RBEGDR

Revista Brasileira de Estudos de Gestão e Desenvolvimento Regional

v. 02, n. 01 - 2024

Seção de Artigos

AS INFORMAÇÕES INDIVIDUAIS PRIVADAS NA INTERNET: A LGPD APLICADA NA OBTENÇÃO E NO DEVIDO USO DOS DADOS DE NATUREZA PESSOAL

PRIVATE INDIVIDUAL INFORMATION ON THE INTERNET: LGPD APPLIED TO THE ACQUISITION AND PROPER USE OF PERSONAL DATA

INFORMACIÓN PRIVADA DE LAS PERSONAS EN INTERNET: LA LGPD APLICADA EN LA OBTENCIÓN Y USO CORRECTO DE LOS DATOS PERSONALES

João Vitor Santos da Conceição- joaovitorsc@live.com

Submissão em: 11/06/2024 Aceito em: 01/07/2024

RESUMO

Este artigo apresenta uma análise detalhada da proteção de dados pessoais na era digital, com especial enfoque no Regulamento Geral de Proteção de Dados (RGPD). A LGPD trouxe mudanças importantes no tratamento de dados pessoais e confirmou os princípios, direitos e obrigações que garantem a privacidade e a segurança dos dados das pessoas físicas. A implementação da LGPD é um momento importante na legislação brasileira, promovendo melhor proteção e respeito à privacidade dos usuários. As empresas enfrentam de- safios na adaptação às novas regras e na implementação de mecanismos eficazes de proteção de dados, o que exige investimentos em tecnologia, formação e práticas de segurança da in- formação. A LGPD não afeta apenas as empresas, mas também órgãos governamentais e organizações trisetoriais. O objetivo da lei é criar uma cultura de proteção de dados que incentive todos os intervenientes relevantes a assumir responsabilidades. É importante conscientizar a sociedade sobre os seus direitos e a importância da proteção dos dados pessoais. Os utilizadores devem compreender os riscos associados à divulgação dos seus dados e exercer o seu direito de consentir, utilizar, eliminar e corrigir os dados. Além disso, enfatiza-se a importância do monitoramento e da aplicação de sanções às violações da LGPD. As autoridades devem garantir que a lei seja cumprida e processar aqueles que não o fazem. Em resumo, a LGPD representa um avanço na proteção de dados pessoais, dando aos indivíduos mais controle sobre seus dados. A aplicação efetiva desta lei promoverá um ambiente digital mais seguro e respeitoso que beneficiará todos os envolvidos no mundo dos dados pessoais.

Palavras-chave: Segurança. Privacidade. LGPD. Internet. Proteção de dados pessoais

ABSTRACT

This article presents a detailed analysis of personal data protection in the digital era, with special focus on the General Data Protection Regulation (GDPR). The LGPD has brought significant changes in the treatment of personal data and has confirmed the principles, rights, and obligations that ensure the privacy and security of individuals' data. The implementation of the LGPD is a crucial moment in Brazilian legislation, promoting better protection and respect for users' privacy. Companies face challenges in adapting to the new rules and implementing effective data protection mechanisms, which requires investments in technology, training, and information security practices. The LGPD not only affects companies but also governmental agencies and trisectoral organizations. The objective of the law is to create a data protection culture that

encourages all relevant stakeholders to assume responsibilities. It is important to raise awareness in society about their rights and the importance of personal data protection. Users should understand the risks associated with disclosing their data and exercise their right to consent, use, delete, and correct data. Furthermore, the importance of monitoring and applying sanctions for LGPD violations is emphasized. Authorities must ensure that the law is complied with and prosecute those who do not comply. In summary, the LGPD represents an advancement in personal data protection, giving individuals more control over their data. The effective application of this law will promote a safer and more respectful digital environment that will benefit all involved in the world of personal data.
Keywords: Security. Privacy. LGPD. Internet. Personal data protection

RESUMEN
Este artículo presenta un análisis detallado de la protección de datos personales en la era digital, con especial énfasis en el Reglamento General de Protección de Datos (RGPD). La LGPD ha traído cambios importantes en el tratamiento de datos personales y ha confirmado los principios, derechos y obligaciones que garantizan la privacidad y la seguridad de los datos de las personas físicas. La implementación de la LGPD es un momento importante en la legislación brasileña, promoviendo una mejor protección y respeto por la privacidad de los usuarios. Las empresas enfrentan desafíos en la adaptación a las nuevas reglas y en la implementación de mecanismos efectivos de protección de datos, lo que requiere inversiones en tecnología, capacitación y prácticas de seguridad de la información. La LGPD no solo afecta a las empresas, sino también a los organismos gubernamentales y organizaciones trisectoriales. El objetivo de la ley es crear una cultura de protección de datos que incentive a todos los actores relevantes a asumir responsabilidades. Es importante concienciar a la sociedad sobre sus derechos y la importancia de la protección de datos personales. Los usuarios deben comprender los riesgos asociados con la divulgación de sus datos y ejercer su derecho a consentir, usar, eliminar y corregir los datos. Además, se enfatiza la importancia del monitoreo y la aplicación de sanciones por violaciones de la LGPD. Las autoridades deben asegurar que se cumpla la ley y procesar a aquellos que no lo hacen. En resumen, la LGPD representa un avance en la protección de datos personales, otorgando a los individuos más control sobre sus datos. La aplicación efectiva de esta ley promoverá un entorno digital más seguro y respetuoso que beneficiará a todos los involucrados en el mundo de los datos personales.
Palabras clave: Seguridad. Privacidad. LGPD. Internet. Protección de datos personales

1 INTRODUÇÃO

A proteção de dados se tornou um tema muito importante na era tecnológica, pois afeta diretamente a privacidade e a segurança dos usuários da Internet. A recolha indiscriminada de dados pode levar à violação dos direitos individuais e à divulgação injustificada de informações confidenciais. Nesta situação, é muito importante estabelecer atos jurídicos especiais que garantam a proteção dos dados pessoais e estabeleçam instruções claras para o seu tratamento. No Brasil, a Lei de Proteção de Dados (LGPD), que entrou em vigor em setembro de 2020, desempenha um papel fundamental na segurança dos dados pessoais dos internautas. A LGPD é um avanço

significativo na legislação brasileira porque promove a proteção da privacidade e cria uma base para o tratamento adequado de dados pessoais.

