GOVERNANÇA DE DADOS:
impactos e ferramentas de conformidade com a GDPR

Regis Adriano Rodrigues[1]
Alexandre Gomes da Silva[2]

Resumo
Este artigo examina a relevância da proteção de dados pessoais na era digital, traçando a trajetória dessa proteção globalmente, desde a criação da Lei Geral de Proteção de Dados (LGPD) no Brasil até comparações com legislações internacionais. As ferramentas de proteção conforme a LGPD e os impactos e desafios que a lei enfrenta, abordando as perspectivas futuras da proteção de dados no Brasil. A pesquisa foi fundamentada em artigos e publicações online criteriosamente escolhidas por sua relevância. Essa abordagem permitiu identificar os principais aspectos da proteção de dados pessoais, revelando que é um assunto de grande importância, relacionado à garantia de direitos fundamentais, como o direito à privacidade e à liberdade de expressão. A proteção de dados pessoais é uma questão complexa e em constante transformação; embora a LGPD represente um marco significativo no Brasil, ainda há muitos desafios a serem superados para assegurar a proteção efetiva dos dados dos cidadãos.

Palavra-chave: Desafios. Ferramentas de proteção. Lei Geral de Proteção de Dados. Privacidade. Proteção de dados.

Abstract
This article examines the relevance of personal data protection in the digital era, tracing its global development from the creation of Brazil's General Data Protection Law (GDPL) to comparisons with international regulations. It exploits compliance tools under the GDPL, the challenges faced by the law, and future perspectives for data protection in Brazil. The research was based on carefully selected articles and online publications due to their relevance. This approach allowed the identification of key aspects of personal data protection, highlighting its importance in safeguarding fundamental rights such as privacy and freedom of expression. Personal data protection is a complex and evolving matter; although the GDPL marks a significant milestone in Brazil, many challenges remain to ensure the effective protection of citizens' data.

Keywords: *Challenges. Protection tools. General Data Protection Law. Privacy. Data protection.*

1 Introdução

[1] Graduando em Análise e Desenvolvimento de Sistemas pela Fatec Dr. Thomaz Novelino – Franca/SP. Endereço eletrônico: regisarodrigues@gmail.com
[2] Docente no curso de Análise e Desenvolvimento de Sistemas pela Fatec Dr. Thomaz Novelino – Franca/SP. Endereço eletrônico: alexandre.silva251@fatec.sp.gov.br

A crescente digitalização da sociedade e o volume massivo de dados pessoais coletados e processados por empresas e organizações têm gerado uma preocupação global em relação à privacidade e proteção de dados. Diante desse cenário, diversos países têm buscado regulamentar o tratamento de dados pessoais, com destaque para a União Europeia com o Regulamento Geral sobre a Proteção de Dados (GDPR) e o Brasil com a LGPD, Lei n.º 13.709/2018.

Inspirada no GDPR e em outras legislações internacionais, como a Lei de Privacidade do Consumidor da Califórnia (CCPA), a lei de proteção brasileira busca garantir os direitos fundamentais de liberdade e privacidade dos cidadãos, estabelecendo diretrizes para a coleta, processamento, armazenamento e descarte de dados pessoais. No entanto, a adequação à LGPD impõe desafios para as organizações, que precisam adaptar seus processos, tecnologias e cultura para garantir a conformidade com a lei.

Neste contexto, o presente artigo visa analisar a LGPD e as ferramentas de proteção de dados disponíveis para auxiliar as organizações no cumprimento da legislação. A pesquisa, de caráter bibliográfico, utiliza artigos científicos, leis e publicações online para traçar um panorama da proteção de dados no Brasil e no mundo, comparando a LGPD com legislações internacionais e explorando as funcionalidades e os benefícios das ferramentas de proteção de dados.

O artigo está estruturado em seções que abordam desde o contexto histórico e a evolução da proteção de dados até os desafios e as perspectivas futuras. Inicialmente, apresenta-se um breve histórico da proteção de dados no mundo, contextualizando a criação da LGPD no Brasil. Em seguida, são exploradas as definições, os princípios e as bases legais da lei, aprofundando a análise da legislação brasileira. A seção seguinte compara a lei de proteção de dado brasileira com o GDPR e a CCPA, destacando as semelhanças e diferenças entre as leis. Na sequência, são examinadas as ferramentas de proteção de dados disponíveis no mercado, com exemplos de soluções e seus impactos na adequação à LGPD. Por fim, são discutidos os desafios e as perspectivas da proteção de dados no Brasil, concluindo com considerações finais sobre a importância da LGPD e seu papel na construção de uma cultura de proteção de dados no país.

2 Lei Geral de Proteção de Dados Pessoais

A proteção de dados pessoais tornou-se uma questão crítica na era digital devido ao volume crescente de informações pessoais coletadas, armazenadas e processadas por empresas e organizações em todo o mundo. A privacidade é um direito fundamental, e a proteção de dados pessoais é essencial para garantir que os indivíduos mantenham controle sobre suas informações pessoais.

Na era digital, dados como nome, endereço, número de telefone, informações financeiras, histórico de navegação e dados de localização são frequentemente coletados sem medidas adequadas de proteção, ou seja, esses dados podem ser acessados e utilizados por terceiros de maneira indevida, resultando em riscos à segurança pessoal, como fraudes, roubos de identidade e outras formas de abuso (Martins, 2023).

A confiança é um ativo para qualquer organização, uma vez que empresas que demonstram um compromisso sólido com a proteção de dados pessoais são mais propensas a ganhar e manter a confiança de seus clientes. Incidentes de vazamento de dados podem ter consequências severas para a reputação de uma empresa, resultando em perda de clientes e impactos financeiros significativos (Martins, 2023).

Segundo Martins (2023) em um artigo publicado no site JusBrasil, legislações como a Lei Geral de Proteção de Dados no Brasil e o Regulamento Geral sobre a Proteção de Dados na União Europeia que impõem requisitos rigorosos para o tratamento de dados pessoais são leis projetadas para garantir que as organizações adotem práticas de proteção de dados robustas e a não conformidade pode resultar em multas substanciais, sanções administrativas e ações judiciais, destacando a importância de uma abordagem proativa para a proteção de dados.

