FUNDAÇÃO EDUCACIONAL DE ITUVERAVA
FACULDADE DR. FRANCISCO MAEDA

Julia Vaz Alves

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A EFETIVIDADE DO CONTROLE DE DIVULGAÇÃO DE DADOS PESSOAIS NO BRASIL

ITUVERAVA
2022

JULIA VAZ ALVES

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A EFETIVIDADE DO CONTROLE DE DIVULGAÇÃO DE DADOS PESSOAIS NO BRASIL

Trabalho de Conclusão de Curso apresentado à Faculdade Dr. Francisco Maeda. Fundação Educacional de Ituverava para obtenção do título de Bacharel em Direito.

Orientador: Cristina Iaroszeski

ITUVERAVA
2022

JULIA VAZ ALVES

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A EFETIVIDADE DO CONTROLE DE DIVULGAÇÃO DE DADOS PESSOAIS NO BRASIL

Trabalho de Conclusão de Curso apresentado à Faculdade Dr. Francisco Maeda. Fundação Educacional de Ituverava para obtenção do título de Bacharel em Direito.

Ituverava, _____ de _____de 2022.

Orientador: _____
Nome do Orientador

Examinador:_____
Nome do Examinador

Examinador:_____
Nome do Examinador

DEDICATÓRIA

Aos meus pais Fernando e Priscila.
Aos meus avós Vera, Rita, Renê e Wander.

AGRADECIMENTOS

Agradeço a Deus pela vida, e pela oportunidade.
Agradeço sempre, a minha família, em especial aos meus pais, Fernando e Priscila, e aos meus avós que não mediram esforços para que eu chegasse até aqui.
Aos professores do curso de Direito pelos conhecimentos transmitidos e pela compreensão ao longo de todos esses anos de aprendizado.
A todos os colegas de universidade, em especial aos amigos Maria Luisa, Vanessa, Sabrina e Maria Julia, pelo companheirismo, amizade e apoio durante todo o curso.

"Não fui eu que ordenei a você? Seja forte e corajoso! Não se apavore nem desanime, pois o Senhor, o seu Deus, estará com você por onde você andar". Josué 1:9

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A EFETIVIDADE DO CONTROLE DE DIVULGAÇÃO DE DADOS PESSOAIS NO BRASIL

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES - LEY N° 13.709/2018

Julia Vaz Alves
Cristina Iaroszeski

RESUMO: A Lei Geral de Proteção de Dados (n°13.709/2018) foi instituída a fim de resguardar a utilização e tratamento dos dados pessoais em face aos avanços e transformações tecnológicas no Brasil, sendo essa regulamentação jurídica voltada aos meios digitais, incorporando-se nas novas relações sociais, econômicas e políticas presentes no comércio eletrônico. Diante da ausência de uma norma internacional que protegesse tais direitos, o ordenamento jurídico brasileiro elaborou tal instrumento normativo no intuito de garantir a aplicabilidade do direito à liberdade e privacidade fundamentais aos indivíduos, preservando-os no ambiente digital. A presente pesquisa dedica-se ao estudo histórico e estrutural por trás da aprovação da Lei n°13.709/2018, abordando os princípios e conceitos presentes em seus dispositivos, realizando uma análise ante sua aplicabilidade pelas empresas, suas formas de fiscalização e as penalidades delimitadas pela legislação. Além desses aspectos, vale dizer que a aprovação para a presente legislação foi impulsionada pela necessidade de adequação às exigências para celebração de tratados internacionais e acordos de cooperação, que estabelecem a obrigatoriedade de normas que respaldam o compartilhamento ou transferência de dados entre fronteiras, criando limites à sua efetivação. Para a realização da presente pesquisa a metodologia abordada trata-se de uma revisão bibliográfica crítica, com a utilização de pesquisas bibliográficas e legislativas, em materiais de autores especialistas nas questões abordadas, além de artigos jurídicos pertinentes, julgados, monografias e notícias de sites, com um estudo aprofundado sobre as legislações aplicadas ao tema. O estudo demonstra que a Lei Geral de Proteção de Dados ainda possui muitas instabilidades ante sua aplicabilidade no país, diante dos inúmeros vazamentos de dados que ocorreram, evidenciando uma necessidade na fiscalização concreta pelos órgãos responsáveis no tratamento e armazenamento dos dados, a fim de criar uma conscientização preventiva em face da legislação.

Palavras-chave: Lei Geral de Proteção de Dados. Direito Digital. Direito Fundamental à Privacidade. Internet. Globalização.

RESUMEN: La Ley General de Protección de Datos (n° 13.709/2018) fueinstituidaconelfin de proteger el uso y tratamiento de datospersonales frente a los avances y transformaciones tecnológicas en Brasil, con esta regulación legal enfocada enlosmediosdigitales, incorporando a lasnuevas redes sociales , relaciones económicas y políticas presentes enel comercio electrónico. Ante laausencia de unestándar internacional para proteger tales derechos, elordenamiento jurídico brasileñodesarrolló tal instrumento normativo conelfin de garantizarlaaplicabilidaddelderecho a lalibertad fundamental yalaprivacidad de las personas, preservando lasenel entorno digital. La presente investigación está dedicada al estudio histórico y estructural detrás de laaprobación de laLey N° 13.709/2018, abordando losprincipios y conceptos presentes en sus disposiciones, realizando unanálisis de suaplicabilidad por las empresas, sus formas de fiscalización y las sanciones definidas. por legislación. Además de estos aspectos, cabe mencionar que laaprobación de la presente legislaciónfue impulsada por lanecesidad de adecuarse a los requisitos para lacelebración de tratados internacionales y acuerdos de cooperación, loscualesestablecen normas de obligadocumplimiento que respaldanel intercambio o transferencia de datos a través de fronteras, creandolímites a suimplementación. Para llevar a cabo la presente investigación, lametodología abordada es una revisión bibliográfica crítica, utilizando investigaciones bibliográficas y legislativas, enmateriales de autores especialistas enlos temas abordados, además de artículos jurídicos relevantes, juzgados, monografíasy noticias de sitios web, conun -estudio profundo de lasleyes aplicadas a lamateria. El estudiodemuestra que laLey General de Protección de Datosaún presenta muchasinestabilidadesencuanto a suaplicabilidadenel país, en vista de las numerosas filtraciones de datosocurridas, evidenciando lanecesidad de una supervisión concreta por parte de losórganosresponsablesdeltratamiento y almacenamiento de datos, en para crearconciencia preventiva de lalegislación.
Palabras clave: Ley General de Protección de Datos. Derecho Digital. Derecho Fundamental a laPrivacidad.. Internet.