O objetivo deste estudo é analisar o efeito da LGPD na proteção de dados pessoais. dados. dados *on-line*, para examinar como as empresas e organizações brasileiras aplicam a lei na prática. A LGPD busca criar uma cultura de proteção de dados, garantindo transparência e responsabilidade aos envolvidos no tratamento desses dados. Diversas fontes são utilizadas para conduzir esta análise, incluindo pesquisas acadêmicas, relatórios governamentais e análises de violações de dados pessoais no Brasil. Além disso, representantes de empresas e organizações serão entrevistados para conhecer as práticas de aplicação da LGPD no Brasil.

Os desafios enfrentados pelas empresas na implementação da LGPD incluem a conscientização e a capacitação de profissionais responsáveis pelo tratamento de dados, além à necessidade de investimento em tecnologias e sistemas de segurança adequados, conforme discutido em trabalhos como "Proteção de Dados Pessoais no Brasil: Aspectos Jurídicos e Desafios da Implementação da Lei Geral de Proteção de Dados (LGPD)". É importante ressaltar que a LGPD não só impõe obrigações às empresas, mas também confere direitos aos usuários. Os indivíduos têm o direito de aceder, corrigir, solicitar o apagamento e receber in- formações claras sobre como as empresas utilizam os seus dados pessoais. Nesse contexto, a LGPD é um desafio e uma oportunidade para as empresas brasileiras. A implementação adequada da lei pode fortalecer a proteção de dados pessoais, promover a transparência e a confiança dos usuários e alinhar as empresas com os padrões internacionais de proteção e segurança de dados.

2 A LEI GERAL DE PROTEÇÃO DE DADOS

O principal objetivo da Lei Geral de Proteção de Dados Pessoais (LGPD) instituída pela Lei nº 13.709/2018 é proteger os direitos fundamentais à liberdade e à privacidade e ao desenvolvimento independente da personalidade de cada pessoa. Fundamentalmente, a legislação diz respeito ao tratamento de dados pessoais, seja em formato físico ou digital, por pessoas singulares ou coletivas, entidades públicas ou privadas, abrangendo um vasto leque de atividades que podem ser manuais ou não manuais em formato digital.

Dentro da LGPD, o tratamento de dados pessoais pode ser atribuído a dois clientes principais, o controlador e o operador. Além disso, existe um responsável indicado pelo controlador, que atua como canal de comunicação entre este, a operadora, os titulares dos dados e a Diretoria Nacional de Proteção de Dados (ANPD). Um dos principais temas que o controlador aborda. lida com A lei é o tratamento de dados, que, na sua aplicação, inclui todas as atividades relacionadas com a utilização de dados pessoais, tais como recolha, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, tratamento, arquivamento de dados, armazenamento, eliminação, avaliação ou monitorização, modificação, transmissão, transferência, transmissão ou extração.

Antes de iniciar o tratamento de dados pessoais, o responsável deve garantir que a finalidade da atividade é clara e inequívoca e expressar clara e inequivocamente as especificidades finalidades dos dados pessoais. titular dos dados. No setor público, a principal finalidade do tratamento está relacionada com a implementação de políticas públicas, que se encontram devidamente amparadas por leis, regulamentos ou se baseiam em contratos, acordos etc. Na implementação de práticas públicas da administração pública, o compartilhamento de informações é regulamentado por lei e

não é necessário consentimento especial. Contudo, a agência responsável pela recolha deve fornecer informações abertas sobre que informações são partilhadas e com quem. Por sua vez, a autoridade solicitante do compartilhamento deverá justificar a necessidade desse acesso com base na implementação de uma ordem pública específica e fornecer detalhadamente o motivo da solicitação e a finalidade da utilização dos dados. As informações confidenciais são protegidas e sujeitas a regras e regulamentos especiais. Os órgãos e unidades do governo federal devem seguir tais aspectos e outros pontos de extrema importância para garantir que o tratamento de dados pessoais seja realizado de acordo com as normas e princípios legais da LGPD.

Os atos legais fornecem a estrutura jurídica dos direitos dos titulares dos dados pessoais, que todo o órgão ou unidade deve respeitar durante o tratamento dos dados. Para possibilitar o exercício desses direitos, a LGPD fornece um conjunto de ferramentas que aumentam a transparência e estabelecem procedimentos para a participação governamental.

É importante compreender o conceito de dados pessoais no âmbito da LGPD, pois permite que os atores públicos entendam o tipo de dados que tratam e tenham consciência da utilização de seus dados como cidadãos.

-Dados Pessoais: Desde a entrada. com a vigência da Lei nº 13.709/2018, a proteção de dados passou a ser responsabilidade dos cidadãos, da administração pública e da responsabilidade solidária das empresas que tratam desses dados. Dado pessoal é tudo que pode ser utilizado para identificar direta ou indiretamente a pessoa natural. Exemplos dessas informações incluem nome completo, data e local de nascimento, RG, CPF, foto, endereço residencial, endereço de e-mail etc.

-Dados Sensíveis: As informações pessoais incluem aquelas que requerem atenção especial no processamento: informações confidenciais que contenham informações sobre raça ou origem étnica, crenças religiosas ou filosóficas, opiniões políticas, filiação sindical, dados genéticos, biométricos, saúde ou vida sexual.

-Dados Públicos: No caso de dados pessoais públicos, é importante considerar a finalidade, a boa fé e o interesse público que incentiva a sua divulgação. De acordo com a LGPD, uma organização pode processar informações anteriormente divulgadas pelo proprietário se o novo tratamento tiver finalidade legítima e específica e respeitar os direitos do proprietário. Porém, caso a organização queira compartilhar essas informações com terceiros, deverá ser obtido um novo consentimento, salvo casos excepcionais previstos em lei.

É importante ressaltar que a LGPD também trata de acesso. Lei de Informação (LAI) e princípios constitucionais como o Artigo 5 XXXIII da Constituição. sua identificação. Nestes casos, a LGPD não se aplica aos dados. No entanto, é importante notar que a informação só é considerada anónima se a pessoa registada não puder ser identificada por meios técnicos ou outros. Se a identificação for possível, trata-se de dados pseudônimos de acordo com a LGPD.