Além disso, a coleta e o processamento inadequados de dados pessoais podem levar a abusos e discriminação, por exemplo, dados sensíveis relacionados a saúde, orientação sexual, ou crenças religiosas podem ser usados de maneira discriminatória se não forem devidamente protegidos e esses dados pessoais também está intrinsecamente ligado à segurança nacional e econômica, pois dados pessoais podem ser alvo de ataques cibernéticos que visam desestabilizar sistemas

críticos e roubar informações sensíveis e a proteção robusta de dados é essencial para proteger as infraestruturas nacionais e para assegurar que as economias possam operar de forma segura e eficiente na era digital (Martins, 2023).

A Lei n.º 13.709 que aborda sobre a LGPD foi sancionada em 14 de agosto de 2018 e entrou em vigor em setembro de 2020 e surgiu em um contexto de crescente preocupação global com a privacidade e a proteção de dados pessoais, motivada por avanços tecnológicos e o aumento exponencial na coleta e processamento de dados (SEBRAE, s.d.).

Similar ao Regulamento Geral sobre a Proteção de Dados da União Europeia, que entrou em vigor em maio de 2018, o GDPR estabeleceu padrões rigorosos para a proteção de dados pessoais e inspirou outros países a seguir um caminho semelhante e além do GDPR, outros marcos internacionais de proteção de dados, como a Lei de Privacidade do Consumidor da Califórnia, também assemelham- se a LGPD (Weiss, 2020).

Antes da LGPD, Weiss (2020) destaca que o Brasil não possuía uma legislação específica abrangente para a proteção de dados pessoais. A proteção de dados era tratada de maneira fragmentada em várias leis, tais como o Marco Civil da Internet (MCI), além de outros, e essa legislação aborda aspectos específicos da privacidade e proteção de dados, mas não forneciam um quadro unificado e robusto.

A principal motivação para a criação da LGPD foi a proteção dos direitos fundamentais de privacidade e liberdade dos cidadãos brasileiros. Em uma era onde os dados pessoais são coletados e compartilhados em larga escala, havia uma necessidade urgente de regulamentação para garantir que os indivíduos tivessem controle sobre suas informações pessoais e que essas informações fossem tratadas de maneira justa e transparente (SEBRAE, s.d.).

A LGPD também foi criada para harmonizar as práticas de proteção de dados do Brasil com os padrões internacionais, facilitando o comércio e o fluxo de dados entre o Brasil e outras nações, uma vez que, a conformidade com normas internacionais como o GDPR segundo Weiss (2022) é crucial para as empresas brasileiras que operam globalmente ou que desejam expandir seus negócios para o exterior. A adoção de uma legislação compatível com o GDPR ajuda a garantir que

as empresas brasileiras possam participar de maneira competitiva no mercado global.

O aumento de incidentes de segurança e escândalos de privacidade, como o caso do vazamento de dados do Facebook e Cambridge Analytica, reforçou a necessidade de uma legislação robusta para a proteção de dados no Brasil. Esses incidentes mostraram como a coleta e o uso inadequado de dados pessoais podem ter consequências graves para a privacidade e a segurança dos indivíduos (BBC, 2018).

2.1 Evolução da Proteção de Dados ao Redor do Mundo

A proteção de dados pessoais evoluiu significativamente ao longo das décadas à medida que a digitalização e a globalização aumentaram a coleta, o armazenamento e o processamento de dados. A preocupação com a privacidade e a proteção de dados começou a ganhar forma na década de 1970, quando os computadores começaram a ser usados para processar grandes volumes de dados pessoais (Assis e Mendes, 2019).

Monteiro et al. (2019) relatam que, em 1970, o estado de Hessen, na Alemanha, promulgou a primeira lei de proteção de dados do mundo, criando um precedente na legislação de privacidade. Em 1973, a Suécia introduziu a *Data Act*, primeira lei nacional sobre o tema, e, em 1981, a Convenção 108 do Conselho da Europa tornou-se o primeiro tratado internacional vinculativo sobre proteção de dados.

A Diretiva 95/46/EC do Parlamento Europeu e do Conselho, adotada em 1995, foi um marco importante na proteção de dados na Europa, pois estabeleceu um quadro legal para a proteção de dados pessoais dentro da União Europeia (UE) e harmonizar as legislações nacionais dos Estados-Membros, além de que a diretiva introduziu conceitos-chave, como o consentimento do titular dos dados e os direitos de acesso e retificação (Monteiro *et al.*, 2019).

O GDPR, que entrou em vigor em 25 de maio de 2018, substitui a Diretiva 95/46/EC e modernizou o quadro legal de proteção de dados na UE para a era digital O GDPR é amplamente considerado a legislação de proteção de dados mais

rigorosa e abrangente do mundo segundo (Monteiro *et al.*, 2019), e estabeleceu regras rigorosas para a proteção de dados pessoais.

A Lei de Privacidade do Consumidor da Califórnia ou *California Consumer Privacy Act* entrou em vigor em 1º de janeiro de 2020 e é uma das leis de privacidade de dados mais rigorosas dos Estados Unidos, visto que, concede aos residentes da Califórnia direitos significativos sobre seus dados pessoais, tais como, qualquer identificador que seja exclusivo para os consumidores, informações biométricas, informações comerciais relacionadas a bens ou serviços adquiridos, informações relacionadas ao emprego profissional entre outros.

2.2 A Origem da LGPD no Brasil

A criação da LGPD no Brasil foi motivada por uma combinação de fatores políticos, sociais e econômicos, visando proteger os direitos dos cidadãos, harmonizar a legislação brasileira com os padrões internacionais e promover a inovação e o desenvolvimento econômico, visto que, similar a GDPR e a CCPA, a LGPD estabelece um quadro legal robusto para a proteção de dados pessoais no Brasil, assegurando que as práticas de tratamento de dados sejam transparentes, seguras e conforme os direitos dos indivíduos (Quintiliano, 2021).

O Contexto Político e Social que Levou à Criação da LGPD, Lei n.º 13.709, de 14 de agosto de 2018, de acordo com Quintiliano (2021) foi estabelecido em um momento de crescente conscientização sobre a importância da privacidade e da proteção de dados pessoais, dado que, diversos fatores políticos e sociais contribuíram para a necessidade e a urgência de uma legislação abrangente de proteção de dados no Brasil.

A proteção de dados pessoais é vista como um facilitador para a inovação e o desenvolvimento econômico, um marco legal claro e robusto pode aumentar a confiança dos consumidores e das empresas, promovendo um ambiente mais seguro para o desenvolvimento de novas tecnologias e serviços digitais (Quintiliano, 2021).

