# O TRATAMENTO DE DADOS SUBMETIDOS À LGPD:
DESAFIOS DA CIBERSEGURANÇA

**Giovani Gonçalves Carvalho Ronchi**[1]

**Resumo:** Este artigo oferece uma análise aprofundada do embasamento jurídico, da aplicação e da implementação da Lei Geral de Proteção de Dados (LGPD), um marco significativo na legislação brasileira que estabelece direitos essenciais para a proteção e privacidade de dados pessoais em relação aos mecanismos de cibersegurança. Para isso, adotamos uma abordagem de pesquisa que combina análise documental, revisão de literatura e estudo de caso. Exploramos as influências globais, notadamente o General Data Protection Regulation (GDPR) europeu, e os eventos históricos que motivaram a criação da LGPD, com ênfase na solução e prevenção de ciberataques e na mitigação de vazamentos de dados.
**Palavras-chave:** Cibersegurança. LGPD. GDPR. Gerenciamento. Ciberataques.

**Abstract:** This article offers na in-depth analysis of the legal basis, application and implementation of the General Data Protection Law (LGPD), a significant milestone in Brazilian legislation that establishes essential rights for the protection and privacy of personal data in relation to cybersecurity mechanisms. To achieve this, we adopted a research approach that combines documentary analysis, literature review and case study. We explore global influences, notably the European General Data Protection Regulation (GDPR), and the historical events that motivated the creation of the LGPD, with na emphasis on solving and preventing cyberattacks and mitigating data leaks.
**Keywords:** Cybersecurity. LGPD. GDPR. Management. Cyberattacks.

[1] Acadêmico do curso de Direito da Faculdade Dom Bosco

## INTRODUÇÃO

Analisando o atual contexto histórico, percebe-se o aumento crescente de uma sociedade digital e o aumento exponencial da quantidade de dados pessoais tratados e armazenados, onde tornou-se necessária a implementação de legislações que protejam os direitos individuais e promovam a segurança cibernética. Nesse contexto, a LGPD surge como um marco regulatório no Brasil, inspirada em iniciativas internacionais como o General Data Protection Regulation (GDPR), visando garantir a privacidade dos cidadãos e estabelecer regras claras para o tratamento adequado dos dados.

A LGPD aborda diversas questões fundamentais relacionadas à proteção de dados, desde a coleta, até o seu compartilhamento e descarte. Ela estabelece diretrizes para a obtenção de consentimento dos titulares, exigindo transparência por parte das organizações em relação às finalidades do tratamento, bem como a garantia de que os dados sejam utilizados apenas para os fins autorizados.

No entanto, a implementação efetiva da LGPD requer uma compreensão abrangente dos mecanismos de cibersegurança, essencial para que as organizações adotem medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra acessos não autorizados, vazamentos e ciberataques. Essas medidas podem incluir a criptografia dos dados, o estabelecimento de políticas de acesso restrito e a implementação de protocolos de segurança robustos.

Além disso, é importante destacar a relevância do GDPR como um catalisador para a adoção de leis de proteção de dados em diferentes países. O impacto global do GDPR incentivou a criação de marcos regulatórios similares em diversas regiões do mundo, evidenciando a necessidade de uma abordagem unificada para a proteção da privacidade e dos dados pessoais.

Apesar dos avanços proporcionados pela LGPD e outras regulamentações, ainda existem desafios a serem enfrentados. A crescente dependência de sistemas terceirizados para o gerenciamento de bancos de dados pode representar vulnerabilidades e riscos de violações de dados, apesar das vantagens oferecidas, como expertise técnica e redução de custos. Além disso, a intervenção de Inteligências Artificiais (IA) em procedimentos relacionados à proteção de dados pessoais deve ser cuidadosamente implementada para garantir conformidade e respeito aos direitos dos indivíduos.

A LGPD não se limita apenas à proteção dos dados pessoais dos indivíduos, mas também estabelece diretrizes para a responsabilidade das organizações no que diz respeito ao tratamento desses dados. As empresas são incentivadas a adotar uma abordagem proativa na implementação de políticas de privacidade, realizando avaliações de impacto e adotando medidas preventivas para mitigar riscos de violações de dados, implementando um sistema de gestão de dados robusto que combine segurança, transparência e eficiência, juntamente com a utilização responsável da Inteligência Artificial, podendo abordar esses desafios. Ao adotar um sistema de gestão de dados que integre medidas de segurança avançadas, treinamento de funcionários e uma cultura de privacidade sólida, juntamente com o uso criterioso da Inteligência Artificial para identificar e evitar riscos, é possível alcançar uma redução significativa no número de violações de dados e aumentar a eficiência nas operações de proteção de dados. Essa abordagem também deve resultar em maior confiança dos clientes e no cumprimento contínuo das regulamentações de privacidade, como a LGPD. No entanto, isso requer investimentos em tecnologia, treinamento e conscientização para assegurar a conformidade e proteção de dados a longo prazo.