1 INTRODUÇÃO

A criação da legislação voltada a regulamentar a proteção dos dados pessoais surgiu no Brasil tardiamente, no ano de 2018, com a instituição da Lei n°13.709/2018, que foi fortemente inspirada na diretiva européia, no intuito de adequar o ordenamento jurídico brasileiro à evolução dos novos meios digitais e as redes de comunicações, principalmente voltada a internet, em decorrência da infraestrutura criada pela grande circulação de dados pessoais. Tal legislação teve iniciativa parlamentar, sendo fruto do Projeto de Lei 4.060/2012 em conjunto ao Projeto de Lei 5.276/2016, ambos apresentados pela Presidência da República, os quais auxiliaram na elaboração do texto final aprovado da Lei n°13.709/2018.

A Lei Geral de Proteção de Dados trouxe a segurança jurídica dentro do "Universo Cibernético" no país, facilitando além do o comércio de bens e serviços, maiores investimento ao Brasil, posto que a criação desta legislação especial possibilitou que o país participasse de acordos internacionais de comércio baseados na livre circulação de dados e cooperações internacionais, auxiliando no combate do crime organizado e nas investigação de crimes cibernéticos, além de ter permitido à entrada na Organização para a Cooperação e o Desenvolvimento Econômico.

Justifica-se que a necessidade de estudo sobre o tema se dá pela ausência de uma regulamentação internacional que regule o tráfego dos dados pessoais dentro dos meios digitais, de maneira uniforme, tendo sido de extrema notoriedade a instituição da Lei n°13.709/2018 no país, visto que disciplina sobre o tratamento e utilização dos dados pessoais nos meios digitais, resguardando os direitos fundamentais de liberdade e de privacidade, que apresentam-se como indispensáveis no ordenamento jurídico..

O objetivo do presente artigo é evidenciar a necessidade em resguardar a inviolabilidade de dados que esta diretamente entrelaçada ao direito fundamental à privacidade, considerando que a tutela da privacidade deve acompanhar o avanço tecnológico, que acarreta uma grande preocupação a própria consagração dos direitos humanos. As mudanças políticas, sociais e econômicas implicam no reconhecimento de novos direitos a fim de atender às novas demandas da sociedade.

O desenvolvimento da lei a partir da evolução dos meios digitais é inevitável, posto que o avanço das civilizações vem tornando evidente que os indivíduos demandam de aprimoramentos jurídicos para a proteger de sua privacidade, em qualquer natureza ou extensão.

O primeiro tópico tratará sobre a evolução histórica do tema, trazendo desde os primeiros indícios da conceituação do direito à privacidade, com o artigo escrito por Louis

Dembitz Brandeis, denominado “RighttoPrivacy”, à Harvard Law Review, e ao reconhecimento universal de tal conceito pela Declaração Universal dos Direitos Humanos de 1948, até a evolução dos meios digitais, proporcionado pela Guerra Fria, que estabeleceu a necessidade da implantação de regulamentos jurídicos para uniformizar os níveis de proteção ao tratamento de dados pessoais entre os indivíduos em tais sistemas, evidenciando a importância do Direito Digital.

Já o segundo tópico destaca de maneira individual os dispositivos que norteiam a Lei Geral de Proteção de Dados instituída no Brasil em 2018, fazendo o estudo metodológico e sistemático das principais conceituações e terminologias, dos fundamentos e princípios que norteiam-a, além das penalidades ocasionadas por seu descumprimento.

Posto isto, a pesquisa demonstra a necessidade da eficiência dos métodos e sistemas de tratamento de dados estarem a serviço do indivíduo, de forma a cumprir com os direitos e liberdades fundamentais, especialmente em relação à vida privada e à vontade. A criação da Lei n°13.709/2018 cria critérios para os conflitos envolvendo a privacidade de dados e os demais direitos fundamentais, de forma a equilibrar o tratamento de dados quanto ao progresso econômico e social em face do bem-estar dos indivíduos, considerando o cenário atual em vista ao aumento do fluxo transfronteiriço de dados, decorrente da Globalização, que exige uma atuação conjunta dos países.

A metodologia do presente trabalho será uma revisão bibliográfica crítica, com a utilização de pesquisas bibliográficas e legislativas, em materiais de autores especialistas nas questões abordadas, além de artigos jurídicos pertinentes, julgados, monografias e notícias de sites, com um estudo aprofundado sobre as legislações aplicadas ao tema.

2. CONTEXTO HISTÓRICO

A história da evolução da proteção dos dados pessoais teve início no ano de 1890, por Louis Dembitz Brandeis, um advogado norte-Americano formado na Escola de Direito de Harvard que, na época, era associado de justiça da Suprema Corte no Supremo Tribunal dos Estados Unidos. Brandeis auxiliou no desenvolvimento da concepção referente ao direito à privacidade, através de seu renomado artigo denominado “RighttoPrivacy”, para Harvard Law Review.