Devido aos avanços tecnológicos, a rápida digitalização da economia e da sociedade brasileira aumentou significativamente a coleta, o processamento e o

armazenamento de dados pessoais por empresas e governos e a proliferação de dispositivos conectados, o uso extensivo da internet e o crescimento das redes sociais criaram vastas quantidades de dados pessoais, destacando a necessidade de um marco legal que regulamenta essas atividades segundo (Quintiliano, 2021).

O Brasil é um importante ator no cenário global e tem relações comerciais significativas com a União Europeia, os Estados Unidos e outros países que já possuíam legislações avançadas de proteção de dados, como o GDPR e o CCPA, além de que, Weiss (2022) destaca que a ausência de uma legislação nacional adequada dificultava a participação das empresas brasileiras no mercado internacional e a transferência de dados entre fronteiras.

A LGPD quanto o GDPR se baseiam em princípios fundamentais de proteção de dados, como transparência, finalidade específica, minimização de dados, precisão, integridade e confidencialidade. Ambas as legislações garantem direitos aos titulares dos dados, incluindo acesso, retificação, exclusão, portabilidade e oposição ao processamento de dados pessoais (Weiss, 2020).

A LGPD quanto o GDPR especificam várias bases legais para o processamento de dados pessoais, como consentimento, execução de contrato, o cumprimento de obrigação legal e interesse legítimo. O GDPR estabeleceu a criação de autoridades de proteção de dados em cada país da União Europeia, enquanto a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD) para supervisionar e regular a conformidade no Brasil, uma vez que, ambas as legislações preveem sanções severas por não conformidade com a lei (Adopt, 2022).

A LGPD e a CCPA têm escopos semelhantes no que diz respeito à proteção dos dados dos consumidores segundo a Adopt (2022), no entanto, a LGPD aplica-se a todas as organizações que processam dados pessoais no Brasil, independentemente do tamanho, enquanto a CCPA se aplica principalmente a grandes empresas que atendem a certos critérios de receita e volume de dados e ambos os regulamentos oferecem direitos aos consumidores, como o direito de saber quais dados estão sendo coletados, o direito de solicitar a exclusão e o direito de optar por não vender seus dados, além de que, a CCPA é mais focada na transparência e controle sobre a venda de dados pessoais e é aplicada

principalmente pelo procurador-geral da Califórnia e a LGPD estabelece uma autoridade nacional para supervisão.

2.3 Definições e Princípios Fundamentais da LGPD

A LGPD estabelece um conjunto claro de definições e princípios que orientam o tratamento de dados pessoais no Brasil e essas diretrizes garantem que os dados pessoais sejam tratados de maneira ética, segura e transparente, protegendo os direitos dos titulares e promovendo a confiança nas práticas de tratamento de dados, ou seja, as definições mais importantes da Lei n.º 13.709/2018 segundo o (SEBRAE, s.d.) são:

- Os dados pessoais devem abranger qualquer informação que possa levar à identificação de uma pessoa física, seja de forma direta (nome, e-mail, telefone, RG, CPF, endereço) ou indireta (endereços de IP, geolocalização, etc.), dado que essas informações permitem traçar o perfil e monitorar o comportamento de um indivíduo, e por isso, qualquer dado que possibilite essa identificação específica é classificado como dado pessoal.
- Os dados sensíveis são informações pessoais que revelam aspectos íntimos e vulneráveis de um indivíduo, como origem racial, religião, opiniões políticas, saúde, vida sexual, genética e biometria. Devido à sua natureza delicada, esses dados exigem um cuidado especial e só podem ser tratados com o consentimento explícito da pessoa a quem pertencem.
- Os dados Anonimizados ou Anônimos são dados referentes a um titular que não permitem sua identificação, levando em conta os meios técnicos razoáveis e disponíveis no momento do tratamento, ou seja, esses dados perdem a possibilidade de serem associados, direta ou indiretamente, a uma pessoa. Como resultado, eles não estão sujeitos às proteções da Lei Geral de Proteção de Dados. Um exemplo seria o uso de estatísticas que mostram a faixa etária de pessoas que compraram determinado produto, sem que seja possível identificar quem são essas pessoas.
- Semelhante aos dados anonimizados, os dados pseudo-anonimizados referem-se a um processo que impede a identificação direta ou indireta de um

indivíduo, no entanto, a reconexão desses dados à pessoa titular só é possível mediante o uso de informações adicionais, mantidas separadamente em um ambiente controlado e seguro pelo controlador. Esse método, que reduz os riscos, é incentivado pelo regulamento da LGPD e está sujeito às suas regras, como exemplo de um banco de dados que consiste em um conjunto estruturado de dados pessoais, podendo ser armazenado em meios físicos ou eletrônicos, como documentos guardados em nuvem.

2.4 Etapas do tratamento de dados na LGPD e Gestão do Ciclo de Vida dos Dados

A LGPD estabelece bases legais claras e específicas para o tratamento de dados pessoais, assegurando que tais práticas sejam realizadas de maneira legítima e transparente. Entender e classificar os dados corretamente é crucial para atender às exigências legais, implementando políticas, processos e programas eficazes para gerir a coleta, processamento, análise, armazenamento, compartilhamento, reutilização e descarte desses dados (Alves, s.d.).

No contexto atual, a incorporação da Gestão do Ciclo de Vida dos Dados nas operações de uma empresa deve ser alinhada com os objetivos e a natureza de seus produtos e serviços, ou seja, significa que o tratamento dos dados deve considerar desde a coleta até o descarte, assegurando que sejam geridos de maneira responsável e conforme a legislação, garantindo segurança e transparência durante todo o processo (Gatefy, 2021).

A figura 1 ilustra o ciclo de vida dos dados, desde a coleta até a eliminação, destacando a importância da LGPD em cada etapa, visto que garante que os dados pessoais sejam tratados de forma transparente e segura, protegendo os direitos dos titulares destacando a importância desse ciclo para empresas e indivíduos que lidam com dados pessoais.