É fundamental reconhecer que as leis de proteção de dados, como a LGPD, são um reflexo das transformações sociais e tecnológicas pelas quais passamos. Com o avanço da tecnologia e a interconexão global, tornou-se necessário estabelecer normas e regulamentações que protejam os direitos dos indivíduos em relação aos seus dados pessoais.

Acontece que muitas das vezes essas diretrizes não são devidamente abordadas nem acompanhadas como devem ser, a maioria das empresas não estão adequadas a LGPD em seus termos de contrato, onde uma possível irregularidade pode ser detectada, e caso seus dados forem comprometidos será tarde demais. Por isso é de suma importância que cada agência reguladora responsável deve estar sempre abrindo canais de denúncia de possíveis violações de dados vazados e constante fiscalização. Para abordar o desafio da gestão de dados e privacidade à luz da LGPD, propomos uma abordagem de pesquisa mista que combina análise quantitativa e qualitativa. A coleta de dados quantitativos envolverá a análise de registros de violações de dados antes e depois da implementação das medidas propostas. Ao mesmo tempo, realizaremos análises qualitativas de políticas

e práticas de privacidade de empresas, além de entrevistas com especialistas em proteção de dados.

Com isso, vemos que os principais objetivos são o de avaliar o impacto das medidas de segurança avançadas e da integração da Inteligência Artificial no gerenciamento de dados na redução de violações de dados sob a LGPD, além de investigar como as empresas estão adotando políticas proativas de privacidade, realizando Avaliações de Impacto à Proteção de Dados (AIPD) e se comprometendo com a conformidade. Percebemos que, também é de suma importante que haja uma avaliação de eficácia e transparência das intervenções da Inteligência Artificial em procedimentos de proteção de dados, focando no equilíbrio entre eficiência e respeito aos direitos dos indivíduos.

## PROCESSO HISTÓRICO DE FORMAÇÃO DO DIREITO À PROTEÇÃO DE DADOS

A proteção de dados pessoais tem se tornado uma preocupação crescente ao longo da história, especialmente com o avanço da tecnologia e o aumento da coleta e uso de informações pessoais. Embora as preocupações com a privacidade existam há muito tempo, o contexto histórico especifico na proteção de dados pessoais pode ser traçado até o século XX.

Até meados do século XX, a coleta e o uso de dados pessoais eram limitados principalmente a registros físicos, como arquivos em papel mantidos por organizações governamentais e empresas. No entanto, o rápido desenvolvimento da tecnologia da informação e o advento da computação mudaram drasticamente esse cenário.

A partir da década de 1960, o uso de computadores para armazenar e processar dados pessoais se tornou mais comum. Isso levantou preocupações sobre a segurança e a privacidade das informações pessoais, especialmente em relação ao potencial abuso e acesso indevido a esses dados. As pessoas começaram a perceber que suas informações pessoais poderiam ser coletadas, compartilhadas e utilizadas sem o seu conhecimento ou consentimento.

No final do século XIX e início do século XX, surgiram preocupações iniciais sobre a privacidade e a proteção de dados pessoais. Um exemplo importante é a obra *O Direito de Ser Deixado em Paz (The Right to Privacy),* de Warren e Brandeis, publicada

em 1890 (PEIXOTO; EHRHARDT JÚNIOR, 2020). Nesse ensaio, os autores argumentaram que os avanços tecnológicos, como a fotografia e a imprensa, estavam ameaçando a privacidade individual. Durante as duas guerras mundiais e a Guerra Fria, os governos começaram a coletar e processar grandes quantidades de informações pessoais para fins de segurança nacional e inteligência. Isso levou a preocupações adicionais sobre a vigilância e a invasão de privacidade por parte dos governos.