-Dados Anonimizados: O anonimato é uma técnica que remove ou modifica informações que permitem que um indivíduo seja identificado e permaneça anônimo. Nestes casos, a LGPD não se aplica aos dados. No entanto, é importante notar que a informação só é considerada anónima se a pessoa registada não puder ser identificada por meios técnicos ou outros. Se a identificação for possível, trata-se de dados pseudônimos de acordo com a LGPD.

2.1 Entrada em vigor da Lei Geral de Proteção de Dados

Quando entendemos o momento de introdução da LGPD e em seguida fazemos análise da eficácia da Lei Geral de Proteção de Dados (LGPD) na proteção de dados pessoais online em empresas e organizações brasileiras revela os desafios e oportunidades do cenário. A metodologia utilizada incluiu uma revisão minuciosa da literatura acadêmica utilizando fontes como Scientific Electronic Library Online (SciELO) e Google Acadêmico, além de dados estatísticos do Instituto Brasileiro de Geografia e Estatística (IBGE). São destacados os importantes efeitos da LGPD nas práticas empresariais, que exigem adaptações e mudanças nos procedimentos relacionados à coleta, tratamento e armazenamento de dados pessoais.

A LGPD trouxe mudanças importantes no tratamento de dados pessoais, deu aos usuários novas direitos e obrigações fixas. empresas O consentimento do usuário tornou-se uma questão fundamental que exige transparência e clareza dos dados coletados pelas empresas. Além disso, a LGPD confere aos titulares dos dados direitos específicos para acessar, corrigir e excluir seus dados pessoais, o que promove melhor controle e privacidade.

No entanto, a implementação da LGPD continua sendo um desafio para muitas empresas, e a conformidade continua sendo uma meta. alcançar. As penalidades pelo não cumprimento da LGPD pode ser significativas, incentivando as empresas a se adaptarem às novas exigências legais. É importante conscientizar sobre a importância da proteção de dados pessoais e torná-la uma prática global. Apesar dos desafios, a LGPD oferece às empresas uma oportunidade de melhorar seus processos de privacidade e proteção de dados pessoais. A revisão das práticas de coleta e processamento de dados pode não apenas fortalecer a proteção dos dados dos usuários, mas também melhorar a eficiência dos processos internos de negócios.

A aplicação da Lei Geral de Proteção de Dados (LGPD) trouxe consequências significativas para a segurança dos dados pessoais na era digital. Com o avanço das tecnologias de comunicação e informação, o crescente uso e coleta indiscriminada de informações pessoais tornaram-se uma preocupação crescente, afetando diretamente a privacidade e a segurança dos usuários da internet. A LGPD surge como uma resposta legal crucial para mitigar esses riscos e estabelecer diretrizes claras para o manejo de dados pessoais. A LGPD representa um avanço marcante na legislação brasileira, demandando mudanças e adaptações por parte das empresas e organizações que lidam com dados pessoais. Em vigor desde setembro de 2020, seu principal propósito é assegurar a proteção dos direitos fundamentais de privacidade e autodeterminação informativa dos indivíduos.

Uma das contribuições mais importantes da LGPD é a imposição de diretrizes claras para a coleta, uso e armazenamento de dados pessoais. A lei estipula que as empresas devem obter o consentimento explícito dos usuários antes de coletar seus dados pessoais, além de in- formar claramente a finalidade e o método de utilização desses dados. Isso promove a transparência e concede aos usuários maior controle sobre suas informações pessoais.

Além disso, a LGPD requer a adoção de medidas de segurança adequadas para proteger os dados pessoais contra acesso não autorizado, perda ou vazamento. As empresas são obrigadas a implementar mecanismos de proteção, como criptografia e autenticação de acesso, para garantir a integridade e confidencialidade dos dados.

A lei também exige que as organizações estabeleçam políticas de privacidade claras e acessíveis aos usuários, informando de maneira compreensível como os dados pessoais serão coletados, utilizados, compartilhados e armazenados. Isso permite que

os usuários conheçam seus direitos e tomem decisões informadas sobre a divulgação de suas informações.

Com a implementação da LGPD, o Brasil se alinha a outras legislações internacionais de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, favorecendo a realização de negócios internacionais e fortalecendo a proteção dos dados pessoais dos usuários.

É fundamental ressaltar que a LGPD não apenas impõe obrigações às empresas, mas também confere direitos aos usuários, incluindo o acesso, correção, exclusão e limitação do uso de seus dados pessoais. Para garantir a eficácia da LGPD, é essencial contar com uma autoridade de fiscalização eficiente, como a Autoridade Nacional de Proteção de Dados (ANPD), e mecanismos de punição adequados para as empresas que não cumprem a lei. Essa estrutura regulatória é crucial para garantir a conformidade e responsabilização das empresas.

Em resumo, a aplicação da LGPD teve um impacto significativo na proteção de dados pessoais na internet, estabelecendo diretrizes claras para o manejo de dados, promovendo transparência, segurança e autodeterminação informativa dos usuários, além de alinhar o Brasil a padrões internacionais de proteção de dados e conferir direitos aos usuários. A existência de uma autoridade reguladora e a imposição de sanções são elementos essenciais para garantir a eficácia da lei e promover uma cultura de proteção de dados no país. A LGPD é uma legislação importante que protege os dados pessoais on-line e sua eficácia. a implementação pode contribuir para um ambiente digital mais seguro e respeitoso. Ao enfrentar os de- safios e aproveitar as oportunidades oferecidas pela LGPD, as empresas podem não apenas atender aos requisitos legais, mas também ganhar a confiança e a satisfação dos clientes, cumprindo os padrões internacionais de proteção da “honra virtual” e da privacidade.

2.2 A eficiência da LGP em relação a segurança dos dados na internet

Segundo Marcondes (2021, p. 57), o Brasil possui uma das mais importantes legislações relacionadas à proteção de dados pessoais (Lei Geral de Proteção de Dados – LGPD). Apesar de ter sido adotado em 2018, só entrou em vigor em 2020, mas já é perceptível o impacto significativo nas empresas que operam no setor digital. Para se adaptarem às novas exigências legais, as empresas tiveram que fazer ajustes e alterar a sua privacidade e práticas de segurança de dados. Conforme observado por Simões (2020, p. 46), a LGPD trouxe mudanças importantes nos procedimentos relacionados aos dados pessoais e novos direitos para os titulares dos dados. Segundo Saff (2019, p. 46), a LGPD desempenhou um papel importante na manutenção da privacidade e da proteção dos dados pessoais dos cidadãos brasileiros.