Figura 1 - Ciclo de Vida dos Dados

Fonte: Página *Xpositum* Consultoria Empresarial.[3]

A figura 2 apresenta um comparativo entre o tratamento de dados pessoais antes e depois da implementação da LGPD. Fica evidente que a lei trouxe maior controle e transparência ao ciclo de vida dos dados, exigindo consentimento e finalidade específica para cada etapa, pois a lei garante que os direitos dos titulares sejam respeitados, promovendo um ambiente mais seguro e ético no uso de dados pessoais.

3 Disponível em: <https://xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd>. Acesso em: 20 ago. 2024

Figura 2 - Tratamento dos dados antes e depois da LGPD

CICLO DE VIDA DOS DADOS		
FASE DO CICLO	**ANTES DA LGPD**	**COM A LGPD**
Coleta	Os dados pessoais são coletados indiscriminadamente.	Os dados pessoais coletados devem obedecer ao princípio da necessidade e da finalidade.
Processamento	Os dados podem ser processados sem um tratamento específico.	O processamento de dados só poderá ser realizado se o tratamento estiver enquadrado no Art. 7º da LGPD.
Análise	A análise de dados é feita para entender o mercado, conhecer o perfil das pessoas e definir estratégias para oferecer bens e serviços para o público-alvo.	A análise de dados deve levar em consideração a finalidade da coleta. Devem ser obedecidos os princípios de tratamento, com propósito legítimo, específico e explicito.
Compartilhamento	Os dados pessoais são compartilhados sem a necessidade do consentimento de seus titulares.	O compartilhamento de dados deve ser consentido pelos seus titulares.
Armazenamento	Os dados pessoais são armazenados e mantidos por tempo indeterminado.	Os dados pessoais devem ser armazenados e mantidos por prazos definidos, ou seja, até que finalidade seja alcançada ou deixem de ser necessários ou pertinentes ao alcance da finalidade.
Reutilização	Os dados pessoais são reutilizados sem a necessidade de consentimento de seus titulares.	Um novo consentimento deve ser solicitado sempre que houver mudança de finalidade.
Eliminação	Os dados pessoais são mantidos sem a obrigatoriedade de serem eliminados.	Os dados pessoais devem ser eliminados após o término de seu tratamento.

Fonte: Página *Xpositum* Consultoria Empresarial.

No ciclo de vida dos dados pessoais, segundo Giarllarielli (s.d.) tudo começa com a coleta dos dados que é uma das mais importantes do ciclo de vida dos dados, após coletados, os dados são processados, ou seja, são organizados, classificados e utilizados para diversos fins e armazenados em servidores ou outros dispositivos de forma segura e protegida.

Os dados, de acordo com Giarllarielli (s.d.), podem ser compartilhados com terceiros, como parceiros comerciais ou órgãos governamentais, e após armazenados podem ser analisados para gerar *insights*, identificar tendências e auxiliar na tomada de decisões estratégicas, e podem ser reutilizados para novas finalidades, desde que haja consentimento do titular ou outra base legal que justifique o tratamento, sempre respeitando as normas da LGPD.

Por fim, quando os dados não são mais necessários ou o titular solicitar sua exclusão, eles devem ser eliminados de forma segura e definitiva Giarllarielli (s.d.).

Para garantir que todas essas etapas sejam executadas conforme a legislação, é fundamental que as organizações façam uso de ferramentas

específicas para proteção de dados. Tais ferramentas, que abrangem desde sistemas de gerenciamento de consentimento até soluções para anonimização, possibilitam que as empresas cumpram suas obrigações legais e salvaguardam os direitos dos titulares. E sobre essas ferramentas iremos abordar na próxima seção.

3 Ferramentas de Proteção de Dados em Conformidade com a LGPD

A LGPD estabelece diversas responsabilidades às organizações que realizam a coleta e o tratamento de dados pessoais. Para apoiar o cumprimento dessas obrigações, há uma variedade de ferramentas disponíveis baseadas nas diretrizes da Lei n.º 13.709/2018, abrangendo desde soluções para a gestão de consentimento e monitoramento de informações até plataformas voltadas para segurança e anonimização dos dados.

Esses sistemas permitem que as empresas mapeiem e classifiquem todos os dados pessoais coletados, processados e armazenados, organizando-os por nível de sensibilidade e identificando quem é responsável por seu tratamento, Iubenda (s.d.) também destaca que ao manter um inventário completo dos dados, as empresas podem detectar vulnerabilidades e implementar medidas de segurança mais eficazes, o que reduz significativamente o risco de vazamentos e outros incidentes de segurança, além disso, esses softwares automatizam a coleta e o registro do consentimento dos titulares de dados, assegurando que as empresas possuam evidências claras e válidas desse consentimento, um aspecto crucial para o cumprimento dos direitos dos titulares, como o acesso, a retificação, a exclusão e a portabilidade dos dados.

Softwares de Gestão da Privacidade são ferramentas indispensáveis para empresas que lidam com dados pessoais, especialmente no contexto da LGPD no Brasil, pois esses softwares desempenham um papel crucial na organização, proteção e gestão de dados, garantindo que as empresas cumpram as normas de privacidade e evitem sanções legais. Eles oferecem funcionalidades abrangentes, como mapeamento de dados, gestão de consentimento, registro de atividades de tratamento, gestão de incidentes de segurança, relatórios, análises e até treinamento e conscientização sobre privacidade (Iubenda, s.d.).

Os sistemas de gestão de privacidade ajudam as empresas a mapearem, classificar e organizar os dados pessoais conforme seu nível de sensibilidade, além de identificar os responsáveis por seu tratamento, pois as organizações conseguem detectar falhas e implementar medidas de segurança mais eficazes, diminuindo o risco de vazamentos e problemas de segurança. Iubenda (s.d.) destaca que eles também automatizam a coleta e registro de consentimento dos titulares de dados, assegurando provas válidas para atender direitos como acesso, correção e exclusão, reduzindo o risco de multas e sanções por descumprimento das leis. Eles organizam, protegem e gerenciam informações pessoais, garantindo conformidade com a legislação e suas funcionalidades incluem mapeamento de dados, controle de consentimento, registros de atividades, gestão de incidentes de segurança e até treinamento para conscientização sobre privacidade, uma vez que a adoção desses softwares é uma estratégia eficaz para assegurar proteção e evitar sanções legais (Iubenda, s.d.).

Esses sistemas também desempenham um papel fundamental na capacitação dos funcionários, fornecendo recursos que promovem a conscientização sobre a importância da proteção de dados e as melhores práticas de privacidade. Ao educar os colaboradores sobre os riscos e responsabilidades associados ao tratamento de dados, as empresas conseguem reduzir a probabilidade de erros humanos que podem resultar em violações de privacidade.

