

CENTRO UNIVERSITÁRIO UNINOVAFAPÍ
BACHARELADO EM DIREITO

IASMIN SILVEIRA ALVES
KLEBER SALES MENEZES
ROBERTO NUNES E SILVA

LEI GERAL DE PROTEÇÃO DE DADOS: aplicabilidade às empresas privadas

TERESINA

2024

IASMIN SILVEIRA ALVES

KLEBER SALES MENEZES

ROBERTO NUNES E SILVA

LEI GERAL DE PROTEÇÃO DE DADOS: aplicabilidade às empresas privadas

Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do Centro
Universitário UNINOVAFAPI, como requisito
parcial para obtenção do grau de Bacharel em
Direito.

Orientadora: Prof^a Ma. Sara Morgana Silva
Carvalho Lopes

TERESINA

2024

FICHA CATALOGRÁFICA

A474l Alves, lasmin Silveira.

Lei geral de proteção de dados : aplicabilidade às empresas privadas./ lasmin Silveira Alves ; Kleber Sales Menezes ; Roberto Nunes e Silva. – Teresina: UNINOVAFAPI, 2024.

Orientador (a): Prof. Ma. Sarah Morgana Silva Carvalho Lopes – UNINOVAFAPI, 2024.

25. p.; il. 23cm.

Trabalho (Graduação em Direito) – UNINOVAFAPI, Teresina, 2024.

* Dados. 2. Proteção. 3. Legislação. 4. Empresas. Título. II. Alves, lasmin Silveira. III. Menezes, Kleber Sales. IV. Silva, Roberto Nunes e.

CDD 343.13

Catálogo na publicação
Francisco Renato Sampaio da Silva – CRB/1028

IASMIN SILVEIRA ALVES
KLEBER SALES MENEZES
ROBERTO NUNES E SILVA

LEI GERAL DE PROTEÇÃO DE DADOS: aplicabilidade às empresas privadas

Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do Centro
Universitário UNINOVAFAPI, como requisito
parcial para obtenção do grau de Bacharel em
Direito.

Data de Aprovação: ____/____/____

BANCA EXAMINADORA

Prof.^a Ma. Sara Morgana Silva Carvalho Lopes
Centro Universitário UNINOVAFAPI
(Orientadora)

Prof.^a titulaçãoxxxxxxxxxx
Centro Universitário - UNINOVAFAPI
(1º Examinador)

Prof.^a titulaçãoxxxxxxxxxx
Centro Universitário - UNINOVAFAPI
(2º Examinador)

AGRADECIMENTOS

O término deste trabalho de conclusão de curso representa não apenas o fim de uma etapa acadêmica, mas também a realização de um sonho que não seria possível sem o apoio e a colaboração de muitas pessoas.

Primeiramente, agradeço a Deus, pela força e sabedoria concedidas ao longo desta jornada.

Aos nossos pais, cônjuges e filhos, pelo amor incondicional, apoio constante e por acreditarem em nós em todos os momentos. Vocês são nossas maiores inspirações.

Aos nossos amigos e colegas de curso, pela parceria, incentivo e pelas inúmeras horas de estudo compartilhadas. A amizade de vocês tornou essa caminhada mais leve e prazerosa.

Aos professores e orientadores, em especial à Prof^a Ma. Sara Morgana Silva Carvalho Lopes, pela paciência, orientação e valiosas contribuições para a realização deste trabalho. Suas palavras de incentivo e críticas construtivas foram fundamentais para o nosso crescimento acadêmico e pessoal.

A todos que, direta ou indiretamente, contribuíram para a realização deste trabalho, nossos sinceros agradecimentos.

RESUMO

Este trabalho apresenta uma pesquisa dos impactos da implementação da Lei Geral de Proteção de Dados (LGPD) nas empresas privadas, abordando como o tratamento dos dados dos consumidores impacta nos resultados positivos e negativos da empresa. Partindo do questionamento de como a proteção de dados dos clientes pode ser um diferencial na relação entre a empresa e o cliente. Com o objetivo de analisar os desafios de aplicação da LGPD nas empresas privadas, foi possível verificar que a governança de dados e a segurança da informação são fatores primordiais no cumprimento dessa lei e que isso influencia diretamente na melhoria das relações entre o cliente e a empresa. A transparência nas operações e o respeito aos direitos dos titulares contribuem para o aumento da confiança de clientes e parceiros, melhorando a reputação da empresa no mercado. Além disso, a adoção de práticas de segurança robustas reduz o risco de vazamentos e fraudes, evitando custos com penalidades e crises de imagem. Assim, foi realizada uma pesquisa bibliográfica com abordagem qualitativa das principais medidas adotadas por empresas para a implementação da LGPD. Dessa forma, é possível concluir que a aplicação da LGPD nas empresas produziu frutos positivos em diversos aspectos, como econômicos e nas relações entre clientes e empresários.

Palavras-chave: Dados. Proteção. Legislação. Empresas

ABSTRACT

This work presents research into the impacts of the implementation of the General Data Protection Law (LGPD) on private companies, addressing how the processing of consumer data impacts the company's positive and negative results. Starting from the question of how protecting customer data can be a differentiator in the relationship between the company and the customer. With the aim of analyzing the challenges of applying the LGPD in private companies, it was possible to verify that data governance and information security are key factors in the enforcement of this law and that this directly influences the improvement of relationships between the customer and the company. Transparency in operations and respect for holders' rights contribute to increasing the trust of customers and partners, improving the company's reputation in the market. Furthermore, the adoption of robust security practices reduces the risk of leaks and fraud, avoiding costs with penalties and image crises. Thus, a bibliographical research was carried out with a qualitative approach on the main measures adopted by companies to implement the LGPD. In this way, it is possible to conclude that the application of the LGPD in companies produced positive results in several aspects, such as economic aspects and in relations between customers and entrepreneurs.

Keywords: Data. Protection. Legislation. Companies

1 INTRODUÇÃO

A proteção de dados é essencial para garantir a privacidade e a segurança das informações pessoais em um mundo cada vez mais digitalizado. Em um cenário onde dados são coletados e compartilhados por empresas e governos, proteger essas informações é fundamental para evitar abusos, como fraudes, roubos de identidade e vazamentos. Além disso, a proteção de dados assegura que os indivíduos mantenham controle sobre como suas informações são utilizadas, fortalecendo seus direitos e promovendo maior confiança nas relações com organizações e plataformas digitais.

No âmbito corporativo, a proteção de dados é um diferencial competitivo e um requisito legal em muitos países, como previsto na Lei n.º 13.709/2018, Lei Geral de Proteção de Dados (LGPD) no Brasil e no Regulamento Geral de Proteção de Dados (GDPR) na Europa. Empresas que investem em segurança da informação e transparência no uso de dados não apenas evitam sanções legais, mas também conquistam a confiança de consumidores e parceiros. A proteção adequada das informações contribui para um ambiente mais seguro e ético, permitindo que a tecnologia seja utilizada de maneira inovadora e sustentável, sem comprometer a privacidade e a integridade das pessoas envolvidas.