Por lei, as empresas que coletam dados de internautas devem seguir determinadas práticas para garantir a proteção dos dados pessoais dos usuários. O consentimento do usuário é um dos principais pontos da LGPD. É imprescindível que os usuários tenham pleno conheci- mento das informações que as empresas coletam e de como elas são utilizadas. Como enfatiza Oliveira (2020, p. 12), as empresas devem obter o consentimento do titular dos dados para coletar e armazenar dados. Além do consentimento, a LGPD também garante aos titulares dos dados direitos específicos de acesso, correção e exclusão. dos seus dados pessoais. Segundo Pereira (2021, p. 74), os indivíduos têm o direito de acessar todos os dados pessoais coletados pelas empresas e exigir a exclusão desses dados. A aplicação da LGPD à proteção de dados pessoais na Internet continua sendo um desafio. Segundo Saffi (2019, p. 31), muitas

empresas ainda não cumprem a lei, e as penalidades pelo descumprimento da LGPD podem ser significativas. Além disso, a LGPD é uma legislação relativamente nova no Brasil e sua interpretação ainda pode mudar ao longo do tempo e da prática, criando incerteza para as empresas.

Conforme observa Oliveira (2020, p. 17), a LGPD pode ser vista como uma oportunidade para as empresas melhorarem seus processos de privacidade e proteção de dados pessoais. A lei exige que as empresas revejam suas práticas de coleta e processamento de dados pessoais, o que pode melhorar tanto a proteção dos dados pessoais dos usuários quanto a eficiência dos processos internos da empresa.

Finalmente, a LGPD representa uma legislação fundamental para a proteção de dados pessoais. dados na Internet e a sua implementação continua a ser um desafio para as empresas. No entanto, também pode constituir uma oportunidade para aumentar a sensibilização e melhorar as práticas de privacidade e proteção de dados pessoais.

3 CONSCIÊNCIA SOBRE A PRIVACIDADE INDIVIDUAL

Com o meio ambiente sempre mais centrado na digitalização, na segurança dos dados pessoais dos cidadãos e numa preocupação central das empresas e organizações. A introdução da Lei Geral de Proteção de Dados (LGPD) no Brasil em 2020 cria um conjunto de padrões e diretrizes que visam preservar a privacidade e a segurança dos indivíduos.

Além disso, a LGPD estabelece requisitos para segurança de dados, incluindo a implementação de salvaguardas e medidas adequadas. gestão do uso de dados pessoais (BITTAR; TOMASCHEWSKI, 2021, p. 183). O objetivo dessas medidas é prevenir fraudes, vazamentos e crimes cibernéticos que possam ameaçar a privacidade e a segurança das informações pessoais. Outro aspecto importante é a conscientização dos funcionários e parceiros de negócios sobre a LGPD e as melhores práticas de segurança cibernética. Finalmente, é importante que os indivíduos tenham mecanismos eficazes para exercer os seus direitos em relação à proteção de dados pessoais. Segundo Bittar e Tomaschewski (2021, p. 201), a LGPD permite que os envolvidos tomem medidas legais e administrativas para garantir o cumprimento da lei e buscar indenização por violações de privacidade e segurança de dados pessoais.

É decisivo sublinham que os direitos de proteção de dados devem ser vistos não apenas como uma obrigação legal, mas também como uma responsabilidade social e ética. Como argumentam Guimarães e Junior (2021, p. 120), a privacidade e a proteção de dados pessoais são elementos-chave do respeito aos direitos humanos, à liberdade de expressão e à democracia.

Em resumo, para criar um ambiente mais seguro e compatível com a LGPD, é necessário aumentar a conscientização dos cidadãos sobre seus direitos à privacidade. ambiente digital. As empresas, organizações e indivíduos devem estar conscientes dos seus direitos e responsabilidades em relação à proteção de dados pessoais, à implementação de medidas de proteção e segurança de dados, à autorização e formação dos colaboradores e ao cumprimento dos requisitos de proteção de dados.

3.1 A proteção de dados se relacionando com o Princípio da Dignidade Humana

A implementação de medidas de segurança da informação nas empresas para proteger os dados pessoais está a tornar-se uma necessidade essencial num ambiente cada vez mais digitalizado. Segundo Marcondes (2021, p. 68), é importante

implementar medidas técnicas e organizacionais como criptografia, controle de acesso e backups regulares, e estabelecer práticas de segurança da informação que, além de fornecer informações adequadas, também garantam a proteção de dados pessoais armazenados, treinar os funcionários sobre o uso correto dessas medidas.

Oliveira (2020, p. 109) enfatiza que a análise de risco desempenha um papel fundamental na aceitação dessas medidas, o que permite a identificação de potenciais vulnerabilidades e ameaças, tanto internas quanto externas, para apoiar uma decisão adequada na implementação de medidas de segurança eficazes. Pereira (2019, p. 91) enfatiza a importância de uma abordagem holística à proteção de dados e sublinha que as medidas de segurança devem abranger toda a infraestrutura empresarial, não se limitando a sistemas específicos, devendo ser monitorizados continuamente para identificar novas ameaças e atualizar sistemas.

Sousa e Cabral (2018, p. 123) destaca os efeitos positivos das medidas de segurança conforme regulamentos e leis, como a Lei Geral de Proteção de Dados (LGPD), que complementam tais medidas para a proteção de dados pessoais. A LGPD estabelece padrões específicos para o tratamento desses dados para garantir a privacidade e segurança dos dados e a transparência no uso desses dados nas empresas. Segundo Oliveira (2020, p. 20), a LGPD exige que as empresas implementem técnicas e medidas organizacionais para proteção de dados pessoais, incluindo políticas internas e treinamento de funcionários.

A LGPD também exige consentimento para o tratamento de dados pessoais e informações sobre a finalidade do tratamento (PEREIRA, 2019, p. 64). Além disso, a lei obriga as em- presas a informar sobre possíveis violações de segurança de dados que possam ameaçar a integridade dos dados pessoais (MARCONDES, 2021, p. 92). Conforme enfatizado por Sousa e Cabral (2018, p. 138), implementar medidas de segurança e cumprir a LGPD pode trazer benefícios às empresas, como melhoria da reputação e fidelização dos clientes. Além disso, o cumprimento da lei pode reduzir o risco de sanções e multas por parte das agências reguladoras.