Um exemplo a ser citado é o caso da empresa British Airways, na qual, em setembro de 2018, ocorreu uma falha de segurança no site da companhia, resultando no vazamento de dados pessoais e financeiros de 500 mil clientes. De acordo com Higa (2019), o *Information Commissioner's Office* (ICO), órgão do Reino Unido responsável pela privacidade dos usuários, multou a companhia em 183,39 milhões de libras esterlinas por infringir o Regulamento Geral sobre a Proteção de Dados e o incidente envolveu o redirecionamento de tráfego para um site fraudulento, comprometendo informações sensíveis, ou seja, um software de gestão da privacidade poderia ter auxiliado na identificação e correção de vulnerabilidades nos sistemas, prevenindo o vazamento de dados (Higa, 2019).

3.1 Exemplos de Soluções Tecnológicas para Adequação à LGPD

Um sistema de gestão da privacidade é um *software* que centraliza diversas demandas, operações e atividades para cumprir os requisitos e boas práticas de privacidade, além das exigências regulatórias de proteção de dados.

Devido à complexidade das regulações e exigências, Costa (2023) ressalta que a gestão da privacidade abrange vários tópicos que orientam as principais funcionalidades das soluções. Esses tópicos devem ser abordados pelo Data Protection Officer de uma empresa e pelo *software* de gestão da privacidade, incluindo Gestão de Consentimento e Autorização, Direitos e Requisições dos Titulares de Dados (DSARs), Incidentes com Dados Pessoais, Mapeamento de Processos e Inventário de Dados, Gerenciamento de Políticas, Processos e Procedimentos, e Transparência e Acesso. O objetivo principal de um *software* de conformidade com a LGPD é garantir que os responsáveis pela privacidade em uma organização possam atender a esses tópicos com segurança, agilidade, automação e eficiência, em outras palavras, essas soluções são a maneira mais eficaz de cumprir as exigências regulatórias e as demandas dos titulares de dados (Costa, 2023).

Escolher o software adequado para a gestão da privacidade é uma etapa fundamental que auxilia as empresas na simplificação dos processos ligados à privacidade dos dados de seus usuários, ao mesmo tempo, em que garante a conformidade com diversas leis e regulamentos. A seguir, serão apresentados alguns exemplos, de acordo com Costa (2023), de sistemas utilizados para essa finalidade.

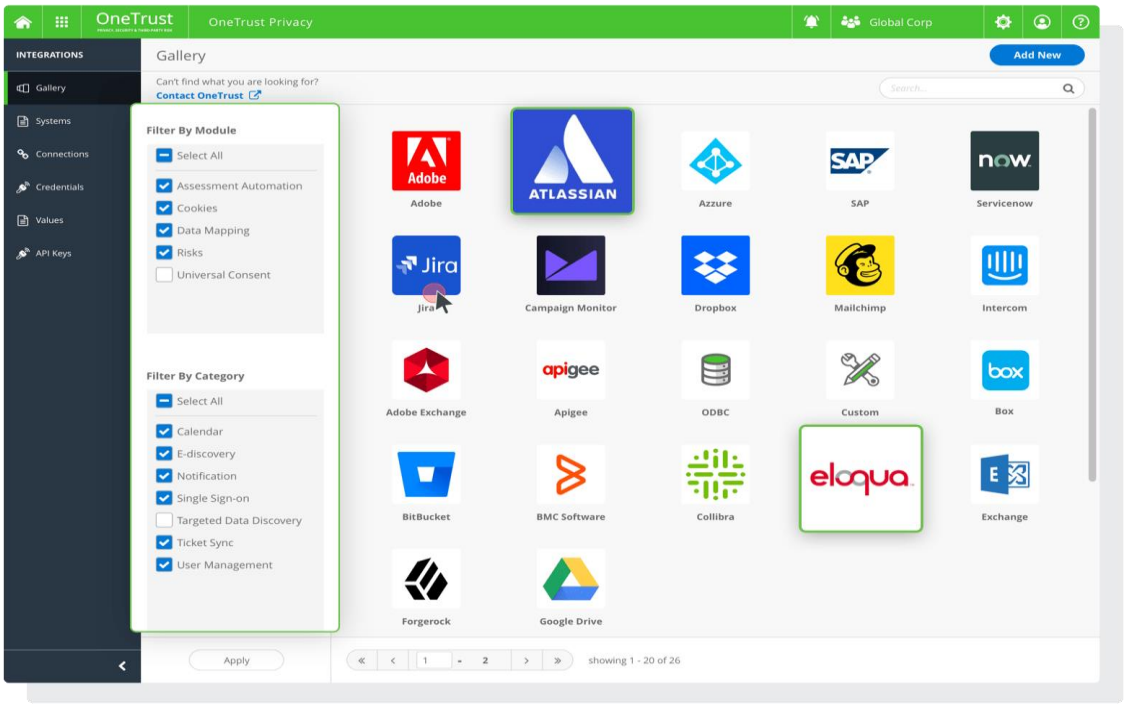
3.1.1 *OneTrust*

Segundo o *site* da *One Trust* (2024), a ferramenta opera por meio de uma plataforma abrangente e baseada na nuvem, projetada para ajudar as empresas a gerenciarem de maneira centralizada e eficiente seus programas de privacidade, segurança e governança de dados. Ela disponibiliza uma variedade de módulos e funcionalidades que se integram para cobrir todo o ciclo de vida dos dados, desde a coleta até o descarte, assegurando a conformidade com legislações como a LGPD e

a GDPR. A implementação geralmente ocorre via solução em nuvem, eliminando a necessidade de instalar *software* diretamente nos servidores da empresa.

Na figura 3, são exibidas funcionalidades como filtros para segmentar integrações por módulos (como *Cookies, Assessment* e *Data Mapping*) e por categorias (como Calendário, *E-discovery* e *Single Sign On*). Além disso, são apresentados ícones que representam várias plataformas e ferramentas que podem ser integradas ao *One Trust*, incluindo *Jira*, *Adobe*, *Atlassian* e SAP, entre outras. Essas integrações permitem que as empresas conectem a ferramenta a outras soluções já utilizadas, automatizando processos e centralizando o gerenciamento de dados, o que otimiza a gestão de privacidade e conformidade, tornando as operações mais ágeis e eficientes.