Tal artigo foi abordado a princípio que o denominado direito à privacidade seria a solução para os crescentes abusos da imprensa, considerando seu intuito na proteção do indivíduo contra tais ocasiões. Refere-se a ideia de que a privacidade seria o direito de ser deixado em paz (therighttobeletalone), melhor evidencia-se a fala:

> Imunidade Pessoal: o direito à personalidade pode ser considerado como sendo um direito de completa imunidade: o direito de ser deixado em paz. O dever correspondente é, não para infligir uma lesão, nem, dentro de tal proximidade que possa torná-lo bem-sucedido, tentar infligir uma lesão. Neste particular, o dever vai além do que é exigido na maioria dos casos; geralmente uma finalidade não executada ou uma tentativa mal sucedida não é considerada. Mas a tentativa de cometer uma battery envolve vários elementos da lesão que nem sempre estão presentes nas violações do dever; envolve geralmente um insulto, uma situação que cause medo, um chamado repentino sobre as energias para pronta e efetiva resistência. Há uma grande possibilidade de um choque nos nervos, e a paz e quietude da pessoa é perturbada por um período de maior ou menor duração. Há, consequentemente, razão suficiente para que o estado de direito faça do assalto um legal wrong, mesmo sem ter havido battery. Assim, neste caso, a lei vai ainda mais longe e faz com que o dano tentado seja uma ofensa criminal também. (COOLEY, 1879, p. 29)

Após isso, com as invenções e métodos de negócios que norteavam a sociedade naquela época, voltou-se a atenção sobre criar meios efetivos para resguardar a proteção dos indivíduos de maneira particular. A partir disso, em 10 de dezembro de 1948, pela primeira vez a Declaração Universal dos Direitos Humanos proclamada pela Assembleia Geral das Nações Unidas em Paris, instituiu uma norma comum a ser alcançada a todos os povos e nações, estabelecendo de maneira uniforme a proteção universal dos direitos humanos. Tal dispositivo previa de forma genérica e implicitamente o direito à privacidade, dispondo:

> Artigo XII – Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. (BRASIL, 1948)

Antes da Guerra Fria o conceito de segurança nacional baseava-se nas ações e instrumentos necessários para a proteção de uma nação contra possíveis invasões e ataques militares externos. Contudo, com seu início tal conceito recebeu um novo sentido, visto que os demais países das nações latino-americanas, como o Brasil, durante o conflito compartilhavam dos mesmos ideais capitalistas, ganhando uma designação voltada para uma batalha política dos governos nacionais contra grupos de oposição internos.

Com a chegada da internet, em 1969, iniciou-se a revolução tecnológica que vivenciamos até os dias atuais, produzindo o que conhecemos como "Universo Cibernético", transformando velozmente as relações sociais, econômicas, políticas e jurídicas. Tal acontecimento proporcionou à sociedade um maior consumo de informação, cultura, serviços e entretenimento, ocasionando a globalização dos meios digitais.

Em particular no Brasil, a proteção de dados foi instituída mais tarde, com o advento da Constituição Federal de 1988, nos incisos X e XII de seu art. 5°, sendo a primeira constituição brasileira a se preocupar expressamente com a proteção de dados, reconhecendo a proteção à intimidade, à vida privada e à imagem, que também inexistiam nas constituições

anteriores. A primeira iniciativa brasileira em instituir uma legislação mais específica sobre o tema foi em 2010, quando as discussões mais sérias se intensificaram com diversas consultas públicas, debates e a delimitação de um escopo do anteprojeto. Em 2011 deu-se o pontapé inicial à transparência das informações de posse do poder público, com a aprovação da Lei 12.527, disciplinando o direito de acesso à informação previsto na Constituição Federal. No ano seguinte, ocorreu o escândalo envolvendo uma famosa atriz, Carolina Dieckmann, ocasionando a criação da Lei 12.737/2012, que criminaliza a invasão de aparelhos eletrônicos com a intenção de obtenção de dados pessoais. Já em 2014, houve a instituição da Lei 12.965 que reforçou, de maneira mais moderna, o direito à privacidade na internet, mas obstando-se da garantia de proteção de dados. Por fim, mesmo diante dessa previsão e a constante evolução dos meios digitais, foi apenas em 2018, após 30 anos da promulgação da atual Constituição, que ocorreu a elaboração de uma lei regulamentando, de n° 13.709/2018, resguardando a proteção de dados pessoais no Brasil.

Diante do descrito cenário, onde a informação e a comunicação são determinantes aos internautas, as organizações e governos passam a exercer um papel indispensável frente a essas novas tecnologias. Nesse contexto, Purkyt comenta:

> Muito se tem falado sobre o Direito Digital chegando alguns a entender como uma "área do Direito", contudo é certo que hoje o Direito Digital não possui autonomia científica, ou seja, não possui institutos, fins, objeto e princípios informativos próprios, que não se confundem com os existentes em outras áreas do Direito. Desta forma, o Direito Digital não se trata de uma nova área do Direito, mas de uma nova visão, que pode ser entendida como um vetor que afeta a relação entre as pessoas (físicas e/ou jurídicas) devido à utilização intensiva de tecnologia e que, em consequência, afeta o Direito de cada um desses atores. (PURKYT, 2018)

Dessarte, o ramo do Direito Digital refere-se a evolução do próprio Direito, introduzindo novos institutos e elementos para o ordenamento jurídico, de forma a pautar-se nos princípios fundamentais que prevalecem na aplicação das normas brasileiras. è notório que o Direito aplicado à internet tem o intuito de regulamentar as diversas questões originadas no universo digital, designando uma compreensão mais dinâmica aos conflitos inerentes à sociedade usuária deste ciberespaço, a fim de garantir o desenvolvimento auspicioso da internet.

Assim, a construção dos dispositivos normativos presentes no ordenamento jurídico brasileiro atualmente sobre o tratamento e utilização dos dados derivam-se a evolução histórica dos demais países diante o avanço do universo digital, promovida pela necessidade de adequação às exigências internacionais, com o advento da internet e a proliferação de dispositivos capazes de armazenar dados, tornando-se imperiosa a adoção da LGPD.

