às condutas relativas à tratamento e manipulação de dados pessoais indevida (FERRACIOLI, 2022, p. 27).

Analisa-se um caso hipotético: um empregado da empresa, observando o descuido de seu empregador, aproveita o momento para extrair dados do computador de trabalho para si. Seria possível enquadrar o comportamento ilícito deste empregado dentro do crime de furto, presente no artigo 155 do Código Penal (afinal, o indivíduo subtraiu, para si, coisa alheia móvel).

Há diversos entendimentos doutrinários sobre o assunto. Porém, o predominante diz respeito ao fato de que os dados pessoais têm valor econômico. E se possuem valor econômico, podem ser caracterizados como bens móveis, possibilitando a imputação dos agentes no crime praticado. A jurisprudência, ainda que não esteja totalmente consolidada no assunto, entende que é devida reparação individual ou coletiva, devendo-se apenas comprovar a ocorrência do dano ao consumidor:

> Apelação. Ação de indenização por danos morais. Prestação de serviço de telefonia. Direito do Consumidor. Responsabilidade civil. Sentença de improcedência. Recurso do Autor. Ré que confirmou dados do Autor à pessoa estranha não titular da linha telefônica. Conduta perpetrada pela Ré que violou seu dever de sigilo de dados. Ofensa aos ditames da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD). Falha na prestação de serviço verificada. Responsabilidade objetiva do prestador de serviço. Risco da atividade que não pode ser transferido ao consumidor. Situação que levou ao fim do noivado do Autor. Indenização por danos morais no importe de R$10.000,00 (dez mil reais). Sentença reformada.

> Litigância de má-fé afastada. Sucumbência invertida. RECURSO PROVIDO. (TJSP.AC 1065936-51.2020.8.26.0002 SP, Relator: L.G. COSTA WAGNER, Data do Julgamento: 20/02/2022, 34ª Câmara de Direito Privado, Data de Publicação: 28/02/2022. p.1).

No caso jurisprudencial acima, uma empresa telefônica confirmou dados de um indivíduo a uma pessoa que não era titular da linha telefônica. Essa conduta atentou contra os princípios e dizeres dos artigos da LGPD, expondo os dados do titular a terceiro, e ocasionando o fim de seu noivado. Foi possível confirmar claramente os danos que a má prestação de serviços ocasionou ao consumidor, e por isso a empresa foi condenada a indenizá-lo moralmente na quantia de R$10.000,00.

A LGPD, desse modo, consolidou-se como a primeira lei que juntou princípios e diretrizes específicas para a proteção da privacidade e personalidade das pessoas naturais. Ela foi um marco dentro da proteção dos direitos fundamentais, surgindo diante da necessidade de resguardar os mesmos dentro de um mundo globalizado e com enorme fluxo de circulação de informação. Como qualquer dispositivo legal, a LGPD não abarca todas as situações concretas, e não foca na punição legal dos infratores, devendo as empresas tomarem as medidas necessárias para impedir que vazamentos de dados ocorram, de acordo com o comentado neste tópico do trabalho.

CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados Pessoais foi criada em 2018, diante da necessidade de proteger o direito fundamental das pessoas relacionado à privacidade e liberdade. Ela traz princípios e conceitos essenciais ao mundo globalizado e digital em que se vive atualmente, como as figuras do controlador, operador e encarregado, que surgem para garantir que os dados dos titulares não caiam nas mãos de infratores ou terceiros não autorizados. A criação da Autoridade Nacional de Proteção de Dados (ANPD) também contribuiu significativamente para o avanço desta proteção.

A Lei nº 13.709/2018 traz consigo diversos princípios que norteiam o manuseio responsável de dados pessoais, como por exemplo o princípio da boa-fé, da finalidade, da adequação e da necessidade. Destaca que é direito do cidadão ter acesso ao modo que seus dados são coletados, processados e armazenados, explicando que a transparência entre o controlador e o titular é um elemento que sempre deve estar presente.

Após um estudo aprofundado dos conceitos e diretrizes legais da LGPD, se torna essencial compreender a gravidade do vazamento de dados. Em 2021, um vazamento de dados comprometeu informações de 223 milhões de brasileiros, número maior que a população total do país na época porque também continha informações de pessoa já falecidas. Esses dados foram publicados em fóruns utilizados por criminosos digitais, incluindo número de CPF e informações de veículos dos titulares. Os infratores vendiam referidos dados, inclusive publicando-os na *Dark Web*, o que poderia ocasionar danos irreparáveis às vítimas. Muitas vezes, o vazamento de dados pode até ocasionar sequestros e comprometer a integridade física das pessoas, sem mencionar o dano patrimonial e emocional.

Percebe-se assim que a aplicação da LGPD é essencial às empresas, a fim de evitar danos permanentes e tentar prevenir ataques cibernéticos, com a existência de medidas administrativas e técnicas preparadas em caso de violações de dados. A eficácia da lei depende da aderência das empresas a essas medidas, e do entendimento da importância de sua aplicação. Essas medidas incluem o uso de *firewalls, antimalware, tokens*, antivírus e criptografias. Aplicar subsidiariamente o Código penal também é um modo eficiente de desestimular os infratores de cometerem tais fraudes, visto que a LGPD não traz sanções criminais relativas ao assunto.

Conclui-se assim que a criação da Lei Geral de Proteção de Dados foi um enorme avanço da proteção dos direitos fundamentais, mas ainda carece de força normativa necessária para consolidar-se em casos concretos. Ela precisa ter sua importância destacada cada vez mais, com maior taxa de aplicação de sanções administrativas e criminais, para que os vazamentos de dados possam diminuir. Apenas assim as pessoas poderão viver com a segurança e liberdade de que tanto carecem em mundo onde o avanço tecnológico é constante.