Figura 3 - Plataforma do software *OneTrust*



Fonte: Página *OneTrust*[4]

3.1.2 *Tee Global*

4 Disponível em: <https://dbmstools.com/tools/onetrustt>. Acesso em: 19 set. 2024

Segundo Costa (2023), a *Tee Global* é uma *regtech* brasileira com sede em Campinas–SP e tem clientes espalhados por todo o país. Reconhecida como um dos principais nomes no mercado nacional de *softwares* voltados para privacidade e conformidade com a LGPD, a empresa foi fundada em 2022 com a proposta de oferecer uma solução eficiente e direcionada. Além disso, destaca-se por sua fácil implementação e modelo *plug-and-play*, que dispensa conhecimentos de programação. A *startup* foca em eliminar funcionalidades desnecessárias, tornando o sistema simples, intuitivo e rápido, pois utiliza uma metodologia própria com automação e integração via *Application Programming Interface* (*API)*, o que, segundo a empresa, pode reduzir o tempo investido em atividades relacionadas à proteção de dados e privacidade.

3.1.3 *IBM Guardium*

O IBM Guardium, conforme o *site* da *IBM* (2024)*,* é uma poderosa solução de *software* de segurança de dados que ajuda as empresas a protegerem seus dados sensíveis, independentemente de estarem armazenados em ambientes locais ou na nuvem. Ele oferece uma combinação abrangente de funcionalidades que incluem descoberta, monitoramento, proteção e controle de acesso a dados, garantindo a conformidade com regulamentações como a LGPD e o GDPR.

Um dos principais recursos do *IBM Guardium* é a prevenção de vazamentos de dados e o controle de acesso não autorizado. A solução monitora constantemente as atividades de acesso e manipulação de dados em tempo real, permitindo a identificação de comportamentos suspeitos e possíveis violações de segurança antes que causem danos significativos. O controle de acesso detalhado permite que as empresas definam permissões detalhadas para diferentes usuários e grupos, assegurando que apenas pessoas autorizadas tenham acesso a dados sensíveis. Além disso, o *Guardium* oferece mascaramento de dados, ofuscando ou substituindo dados sensíveis por valores fictícios, o que protege a privacidade dos indivíduos em ambientes de desenvolvimento e teste. A criptografia de dados, por sua vez, garante que os dados sejam inelegíveis para pessoas não autorizadas,

mesmo em caso de vazamento, ao criptografar os dados tanto em repouso quanto em trânsito.

3.1.4 *CookieYes*

CookieYes é uma ferramenta de conformidade de *cookies* projetada para ajudar *websites* a cumprir regulamentações de proteção de dados, como a LGPD no Brasil, o GDPR na Europa e a CCPA nos Estados Unidos, conforme o Site *CookiYes* a principal função do *software* é permitir que os proprietários de *sites* obtenham o consentimento explícito dos visitantes para o uso de *cookies*, que são pequenos arquivos de texto armazenados no navegador do usuário e que podem conter informações sobre suas preferências, comportamento de navegação e outras atividades *online*.

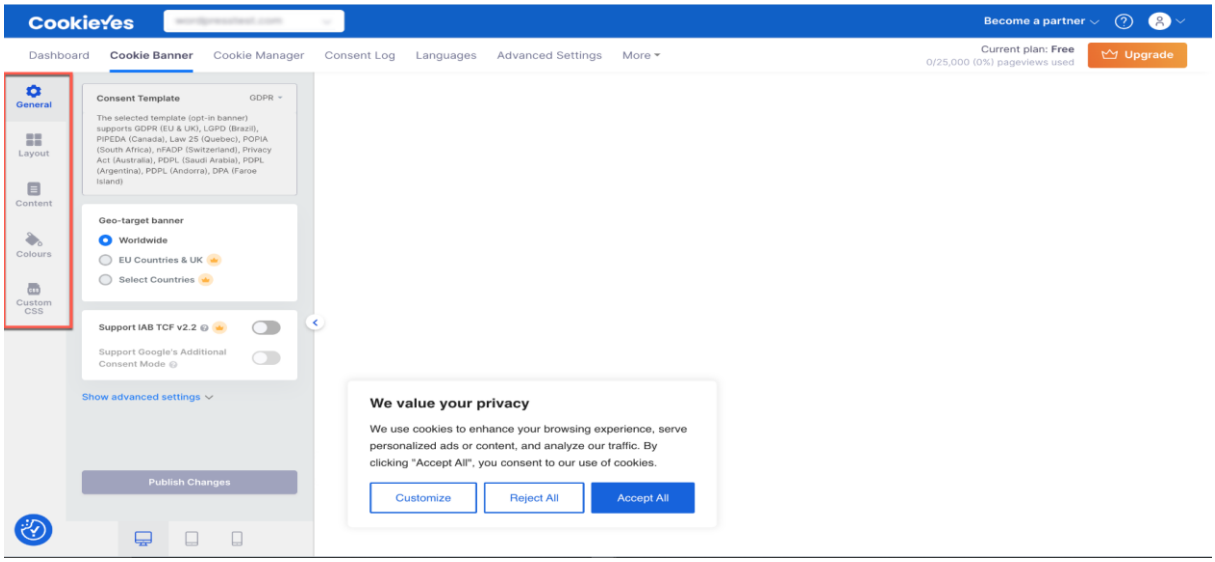
Quando um usuário acessa um site que utiliza *CookieYes*, um *banner* de consentimento de *cookies* é automaticamente exibido. Este *banner* informa o usuário sobre o uso de *cookies* no *site* e solicitar seu consentimento para armazenar esses *cookies* em seu dispositivo. O *banner* pode ser personalizado para se adequar ao *design* do *site* e às regulamentações específicas que o *site* precisa cumprir. O usuário tem a opção de aceitar ou rejeitar os *cookies*, ou de escolher quais tipos de *cookies* permitir, que geralmente são categorizados como essenciais, de desempenho, de funcionalidade e de publicidade. *CookieYes* permite que os usuários personalizem suas preferências de *cookies*, garantindo que apenas os *cookies* selecionados sejam ativados.