3. A EFETIVIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS

A presente Constituição Federal em vigor no país, apesar de preceder aos acontecimentos que propagaram da "Era Digital", estabelece normas para a aplicação do direito fundamental à proteção dos dados pessoais. No entanto, em virtude da grande disseminação da necessidade de garantia de segurança de dados pessoais, entre os anos de 2010 à 2014, algumas leis esparsas passaram a abranger matérias que influenciaram no modo de tratamento de tais dados. Diante da constante evolução da internet, houve a nítida necessidade da criação de normas voltadas particularmente as atividades desenvolvidas nos meios digitais.

Em 2016, antes da promulgação da lei especial sobre o tema, foi evidenciado:

> Cabe salientar a importância de sistematizar de maneira orgânica os conceitos e princípios de proteção de dados pessoais, delimitando de maneira clara seu escopo e os critérios interpretativos necessários para a sua aplicação, abordando dentre outros pontos: os direitos dos cidadãos de acesso, retificação, correção e oposição aos tratamentos de seus dados pessoais e a responsabilidade civil de todas a cadeia de agentes nela inserida. Outrossim, busca-se na proposição, a obtenção de benefícios econômicos e sociais potencializados pela tecnologia da informação, ao criar no país uma arquitetura regulatória capaz de proteger os dados pessoais. (CÂMARA DOS DEPUTADOS, 2016)

Assim, depois de inúmeros debates, houve a instituição da Lei n° 13.709/2018, com o intuito de preservar efetivamente os direitos fundamentais relacionados à liberdade e privacidade, previstos no artigo 5° da CF, de maneira a conduzir o livre desenvolvimento da sociedade à modernização em equilíbrio a garantia plena dos direitos individuais. Essa implementação voltada aos meios digitais possibilitou uma segurança jurídica eficiente no Brasil, padronizando os regulamentos e práticas dentro das atividades de tratamento aos dados pessoais, de forma a se igualar aos parâmetros internacionais já existentes.

Nesse contexto, Soares escreveu:

> A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709/2018, tem como objetivo regulamentar o tratamento de dados pessoais pelas empresas, vez que os dados pessoais ganharam grande importância na economia moderna, pois permitem fazer predições, analisar perfis de consumo, opinião, entre outras atividades. Hoje, mais de 126 países possuem leis visando à regulamentação do tratamento de dados pessoais, evitando-se o mau uso destes, bem como a responsabilização das empresas por incidentes e acidentes com dados. A LGPD como objetivos a proteção à privacidade, intimidade, honra e imagem bem como também protege o desenvolvimento econômico e a livre iniciativa das empresas. (SOARES, 2019)

Portanto, essa nova diretriz mostra-se extremamente técnica, reunindo uma série de itens de controle para garantir seu integral cumprimento, fundamentando-se na proteção dos direitos humanos, de forma a constituir um regramento específico que traz princípios, direitos e obrigações ligados às bases de dados pessoais. Seu objetivo é poder contribuir para um ciberespaço de liberdade, segurança e justiça, para o progresso econômico e social, além de possibilitar uma cooperação efetiva entre as autoridades de controle dos

diferentes Estados-Membros, sempre zelando pelos direitos fundamentais de liberdade, privacidade e o livre exercício dos direitos de personalidade, sob a premissa da boa-fé.

O consentimento do titular dos dados, conforme dispõe os casos do art. 11 no dispositivo, é considerado elemento essencial para o tratamento, abordando diversas garantias aos indivíduos, sendo eles o poder solicitar que os seus dados pessoais sejam excluídos dos bancos de dados, transferir os dados para outro fornecedor de serviços, além de poder revogar o consentimento a qualquer momento. O tratamento deve ser realizado considerando os requisitos da finalidade e necessidade, de maneira a serem previamente acertados e informados ao titular.

A nova legislação estabelece que todos os dados tratados, tanto no meio físico quanto no digital, estão sujeitos à regulação, independentemente se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior, atuando de forma extraterritorial, autorizando também o compartilhamento de dados pessoais com organismos internacionais e com outros países, desde que observados os requisitos nela estabelecidos.

A fiscalização e aplicação das penalidades referente aos descumprimentos de seus dispositivos é realizada através da ANPD (Autoridade Nacional de Proteção de Dados Pessoais), juntamente com os agentes de tratamento de dados, estipulados pela LGPD. A ANPD é uma instituição que possui a finalidade de regular e orientar, preventivamente, a aplicação da norma, já os agentes mencionados atuam nas organizações sob os cargos de controlador, tomando as decisões sobre o tratamento; operador, realizando o tratamento, em nome do controlador; e o encarregado, que interage com os titulares dos dados pessoais e a autoridade nacional. Há, ainda, a administração de riscos e falhas, que atua como responsável por gerir dados pessoais, de maneira a adotar medidas preventivas de segurança, através de auditorias, além de resolver incidentes com agilidade, notificando de imediato as possíveis violações à ANPD e aos indivíduos afetados. Vale dizer que caberá à autoridade nacional fixar os níveis de penalidade de acordo com a gravidade da falha e enviar alertas e orientações antes de aplicar sanções às organizações.

Houve junto a sua aprovação a implantação da regulamentação da administração de riscos e falhas, referindo-se a medidas de prevenção no processo de gerenciamento da base de dados pessoais que as empresas de tratamento e utilização deverão adotar, a fim de garantir a segurança das informações ali presentes e replicar boas práticas e certificações existentes no mercado. Nessa questão, haverá a necessidade de elaboração de planos de contingência, relacionados aos agentes de tratamento.

O cumprimento das disposições da nova legislação baseia-se na identificação e classificação dos ativos informacionais existentes, com a avaliação da necessidade de obtenção de consentimento dos titulares dessas informações, além de impor o levantamento dos eventuais riscos inerentes à atividade de tratamento e utilização de dados.

Em síntese, a LGPD discorre sobre a regulamentação sobre a proteção de dados pessoais no Brasil, abrangendo os digitais e externos da sociedade, fazendo-se como uma nova diretriz espelhada nos diplomas internacionais, em especial, à Regulação Geral de Proteção de Dados da União Europeia. Essa mudança tornou-se primordial para a manutenção do direito individual em face ao mercado digital, passando a resguardar a privacidade de cidadãos e consumidores brasileiros.