Com a aprovação da LGPD em 2018, o Brasil deu um passo importante na consolidação de uma legislação moderna e alinhada às práticas internacionais, como o GDPR da União Europeia. A LGPD estabeleceu princípios e diretrizes para o tratamento de dados pessoais, exigindo que organizações públicas e privadas adotem medidas de segurança e garantam o consentimento claro dos titulares para o uso de suas informações. Além disso, a lei criou a Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar o cumprimento das normas e orientar sobre boas práticas.

A implementação da LGPD marcou um avanço significativo, mas a evolução das leis de proteção de dados no Brasil continua em andamento. A ANPD vem editando regulamentações complementares e orientações específicas para adequar a lei às inovações tecnológicas e às novas demandas do mercado. Também há um esforço contínuo para conscientizar a sociedade sobre a importância da privacidade e da segurança digital, com foco em garantir a proteção de dados de forma eficaz. Assim, o Brasil está se consolidando como uma referência na promoção da privacidade, buscando equilibrar o desenvolvimento econômico com a proteção dos direitos fundamentais dos cidadãos.

Dessa forma esse trabalho tem por objetivo geral analisar a aplicação da LGPD nas empresas privadas, identificando os desafios e as oportunidades relacionados ao cumprimento da legislação, com foco em práticas de governança de dados, segurança da informação e impacto na relação com consumidores, a fim de compreender como a adequação à LGPD pode contribuir para a competitividade, ética empresarial e proteção da privacidade. Partindo da questão norteadora de como a proteção dos dados dos clientes pode ser um diferencial na relação entre a empresa e o seu cliente.

Com isso os objetivos específicos foram estabelecidos, por exemplo: investigar como as organizações estão implementando políticas de governança de dados, identificando as principais práticas adotadas, os desafios enfrentados e as áreas críticas que precisam de melhorias para garantir o cumprimento da legislação.

Examinar de que forma a adaptação à LGPD tem influenciado a rotina organizacional, desde processos internos e tecnologia até a relação com clientes, parceiros e fornecedores, além de verificar possíveis mudanças na competitividade e inovação. Verificar como as organizações avaliam os impactos econômicos e reputacionais da conformidade com a lei, considerando tanto as vantagens competitivas de preservar a privacidade quanto os riscos legais e financeiros associados a possíveis violações.

A metodologia usada neste trabalho é uma revisão bibliográfica com o uso da pesquisa qualitativa, é uma abordagem metodológica que visa explorar e compreender fenômenos sociais, culturais e comportamentais a partir da perspectiva dos indivíduos envolvidos. Esse tipo de pesquisa permite uma análise mais profunda das motivações, sentimentos e percepções dos participantes, revelando nuances que muitas vezes são perdidas em análises estatísticas.

Os resultados obtidos são descritivos e interpretativos, oferecendo insights valiosos que podem informar políticas, práticas e futuras pesquisas. A flexibilidade da pesquisa qualitativa a torna uma ferramenta poderosa para entender realidades sociais dinâmicas e multifacetadas.

A pesquisa é dividida em quatro capítulos, sendo o primeiro Introdução, o segundo Leis Subsidiárias, o terceiro Lei Geral de Dados estrutura e aplicabilidade no mundo empresarial, o quarto discorre sobre A LGPD no contexto das empresas privadas e o quinto são apresentadas as considerações finais.

2 LEIS SUBSIDIÁRIAS À APLICAÇÃO DA LGPD

A proteção de dados envolve práticas e regulamentos destinados a garantir a privacidade e segurança das informações pessoais, assegurando que dados como nome, Cadastro Nacional de Pessoa Física (CPF), endereços, físico e eletrônico, e informações sensíveis (como saúde e crenças) sejam usados de forma ética e segura, com o consentimento do titular. Leis como a LGPD no Brasil e a GDPR na Europa estabelecem regras claras para empresas e órgãos públicos, obrigando-os a coletar, armazenar e processar dados de maneira responsável (Moraes, 2020).

A proteção de dados evita vazamentos e fraudes, preservando a confiança entre empresas e clientes. Além disso, garante que os titulares tenham controle sobre suas informações, podendo acessá-las, corrigi-las ou excluí-las. Ferramentas como criptografia e autenticação são essenciais para evitar acessos indevidos. Assim, a proteção de dados é fundamental na era digital, equilibrando inovação e privacidade.

A LGPD no Brasil e a GDPR na Europa obrigam essas plataformas a pedir consentimento explícito do usuário para coleta e uso de dados. Além disso, garantem o direito à transparência, permitindo que o usuário saiba como suas informações são utilizadas e solicitando a exclusão ou correção de dados. Vazamentos e violações são riscos frequentes, reforçando a importância de boas práticas de segurança, como criptografia e autenticação forte.

Com isso, a necessidade de proteção de dados no Brasil surgiu com o crescimento acelerado da digitalização, do uso de redes sociais e da coleta massiva de informações pessoais por empresas e governos. Com o aumento da conectividade e a popularização da internet, passou a ser comum o uso de dados pessoais em transações online, campanhas de marketing digital e até na gestão pública. Esse cenário trouxe riscos, como vazamento de informações, fraudes, e violação da privacidade dos cidadãos (Moraes, 2020).

Casos de escândalos envolvendo o uso indevido de dados pessoais e práticas abusivas de vigilância também aumentaram a pressão para regulamentar o setor. A ausência de uma legislação específica deixava os usuários vulneráveis, uma vez que empresas podiam compartilhar ou vender dados sem o consentimento claro dos titulares. Além disso, a entrada em vigor da GDPR na Europa, em 2018, inspirou outros países, como o Brasil, a criar suas próprias leis para garantir transparência, segurança e controle no tratamento de dados.

A primeira Lei que pode ser considerada como proteção de dados no Brasil é a Lei de Propriedade Industrial (Lei n.º 9.279/1996), conhecida como Lei das Patentes, que regulamenta os direitos de propriedade sobre invenções e modelos de utilidade no Brasil. O objetivo dessa legislação é incentivar a inovação e proteger inventores, garantindo exclusividade temporária para a exploração de suas criações. Com essa exclusividade, o titular da patente tem o direito de impedir terceiros de produzir, usar, vender ou distribuir a invenção sem autorização, promovendo o desenvolvimento econômico e tecnológico (Brasil, 1996).

Outro importante avanço foi a Lei de Acesso à Informação (LAI), sancionada em 2011 por meio da Lei n.º 12.527, garante a qualquer cidadão o direito de acessar dados públicos de órgãos e entidades dos três poderes (Executivo, Legislativo e Judiciário), tanto ao nível federal quanto estadual e municipal. Seu objetivo é promover transparência na administração pública, permitindo o controle social e o monitoramento das ações governamentais (Brasil, 2011). A lei também estabelece que informações de interesse coletivo devem ser divulgadas proativamente em portais de transparência, facilitando o acompanhamento por parte da sociedade.