Na década de 1960, a era da computação começou, e a coleta e o processamento de dados pessoais foram ampliados de maneira significativa. Surgiram bancos de dados e sistemas informatizados para armazenar e manipular informações pessoais em larga escala. Com o rápido crescimento da tecnologia da informação, surgiram preocupações cada vez maiores sobre o acesso não autorizado, a divulgação indevida e o uso indevido de dados pessoais, em resposta a essas preocupações, começaram a surgir regulamentações e legislações especificas para a proteção de dados pessoais em diferentes países. Por exemplo, em 1970, o governo sueco foi pioneiro ao estabelecer uma lei nacional de proteção de dados, a *Data Act* que garantia a proteção dos dados pessoais processados por agências governamentais, nos anos seguintes, outros países seguiram o exemplo e promulgaram leis semelhantes.

A França aprovou a Lei de Proteção de Dados em 1978, já a Alemanha introduziu a Lei Federal de Proteção de Dados em meados de 1977, com forte influência de Spiros Simitis, um jurista alemão conhecido por seu trabalho pioneiro no campo da proteção de dados (MENKE, 2021). Ele é considerado o principal arquiteto da primeira lei de proteção de dados do mundo, que foi promulgada na Alemanha em 1970 e é conhecida como a Lei Federal de Proteção de Dados (*Bundesdatenschutzgesetz* - BDSG) **(**PREIS, 2021). A Lei Federal de Proteção de Dados alemã foi um marco importante na história da proteção de dados pessoais, estabelecendo diretrizes e princípios para o tratamento dessas informações por parte de organizações e instituições públicas e privadas. Ela buscava proteger a privacidade dos cidadãos e regular a coleta, armazenamento, processamento e uso de dados pessoais por terceiros. Simitis desempenhou um papel fundamental na elaboração dessa lei, que estabeleceu diversos direitos dos indivíduos em relação aos seus dados pessoais, como o direito de acesso, correção e exclusão de informações, bem como a necessidade de consentimento informado para o tratamento de dados pessoais.

Em 1979, outros países europeus, incluindo França, Dinamarca, Portugal. Espanha e Áustria, seguiram o exemplo e promulgaram suas próprias legislações de

proteção de dados. Essas leis refletiam a crescente conscientização sobre a importância da privacidade e do controle das informações pessoais em uma era de avanços tecnológicos e fluxo transfronteiriço de dados.

É importante ressaltar que alguns países foram além da simples legislação e consideraram a privacidade como um direito fundamental em suas Constituições. Portugal, Espanha e Áustria foram exemplos disso, reconhecendo explicitamente a privacidade como um direito básico dos cidadãos.

No ano de 1981, o Conselho da Europa, uma organização internacional dedicada à promoção dos direitos humanos e à cooperação europeia, aprovou a Convenção 108 para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais. Essa convenção foi um marco importante, pois representou o primeiro instrumento legal transnacional específico para a proteção de dados.

A Convenção 108 foi motivada pelo reconhecimento da necessidade de ampliar a proteção dos direitos e liberdades fundamentais das pessoas, especialmente o direito ao respeito à vida privada, em um contexto de crescente fluxo transfronteiriço de dados sujeitos a tratamento automatizado. A convenção estabeleceu princípios gerais para o tratamento de dados pessoais, como a limitação da finalidade, a minimização dos dados, a qualidade dos dados, a segurança e a transparência, recentemente, a Convenção 108 passou por um processo de modernização para abordar os desafios trazidos pelas rápidas mudanças tecnológicas e pelo aumento do uso de dados pessoais. A nova versão, conhecida como Convenção 108+, foi adotada em 2018 e visa fortalecer ainda mais a proteção de dados pessoais, promovendo a cooperação entre os países signatários e incentivando a adesão de outras nações fora da Europa.

A evolução das leis e convenções de proteção de dados reflete a crescente conscientização sobre os desafios e riscos associados ao processamento de informações pessoais. À medida que avanços tecnológicos como a internet, a computação em nuvem e a inteligência artificial se tornaram mais difundidos, a necessidade de regulamentações robustas e abrangentes se tornou ainda mais evidente.

Um marco significativo nesse sentido foi a adoção do Regulamento Geral de Proteção de Dados (GDPR) pela União Europeia em 2016. O GDPR entrou em vigor em maio de 2018 e representa uma reforma abrangente das leis de proteção de dados na Europa. Ele estabelece diretrizes detalhadas sobre como as organizações devem coletar,

armazenar, processar e transferir dados pessoais, garantindo a proteção dos direitos individuais.