Podemos observar na figura 4, a interface de configuração de um *banner* de *cookies* na plataforma *Cookieyes*, que auxilia *sites* a se adequarem às leis de privacidade como a LGPD e a GDPR. Entre as funcionalidades exibidas, destaca-se o recurso de *geo-targeting*[5], que permite segmentar o *banner* conforme a localização, com opções como "*Worldwide*" e *"Europe (EU) Countries & United Kingdom (UK)*", além da possibilidade de selecionar países específicos. A plataforma

[5]Segundo a Serasa (2024), o geotargeting é uma estratégia publicitária que utiliza a localização geográfica dos dispositivos dos consumidores, como celulares, tablets e computadores, para desenvolver anúncios com base na região e no tipo de buscas dos usuários.

também disponibiliza *templates* de consentimento pré-configurados para diferentes legislações, como LGPD, GDPR e CCPA. A interface também sugere personalização, permitindo ajustes na aparência e comportamento do *banner*, e oferece botões de ação como *"Reject All*" e "*Accept All*", que facilitam a escolha dos usuários. Assim, a *Cookieyes* simplifica a gestão de consentimento ao fornecer um *banner* personalizável e informativo, que ajuda os sites a garantirem transparência e conformidade com as normas de privacidade.

Figura 4 - Plataforma do *software CookieYes*



Fonte: Página *CookieYes*[6]

4 Os impactos da LGPD no Brasil

A LGPD trouxe mudanças significativas para empresas e organizações no Brasil, afetando tanto aspectos operacionais quanto estratégicos, exigindo a adaptação de processos internos e a implementação de novas tecnologias (Rei Advogado, s.d.). As empresas precisam mapear os dados pessoais que coletam e garantir uma base legal para seu uso. A conformidade com a LGPD envolve investimentos em tecnologia, consultoria, treinamento e auditorias, tornando o processo complexo e oneroso (Rei Advogado, s.d.).

6 Disponível em: <https://www.cookieyes.com/documentation/install-cookieyes-wordpress-plugin/>. Acesso em: 19 set. 2024

A cibersegurança é essencial nesse contexto, com medidas como firewalls, criptografia e sistemas de detecção de invasões, que vão além do mero cumprimento legal e asseguram a proteção dos dados dos clientes e parceiros (Castro, s.d.). A área de TI foi especialmente impactada, com empresas formando equipes multidisciplinares de TI e Direito para lidar com a nova legislação. O gerenciamento contínuo de dados e a integração de soluções automatizadas são essenciais para evitar vulnerabilidades e invasões (Sena, 2021).

A governança dos dados se tornou um desafio crítico, exigindo soluções que proporcionem acesso rápido e seguro às informações dos titulares. A computação em nuvem amplia essa complexidade, demandando visibilidade e rastreabilidade dos dados. Aplicações e automatizações são estratégicas para garantir a conformidade, especialmente no gerenciamento de APIs e consentimentos de usuários.

Por fim, é crucial que todos os colaboradores, da gestão às operações, sejam treinados em boas práticas de proteção de dados. A criação de uma cultura organizacional voltada à privacidade, envolvendo também clientes e parceiros, fortalece o compromisso com a proteção de dados e promove um ambiente colaborativo e ético, alinhado às diretrizes da LGPD (GetPrivacy, s.d.).

5 Resultados e Discussões

Com base na análise bibliográfica realizada, indicam que a implementação da LGPD trouxe mudanças significativas para empresas e organizações no Brasil, exigindo adaptações em processos operacionais e estratégicos. As ferramentas tecnológicas de conformidade, como sistemas de gestão de consentimento, anonimização e segurança de dados, emergem como essenciais para garantir a proteção de dados pessoais e evitar sanções legais.

A comparação entre a LGPD e legislações internacionais, como o GDPR europeu e a CCPA americana, revela tanto alinhamentos quanto desafios para as empresas brasileiras que operam globalmente. O uso de soluções, como OneTrust, Tee Global, IBM Guardium e CookieYes, mostra-se eficaz na gestão de privacidade

e na mitigação de riscos de vazamento de dados, além de promover a conformidade contínua.

O estudo também destaca que a adoção dessas ferramentas, embora necessária, é um processo complexo e oneroso. Empresas que investem em cibersegurança, com medidas como criptografia e firewalls, não apenas atendem à legislação, mas fortalecem a confiança com clientes e parceiros, proporcionando vantagem competitiva. A formação de equipes multidisciplinares, integrando especialistas em TI e Direito, é outra estratégia crítica para garantir a implementação eficaz da LGPD.

Entretanto, os desafios não se restringem ao aspecto técnico. A pesquisa indica que a governança de dados e a necessidade de melhorias contínuas na infraestrutura e na gestão de APIs representam barreiras importantes para muitas organizações. A automatização de processos e a adoção de soluções em nuvem são vistas como tendências, mas demandam um gerenciamento rigoroso para evitar vulnerabilidades e manter a transparência no tratamento dos dados.

Por fim, foi identificado que a criação de uma cultura organizacional voltada para a privacidade é indispensável para o sucesso na implementação da LGPD. O treinamento contínuo dos colaboradores e o engajamento de clientes e parceiros são elementos fundamentais para promover práticas éticas e fortalecer a proteção dos direitos dos titulares. Dessa forma, a LGPD não apenas estabelece novas diretrizes legais, mas também impulsiona a transformação digital e a responsabilidade corporativa em torno da proteção de dados.

Consideração Final

A proteção de dados pessoais é uma preocupação crescente na era digital, dado o aumento exponencial da coleta e processamento de informações. A LGPD se destaca como um marco regulatório essencial para assegurar a privacidade e os direitos dos cidadãos brasileiros, alinhando-se a padrões internacionais, como o GDPR e a CCPA, e promovendo transparência e segurança no tratamento de dados.

Sua implementação trouxe desafios significativos para empresas, exigindo adaptações em processos internos e altos investimentos em ferramentas e capacitação. No entanto, a LGPD também oferece uma oportunidade de fortalecer a confiança dos clientes e transformar a conformidade em um diferencial competitivo, agregando valor às relações entre empresas e consumidores.

Diante da constante evolução desse campo, um projeto futuro relevante é o desenvolvimento de uma plataforma automatizada de compliance, utilizando inteligência artificial para mapear e gerenciar dados em tempo real, automatizar consentimentos e identificar riscos. Outra iniciativa importante seria a criação de um consórcio colaborativo entre governo, empresas e universidades para promover educação continuada sobre privacidade e incentivar pesquisas em tecnologias emergentes, como blockchain.