O Marco Civil da Internet, instituído pela Lei n.º 12.965/2014, estabelece os direitos e deveres de usuários, empresas e do governo no uso da internet no Brasil (Brasil, 2014). Considerado uma espécie de "Constituição da Internet", a lei tem como princípios fundamentais a liberdade de expressão, a privacidade e a proteção de dados pessoais, buscando garantir que a rede permaneça um ambiente democrático e seguro. O Marco Civil surgiu para regulamentar questões como neutralidade da rede, segurança cibernética e responsabilidade dos provedores (Moraes, 2020).

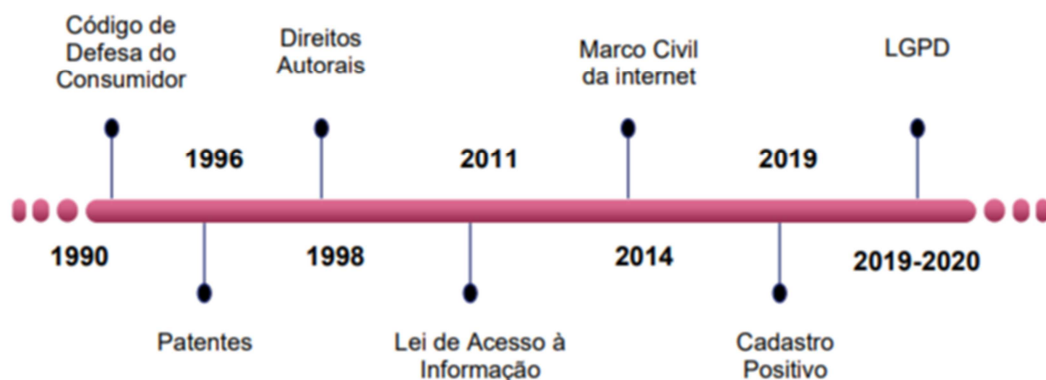
Atualmente, há aproximadamente 120 países com leis vigentes de proteção de dados pessoais e até 2020 esse número deverá subir para cerca de 134. Destes 120 países, aproximadamente 80% editaram uma lei de proteção de dados pessoais e possuem uma autoridade nacional independente, enquanto somente 10% não contam com um órgão independente, por previsões legislativas expressas em obediência a diretivas ou orientações de outros órgãos do Poder Executivo. Nota-se que, embora os modelos de autoridades nacionais sejam os mais variados, estudos demonstram que a maioria dos países optou por um modelo em que o órgão de controle desfruta de um grau de independência bastante elevado (Bezerra, 2019, p. 56).

Dito isso, chega-se à LGPD, sancionada por meio da Lei n.º 13.709/2018, que estabelece regras sobre a coleta, armazenamento e uso de dados pessoais no Brasil. Seu

principal objetivo é garantir a privacidade e a proteção das informações dos cidadãos, promovendo mais transparência nas práticas das organizações públicas e privadas. A LGPD determina que o tratamento de dados só pode ser feito com o consentimento do titular ou com base em outras hipóteses legais, como cumprimento de obrigações legais ou interesse legítimo, reforçando o controle dos indivíduos sobre suas informações.

Para mostrar a evolução dessas Leis no Brasil, a Figura 1 apresenta em ordem cronológica conforme a data de aprovação o conjunto de leis brasileiras que tratam da proteção de dados.

Figura 1 Cronologia das Leis de Proteção de Dados



Fonte: Langen, 2020,p.56.

A proteção de dados pessoais é fundamental para garantir a privacidade e segurança dos indivíduos em um mundo cada vez mais digitalizado. Com a crescente coleta e processamento de informações em plataformas online, proteger esses dados é essencial para evitar abusos, como o uso indevido, fraudes e vazamentos. Sem regulamentações adequadas, dados sensíveis, como informações financeiras e de saúde, podem ser explorados de forma indevida, comprometendo direitos fundamentais e a confiança nas relações digitais (Langen, 2020).

3 LEI GERAL DE PROTEÇÃO DE DADOS- ESTRUTURA E APLICABILIDADE NO MUNDO EMPRESARIAL

O principal objetivo da (LGPD) é garantir a privacidade e a proteção dos dados pessoais dos cidadãos, assegurando que empresas e órgãos públicos tratem essas informações de forma transparente e segura. A lei visa dar maior controle aos indivíduos sobre seus dados,

permitindo que eles saibam como suas informações são coletadas, armazenadas e utilizadas. Além disso, a LGPD exige que o tratamento dos dados pessoais ocorra apenas mediante consentimento do titular ou em outras hipóteses legais, como o cumprimento de obrigações jurídicas ou interesse legítimo (BRASIL, 2018).

Outro objetivo central da LGPD é estabelecer padrões claros para o uso responsável de dados, aumentando a confiança nas relações digitais e promovendo a segurança jurídica para empresas e consumidores. A criação da ANPD é um ponto-chave, pois esse órgão é responsável por fiscalizar o cumprimento da lei e orientar boas práticas. Assim, a LGPD não apenas protege os indivíduos contra abusos, como também alinha o Brasil às normas internacionais, fomentando uma economia digital baseada em transparência e respeito à privacidade.

Originalmente, a LGPD entraria em vigor em 2020, mas devido à pandemia de Covid-19 e às dificuldades enfrentadas pelas empresas para se adequar às novas regras, sua vigência foi parcialmente adiada. Em setembro de 2020, a lei finalmente entrou em vigor, enquanto as sanções administrativas passaram a ser aplicadas apenas a partir de agosto de 2021. A criação da ANPD foi um dos últimos passos importantes da tramitação, garantindo a fiscalização e o cumprimento da legislação, consolidando a proteção de dados como um direito fundamental no Brasil.

A LGPD, instituída pela Lei n.º 13.709/2018, é dividida em 10 capítulos que organizam seus dispositivos de forma clara e estruturada. Essa divisão aborda desde princípios e conceitos fundamentais até as sanções aplicáveis em casos de descumprimento. Essa estrutura permite que a LGPD funcione de forma abrangente, proporcionando clareza para empresas, cidadãos e órgãos públicos sobre suas responsabilidades e direitos no tratamento de dados pessoais.

O Capítulo I da LGPD é intitulado “Disposições Preliminares” e apresenta os conceitos e fundamentos essenciais da lei. Ele estabelece o âmbito de aplicação da LGPD, ou seja, quais situações e entidades estão sujeitas à legislação, e define os princípios e objetivos que orientam o tratamento de dados pessoais no Brasil. Além disso, é nesse capítulo que são explicados os termos-chave utilizados ao longo da lei, como dados pessoais, dados sensíveis, anonimização, controlador e operador (BRASIL, 2018).

Esse capítulo também reforça que a LGPD se aplica a qualquer operação de tratamento de dados realizada em território nacional, inclusive em ambientes digitais, desde que envolva dados de pessoas físicas. A lei se aplica tanto para agentes públicos quanto privados, desde que os dados tratados possam identificar ou individualizar uma pessoa. Entre

os princípios estabelecidos, destacam-se os da finalidade (uso dos dados apenas para objetivos legítimos e explícitos), necessidade (tratamento mínimo necessário), e transparência, que visa garantir que os titulares tenham acesso claro e facilitado às informações sobre o uso de seus dados.