O GDPR introduziu uma série de requisitos importantes, como o consentimento explícito e informado para o processamento de dados, o direito dos indivíduos de acessar e corrigir suas informações pessoais, o direito ao esquecimento, a notificação obrigatória de violações de dados e a imposição de multas significativas para o não cumprimento das disposições do regulamento. Essa legislação teve um impacto significativo não apenas na União Europeia, mas também globalmente, já que muitas empresas ao redor do mundo precisaram se adequar as suas exigências para operar no mercado europeu, além do GDPR, outros países e regiões adotaram legislações semelhantes para fortalecer a proteção de dados pessoais. No Japão, por exemplo, a Lei de Proteção de Informações Pessoais foi aprovada em 2003 e passou por revisões em 2015 para se alinhar às normas internacionais. No Brasil, a Lei Geral de Proteção de Dados (LGPD) entrou em vigor em setembro de 2020, estabelecendo princípios semelhantes aos do GDPR e conferindo aos indivíduos maior controle sobre seus dados pessoais.

A proteção de dados também se tornou um tema importante em nível global. Em 2018, a Assembleia Geral das Nações Unidas adotou a Resolução sobre Privacidade no Contexto Digital, reconhecendo a importância fundamental da privacidade e da proteção de dados como direitos humanos. Além disso, várias organizações internacionais, como a Organização para Cooperação e Desenvolvimento Econômico (OCDE) e a Comissão Internacional de Proteção de Dados (ICDPPC), têm promovido a cooperação e o intercâmbio de boas práticas entre os países.

Essas leis buscavam estabelecer princípios para o processamento justo e legal de dados pessoais, bem como garantir os direitos individuais de acesso, retificação e exclusão de informações. No final da década de 1990 e também no inicio dos anos 2000, com o rápido crescimento da internet e do comércio eletrônico, surgiram novos desafios para a proteção de dados pessoais. A coleta massiva de informações online, juntamente com práticas questionáveis de empresas no uso desses dados, levou à necessidade de regulamentações mais abrangentes.

Posteriormente, em 1995, a União Europeia promulgou a Diretiva de Proteção de Dados, que estabeleceu princípios semelhantes em toda a União Europeia. Essa diretiva for substituída pelo Regulamento Geral de Proteção de Dados (GDPR) em 2018, que é a

legislação mais abrangente e influente sobre proteção de dados pessoais até o momento- (CALIL, 2022)**.**

## INFLUÊNCIA DA GDPR SOBRE A LGPD

A União Europeia desempenhou um papel fundamental ao adotar a Diretiva de Proteção de Dados em 1995. Essa diretiva estabeleceu padrões mínimos para a proteção de dados pessoais nos países membros e foi um marco importante no desenvolvimento de leis de proteção de dados em nível internacional. Nos últimos anos, a proteção de dados pessoais tem ganhado ainda mais destaque com a crescente conscientização do público sobre privacidade e segurança digital. O GDPR, mencionado anteriormente, é um exemplo proeminente desse avanço, estabelecendo um conjunto abrangente de regras para a proteção de dados pessoais.

O Regulamento Geral de Proteção de Dados - GDPR, é uma legislação da União Europeia que entrou em vigor em maio de 2018, com o objetivo de fortalecer e unificar as leis de proteção de dados pessoais na região, A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira, inspirada no GDPR, que entrou em vigor em setembro de 2020.

Embora o GDPR seja uma legislação europeia e a LGPD seja brasileira, há uma forte influência do GDPR na criação e implementação da LGPD. Ambas as leis compartilham princípios e diretrizes semelhantes em relação à proteção de dados pessoais. Uma das principais influências do GDPR na LGPD é a abordagem de proteção de dados baseada em princípios. Ambas as leis enfatizam a necessidade de obter o consentimento dos indivíduos para o processamento de seus dados pessoais, bem como a importância de garantir a transparência no tratamento desses dados. Além disso, ambas as leis promover a adoção de medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais.

Outra influência significativa do GDPR na LGPD é o reconhecimento dos direitos dos titulares de dados. Ambas as leis conferem aos indivíduos o direito de acessar, corrigir e excluir seus dados pessoais, além do direito de solicitar a portabilidade de seus dados para outro fornecedor de serviços.