3.1. FUNDAMENTOS UTILIZADOS NA INTERPRETAÇÃO DA LEI

Em consequência aos reflexos resultantes das consolidações europeias sobre o tratamento e utilização dos dados pessoais, a Lei n° 13.709/2018 tratou de maneira cautelar os fundamentos a serem observados para a aplicação e interpretação de suas normas.

Seu art. 2º apresenta um rol de fundamentos, incluindo:

> I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - à inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018)

Esses fundamentos apresentados de forma inicial nas normas da LGPD tem o intuito de estabelecer-se como uma base geral na interpretação de todos os dispositivos presentes na lei, de maneira a resguardar a relação com os direitos fundamentais previstos na Constituição Federal.

Ao analisar de maneira singular os dizeres do citado artigo é possível notar que os principais elementos para o exercício da aplicação legislativa são o consentimento do titular e o cumprimento da finalidade para o tratamento e utilização. Nenhuma das atividades descritas nos fundamentos é possível antes de obter o consentimento do título, salvo os casos excepcionais. Ressalta-se que, mesmo com o consentimento, o tratamento dos dados não poderá ser realizado por tempo indeterminado e nem com a perda de sua finalidade inicial, devendo ocorrer o término do tratamento juntamente ao final do prazo estipulado, com determinação da ANPD ou a partir da revogação de consentimento do titular.

Valendo-se a LGPD para o setor privado e/ou público, há a ocorrência da colisão dos princípios referentes à privacidade e publicando, visto que como ocorre a

necessidade de consentimento do titular quanto ao tratamento e coleta de seus dados pessoais, há também a exigência de transparência do poder público, em garantir a divulgação das informações relevantes aos cidadãos. Diante disso, com o Estado que preza pela transparência e democracia das informações, devendo estar em equilíbrio a privacidade do sujeito, o art. 4º da LGPD, estabelece a aplicação da lei em fins direcionados à segurança pública, defesa nacional ou atividades de investigação.

Vale ressaltar que tal exceção não pode servir de justificação para a criação de um Estado de constante vigilância, considerando que não há possibilidade de utilizar-se somente de um princípio em detrimento do outro, devendo constantemente realizar-se a ponderação entre eles, garantindo a proporcionalidade.

Portanto, a aplicação dos preceitos normativos presentes na Lei n° 13.709/2018 se alinham as diretrizes resguardadas pelos direitos fundamentais que constam na Constituição Federal, se adaptando às necessidades do setor público, de maneira a manter a proteção do indivíduo e suprir a premência do Estado sob os dados preponderadamente.

3.2 OS PRINCÍPIOS NORTEADORES DA LGPD QUE DELIMITAM A SUA EFETIVIDADE

As atividades que norteiam o tratamento de dados pessoais, segundo dispõem a LGPD, deverão alinhar-se aos princípios que conduzem o Sistema Jurídico, de maneira a aplicar o Direito, direta ou indiretamente, em suas normas de comportamento.

O princípio da Boa-fé, previsto no art. 6º, "caput", remete-se à consciência objetiva nas ações do indivíduo dentro do mundo digital, de maneira institucional, não bastando somente ao agente alegar a intenção de agir em conformidade com a legislação, devendo ser demonstrada por elementos concretos em suas ações. Tal princípio carrega as exigências objetivas de comportamento instituídas pela ordem jurídica, se entrelaçando aos princípios de equilíbrio da conduta, razoabilidade e probidade dentro da concepção operacional. (BRASIL 2018)

Já o princípio da Finalidade, estabelecido no art. 6º, inciso I, trata sobre a utilidade dos dados pessoais, prevendo que as empresas de tratamento possuam propósitos evidentemente determinados, estando notoriamente dispostos para ao titular dos dados, justificando e apontando sua utilização. Ainda, vale ressaltar que qualquer utilização incompatível à finalidade informada acarretará em punições. (BRASIL, 2018)

O inciso II, do art. 6°, aborda sobre o princípio da Adequação, que versa sobre a compatibilidade dos dados solicitados à finalidade de sua utilização. Um exemplo praticado

desta situação seria uma academia que vem a solicitar, na matrícula, informações de caráter religioso e político de seu cliente. Vejamos que é completamente antagônico o fornecimento de tais informações no citado exemplo, visto que não há relevância nenhuma com o serviço que será fornecido pela empresa, estando em desconformidade a este princípio e, consequentemente, tornando a coleta e o tratamento injustificáveis, sendo passíveis de punições e multas. (BRASIL, 2018)

O princípio da Necessidade, disposto no art. 6°, inciso III, estabelece a responsabilidade das empresas acerca dos dados tratados, de maneira a garantir que apenas os dados pessoais realmente essenciais ao desenvolvimento do negócio sejam coletados e devidamente tratados, afastando-se dos possíveis excessos. Nesse contexto, ainda é possível citar o princípio da Responsabilização e prestação de contas, previsto no inciso X do mesmo artigo, tratando sobre o cumprimento da lei na apresentação de provas e evidências de que demonstrem os procedimentos necessários tomados a fim de garantir a proteção dos dados. (BRASIL 2018)

Em relação ao princípio do Livre Acesso, o principal preceito desta legislação, estabelecido no art. 6°, inciso IV, prevê que os titulares dos dados tenham o direito ao acesso das informações fornecidas, de modo que a empresa crie mecanismos de consulta aos seus usuários de forma gratuita, além de constar a periodicidade de tempo que tais dados serão utilizados. Assim, o princípio da Transparência, previsto no inciso VI do mesmo artigo, realça essa determinação, complementando o fato de que essas empresas também vão possuir o encargo de informar aos titulares dos dados os respectivos agentes de tratamento, sendo outras empresas que possam estar conexas no processo de tratamento dos dados. (BRASIL, 2018)