No segundo capítulo da LGPD trata das hipóteses e regras para o tratamento de dados pessoais. Ele define as condições em que é permitido coletar, armazenar e utilizar dados pessoais, detalhando as bases legais que justificam o tratamento, como o consentimento do titular, cumprimento de obrigação legal, execução de contrato e legítimo interesse. Além disso, o capítulo diferencia o tratamento de dados comuns e dados sensíveis, estabelecendo critérios mais rígidos para a proteção das informações que envolvem, por exemplo, origem racial, religião, saúde e opinião política (BRASIL, 2018).

Esse capítulo também prevê cuidados especiais para o tratamento de dados de crianças e adolescentes, exigindo o consentimento específico dos pais ou responsáveis. Outra questão relevante é a revogação do consentimento, que pode ser solicitada pelo titular a qualquer momento, reforçando seu controle sobre as informações. O Capítulo II é fundamental para garantir que o uso de dados seja limitado e proporcional, respeitando a privacidade dos indivíduos e evitando abusos, ao mesmo tempo, em que permite o funcionamento das atividades econômicas e governamentais de forma legal e ética.

No terceiro capítulo da LGPD, são apresentados os direitos dos titulares de dados pessoais, assegurando transparência e controle sobre o uso de suas informações. Entre os principais direitos garantidos estão o de acesso aos dados, confirmação da existência do tratamento e correção de informações incorretas, incompletas ou desatualizadas. O titular também pode solicitar a portabilidade dos dados para outro fornecedor de serviço, a anonimização, bloqueio ou eliminação de dados desnecessários, e revogar o consentimento previamente concedido a qualquer momento (BRASIL, 2018).

Além disso, o capítulo determina que o titular tem o direito de ser informado sobre o compartilhamento dos seus dados com terceiros e sobre eventuais consequências caso decida não fornecer determinadas informações. O controlador dos dados é obrigado a fornecer essas respostas de forma clara e em prazo adequado. Esses dispositivos fortalecem o direito à privacidade e buscam garantir que os indivíduos possam exercer maior controle sobre como suas informações pessoais são tratadas, promovendo um ambiente de maior confiança e segurança nas relações que envolvem dados.

Já no quarto capítulo se estabelecem as regras aplicáveis aos agentes de tratamento de dados pessoais, distinguindo duas figuras principais: o controlador e o operador. O

controlador é o responsável por tomar as decisões sobre o tratamento dos dados, enquanto o operador apenas realiza o processamento seguindo as instruções do controlador. Ambos têm responsabilidades, mas o controlador assume uma posição mais central, pois deve garantir que o tratamento ocorra conforme a legislação, incluindo o dever de adotar medidas de segurança e de prestar contas sobre suas práticas de proteção de dados (BRASIL, 2018).

Esse capítulo também destaca a importância de contratos e acordos formais entre controladores e operadores para definir claramente as obrigações de cada parte. O controlador, além de supervisionar o operador, é obrigado a indicar um Encarregado de Proteção de Dados (DPO), responsável por intermediar a comunicação entre o controlador, os titulares dos dados e a ANPD. Essa estrutura pretende assegurar que o tratamento de dados seja realizado de maneira transparente e segura, estabelecendo mecanismos de governança que reforcem a confiança e a conformidade com a LGPD.

O quinto capítulo da LGPD regula a transferência internacional de dados pessoais, estabelecendo as condições sob as quais essas transferências podem ocorrer para países estrangeiros ou organizações internacionais. A transferência é permitida apenas quando o país destinatário oferece um nível de proteção de dados pessoais equivalente ao garantido pela LGPD ou se houver garantias específicas, como cláusulas contratuais, normas corporativas globais ou certificações aprovadas pela ANPD. Essa medida busca assegurar que os dados dos brasileiros não fiquem vulneráveis ao serem enviados para jurisdições com regras mais frágeis de privacidade (BRASIL, 2018).

Outro ponto importante é que o capítulo prevê exceções que permitem a transferência internacional mesmo quando o país de destino não oferece proteção equivalente. Essas exceções incluem situações como a obtenção de consentimento explícito do titular, o cumprimento de obrigações legais ou contratuais, e a proteção da vida ou integridade física do titular ou de terceiros. A transparência também é fundamental: o titular tem o direito de saber para onde seus dados estão sendo enviados e para quais finalidades. Essas diretrizes garantem que a circulação internacional de dados ocorra de maneira controlada, minimizando riscos e fortalecendo a confiança no tratamento global de informações pessoais.

No sexto capítulo da LGPD, é abordada a responsabilidade e a reparação de danos causados pelo tratamento inadequado de dados pessoais. Ele estabelece que os agentes de tratamento, como o controlador e o operador, são responsáveis por eventuais danos causados a titulares em decorrência da violação das normas da LGPD. Essa responsabilidade é objetiva, ou seja, mesmo sem a comprovação de dolo ou culpa, os agentes podem ser obrigados a

reparar os danos. No entanto, o operador só responderá diretamente se descumprir as instruções do controlador ou agir em desacordo com a legislação (BRASIL, 2018).

Dessa forma, o capítulo prevê algumas hipóteses que podem excluir ou mitigar a responsabilidade dos agentes. O controlador e o operador não serão responsabilizados se provarem que não realizaram o tratamento dos dados em questão, que não houve violação da legislação ou que o dano foi causado exclusivamente por culpa do titular ou de terceiros. Esse sistema busca equilibrar as obrigações entre as partes envolvidas, promovendo uma cultura de proteção e governança de dados, ao mesmo tempo, em que oferece meios de reparação justa aos titulares prejudicados.

Já no Capítulo 7 da LGPD trata da segurança e das boas práticas no tratamento de dados pessoais, estabelecendo que os agentes de tratamento devem adotar medidas técnicas e administrativas para proteger os dados contra acessos não autorizados e situações acidentais ou ilícitas, como perda, destruição ou alteração. Essas medidas devem ser proporcionais aos riscos e à natureza dos dados tratados, garantindo um nível adequado de segurança. Além disso, é necessário que o controlador e o operador realizem avaliações periódicas para assegurar a eficácia das políticas e procedimentos implementados, promovendo um ciclo contínuo de melhoria na proteção dos dados (BRASIL, 2018).

Outro ponto central deste capítulo é a previsão de boas práticas e governança. A LGPD incentiva que as organizações desenvolvam programas internos de conformidade, com regras claras para o tratamento de dados e mecanismos de supervisão. A adoção de códigos de conduta e certificações reconhecidas também é recomendada, funcionando como ferramentas para demonstrar o compromisso com a proteção de dados. Em caso de incidentes de segurança que possam comprometer os dados pessoais, como vazamentos, os agentes devem notificar a ANPD e, quando necessário, informar os titulares, assegurando transparência e permitindo ações para mitigar danos.