É por isso que a implementação de medidas de segurança corporativa juntamente com a conformidade com a LGPD é fundamental para garantir a privacidade e a segurança dos indivíduos. dados em um cenário cada vez mais digital. Isto exige investimento em tecnologia, recursos humanos e formação, mas é uma medida essencial para garantir a confiança dos clientes nas empresas e evitar perdas financeiras e reputacionais.

3.2 Assegurando o consentimento dos indivíduos para o uso de dados

Um dos aspectos fundamentais da Lei Geral de Proteção de Dados (LGPD) reside na necessidade de obtenção do consentimento explícito dos usuários para o tratamento de seus dados pessoais. Segundo Oliveira (2020, p. 65), a LGPD estabelece que as empresas devem comunicar de forma clara e inequívoca a finalidade e o método de utilização dos dados, permitindo aos usuários controlarem e compreender as informações compartilhadas. Para atender a esse requisito, as empresas precisam desenvolver políticas de privacidade que sejam transparentes, de fácil entendimento, acessíveis e compreensíveis para os usuários. Tais políticas devem esclarecer quais informações são coletadas, como são utilizadas, com quem são compartilhadas e por quanto tempo são mantidas. Além disso, devem explicitar os direitos dos usuários em relação às suas informações, como o direito de acessar, corrigir, excluir e transferir dados (PEREIRA, 2019, p. 45).

A implementação de políticas de privacidade claras e acessíveis representa uma oportunidade para as empresas construírem a confiança dos usuários. Ao demonstrar transparência no processamento de dados pessoais, as empresas reforçam sua reputação e demonstram compromisso com a proteção da privacidade dos usuários. É essencial que essas políticas sejam redigidas de forma simples e objetiva, evitando o uso de termos técnicos, para garantir que os usuários compreendam facilmente como seus dados serão utilizados (MARCONDES, 2021, p. 82). Vale ressaltar que as políticas de proteção de dados não devem ser apenas documentos estáticos, mas sim refletir a cultura de privacidade das empresas. Portanto, as organizações devem garantir que essas políticas sejam atualizadas regularmente para refletir as mudanças nas práticas de tratamento de dados e comunicar efetivamente os usuários. Além disso, as empresas devem oferecer mecanismos que permitam aos usuários concederem ou retirarem consentimento facilmente e de maneira transparente.

Ao adotar o consentimento explícito do usuário e políticas de proteção claras, as empresas não apenas cumprem os requisitos legais da LGPD, mas também promovem um relacionamento mais transparente e confiável com os usuários. Essa abordagem fortalece parcial- mente a proteção de dados pessoais na Internet e promove uma cultura de respeito à privacidade. A transparência e as políticas de privacidade claras são essenciais para que os usuários tenham controle sobre seus dados pessoais e possam tomar decisões informadas sobre seu compartilhamento. Além disso, essa prática é benéfica para as empresas, pois aquelas que tratam os dados pessoais de forma ética e transparente podem conquistar a confiança e a lealdade dos usuários, estabelecendo um relacionamento de longo prazo baseado na proteção da privacidade e na responsabilidade corporativa.

3.3 A clareza dos objetivos do uso dos dados pessoais na internet: A Política de Privacidade

A implementação de diretrizes claras de privacidade desempenha um papel crucial na proteção dos dados pessoais dos utilizadores, conforme recomendado pelo Regulamento Geral de Proteção de Dados (PIB). De acordo com as diretrizes da LGPD, as empresas de- vem informar de forma transparente aos usuários sobre as finalidades da coleta de dados pessoais e garantir a integridade desses dados. Para criar diretrizes transparentes de proteção de dados, é importante que as empresas desenvolvam políticas de proteção de dados que sejam fáceis entender acessível e compreensível para os usuários.

É importante que estas políticas sejam escritas numa linguagem simples e compreensível, evitando termos técnicos que possam ser de difícil compreensão para os utilizadores. Além disso, é importante que as políticas de privacidade sejam facilmente acessíveis aos usuários em todas as plataformas.

Como enfatiza Silva (2019, p. 79):

> As empresas precisam adotar políticas claras e objetivas sobre a coleta, uso e armazenamento dos dados pessoais dos usuários. Essa medida não apenas atende às obrigações legais, mas também fortalece a confiança dos usuários nas empresas e cria uma imagem de transparência e responsabilidade (SILVA, 2019, p. 79).

Outro passo importante que as empresas podem tomar para implementar políticas de privacidade transparentes é usar políticas de privacidade claras e específicas. uns. consenti- mentos para cada finalidade de uso de dados pessoais. Isso garante que os usuários tenham pleno conhecimento das finalidades para as quais seus dados são coletados e possam decidir se desejam divulgá-los para cada finalidade específica. As regulamentações da LGPD tornam igualmente importante que as empresas garantam a proteção dos usuários. dados pessoais. Informação Isto requer a implementação de medidas de segurança adequadas, como a encriptação de dados e o acesso limitado aos dados pessoais.

Segundo Ferreira (2020, p. 103), a implementação de políticas de proteção de dados transparentes e eficazes, juntamente com a utilização de medidas de segurança. Medidas exigidas pela LGPD, fortalecem a relação de confiança entre empresas e seus usuários. Uma política de privacidade bem redigida, clara e objetiva transmite uma imagem de transparência e responsabilidade e é essencial para garantir a proteção dos dados pessoais dos utilizadores. Além disso, é importante que as empresas forneçam acesso fácil às políticas de privacidade nas suas plataformas, para que os utilizadores estejam totalmente informados sobre os seus dados pessoais. Também é crucial garantir o consentimento explícito dos utilizadores para qualquer finalidade para a qual os seus dados pessoais são processados. Um problema parte da construção de um relacionamento de confiança. Promessas claras e direcionadas tornam isso fácil de alcançar.