Além disso, as duas leis estabelecem a obrigação de notificar as autoridades competentes em caso de violação de dados que possa resultar em risco para os direitos e

liberdades dos indivíduos afetados. Para mais, tanto o GDPR quanto a LGPD estabelecem a figura do Controlador de Dados, responsável por determinar as finalidades e os meios de processamento de dados pessoais, e do Operador de Dados, responsável por realizar o processamento em nome do controlador

Embora haja uma influência clara do GDPR na LGPD, é importante destacar que as leis têm algumas diferenças significativas. Por exemplo, o GDPR possui requisitos mais rigorosos para obtenção de consentimento, enquanto a LGPD adota uma abordagem mais flexível nesse sentido. Além disso, o GDPR estabelece multas mais elevadas para violações, com base na receita global das empresas, enquanto a LGPD possui multas limitadas a um percentual do faturamento da empresa no Brasil

Doneda (2011) frisa e salienta a importância dos documentos supracitados, e os princípios estabelecidos na Convenção nº 108 e nas *guidelines* da Organização para a Cooperação e Desenvolvimento Econômico OCDE, a serem aplicados na proteção de dados pessoais. Vale elencar aqui os princípios, tais como citados pelo autor:

> a) Princípio da publicidade (ou da transparência) pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatório periódicos; b) Princípio da exatidão os dados armazenados devem ser fieis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade; c) Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados Este princípio possui grande relevância pratica com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade); d) Principio do livre acesso, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas podendo obter copias desses registros, com a consequente possibilidade de controle desses dados após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos; e) Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação transmissão ou acesso não autorizado (DONEDA, 2011).

Destacando o autor ainda que:

> Estes princípios, mesmo que fracionados, condensados ou adaptados, formam a espinha dorsal das diversas leis, tratados, convenções ou acordos entre privados em matéria de proteção de dados pessoais, formando o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais (DONEDA, 2011).

## VAZAMENTOS DE DADOS POR CIBERATAQUES

O vazamento de dados em sistemas de atendimento é uma preocupação crescente na era digital. Com a digitalização de informações e o aumento da interação online entre empresas e clientes, os sistemas de atendimento, como os *call centers* e os *chats online*, se tornaram alvos atraentes para ataques cibernéticos e violações de segurança. Existem alguns aspectos que contribuem para o risco de vazamento de dados nesses sistemas. Primeiramente, a coleta de informações pessoais dos clientes durante o atendimento é comum e necessária para a prestação de serviços personalizados. No entanto, esses dados, se não forem tratados e protegidos adequadamente, podem ser explorados por terceiros mal-intencionados.

Além disso, os sistemas de atendimento geralmente envolvem uma grande quantidade de interações diárias, muitas vezes realizadas por operadores humanos. Esses operadores podem cometer erros, como enviar informações confidenciais para destinatários errados ou até mesmo serem alvos de engenharia social, resultando em vazamento de dados.

Por fim, os sistemas de atendimento são alvos atraentes para hackers, pois podem fornecer acesso direto a informações sensíveis dos clientes, como números de cartão de crédito, senhas e dados de identificação pessoal. Esses sistemas são frequentemente alvos de ataques de *phishing*, malware ou engenharia social, visando obter acesso não autorizado aos dados dos clientes, o mais comum usado, seria a engenharia social, o aspecto do sabotador, simular e se passar pelo titular dos dados cadastrados, mesmo que previamente tenha algum dado do titular, como exemplo, somente um nome completo possa se infiltrar no banco de dados da empresa para se obter vantagens de outras informações, caso os operadores linha de frente do atendimento, não recebam treinamento necessário, pode-se acarretar em uma irregularidade por vazamentos de dados, e até multa

pelo órgão regulador, nas responsabilidades da empresa que vaze esses dados (PINHEIRO; LEANDRO, 2021).

Os impactos de um vazamento de dados em sistemas de atendimento podem ser significativos. Os clientes afetados podem enfrentar roubo de identidade, fraudes financeiras ou até mesmo danos à reputação. Além disso, as empresas podem sofrer consequências legais e regulatórias, como multas e perda de confiança dos clientes.

Para evitar os riscos de vazamento de dados em sistemas de atendimento, as empresas devem adotar várias medidas de segurança, isso inclui a implementação de criptografia de dados, tanto em trânsito quanto em repouso, a adoção de práticas de autenticação forte, como a autenticação de fatores, e a conscientização e treinamento dos operadores sobre boas práticas de segurança.