No oitavo capítulo da LGPD, estabelecem-se as regras de fiscalização e a atuação da ANPD, órgão responsável por garantir o cumprimento da legislação. A ANPD tem a função de orientar, fiscalizar e aplicar sanções administrativas aos agentes de tratamento que descumprirem as normas da LGPD. Entre suas atribuições estão a elaboração de diretrizes para a aplicação da lei, a análise de infrações e a adoção de medidas educativas para incentivar boas práticas de proteção de dados nas organizações (BRASIL, 2018).

Além disso, o capítulo define as sanções administrativas que podem ser aplicadas pela ANPD em caso de infrações, como advertências, multas simples ou diárias, publicização da infração e até a suspensão ou proibição do tratamento de dados. As penalidades visam ser

proporcionais à gravidade da violação, considerando fatores como reincidência, cooperação do infrator e o impacto causado aos titulares dos dados. Dessa forma, o Capítulo 8 busca garantir um equilíbrio entre a punição e a educação dos agentes de tratamento, fortalecendo a governança e a cultura de proteção de dados no Brasil.

Em seu penúltimo capítulo, a LGPD trata da ANPD, órgão responsável por zelar pela correta aplicação da lei e garantir a proteção dos dados pessoais no Brasil. A ANPD tem como função elaborar diretrizes, fiscalizar o cumprimento das normas e aplicar sanções em caso de infrações. Além disso, a autoridade promove orientações para agentes de tratamento, estimulando a adoção de boas práticas e fortalecendo a cultura de proteção de dados no país. A ANPD também desempenha um papel essencial na mediação de conflitos entre titulares e controladores, contribuindo para a solução de demandas relacionadas ao uso de dados pessoais (BRASIL, 2018).

Outro ponto relevante é a função normativa e consultiva da ANPD, que pode editar regulamentos específicos e interpretar as disposições da LGPD para garantir sua adequada aplicação. A autoridade também participa de cooperações internacionais, acompanhando as práticas globais e garantindo a compatibilidade do Brasil com normas de outros países. Com isso, a atuação da ANPD não se limita à fiscalização, mas busca educar e orientar tanto as organizações quanto os titulares, promovendo um ambiente de confiança e segurança nas relações que envolvem o tratamento de dados pessoais.

No último capítulo, capítulo 10, a LGPD dispõe sobre o tratamento de dados pessoais pelo poder público, estabelecendo que órgãos e entidades da administração pública podem utilizar dados pessoais para o cumprimento de suas competências legais e políticas públicas previstas em lei. No entanto, a utilização desses dados deve respeitar os princípios da finalidade, necessidade e transparência, garantindo que o uso seja limitado aos propósitos específicos definidos. A transferência de dados entre órgãos públicos é permitida desde que seja justificada por finalidades claras de execução de políticas públicas ou cumprimento de obrigações legais, e o titular deve ser informado sobre esses compartilhamentos quando necessário (BRASIL, 2018).

Além disso, o capítulo estabelece que os órgãos públicos devem adotar medidas de segurança e governança, alinhando-se aos padrões exigidos pela LGPD para proteger os dados pessoais tratados. A responsabilidade pelas informações também implica a transparência ativa: os entes públicos precisam disponibilizar ao público, de forma clara e acessível, as bases legais e finalidades do tratamento de dados. Em casos de eventual compartilhamento com entes privados, isso só poderá ocorrer para atender exigências legais ou em situações

específicas previstas em políticas públicas, sempre com a supervisão da ANPD. Dessa forma, o Capítulo 10 visa equilibrar o uso legítimo de dados pelo Estado com a proteção da privacidade dos cidadãos.

A LGPD tem um impacto significativo sobre as empresas que tratam dados pessoais, exigindo que essas organizações adotem práticas rigorosas de proteção e governança de dados. As empresas devem identificar as bases legais que justificam o tratamento de dados, obter o consentimento adequado dos titulares e garantir a transparência sobre como as informações são coletadas, utilizadas e compartilhadas. Isso implica na necessidade de revisar políticas internas, implementar protocolos de segurança e criar um ambiente de conformidade, além de treinar colaboradores sobre as melhores práticas em proteção de dados. A não conformidade pode resultar em sanções financeiras e danos à reputação, tornando essencial que as empresas compreendam suas responsabilidades e obrigações sob a LGPD.

4 A LEI GERAL DE PROTEÇÃO DE DADOS NO CONTEXTO DAS EMPRESAS PRIVADAS

A sociedade de consumo se caracteriza pelo incentivo ao consumo em massa, impulsionado pela publicidade e pela busca por status e satisfação imediata. Nesse contexto, as empresas coletam e utilizam dados pessoais para personalizar ofertas e direcionar campanhas, aumentando a eficiência das vendas. No entanto, essa prática levanta preocupações sobre a privacidade dos indivíduos e o uso ético de suas informações. A proteção de dados surge, então, como uma resposta necessária para garantir que os direitos dos consumidores sejam preservados. Leis como a LGPD no Brasil e a GDPR na Europa buscam regulamentar a coleta, armazenamento e processamento de dados. A transparência e o consentimento tornam-se essenciais para evitar abusos e garantir que as pessoas tenham controle sobre suas informações. Assim, a proteção de dados é fundamental para equilibrar interesses econômicos e direitos individuais na era digital.

O capitalismo não entregou os bens às pessoas; as pessoas foram crescentemente entregues aos bens; o que significa que o próprio caráter e sensibilidade das pessoas foi reelaborado, reformulado, de forma tal que elas se agrupam aproximadamente com as mercadorias, experiências e sensações, cuja venda é o que dá forma e significado a suas vidas (SEABROOK, 1988, p.183).

Dessa forma, a proteção de dados tornou-se um tema central na era digital, especialmente diante do aumento exponencial do compartilhamento de informações pessoais e do uso dessas para fins comerciais e governamentais. Em resposta, diversas nações criaram legislações específicas para regulamentar como dados pessoais podem ser coletados, processados e armazenados. Entre as mais conhecidas está o GDPR da União Europeia, que estabelece padrões rígidos e impõe multas elevadas em casos de violação. Nos Estados Unidos, a regulação é mais fragmentada, com leis estaduais como a CCPA da Califórnia liderando a proteção local, enquanto outros países buscam alinhar suas próprias normas à tendência global.

A harmonização de legislações é um desafio, uma vez que diferentes países têm abordagens diversas sobre privacidade e liberdade de informação. No entanto, leis como a LGPD no Brasil e a PDPB na Índia mostram como economias emergentes também estão avançando nesse campo. Em nível internacional, organizações como a ONU e a OCDE discutem princípios comuns para garantir que a transferência de dados entre fronteiras ocorra de forma segura e ética. A busca por uma proteção global reflete a necessidade de preservar os direitos dos indivíduos, ao mesmo tempo, em que se permite o desenvolvimento econômico e a inovação tecnológica, que dependem da circulação de dados.