A segurança é essencial para a confiança do usuário, por isso as empresas devem implementar medidas de segurança eficazes para proteger os dados pessoais que coletam. Isto inclui a implementação de criptografia de dados e controle limitado de acesso aos dados pessoais. Silva (2019, p. 79) enfatiza que uma política clara ajuda a fortalecer a confiança dos usuários na empresa e aumenta sua transparência. A implementação de políticas de privacidade transparentes ajuda os usuários a se sentirem mais seguros e confortáveis ao compartilhar suas informações pessoais com uma empresa. As empresas podem melhorar suas práticas de privacidade adotando modelos internacionais reconhecidos de práticas de privacidade e segurança. A adoção de padrões pode fornecer segurança de privacidade aos usuários e aumentar a confiança nas empresas. Finalmente, é importante que as empresas cumpram os padrões estabelecidos pela LGPD e aloquem recursos suficientes para aplicar efetivamente suas políticas de privacidade. O incumprimento pode ter consequências graves para as em- presas e minar a confiança dos utilizadores.

4. A FISCALIZAÇÃO DO USO E A DEVIDA APLICAÇÃO DA LGPD

Uma das ações principais para assegurar a eficácia da proteção de dados pessoais na era tecnológica é a constante necessidade de monitoramento e aplicação de sanções efetivas. A Lei Geral de Proteção de Dados (LGPD) estabeleceu um sistema de monitoramento e punição, visando garantir a conformidade com os padrões de proteção de dados definidos pelas empresas e responsabilizar aqueles que violam tais regras (SAFFI, 2019, p. 78). A Agência Nacional de Proteção de Dados (ANPD) é encarregada de supervisionar a conformidade no Brasil, possuindo autoridade para conduzir investigações, monitorar práticas corporativas, receber reclamações, aplicar sanções e desenvolver diretrizes de proteção de dados pessoais (SOUZA; CABRAL, 2018, p. 95). A existência de um órgão regulador fortalece a aplicação da lei e assegura que as empresas sejam responsabilizadas por quaisquer violações não autorizadas.

O propósito da fiscalização da LGPD é garantir que as empresas cumpram as disposições legais, como a obtenção de consentimento explícito dos usuários, a implementação de medidas de segurança adequadas, o desenvolvimento de políticas claras de proteção de dados e a preservação da privacidade dos dados pessoais (OLIVEIRA, 2020, p. 65). Essa supervisão contribui para aumentar a conscientização das empresas sobre a importância da proteção de dados e cria um ambiente propício à adoção de boas práticas. Além da fiscalização, a LGPD prevê a aplicação de penalidades administrativas em casos de violação dos padrões de proteção de dados. Tais sanções podem variar desde advertências até multas significativas, que podem chegar a 2% do faturamento da empresa e até 50 milhões de reais por infração (FERREIRA, 2020, p. 108). O propósito das multas é punir as empresas que negligenciam a proteção de dados pessoais e prevenir práticas inadequadas. A possibilidade de sanções financeiras substanciais incentiva as empresas a adotarem medidas de segurança adequadas e a tratarem com responsabilidade os dados pessoais dos usuários.

Além das sanções administrativas, a LGPD também possibilita ações judiciais individuais ou coletivas em casos de violação de dados pessoais. Os usuários têm o direito de buscar indenização por danos materiais, morais ou coletivos decorrentes da violação de seus dados pessoais (REIS, 2020, p. 113). Essa oportunidade de ação legal realça a importância da proteção de dados e oferece aos usuários meios adicionais para buscar reparação em caso de violação de sua privacidade. A aplicação e punição eficazes são elementos cruciais para garantir a proteção dos dados pessoais na era tecnológica. A existência de um órgão de supervisão e a aplicação de sanções financeiras significativas incentivam as empresas a adotarem práticas adequadas de proteção de dados e a promover o respeito pela privacidade. Além disso, a possibilidade de ação legal oferece aos usuários meios adicionais para buscar reparação em situações em que seus direitos sejam violados.

No entanto, é importante enfatizar que a eficácia do monitoramento e da punição depende da capacidade do órgão regulador de investigar e controlar, além de tomar responsabilidade sobre reclamações, garantindo a eficácia do sistema jurídico no tratamento de casos de proteção de dados. O investimento contínuo na infraestrutura e nos recursos desses órgãos é necessário para garantir a aplicação e o cumprimento efetivo da LGPD.

Concluindo, o monitoramento e a aplicação de penalidades efetivas são fatores-chave para garantir a proteção dos dados pessoais nos meios digitais. A existência de um órgão regulador, a imposição de sanções financeiras significativas e a disponibilidade de recursos legais fortalecem a aplicação da LGPD e incentivam as empresas a adotarem boas práticas de proteção de dados. Tais mecanismos ajudam a criar um ambiente seguro e responsável para o tratamento de dados pessoais na Internet.

4.1 O uso dos dados com a devida concessão dos utilizadores.

Um dos pilares do Regulamento Geral de Proteção de Dados (RGPD) é obter o consentimento explícito dos utilizadores para o tratamento dos seus dados pessoais. A LGPD estipula que as empresas devem declarar de forma clara e inequívoca a finalidade e a forma de uso dos dados para garantir que os usuários controlem e compreendam os dados compartilhados (OLIVEIRA, 2020, p. 65). Para atender a esse requisito, as empresas devem desenvolver políticas de proteção de dados que são transparentes, facilmente acessíveis aos usuários, acessíveis e compreensíveis. Tais

políticas devem detalhar quais informações são coletadas, como são utilizadas, com quem são compartilhadas e por quanto tempo são mantidas. Além disso, deverão explicar os direitos dos usuários em relação aos seus dados, como o direito de acessá-los, corrigi-los, excluí-los e movê-los (PEREIRA, 2019, p. 45).

A implementação de políticas de privacidade abertas e fáceis de usar oferece às empresas uma oportunidade de construir a confiança dos usuários. Ao demonstrarem transparência no tratamento de dados pessoais, as empresas fortalecem a sua reputação e demonstram o seu compromisso com a proteção da privacidade dos utilizadores. Tais políticas devem ser redigidas de forma simples e direta, evitando o uso de terminologia técnica, para que os usuários possam compreender facilmente como seus dados serão utilizados (MARCONDES, 2021, p. 82). É muito importante enfatizar que a privacidade . Políticas não devem ser meros documentos estáticos, mas sim refletir a cultura de privacidade das empresas. As organizações devem garantir que tais políticas sejam atualizadas regularmente para refletir as mudanças nas práticas de tratamento de dados e sejam efetivamente comunicadas aos usuários. Além disso, as empresas devem fornecer mecanismos que permitam aos usuários dar ou retirar consentimento a qualquer momento, de forma fácil e transparente (FERREIRA, 2020, p. 108).