Além disso, é importante que as empresas estabeleçam políticas claras de privacidade e segurança da informação, bem como realizem auditorias regulares de segurança para identificar vulnerabilidades nos sistemas de atendimento. A implementação de sistemas de monitoramento de atividades suspeitas e a resposta rápida a incidentes também são essenciais para identificar e conter vazamentos de dados em tempo hábil.

## INTELIGÊNCIA ARTIFICIAL ATRELADA AOS DADOS

Embora a intervenção de Inteligências Artificiais (IA) nos procedimentos relacionados à Lei Geral de Proteção de Dados (LGPD) possa trazer inúmeros benefícios, como otimização e agilidade, é importante reconhecer também alguns possíveis malefícios que podem surgir. É fundamental considerar essas questões para garantir uma implementação responsável e ética da IA no contexto da proteção de dados pessoais.

Viés algorítmico: A IA é alimentada por conjuntos de dados que podem conter vieses incorporados, refletindo desigualdades sociais e preconceitos existentes na sociedade. Isso pode levar a decisões discriminatórias ou injustas, perpetuando assimetrias e agravando desigualdades. É necessário realizar uma análise cuidadosa dos algorítmos e conjuntos de dados para mitigar o viés algorítmico.

Risco de ataques cibernéticos: A implementação de sistemas de IA em procedimentos ligados à LGPD pode aumentar a superfície de ataque e a vulnerabilidade a ataques cibernéticos. Os sistemas de IA podem se tornar alvos de hackers ou serem

explorados para obter acesso não autorizado a dados pessoais sensíveis. É fundamental adotar medidas de segurança robustas e realizar auditorias de segurança regularmente.

Privacidade comprometida: embora a IA possa ajudar na proteção da privacidade dos dados pessoais, também pode representar um risco se mal utilizada. Sistemas de IA com acesso a grandes quantidades de dados podem potencialmente violar a privacidade dos indivíduos se houver falhas no projeto ou implementação. É necessário garantir que as práticas de segurança e privacidade sejam devidamente implementadas em todos os aspectos relacionados à IA.

Dependência excessiva da IA: a utilização excessiva e indiscriminada da IA nos procedimentos ligados à LGPD pode resultar em uma dependência excessiva da tecnologia. Isso pode diminuir a autonomia e a responsabilidade humana na tomada de decisões, transferindo a responsabilidade para os algoritmos de IA. É importante encontrar um equilíbrio entre a automação e a intervenção humana adequada, falta de transparência e compreensão.

Às vezes, os sistemas de IA podem ser complexos e de difícil compreensão, tornando-se desafiadores para os usuários compreenderem como suas informações pessoais estão sendo tratadas. A falta de transparência nos algoritmos e nas decisões tomadas pela IA pode gerar desconfiança e preocupação por parte dos usuários, prejudicando a conformidade com a LGPD (POETA, 2020).

## O ENCARREGADO DA PROTEÇÃO DE DADOS

O encarregado de proteção de dados, também conhecido como *Data Protection Officer* - DPO, desempenha um papel crucial na implementação e conformidade com a Lei Geral de Proteção de Dados - LGPD. Suas principais responsabilidades incluem:

Monitoramento e aconselhamento: O DPO é responsável por acompanhar as práticas de processamento de dados pessoais dentro da organização e fornecer orientação sobre como cumprir as disposições da LGPD. Garantindo que a organização esteja ciente de suas obrigações legais relacionadas à proteção de dados.

Educação e conscientização: O DPO deve promover a conscientização sobre a proteção de dados pessoais entre os funcionários da organização, isso envolve fornecer treinamentos regulares e materiais educacionais relevantes para garantir que todos os

membros da equipe estejam bem informados sobre as práticas adequadas de proteção de dados.

Cooperação com autoridades de proteção de dados: O DPO atua como ponto de contato entre a organização e a autoridade de proteção de dados. Eles devem cooperar com a autoridade de forma proativa, respondendo a solicitações, relatórios de violações de dados e fornecendo qualquer informação ou documentação necessária.

Avaliação de impacto de proteção de dados: O DPO é responsável por conduzir avaliações de impacto de proteção de dados (AIPD) sempre que forem realizadas atividades de processamento de dados que possam apresentar riscos à privacidade dos indivíduos. Essas avaliações ajudam a identificar e mitigar riscos antes que se tornem problemas.