O consentimento do consumidor é um dos pilares fundamentais da proteção de dados, garantindo que as empresas só utilizem informações pessoais com a autorização explícita do titular. Esse processo envolve a transparência, ou seja, a organização deve informar de forma clara quais dados serão coletados, para que finalidade e por quanto tempo serão armazenados. Além disso, o consumidor deve ter liberdade para aceitar ou recusar o uso dos seus dados, sem sofrer prejuízos ou coerção. Regulamentações como a LGPD no Brasil e o GDPR na Europa reforçam a necessidade de consentimento livre, informado e específico para cada tipo de tratamento de dados.

No entanto, o consentimento não deve ser visto como um processo estático. O consumidor tem o direito de revogar essa autorização a qualquer momento, assim como de solicitar a exclusão de seus dados, garantindo maior controle sobre suas informações. Empresas que agem de forma ética buscam ir além do cumprimento mínimo da lei, oferecendo aos usuários meios práticos e simples para gerenciar suas preferências. Dessa forma, o consentimento torna-se uma ferramenta essencial para construir confiança, reforçando a relação entre consumidores e empresas em um ambiente digital cada vez mais dinâmico e interconectado.

Miragem observa em seu artigo que o objetivo da LGPD é fornecer ao consumidor uma proteção da personalidade.

A edição e plena eficácia da Lei Geral de Proteção de Dados eleva o direito brasileiro a um novo estágio de proteção da personalidade, considerando as transformações operadas pelas novas tecnologias da informação e da internet, que abrangem praticamente todas as dimensões da vida em sociedade. No âmbito das relações de consumo, sua repercussão deve ser tomada sempre de modo a assegurar a efetividade dos direitos do consumidor (Miragem, 2020)

A LGPD e o CDC são legislações complementares no Brasil, ambas voltadas à proteção dos direitos dos cidadãos, especialmente no contexto de relações de consumo. A LGPD, que entrou em vigor em 2020, regula a coleta, o armazenamento e o tratamento de dados pessoais, estabelecendo que qualquer operação envolvendo essas informações deve ser feita com base em princípios como transparência, segurança e consentimento do titular. Por sua vez, o CDC, vigente desde 1990, busca equilibrar as relações entre consumidores e empresas, assegurando direitos como informação clara sobre produtos e serviços, além da proteção contra práticas abusivas.

A integração entre a LGPD e o CDC fortalece a segurança dos consumidores, já que ambos exigem transparência nas operações comerciais e responsabilidade das empresas. Com a LGPD, os consumidores passam a ter maior controle sobre seus dados, podendo consultar como suas informações são utilizadas, solicitar alterações e até a exclusão desses dados. Essa proteção se alinha ao direito à informação previsto pelo CDC, que garante que o consumidor deve ser informado de maneira clara e objetiva sobre qualquer produto ou serviço, o que inclui a forma como seus dados pessoais são tratados pelas empresas. (Miragem, 2020).

Dessa forma, tanto a LGPD quanto o CDC não apenas protegem os consumidores contra abusos, mas também incentivam boas práticas por parte das empresas, promovendo confiança e responsabilidade nas relações de consumo. Empresas que desrespeitam essas normas estão sujeitas a sanções severas, como multas e outras penalidades administrativas. Assim, o alinhamento entre as duas legislações promove um mercado mais justo e equilibrado, no qual o respeito aos direitos do consumidor é fundamental para o desenvolvimento sustentável e ético dos negócios.

O uso da tecnologia é uma poderosa aliada para que o empresário fidelize seus consumidores, desde que seja utilizado de forma ética e conforme a LGPD. Ferramentas como Customer Relationship Management (CRM) permitem personalizar o atendimento,

registrando as preferências e o histórico de compras dos clientes, o que possibilita oferecer produtos e serviços mais alinhados às necessidades deles. No entanto, para que essa personalização respeite a LGPD, é essencial que o consumidor dê consentimento claro para a coleta e o uso desses dados, além de ser informado sobre a finalidade e o período de retenção das informações. (Miragem, 2020).

A ANPD desempenha um papel essencial na regulação e fiscalização das atividades de tratamento de dados pessoais realizadas por empresas privadas no Brasil. Sua principal função é garantir que essas organizações cumpram os princípios e exigências da LGPD, promovendo a privacidade e a proteção dos direitos dos titulares de dados. A ANPD estabelece diretrizes e normas complementares, orientando as empresas sobre como implementar boas práticas de governança e segurança da informação, além de fomentar a conscientização pública sobre a importância da proteção de dados (Miragem, 2020).

Além da função educativa, a ANPD tem poder fiscalizador e pode aplicar sanções administrativas, como advertências e multas, em casos de descumprimento da LGPD. Essas penalidades incentivam as empresas a adotarem mecanismos preventivos, como programas de *compliance* e o mapeamento de dados, para evitar irregularidades e minimizar riscos. A ANPD também atua em processos de mediação entre empresas e consumidores, buscando solucionar conflitos relacionados ao uso indevido de informações pessoais, o que ajuda a manter a confiança nas relações comerciais e a estabilidade do mercado.

A atuação da ANPD é fundamental para equilibrar inovação e privacidade, garantindo que as empresas privadas possam utilizar dados para desenvolver soluções e estratégias de negócio sem comprometer os direitos dos consumidores. Ao exigir transparência e responsabilidade, a ANPD promove um ambiente mais seguro para o crescimento econômico e incentiva o desenvolvimento de tecnologias que respeitem a privacidade desde a concepção (*privacy by design*). Dessa forma, a autoridade cumpre seu papel não apenas como reguladora, mas também como facilitadora de um mercado mais ético e sustentável na era digital.

A LGPD estabelece uma série de penalidades para empresas que descumprirem suas normas, especialmente em casos de vazamento de dados pessoais. Entre as sanções previstas estão advertências formais, exigindo que a empresa adote medidas corretivas em prazos estabelecidos, e multas que podem chegar a 2% do faturamento da organização, limitadas a R\$ 50 milhões por infração. Além disso, a LGPD permite a suspensão parcial ou total das atividades de tratamento de dados, bem como a proibição de realizar tais operações até que a empresa se adeque às exigências legais. Essas penalidades são aplicadas pela ANPD, levando

em consideração a gravidade da infração, o grau de dano aos titulares e o histórico de compliance da empresa (Miragem, 2020).

As empresas privadas também sofrem com o vazamento dos seus dados, assim a segurança dos dados armazenados pelas empresas dentro de sistemas governamentais é uma preocupação central para garantir a conformidade com a LGPD. Quando empresas precisam compartilhar informações com órgãos públicos, seja para cumprir obrigações legais, fiscais ou regulamentares, é essencial que o tratamento desses dados observe rigorosamente os princípios de segurança e minimização. A LGPD exige que tanto empresas quanto instituições governamentais adotem medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, vazamentos, alterações indevidas e outros riscos que possam comprometer a privacidade dos titulares.

A responsabilidade pela proteção dos dados é compartilhada entre as partes envolvidas. As empresas devem garantir que apenas informações estritamente necessárias sejam enviadas para os sistemas governamentais, respeitando a finalidade específica para a qual foram solicitadas. Da mesma forma, os órgãos públicos precisam implementar protocolos de segurança robustos, como criptografia, controle de acesso e auditorias regulares, para assegurar a integridade e a confidencialidade dos dados recebidos.