A efetividade da LGPD dependerá da colaboração entre empresas, governo e sociedade para consolidar uma cultura sustentável de proteção de dados, equilibrando inovação e respeito à privacidade, e garantindo um futuro digital mais seguro e ético.

Referência Bibliográfica

ADOPT. GDPR, LGPD e CCPA: o que são essas leis? Semelhanças e diferenças. *AdOpt*, 2022. Disponível em: <https://goadopt.io/blog/gdpr-lgpd-e-ccpa-o-que-sao-essas-leis-semelhancas-e-diferencas>. Acesso em: 09 ago. 2024.

ALVES, Gervânia. Ciclo de vida dos dados e LGPD. *Xpositum*, s.d. Disponível em: <https://xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd>. Acesso em: 09 ago. 2024.

ASSIS; MENDES. Histórico das leis de proteção de dados e da privacidade na internet. *Assis e Mendes Advogados*, 2019. Disponível em: <http://assisemendes.com.br/historico-protecao-de-dados/>. Acesso em: 09 ago. 2024.

BBC. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. *BBC News Brasil*, 19 mar. 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751>. Acesso em: 09 ago. 2024.

CASTRO, Diego. Como as empresas devem se adaptar à LGPD? s.d. Disponível em: <https://diegocastroadvogado.com.br/adapte-se-ja-empresas-e-a-nova-lgpd/>. Acesso em: 09 ago. 2024.

COSTA, Marcelo. As melhores ferramentas para LGPD no Brasil em 2023. *Tee Global*, 2023. Disponível em: <https://teeglobal.com.br/blog-melhores-ferramentas-para-lgpd-no-brasil-em-2023-%F0%9F%9A%80/>. Acesso em: 09 set. 2024.

COOKIEYES. *CookieYes: Solução de Consentimento de Cookies*. Disponível em: <https://www.cookieyes.com>. Acesso em: 09 set. 2024.

DBMS TOOLS. *OneTrust: Lista de Ferramentas de DBMS*. Disponível em: <https://dbmstools.com/tools/onetrust>. Acesso em: 09 set. 2024.

GATEFY. 10 princípios da LGPD para o tratamento de dados pessoais. 2021. Disponível em: <https://gatefy.com/pt-br/blog/principios-lgpd-tratamento-dados-pessoais/>. Acesso em: 09 set. 2024.

GETPRIVACY. LGPD e GDPR: entenda as diferenças e semelhanças entre as leis. *GetPrivacy*, s.d. Disponível em: <https://getprivacy.com.br/lgpd-gdpr-diferencas-semelhancas/>. Acesso em: 09 set. 2024.

GETPRIVACY. LGPD: 4 vantagens de investir em treinamento de equipe. s.d. Disponível em: <https://getprivacy.com.br/lgpd-vantagens-treinamento-de-equipe>. Acesso em: 09 set. 2024.

GIARLLARIELLI. Ciclo de vida dos dados. *Giarllarielli Advogados*, 2021. Disponível em: <https://www.giarllarielli.adv.br/ciclo-de-vida-dos-dados/>. Acesso em: 09 set. 2024.

HIGA, Paulo. British Airways recebe multa recorde de R$ 900 milhões por vazar dados. 2019. Disponível em: <https://tecnoblog.net/noticias/british-airways-multa-recorde-vazamento-dados/>. Acesso em: 09 set. 2024.

IBM. *IBM Security Guardium: Proteção e Segurança de Dados*. Disponível em: <https://www.ibm.com/br-pt/guardium>. Acesso em: 09 set. 2024.

IUBENDA. Como escolher o software de gerenciamento de privacidade correto. *Iubenda*, s.d. Disponível em: <https://www.iubenda.com/pt-br/help/123039-como-escolher-o-software-de-gerenciamento-de-privacidade-correto>. Acesso em: 09 set. 2024.

MARTINS, A. E. S. Comparando a LGPD com a GDPR: abordagens à proteção de dados pessoais. JusBrasil, 2023. Disponível em: <https://www.jusbrasil.com.br/artigos/comparando-a-lgpd-com-a-gdpr-abordagens-a-protecao-de-dados-pessoais/1971798734>. Acesso em: 8 out. 2024.

MARTINS, A. E. S. Os desafios da proteção de dados pessoais na era digital. JusBrasil, 2023. Disponível em: <https://www.jusbrasil.com.br/artigos/os-desafios-da-protecao-de-dados-pessoais-na-era-digital/1971809645>. Acesso em: 08 out. 2024.

MONTEIRO, R. L. *et al.* Lei Geral de Proteção de Dados e GDPR: Histórico, análise e impactos. *Baptista Luz Advogados*, 2019. Disponível em: <https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf>. Acesso em: 09 out. 2024.

ONETRUST. *OneTrust: Plataforma de Privacidade, Segurança e Governança*. Disponível em: <https://www.onetrust.com/pt>. Acesso em: 10 set. 2024

REI ADVOGADO. Os Impactos e Desafios da LGPD: Descubra as Principais Problemáticas da Lei Geral de Proteção de Dados. s.d. Disponível em: <https://reyabogado.com/brasil/quais-os-problemas-da-lgpd/>. Acesso em: 10 set. 2024.

SEBRAE. LGPD: Lei Geral de Proteção de Dados. s.d. Disponível em: <https://sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/PE/Anexos/LGPD-Connect-Sebrae.pdf>. Acesso em: 10 set. 2024.

SENA, Márcio. LGPD e TI: o guia completo para implementar as regras da nova lei. *Blog Impulso*, 2021. Disponível em: <https://blog.impulso.team/lgpd-e-ti-o-guia-completo-para-implementar-as-regras-da-nova-lei/>. Acesso em: 09 ago. 2024.

WEISS, Fernando Lemme. Paralelo entre a Lei Geral de Proteção de Dados, o CCPA e o GDPR europeu. *Consultor Jurídico*, 28 out. 2020. Disponível em: <https://www.conjur.com.br/2020-out-28/weiss-paralelo-entre-lgpd-ccpa-gdpr-europeu>. Acesso em: 09 ago. 2024.

QUINTILIANO. Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD). JusBrasil, 2020. Disponível em: <https://www.jusbrasil.com.br/artigos/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/1203647706>. Acesso em: 09 ago. 2024.