REFERÊNCIAS

Autoridade Nacional de Proteção de Dados (ANPD). **Guia Orientativo: Segurança da Informação para Agentes de Tratamento de Pequeno Porte, Versão 01**. Brasília, DF, out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em 08 abril 2023.

BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005. p. 1.

BOTELHO, Marcos César. **A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes.** Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE). Vol. 08. N. 2, 2020.

CASTILHO, Luiz Ricardo de. **O que podemos aprender com ano marcado por casos de vazamentos de dados.** Disponível em: https://www.conjur.com.br/2022-abr-19/luiz-castilho-casosvazamentos-dados2. Acesso em 05 abril de 2023. p.1.

CENTRO de estudos, resposta e tratamento de incidentes de segurança no brasil (CERT). Vazamento de Dados - Cartilha de Segurança na Internet, 2021. p. 2. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de dados pessoais comentada**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

CÔRREA et al. Tratado de proteção de dados pessoais. Editora Forense: 2020, p. 65.

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do STJ. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 85-98. ISBN 978-85- 5321-663-5. p. 88.

CUSTOS de vazamento de dados podem ultrapassar R$ 26 mi em 2023. **CANALTECH.** Disponível em**:** https://canaltech.com.br/seguranca/custos-de-vazamento-de-dados-podem-ultrapassar-r-26-mi-em-2023-34616/. Acesso em 06 abril 2023.

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

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. **Tratado de proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2021

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (coords.). **Comentários à lei geral de proteção de dados: Lei 13.709/2018**. São Paulo: Revista dos Tribunais, 2019

FERRACIOLI, Millena Christina. **A aplicação e adequação das empresas aos critérios da lei geral de proteção de dados (lgpd).** Universidade São Judas Tadeu. 2022. 33p.

FRUHLINGER, Fred. Equifax data breach FAQ: What happened, who was affected, what was the impact?, **CSO Online**, Estados Unidos, 2020. Disponível em: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html. Acesso em 07 abril 2023.

GOBEO, Antoni; FOLWER, Connor; BUCHANAN, William J. ***GDPR and Cyber Security for Business Information Systems.*** Gistrup: River, 2018. versão Kindle, p. 2059.

HANSEN, Marit. Kommentar Art. 32 DSGV. In: SIMITIS, Spiros; HORNUNG, Gerrit; SPIECKER, Indra (org.). **Datenschutzrecht: DSGVO mit BDSG**. Nomos: Baden-Baden, 2019. p. 824.

HERNANDEZ, Raphael. No Brasil, empresa que falha ao proteger dados tem perdas menores. **Folha de São Paulo.** São Paulo, 19 jul 2019. Disponível em: https://www1.folha.uol.com.br/tec/2019/07/no-brasil-empresa-que-falha-ao-proteger-dados-tem-perdas-menores.shtml. Acesso em 05 abril 2023.

LEI Geral de Proteção de Dados Pessoais (LGPD). **Brasília, DF**: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em 31 março 2023.

MEGAVAZAMENTOS de dados expõem informações de 223 milhões de números de CPF. **G1.** Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml. Acesso em 06 abril 2023.

MENKE, Fabiano; GOULART, G. D. Segurança da Informação e Vazamento de Dados. In: Bruno Et Al (coords.) Bioni. "**Tratado De Proteção De Dados Pessoais"**. São Paulo: Editora Forense. 2020, versão iBooks, p. 1181.

O QUE é a LGPD. **Ministério Público Federal.** Disponível em:< https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd>. Acesso em: 30 março 2023.

PINHEIRO, Patrícia P. PROTEÇÃO DE DADOS PESSOAIS: COMENTÁRIOS À LEI N. 13.709/2018 (LGPD). [Digite o Local da Editora]: Editora Saraiva, 2021. E-book. ISBN 9786555595123. Disponível em:

https://integrada.minhabiblioteca.com.br/#/books/9786555595123/. Acesso em: 07 abril 2023. p 25.

SAAD, Carolina de Oliveira. **A Lei Geral de Proteção de Dados Pessoais e Incidentes de Segurança: Regulação e Prática de Vazamento de Dados**. Escola de Direito Fgv Direito Rio, 2021. 55 p.

SANTOS, G.P; PRETI, A.S. Proteção geral de dados: invasão e vazamentos de dados. 2022. Disponível em https://repositorio.animaeducacao.com.br/handle/ANIMA/28140. Acesso em 06 abril 2023.

SENADO Federal aprova Proposta de Emenda à Constituição 17 (PEC 17/2019) que inclui a proteção de dados pessoais no rol de direitos e garantias fundamentais. **Gov.br.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/senado-federal-aprova-proposta-de-emenda-a-constituicao-17-pec-17-2019-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-e-garantias-fundamentais. Acesso em: 03 abril 2022.

SMEDINGHOFF, Thomas J. ***Information Security Law: The Emerging Standard for Corporate Compliance. Cambridgeshire****:* ITGP, 2008. p. 15-16.

TJ-SP - AC: XXXXX20218260405 SP XXXXX-71.2021.8.26.0405, Relator: Maria Lúcia Pizzotti, Data de Julgamento: 25/08/2021, 30ª Câmara de Direito Privado, Data de Publicação: 13/09/2021.

TJSP.AC 1065936-51.2020.8.26.0002 SP, Relator: L.G. COSTA WAGNER, Data do Julgamento: 20/02/2022, 34ª Câmara de Direito Privado, Data de Publicação: 28/02/2022. p.1.

QUEIROZ, Renata Capriolli Zocatelli. **Encarregado de proteção de dados pessoais- DPO: regulamentação e responsabilidade civil**. São Paulo: Quartier Latin, 2022. 158 p.