Caso ocorra um incidente de segurança, tanto a empresa quanto o governo devem agir rapidamente, comunicando a ANPD e os titulares afetados, além de tomar medidas corretivas para mitigar os danos. Assim, a cooperação entre empresas e sistemas governamentais, aliada à observância da LGPD, é essencial para garantir uma gestão de dados eficiente e segura no interesse da sociedade.

O respeito à LGPD é essencial para que as empresas garantam a proteção dos dados pessoais de seus clientes, colaboradores e parceiros, promovendo uma relação de confiança no mercado. A lei estabelece regras claras sobre a coleta, armazenamento e tratamento de informações pessoais, exigindo que as organizações adotem práticas transparentes e seguras. Ao cumprir essas diretrizes, as empresas não apenas evitam sanções e multas, mas também demonstram compromisso com a privacidade e o respeito aos direitos dos titulares, o que é cada vez mais valorizado pelos consumidores.

Além de atender a uma obrigação legal, o respeito à LGPD traz benefícios estratégicos para a competitividade da empresa. Em um mercado cada vez mais digital, organizações que investem em segurança da informação e governança de dados se destacam, atraindo clientes que priorizam transparência e privacidade. A adoção de boas práticas, como obter consentimento informado e oferecer aos consumidores controle sobre seus dados, fortalece a

reputação da marca e reduz os riscos de incidentes de segurança, como vazamentos de dados, que podem prejudicar a imagem e a sustentabilidade do negócio.

Respeitar a LGPD também incentiva a inovação responsável, permitindo que as empresas utilizem dados de forma ética para desenvolver produtos e serviços personalizados, sem comprometer a privacidade. Esse alinhamento entre crescimento econômico e proteção de dados é fundamental para consolidar um ambiente de negócios mais seguro e confiável. Assim, além de cumprir suas responsabilidades legais, as organizações que respeitam a LGPD contribuem para a construção de um mercado mais ético e sustentável, onde a confiança é um diferencial competitivo crucial.

Para realizar a implementação da LGPD nas empresas, é necessário a criação de um plano de adequação à LGPD, é importante porque ajuda a garantir que a empresa esteja segundo os requisitos legais e minimize riscos.

A LGPD pretende proteger a privacidade e os direitos fundamentais das pessoas, e a criação de um plano de adequação pode ajudar a aumentar a confiança dos clientes, construir relacionamentos mais duradouros, evitar ou reduzir multas, diminuir o risco de danos à reputação, melhorar a governança corporativa e otimizar custos.

Para criar um plano de adequação, é importante fazer um diagnóstico completo dos processos da empresa. Cada organização tem suas próprias necessidades e ritmo, e não há um caminho único para a conformidade. A LGPD é construída sobre três pilares: Pessoas, Processos e Tecnologia. Extraído dos capítulos II, III e IV, da Lei 13.709, de 14 de agosto de 2018, combinado com as melhores práticas de adequação à LGPD no Brasil, as empresas devem apresentar um modelo de Plano de Adequação, nele, deve haver um passo a passo de como a LGPD será implementada na empresa, essas ações envolvem decisões administrativas pertinentes a cada ramo de atuação, apresentamos cinco importantes ações:

- 1) Criar um Grupo de Trabalho; realizar estudo da Lei e Capacitação;
- 2) Criar comitê de acompanhamento das ações da LGPD.
- 3) Definir o Encarregado pelo Tratamento de Dados Pessoais e Suplente;
- 4) Mapeamento do Ciclo de Vida dos Dados Pessoais tratados.
- 5) Analisar o Mapeamento dos Dados Pessoais, coletando menos dados possíveis dos clientes internos e externos.

5 CONSIDERAÇÕES FINAIS

Diante do exposto, é possível afirmar que a LGPD representa um marco regulatório essencial para garantir a privacidade e a segurança dos dados pessoais no Brasil, alinhando o país às tendências globais de proteção da informação. Ao longo desta pesquisa, foi possível identificar a importância da legislação tanto para as organizações, que precisam adaptar seus processos internos e fortalecer a governança, quanto para os titulares de dados, que ganham maior controle sobre suas informações.

Contudo, o desafio não se limita ao cumprimento formal da norma, mas envolve a criação de uma cultura de proteção de dados, exigindo capacitação contínua, investimentos em tecnologia e conscientização de todos os envolvidos. Assim, conclui-se que a LGPD é não apenas um requisito legal, mas uma oportunidade estratégica para as empresas reforçarem a confiança de clientes e parceiros, promovendo uma atuação ética e responsável no uso de dados pessoais.

A implementação da LGPD nas empresas privadas representa um desafio significativo, mas também uma oportunidade estratégica para reforçar a confiança do mercado. A necessidade de adaptar processos, revisar políticas internas e investir em segurança da informação exige esforços financeiros e organizacionais, mas resulta em maior transparência e eficiência na gestão dos dados.

A pesquisa mostra que a implementação da governança de dados conforme a LGPD nas empresas privadas é essencial para assegurar uma gestão eficiente e segura das informações, promovendo não apenas o cumprimento legal, mas também a criação de valor estratégico. Ao estabelecer processos claros para a coleta, armazenamento, uso e compartilhamento de dados, a governança orientada pela LGPD fortalece a transparência e a confiança dos clientes e parceiros.

Além disso, ela facilita a mitigação de riscos relacionados a incidentes de segurança e sanções legais, incentivando uma cultura organizacional mais ética e comprometida com a privacidade. Dessa forma, as empresas que investem em governança de dados não apenas se protegem contra riscos regulatórios, mas também se posicionam de forma competitiva em um mercado cada vez mais exigente e orientado à proteção de dados pessoais.

Outro fator importante que a pesquisa mostra é que a LGPD influencia profundamente a rotina organizacional das empresas privadas, exigindo uma reestruturação nos processos internos relacionados ao tratamento de dados pessoais. A adequação à lei envolve desde a

criação de políticas e procedimentos específicos até a capacitação contínua de colaboradores e a implementação de tecnologias para garantir a segurança da informação.

Um aspecto bastante positivo pesquisado é que a implementação da LGPD nas empresas privadas gera impactos econômicos significativos, tanto em termos de custos quanto de oportunidades. Inicialmente, as organizações precisam investir em adequação, incluindo auditorias, consultorias jurídicas, treinamentos, contratação de profissionais especializados, e aquisição de tecnologias de segurança e monitoramento. Esses custos podem ser desafiadores, especialmente para pequenas e médias empresas.

No entanto, a conformidade também abre oportunidades econômicas, fortalecendo a confiança de clientes e parceiros, e permitindo que as empresas se diferenciem em mercados que valorizam a proteção de dados. Além disso, a prevenção de multas e prejuízos por vazamentos de dados reduz riscos financeiros a longo prazo. Assim, embora a adaptação demande recursos, a implementação adequada da LGPD pode se tornar um diferencial competitivo, trazendo retorno por meio da fidelização de clientes e da construção de uma imagem sólida e ética no mercado.