Ainda, nessa linha de cautela aos dados, há o princípio da Qualidade, disposto no art. 6°, inciso V, que garante que a base de dados pessoais das respectivas empresas de tratamento deve manter-se verdadeira, devidamente atualizada e alinhada com o propósito do negócio. (BRASIL, 2018)

Já o princípio de Segurança, previsto no inciso VII do artigo 6°, envolve o principal objeto desta legislação, correspondendo a adoção de procedimentos tecnologias que possam garantir a efetiva proteção dos dados pessoais, principalmente em ocasiões de acessos não autorizados, como em ataques hackers, ou em situações acidentais ou ilícitas de perda e alteração dos dados ali dispostos. O princípio de Prevenção, presente no inciso VIII do mesmo artigo, trata analogamente a essa questão, trazendo essa necessidade de preparar técnicos para lidar com eventuais problemas no tratamento dos dados pessoais, de modo a antecipar as soluções. (BRASIL, 2018)

Por fim, o princípio da Não Discriminação, previsto no art. 6°, inciso IX, prevê que o tratamento de tais dados jamais pode ser realizado com intuito de discriminar ou de promover qualquer abuso contra seus titulares, voltando-se principalmente aos dados pessoais sensíveis, como exemplos os que tratam sobre origem racial ou étnica, convicção religiosa e opinião política. (BRASIL, 2018)

Ante o exposto, observa-se que que todos os princípios presentes na LGPD têm como base da sua efetivação o consentimento pessoal, sendo sempre necessário solicitação de autorização do titular dos dados para o tratamento ser realizado. Tal consentimento deve ser concedido de maneira explícita e inequívoca. O único caso de não consentimento refere-se a exceção, quando só será possível processar e tratar os dados, sem autorização do cidadão, na ocasião em que for indispensável para cumprir situações legais.

Esses princípios norteadores da LGPD reconhecem as boas condutas e práticas inadequadas que ocorrem diariamente nos negócios referentes aos tratamentos dos dados, atuando como forma de sustentação e legitimidade da lei para conduzir tais situações.

Dessarte, os princípios que estão previstos nos incisos do art. 6° da LGPD resguardam os internautas das situações que podem ocorrer nos meios digitais, tornando-se o principal protetor da segurança digital, a fim de arquitetar o tratamento e utilização de dados de maneira legítima e cautelosa.

3.3 TERMINOLOGIAS ESSENCIAIS E ABRANGÊNCIA DA LGPD

Tratando-se de uma nova legislação que se utiliza de termos tecnológicos para conceituar, de forma exemplificativa, as atividades a serem regulamentadas, o art. 5° da LGPD elencou cerca de vinte seis nomeações para as ações nos meios digitais, sendo as essenciais para o entendimento da lei:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - 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; III - 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; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; (...) X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (BRASIL, 2018)

Melhor elucidando, o termo mencionado como “dado pessoal” corresponde à informação em que se permite identificar o indivíduo, direta ou indiretamente, podendo ser o

nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, etc.

Já o mencionado "dado pessoal sensível" refere-se ao descrito no art. 11 da LGPD, sendo essenciais para auferir lucro, direcionar a publicidade, e realizar práticas abusivas, como os dados relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, etc. Melhor dizendo, como exemplo prático, o acesso aos dados sensíveis de certo indivíduo, de forma que a empresa descubra que possui tal doença grave fatal e oferece um tratamento a preços e condições abusivas. Essa cadeia é extremamente comum na economia informacional atual e acaba por fragilizar a autonomia e liberdade do consumidor, devendo possuir uma atenuação ao princípio da privacidade.

O denominado "dado anonimizado" está inteiramente ligado à fase de tratamento, visto que diz respeito à informação que, originariamente, era relativa a um indivíduo, contudo, passou por etapas de tratamento que realizaram a desvinculação dela, de forma pessoa, com o indivíduo. Assim, quando se tratar de um "dado anonimizado", não haverá a aplicação da LGPD sobre ele.

Corresponde à conceituação de "banco de dados" o conjunto de informações, derivados de variadas fontes e características, que arquitetam as operações e atividades dos dados. Concomitantemente a isso, o "tratamento" a que se refere o artigo refere-se a atividade que na qual utiliza-se um dado pessoal na execução da sua operação, podendo ser referente a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, etc.

Dessarte, as terminologias previstas nessa legislação tem um papel de exemplificar as características dos itens descritos, podendo-os ser considerado além do que está ali previsto, fazendo-se como um manual para identificação dos critérios.

3.4 PENALIDADES AO DESCUMPRIMENTO DA LGPD

Em caso de não cumprimento das determinações estabelecidas, a LGPD prevê um rol de sanções administrativas, de natureza pecuniária e restritiva de atividades, variando entre a mera advertência, multas ou a proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados pessoais, presente no Seção I do Capítulo VIII.

Fundamentalmente a legislação dispõe, no art. 52, incisos II e III, dois tipos de punições relacionadas aos aspectos financeiros: multa simples de até 2% do faturamento da

empresa, limitada ao teto de R$50 milhões por infração; ou multa diária, também limitada ao teto de R$50 milhões. (BRASIL, 2018)

Ademais, há também as infrações relacionadas à quebra do sigilo de dados pessoais que não ocasionam sanções de cunho financeiro, sendo estabelecidas pela ANPD, deliberadamente, correspondendo à advertência, com indicação de prazo para adoção de medidas corretivas; ou a comunicação pública da infração após devidamente apurada e confirmada a sua ocorrência; ou ao bloqueio dos dados pessoais a que se refere a infração até a sua regularização; ou a eliminação dos dados pessoais a que se refere a infração; ou a suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; ou a suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período; ou ainda a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados, segundo estabelece os incisos IV, V, VI, X, XI e XII do art. 52. (BRASIL, 2018)