A LGPD também exige que as empresas verifiquem a idade dos usuários antes de coletar seus dados pessoais. dados, especialmente para crianças e jovens. Isto porque é importante proteger a privacidade e a segurança dos jovens utilizadores devido à sua vulnerabilidade. As empresas devem implementar mecanismos eficazes para verificar a idade dos usuários e, se necessário, obter o consentimento dos pais ou responsáveis legais (REIS, 2020, p. 113). Ao implementar o consentimento explícito do usuário e práticas de privacidade transparentes, as empresas não podem apenas cumprir as obrigações legais. Mas também promovem um relacionamento mais aberto e de confiança com os usuários. Isto ajuda a reforçar a proteção dos dados pessoais na Internet e cria uma cultura de respeito pela privacidade.

A transparência e a clareza da política de privacidade são essenciais para que os utiliza- dores possam gerir os seus dados pessoais e tomar decisões informadas sobre como e com quem os querem partilhar. Além disso, esta abordagem é mutuamente benéfica, pois as em- presas que tratam os dados pessoais de forma ética e transparente podem ganhar a confiança e a lealdade dos utilizadores e construir relacionamentos de longo prazo baseados na proteção da privacidade e na responsabilidade corporativa.

4.2 A obrigação das empresas em se adequar à LGP para estabelecer medidas de segurança

A entrada em vigor do Regulamento Geral de Proteção de Dados (RGPD) aumentou a necessidade de as empresas implementarem fortes medidas de segurança para proteger os dados pessoais dos utilizadores online. Em meio à crescente ameaça de violações de dados e ataques cibernéticos, a proteção de dados pessoais tornou-se uma prioridade indiscutível tanto para organizações quanto para usuários (REIS, 2020, p. 113). Um dos principais requisitos da LGPD é esse. as empresas implementam mecanismos de segurança apropriados para proteger os dados pessoais contra uso não autorizado, perda ou vazamento. Isto envolve a aplicação de técnicas de criptografia que transformam dados em códigos complexos e ilegíveis, dificultando a escuta e o uso indevido. A criptografia é um meio eficaz de proteção para proteger

informações confidenciais e impedir o acesso de pessoas não autorizadas (MARCONDES, 2021, p. 82).

Além da criptografia, é imperativo que as empresas implementem mecanismos de autenticação de acesso para garantir que apenas indivíduos autorizados tenham acesso às informações pessoais. Isto requer a implementação de senhas fortes, autenticação de dois fatores e outros métodos de verificação de identidade. Essas camadas adicionais de proteção ajudam a proteger os dados pessoais contra acessos não autorizados mesmo no caso de uma possível violação de segurança (OLIVEIRA, 2020, p. 65).

A LGPD também incentiva as empresas a seguirem boas práticas de segurança, como a realização regular de auditorias, identificar vulnerabilidades potenciais e implementar práticas de gerenciamento de incidentes. Estes regulamentos estabelecem procedimentos para lidar com violações de dados, tais como violações de dados, incluindo notificação às autoridades relevantes e aos dados relevantes. Uma resposta inteligente a incidentes ajuda a minimizar danos e mostra o compromisso da empresa em proteger os dados pessoais (PEREIRA, 2019, p. 45). A LGPD também enfatiza a importância de aumentar a segurança da informação e treinar os funcionários. Informações pessoais. As empresas são aconselhadas a investir em programas de formação dos seus colaboradores que visam aumentar a sensibilização para as melhores práticas de segurança, riscos de proteção de dados e responsabilidades individuais pelo tratamento adequado dos dados pessoais.

A conscientização dos funcionários desempenha um papel fundamental na prevenção de erros humanos que ameaçam a segurança da informação (FERREIRA, 2020, p. 108). É importante compreender que a implementação de medidas de segurança não é apenas uma exigência legal, mas também um negócio inteligente. Estratégia. Ao demonstrarem um compromisso com a segurança das informações pessoais, as empresas fortalecem a confiança dos utilizadores, o que pode levar a uma imagem positiva e a uma maior fidelização dos clientes. A segurança dos dados pessoais tornou-se um fator decisivo para os usuários na hora de escolher com quais empresas desejam compartilhar seus dados (REIS, 2020, p. 113). Resumo: A LGPD acelerou a adoção de medidas de segurança pelas empresas para proteger. seus dados. dados pessoais na internet. A implementação de tecnologias como a encriptação, mecanismos de autenticação e boas práticas de segurança são essenciais para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais.

A sensibilização e a formação dos funcionários desempenham um papel fundamental na proteção de dados. Com estas medidas, as empresas não só cumprem a lei, mas também fortalecem a sua reputação e a confiança dos utilizadores. A segurança dos dados pessoais é uma parte importante do sucesso e da sustentabilidade das organizações na era da tecnologia.

5 CONCLUSÃO

Considerando as informações e o contexto histórico sobre a proteção de dados pessoais na internet, com foco na Lei Geral de Proteção de Dados (LGPD), é possível destacar que essa legislação trouxe mudanças significativas no tratamento dessas informações, estabelecendo princípios, direitos e obrigações que visam salvaguardar a privacidade e a segurança dos indivíduos.

A implementação da LGPD no Brasil representa um marco na legislação nacional ao estabelecer um conjunto abrangente de normas e diretrizes para o

tratamento de dados pessoais, buscando promover uma maior proteção e respeito à privacidade dos usuários, o que fortalece a confiança no ambiente digital.

Inspirada em regulamentos internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD reflete a preocupação global com a proteção dos dados pessoais em um mundo cada vez mais conectado. Ela estabelece princípios fundamentais, como a necessidade de consentimento informado para o tratamento de dados, a especificação da finalidade do uso das informações, a transparência no processamento de dados e a implementação de medidas de segurança adequadas.

A implementação da LGPD implica desafios e exigências para as empresas que atuam no Brasil, que precisam se adaptar às novas regras e estabelecer mecanismos eficazes de proteção de dados. Isso envolve investimentos em tecnologia, capacitação de pessoal e a adoção de práticas de governança e segurança da informação, como a implementação de criptografia, autenticação de acesso e políticas de controle de acesso.

Além de afetar as empresas, a LGPD também impacta órgãos governamentais, organizações do terceiro setor e qualquer entidade que lide com dados pessoais, buscando criar uma cultura de proteção de dados e estimular a responsabilidade de todos os agentes envolvidos no tratamento dessas informações.