Um fator surpreendente em relação à implementação da LGPD foi saber que ela gera um impacto direto e significativo na reputação das empresas privadas, influenciando a percepção do mercado, consumidores e parceiros. Organizações que demonstram comprometimento com a proteção de dados fortalecem sua imagem institucional, conquistando a confiança de stakeholders e destacando-se pela transparência e responsabilidade.

Por outro lado, falhas no cumprimento da legislação, como vazamentos ou uso indevido de informações, podem gerar danos reputacionais graves, além de sanções legais e perda de clientes. Assim, a conformidade com a LGPD não apenas evita riscos regulatórios, mas também se torna um diferencial competitivo, posicionando a empresa como ética e preparada para os desafios do mercado digital. Dessa forma, investir em privacidade e segurança deixa de ser apenas uma exigência legal e se transforma em um fator estratégico para a construção e manutenção de uma reputação sólida e confiável.

Por fim, é possível afirmar que a implementação da LGPD traz diversos aspectos positivos para as empresas privadas, indo além da simples conformidade legal. Entre os benefícios, destaca-se o fortalecimento da governança de dados, que promove maior eficiência na gestão das informações e otimiza processos internos. A transparência nas operações e o respeito aos direitos dos titulares contribuem para o aumento da confiança de clientes e parceiros, melhorando a reputação da empresa no mercado. Além disso, a adoção de

práticas de segurança robustas reduz o risco de vazamentos e fraudes, evitando custos com penalidades e crises de imagem.

REFERÊNCIAS

ABES. **ABES anuncia ferramenta sobre a LGPD e parceria para redução do lixo eletrônico durante conferência.** 2019.

BEZERRA, Maria Ruth Borges. **Autoridade nacional de proteção de dados pessoais: a importância do modelo institucional independente para a efetividade da lei.** Caderno Virtual, v. 2, n. 44, p.1-95, 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Editora Forense, 2019.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obla-den de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação.** Rio de Janeiro: Lumen Juris, 2018.

BRANCO, Sérgio. As hipóteses de aplicação da LGPD e as definições legais. *In*: MULHOLLAN, Caitlin (org). **A LGPD e o novo marco normativo no Brasil.** São Paulo: Editora Arquipélago, 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. **Lei n.º 8.078, de 11 de setembro de 1990.** Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 1990.

BRASIL. **Lei n.º 9.279, de 14 de maio de 1996.** Regula direitos e obrigações relativos à propriedade industrial. Brasília, 1996.

BRASIL. **Lei n.º 9.610, de 19 de fevereiro de 1998.** Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília, 1998.

BRASIL. **Lei n.º 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. Brasília, 2011.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018.

BRASIL. **Decreto n.º 9.936, de 24 de julho de 2019.** Regulamenta a Lei n.º 12.414, de 9 de

junho de 2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, 2019.

CHOO, Chun Wei. **A organização do conhecimento**: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. São Paulo: Ed. SENAC São Paulo, 2003.

DATASEBRAE. **Painel de empresas**. 2020. Disponível em: <https://datasebrae.com.br/totaldeempresas/>. Acesso em: 21 ago. 2020.

DERBLI, Ludimila Santos. O transplante jurídico do regulamento geral de proteção de dados da União Europeia (“GDPR”) para o direito brasileiro. *E-legis*, n. 30, p. 181- 193, 2019.

DE SORDI, José Osvaldo. **Administração da informação**: fundamentos e práticas para uma nova gestão do conhecimento. 2. ed. São Paulo: Saraiva, 2015.

DE SORDI, José Osvaldo. **Desenvolvimento de projeto de pesquisa**. São Paulo: Saraiva, 2017a.

DE SORDI, José Osvaldo. **Gestão por processos**: uma abordagem da moderna administração. São Paulo: Saraiva, 2017b.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, 2011.

LEI GERAL DE PROTEÇÃO DE DADOS. **Guia de boas práticas para implementação na administração pública federal**. 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>.

LANGEN, Jeane Firmo; SILVA, Glessia. Desafios para inovar na micro e pequena empresa. **Revista da Micro e Pequena Empresa**, v. 13, n. 2, p. 85-97, 2019.

MACHADO, H. P. V. CONFIGURAÇÃO DE ESTUDOS SOBRE GESTÃO DO CONHECIMENTO EM PEQUENAS EMPRESAS NO BRASIL. **Perspectivas Em Gestão & Conhecimento**, Ano 8, v.3, 209-227, 2018.

MEDEIROS, Lílían O. *et al.* Avaliação da maturidade em gestão de dados das empresas de Uberlândia e região. **e-Rac**, v. 3, n. 1, p.1-17, 2013.

MENEZES, Cassio Roberto Conceição de; OLAVE, Maria Elena Leon. Práticas de gestão do conhecimento em micro e pequenas empresas de Sergipe. **Gestão & Regionalidade**, v. 32, n. 94, p. 4-19, 2016.

MINISTÉRIO PÚBLICO FEDERAL. **Levantamento sobre a lei geral de proteção de dados (LGPD) no MPF**. 2019.

MIRAGEM,. **A LEI GERAL DE PROTEÇÃO DE DADOS (LEI 13.709/2018) E O DIREITO DO CONSUMIDOR**. *Revista dos Tribunais*, Rio Grande do Sul , v. 1009, n. 1, 2019.

MIRAGEM,. **A LEI GERAL DE PROTEÇÃO DE DADOS (LEI 13.709/2018) E O DIREITO DO CONSUMIDOR**. Revista dos Tribunais, Rio Grande do Sul , v. 1010, n. 2, 2020.

MOLINA, Leticia Gorri; SANTOS, Juliana Cardoso dos. Gestão da informação e a 4ª Revolução Industrial. **AtoZ: novas práticas em informação e conhecimento**, v. 8, n. 2, p. 39-48, 2020.

MORAES, Alexandre F. **Segurança em redes: fundamentos**. São Paulo: Érica, 2020.

MOSIMANN, HORN & ADVOGADOS ASSOCIADOS. **Avalie a conformidade do seu negócio com a lei geral de proteção de dados (LGPD)**. 2019.

OLIVEIRA, Ana Paula de *et al.* A LGPD brasileira na prática empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, ano 4, n.1, p. 172-200, 2019.

PIURCOSKY, Fabrício Pelloso *et al.* A LGPD pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma de negócios**, v. 10, n. 23, p.89-99, 2019.

RAHUL, Kumar; BANYAL, Rohitash Kumar. Data life cycle management in big data analytics. **Procedia Computer Science**, v. 173, p. 364-371, 2020.

SILVEIRA, Marco Antonio (org.), Becaro, Taiane Cristiane. **Competitividade com qualidade de vida: O capital humano como fator de produção**. CTI, Campinas – SP, 2014.

SEABROOK, Jeremy. **The Leisure Society**. Oxford: Blackwell, 1988.