Vale ressaltar que, assim como as demais legislações, as penalidades aplicadas aos descumprimentos dos dispostos na LGPD somente ocorrerão após procedimento administrativo que possibilite a garantia do princípio da ampla defesa do acusado, conforme as especificidades de cada caso. Posto isso, a investigação que estabelecerá o inquérito deve considerar os parâmetros e critérios descritos nos incisos do § 1º, do art. 52, diante da gravidade e a natureza das infrações e dos direitos pessoais afetados; da boa-fé ou má-fé do infrator; da vantagem obtida ou pretendida pelo infrator; da condição econômica do infrator; sob sua reincidência; do grau do dano; da cooperação do infrator; da adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; da adoção de políticas de boas práticas e governança; da pronta adoção de medidas corretivas; e da proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Reforça-se que a fiscalização e aplicação das penalidades da lei estão a cargo da ANPD (Autoridade Nacional de Proteção de Dados), em conjunto com os agentes de tratamento de dados. Assim, o objetivo indispensável da Lei n° 13.709/2018 é voltado à impedir o uso indiscriminado dos dados, estabelecendo a oportunidade de correção de eventuais descuidos por meio de advertências e orientações. Em situações de declarada má-fé, as punições serão revertidas nas sanções financeiras e administrativas.

4. APLICABILIDADE DA LGPD NO BRASIL

Antes da regulamentação sobre os dados, uma pesquisa realizada pelo MIT (Massachusetts Instituteof Technology) evidenciou que cerca de 140 milhões de pessoas tiveram suas informações detalhadas (como telefone, salário, endereços, fotos, etc.) expostas durante anos no meio digital, sendo compartilhadas e vendidas na rede. Com a vigência da nova legislação de proteção de dados no Brasil, a partir de agosto de 2020, a qual instituiu novos protocolos a fim de garantir mais segurança ao usuário, incluiu-se a obrigatoriedade se de ter locais para o armazenamento dos dados, o controle de acesso, o tratamento dos dados, entre outros critérios.

Mesmo com tais normativas legislativas que regulassem sobre o tema, no começo de 2021 ocorreu um enorme vazamento de dados a empresas e órgãos do governo, sendo manchete em diversos jornais nacionais e internacionais que o denominaram de Operação Deepwater, que disponibilizou cerca de 223 milhões de números de CPFs, sendo uma base de dados com praticamente todos os brasileiros vivos e, ainda, com alguns já mortos. Além de tais dados, ainda foram vazadas outras informações relacionadas a endereços, telefones e seus nomes completos.

Diante deste desastroso vazamento, o cenário de insegurança sobre a proteção de dados se instalou no país, visto que mesmo já estando em vigência a Lei n° 13.709/2018, tais protocolos não foram suficientes para controlar e evitar o acontecimento, além de que tal ocorrência demonstrou, a partir de uma matéria publicada pela Revista Abril em fevereiro de 2021, que os vazamentos de dados no Brasil aumentaram cerca de 493%, segundo o MIT.

Se analisarmos o contexto histórico de vazamentos de dados no Brasil nos últimos quatro anos, é possível elencar quatro ocasiões, além da mencionada anteriormente, ocorreram desastrosos vazamentos. Note que em 2018, a empresa Netshoes pagou, através de um acordo celebrado com o Ministério Público do Distrito Federal, cerca de R$500 mil de indenização por danos morais, depois de ter exposto informações pessoais de quase 2 milhões de clientes terem sido expostas na internet. (ARAGÃO, 2022)

Já em 2020, houve dois grandes vazamentos envolvendo o banco de dados no Ministério da Saúde, onde cerca de quase 243 milhões de brasileiros cadastrados no Sistema Único de Saúde (SUS) ou os beneficiários de planos de saúde ficaram expostos na internet por falhas de segurança dos sistemas do órgão; e o outro envolvendo os dados da Enel, em Osasco, em que cerca de 290 mil clientes da concessionária de energia tiveram informações sensíveis vazadas após falha de segurança. (ARAGÃO, 2022)

Ainda, em 2021, ocorreu o vazamento de diversos cadastros de chaves PIX comunicado pelo Banco Central, que estavam sob a guarda e a responsabilidade da empresa Acesso Soluções de Pagamento, chegando a ter os dados de 160.147 chaves potencialmente expostas. (ARAGÃO, 2022)

Observando a atual situação do país, é possível verificar que ainda há um número expressivo de organizações, públicas ou privadas, que não pretendem gastar com segurança digital, ocasionando uma enorme instabilidade para a efetiva aplicação dos preceitos normativos trazidos pela LGPD, considerando que os criminosos digitais observam os bancos que apresentam-se mais vulneráveis e conseguem o acesso a redes corporativas a partir de dispositivos que estão potencialmente desprotegidos, aumentando o risco.

Há estudos que evidenciaram que cerca de 40% das empresas nacionais não possuem uma política de segurança digital, não adotando as medidas necessárias de cibersegurança. Além disso, apenas 45% das companhias brasileiras já estabeleceram medidas de segurança digital, com tudo, cerca de 15%, apesar de já as terem estabelecido, não obrigam seus colaboradores a cumpri-las.

Ainda, vale mencionar que a segurança no ciberespaço não se limita apenas aos bancos de dados empresariais ou em suas plataformas, mas também envolve os dispositivos pessoais em que os empregados utilizam para o trabalho, que torna os negócios vulneráveis aos ataques.

Com isso, a aplicação e efetividade da legislação encontra-se muito limitada a um longo processo para localizar os dados sobre os incidentes de segurança, entender o que aconteceu e quem obteve o acesso, em eventual descumprimento, além de determinar a punição para o responsável. A partir disso é iminente observar que a LGPD está diretamente ligada às questões de confiança nas organizações empresariais e em sua equipe de segurança.

No entanto, vale ressaltar que no cenário brasileiro, o nível de confiança não condiz com a cultura do país, visto que os brasileiros só se disponibilizam em resolver os problemas quando aparecem, em vez de preveni-los.