A conscientização da sociedade sobre seus direitos e a importância da proteção de dados pessoais é crucial, pois os usuários precisam compreender os riscos envolvidos na divulgação de suas informações e exercer efetivamente seus direitos, como o direito ao consentimento informado, acesso, exclusão, retificação e portabilidade dos dados.

A fiscalização e a aplicação de sanções em caso de violações à LGPD são elementos cruciais para garantir sua efetividade, sendo a Autoridade Nacional de Proteção de Dados (ANPD) responsável por fiscalizar e orientar as organizações. No entanto, a efetividade dessas medidas depende da capacidade do órgão regulador em investigar e processar denúncias, bem como da agilidade do sistema judiciário em lidar com casos relacionados à proteção de dados.

Em resumo, a LGPD representa um avanço significativo na proteção de dados pessoais na internet, estabelecendo diretrizes claras e conferindo maior controle aos indivíduos sobre suas informações. A sua efetiva implementação e cumprimento contribuirão para um ambiente digital mais seguro e respeitoso, beneficiando todos os envolvidos no ecossistema de dados pessoais.

REFERÊNCIAS

ALMEIDA, N. N.; SANTOS, S. L. F. Gestão de dados pessoais em conformidade com a LGPD. In: Encontro de Administração, 8., 2020, Joinville-SC. **Anais** [...]. Joinville-SC: INESUL, 2020. p. 1-10.

ALMEIDA, V. B.; SANTOS, A. C. **Lei Geral de Proteção de Dados:** comentários artigo por artigo. São Paulo: Thomson Reuters Brasil, 2020.

ARAÚJO, J. R. (2021). **Lei Geral de Proteção de Dados (LGPD):** uma análise prática para empresas. [s.l.]. [s.n.], 2021.

BITTAR, C. A. C.; TOMASCHEWSKI, T. A Lei Geral de Proteção de Dados Pessoais e sua aplicação prática nas empresas. In: Congresso Internacional De Ad-Ministração, XXVI., 2021, Rio de Janeiro-RJ. **Anais** [...]. Rio de Janeiro-RJ: ANPAD.

BITTAR, C. A.; TOMASCHEWSKI, T. A. **Lei Geral de Proteção de Dados Pessoais:** comentários aos Arts. 1º ao 41. São Paulo: Revista dos Tribunais, 2021.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2011/lei/l12527.htm. Acesso em: 11 fev. 2024.

BRASIL. **Medida Provisória nº 954/2020**. Disponível em: http://www.planalto.gov.br/cci- vil_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 8 jan. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pes- soais Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planal- to.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L13943.htm. Acesso em: 11 fev. 2024.

FERREIRA, D. C. Lei Geral de Proteção de Dados Pessoais: a implementação e seus desafios para a administração pública e privada no Brasil. **Revista de Direito**, v. 18, n. 32, p. 97-113, 2020.

FERREIRA, V. P.; SANTOS, L. R. dos (orgs.). **Direitos humanos, corporações e outras responsabilidades**. Rio de Janeiro: Garamond, 2022.

GUIMARÃES, D. F.; JUNIOR, A. S. Vigilância e privacidade na era digital: resistência e (in)visibilidade. In: FERREIRA, V. P.; SANTOS, L. R. dos (orgs.). **Direitos humanos, corpos e outras responsabilidades**. Rio de Janeiro: Garamond, 2022.

LIMA, F. S. **Proteção de dados pessoais no Brasil:** aspectos jurídicos e desafios para a efetivação da Lei Geral de Proteção de Dados (LGPD). [s.l.]. [s.n.], 2022.

MARCONDES, F. R. S. **A Nova Lei Geral de Proteção de Dados Pessoais:** comentários à Lei n. 13.709/18. São Paulo: Thomson Reuters Brasil, 2021.

MENDES, J. A. e Costa, J. R. **Lei Geral de Proteção de Dados:** aspectos conceituais e práticos. Rio de Janeiro: Brasport Livros e Multimídia, 2020.

OLIVEIRA, T. L. S. **A proteção de dados pessoais na internet:** uma análise à luz da Lei Geral de Proteção de Dados Pessoais. São Paulo: Saraiva Educação, 2020.

PEREIRA, L. S. **A Lei Geral de Proteção de Dados (LGPD):** seus aspectos fundamentais. São Paulo: Novo Século Editora, 2019.

REIS, M. A. **LGPD Comentada:** Lei Geral de Proteção de Dados Pessoais. [s.l.]. [s.n.], 2020.

REZEK, F. **Proteção de Dados Pessoais:** a Lei Geral de Proteção de Dados Pessoais (LGPD) e seus reflexos na sociedade. [s.l.]. [s.n.], 2019.

SAFFI, P. C. **Proteção de dados pessoais na era digital:** Lei Geral de Proteção de Dados Pessoais - LGPD. Rio de Janeiro: Forense, 2019.

SANTOS, A. B. **LGPD na prática:** implementação e adequação de empresas à Lei Geral de Proteção de Dados Pessoais. [s.l.]. [s.n.], 2021.

SANTOS, A. M. **LGPD:** Lei Geral de Proteção de Dados comentada. São Paulo: Novatec Editora, 2020.

SCHAEFER, F.; ROSENVALD, N.; MONTEIRO FILHO, C. E. do R.; KHOURI, P. R.; MASCARENHAS, I. de L. **Migalhas de Responsabilidade Civil**. Salvador: Editora JusPodivm, 2020.

SILVA, R. F. A proteção de dados pessoais no Brasil: uma análise da Lei Ge- ral de Proteção de Dados e as perspectivas do direito. **Revista de Direito**, v. 15, n. 32, p. 75-96. Disponível em: https://periodicos.unb.br/index.php/rdsr/article/view/28490. Acesso em: 6 jun. 2024.

SOUSA, R. C.; CABRAL, S. K. **Trabalho docente e tecnologias digitais**. São Paulo: Difusora Sul-Americana, 2018.

BRASIL. Lei Geral de Proteção de Dados Pessoais. Ministério do Desenvolvimento e Assistência Social, Família e Combate a Fome, Brasília, DF. Disponível em: https://www.gov.br/mds/pt-br/acesso-a-informacao/governanca/integridade/campanhas/lgpd.