Posto isto, o Brasil ainda precisa formar uma muralha bem constituída em relação a proteção de dados no país, de forma a conscientizar a essencialidade de se proteger os sistemas de dados nas organizações e diminuir os altos custos que esse investimento tem, para que assim a legislação possa ser realmente cumprida, sendo capaz de suportar qualquer intempérie.

Portanto, podemos dizer que a efetividade e aplicabilidade da LGPD estão diretamente condicionadas ao nível de confiança entre as empresas para que o gerenciamento

dos dados possa ocorrer de forma mais segura e responsável aos usuários e, só assim, valer-se dos dispositivos previstos na legislação.

5 CONSIDERAÇÕES FINAIS

A necessidade de normas que regulassem as relações de privacidade no meio digital inspirou a criação da Lei n°13.709/2018, afim de estabelecer a proteção de dados em tais meios, desenvolvendo de forma fundamental o modelo de negócio no meio digital, posto a crescente dependência das bases de dados no fluxo internacional, especialmente os relacionados aos indivíduos, decorrentes dos efeitos da globalização e o avanço tecnológico.

Contudo, a preocupação em estabelecer normas regulamentadoras no intuito de resguardar os dados no meio digital no Brasil surgiu tardiamente, entre os anos de 2010 à 2014, com a instituição de legislações dispersas no país, ganhando notoriedade somente em 2016, quando a Câmara dos Deputados ergueu-se a fim de iniciar a promulgação de uma legislação especial sobre o tema.

A partir foi instituído a Lei n° 13.709/2018, sendo diretamente relacionada não só ao advento da internet e à proliferação de bases de dados, e em especial à necessidade política do país em se adequar às exigências impostas para os tratados internacionais, que influenciou substancialmente em sua promulgação.

Tal legislação utilizou-se dos fundamentos sobre o respeito à privacidade; à autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, a fim de criar uma base geral para a interpretação dos de seus dispositivos, conservando todos os direitos fundamentais previstos na Constituição Federal e aplicando seu exercício legislativo baseado na relação de consentimento do titular e o cumprimento da finalidade para o tratamento e utilização.

Os princípios em que norteiam a Lei n° 13.709/2018 se apresentam como os responsáveis para a efetivação do consentimento pessoal estabelecido pela legislação, limitando a efetividade das normas de forma explícita e inequívoca para seu cumprimento.

A mencionada legislação também estipulou penalidades em caso de descumprimentos dos preceitos normativos, prevendo um rol de sanções administrativas, de natureza pecuniária e restritiva de atividades, as quais variam entre a mera advertência, multas ou a proibição parcial ou total do exercício de atividades, as quais ficam a cargo de

fiscalização e aplicação sob responsabilidade da ANPD em comunhão com os agentes de tratamento de dados.

Mesmo com a existência da lei visando tutelar tais dados, é possível verificar que sua aplicação dentro do ambiente virtual ainda apresenta visíveis instabilidades, considerando os diversos vazamentos que tivemos no país, mesmo após sua vigência, sendo resultado das problemáticas em relação ao custo alto de sua adequação e a dificuldade na fiscalização das normas.

O atual cenário causa uma grande insegurança jurídica nos usuários dos meios digitais, visto que a Lei n° 13.709/2018 só limita as recomendações necessárias que as organizações precisam ter que lidar em relação ao tratamento de dados, dispondo apenas sobre o gerenciamento dos dados de uma maneira mais responsável. Posto isto, essa responsabilidade encontra-se diretamente baseada em confiança no estrito cumprimento da legislação pelas empresas e instituições, que só é possível se perceber depois que algum problema vier a ocorrer.

Dessa forma, a LGPD ainda necessita da criação de uma jurisprudência sólida e eficaz que consiga dirimir as controvérsias que vêm ocorrendo, para que assim possa possibilitar uma intervenção mais certeira e segura dentro do Direito brasileiro. No mais, sua aplicação íntegra possui preceitos que, evidentemente, tendem a provocar mudanças decisivas no meio digital que derivam de uma fiscalização concreta dos órgãos responsáveis para que o tratamento e armazenamento dos dados possa o ocorrer de forma preventiva, fazendo assim que a legislação seja capaz de coibir as práticas abusivas de forma pontual, proporcionando uma maior segurança jurídica aos usuários no meio digital.

REFERÊNCIAS

ARAGÃO, Alexandre. **5 grandes vazamentos de dados no Brasil — e suas consequências**. JOTA. 2022. Disponível em: https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022. Acesso em: 13 mai. 2022

BRASIL. CÂMARA DOS DEPUTADOS, 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01xs3rvizyrdxf1nm9tz8pdqdnk34372078.node0?codteor=1481261&filename=Tramitacao-PL+4060/2012. Acesso em: 05 jul. 2022.

BRASIL. Declaração Universal dos Direitos Humanos, de 10 de dezembro de 1948. Disponível em: https://www.oas.org/dil/port/1948%20Declara%C3%A7%C3%A3o%20Universal%20dos%20Direitos%20Humanos.pdf. Acesso em 6 jun. 2022.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 jul. 2022

COOLEY, Thomas McIntyre. **A treatise on the law of torts, or the wrongs which arise independent of contract**. Chicago: Callaghan and Company, 1879. p. 29. Disponívelem: https://repository.law.umich.edu /books/11/ .Acesso em: 6 jun. 2022.

PURKYT, Paulo. **Um Direito para o mundo na era digital**. PurkytVeneziani Advogados Associados, 2018. Disponível em: http://www.purkytveneziani.com.br/um-direito-para-o-mundo-na-era-digital/. Acesso em: 28 mar. 2022.

SOARES, Paulo Vinicius de Carvalho. **A Lei Geral de Proteção de Dados frente às relações trabalhistas**. Conjur. 2019. Disponível em: https://www.conjur.com.br/2019-set-03/paulo-vinicius- soares-lgpd -frente-relacoes-trabalhistas. Acesso em 05 jul. 2022

VEIRANO Advogados. **Vazamentos de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.**VoceSA.abril . 2021. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit/. Acesso em 07 abr. 2022.