Resposta a incidentes de proteção de dados: O DPO desempenha um papel fundamental na gestão de incidentes de proteção de dados. Eles devem coordenar a resposta da organização a qualquer violação de dados, avaliar o impacto, notificar as partes relevantes, colaborar com a investigação interna e tomar medidas corretivas para evitar violações futuras.

Auditoria e monitoramento: O DPO deve realizar auditorias regulares para garantir que a organização esteja em conformidade com as políticas de proteção de dados. Eles também devem monitorar continuamente as práticas de processamento de dados para identificar possíveis problemas e implementar melhorias.

Manutenção de registros: O DPO é responsável por manter registros das atividades de processamento de dados realizadas pela organização, incluindo o registro de atividades de processamento e as medidas de segurança implementadas (ÁVILA; CANTERJI; AZEVEDO, 2021).

## CONSIDERAÇÕES FINAIS

A partir disto, concluímos que vários fatores, várias controvérsias e várias circunstâncias possíveis podem ocorrer em uma situação de risco, o que propicia o vazamento de dados: um simples erro, um deslize ou uma mera não confirmação de dados, resultada por uma brecha na segurança, que pode dar acesso à uma infinidade de possibilidades de falsificações ao infiltrado, ocasionando em um dano irreversível, tanto

para o titular dos dados vazados, como também para a empresa detentora das informações pessoais, que possivelmente sofrerá sanções de sua agência reguladora.

Pode-se dizer que não existe um sistema 100% seguro, seja ele regido pelas operações de conferência humana ou controlado por Inteligências Artificiais (IA) automatizadas. São inúmeras as possibilidades de erros. O que se pode fazer é aprimorar e aperfeiçoar o sistema de proteção a cada dia que se passa, não só através do aprendizado com erros, mas com experiências cotidianas, que são enfrentadas nas funções atreladas a operação da organização detentora dos dados.

Sabemos que toda prestação de serviço é regida por contratos. O que se pode fazer é não só observar, mas também conferir suas cláusulas, e se a elas estão atreladas nas conformidades à Lei Geral De Proteção de Dados, e cada terceiro ligado à operação da prestação deve também estar de acordo com as formalidades confidenciais, guardadas a sete chaves de cada informação pessoal.

Por isso, o *compliance* jurídico é de suma importância para a implementação da LGPD nas empresas, uma equipe especializada que guie e norteiem suas atuações em conformidades com a Lei, acontece que muitas das vezes os setores da empresas estão deveras esgotados e sobrecarregados de outras funções, o próprio encarregado na proteção de dados pode estar atrelado a outras funções, e acabam que uma só pessoa administre toda aplicabilidade, aonde erros contratuais de prestação e possíveis vazamentos de dados possam ocorrer, a maioria das pequenas e médias empresas não tem um setor jurídico, em sua maioria são escritórios terceirizados, que muitas das vezes são especialistas na área, mas desconhecem como funcionam as operações cotidianas realizadas pelos setores da empresa.

Uma das possíveis soluções que podemos sugerir é a abertura de um setor jurídico ou uma vaga de auxiliar jurídico com contato direto aos escritórios terceirizados, ou vagas de estágio para estudantes de Direito, para que a constante troca de experiências seja mútua e de fácil compreensão, e as aplicações de regras e as observações devem ser contínuas aos demais setores para o constante aprimoramento de suas operações, repassando ao restante da equipe todo treinamento necessário para estar em conformidade com a LGPD. Outra solução seriam palestras e cursos ofertados para seus procedimentos que devem estar em constante aprimoramento.

Uma das questões mais preocupantes é a falta de abordagem adequada e o acompanhamento insuficiente por parte das empresas em relação aos termos de contrato.

A maioria delas não estão incorporando cláusulas contratuais que estejam em conformidade com a LGPD, o que abre espaço para possíveis irregularidades. Caso ocorra uma violação de dados, as consequências podem ser extremamente danosas para os indivíduos afetados. Portanto, é de suma importância que as agências reguladoras responsáveis estejam constantemente abrindo canais de denúncia para possíveis violações de dados vazados e realizando uma fiscalização rigorosa.

A ausência de medidas efetivas para garantir o cumprimento da LGPD compromete a privacidade e a segurança dos cidadãos. As empresas têm a responsabilidade de coletar, armazenar e processar dados pessoais de forma adequada, garantindo a segurança e a confidencialidade dessas informações. No entanto, muitas vezes, vemos casos de vazamento de dados, invasões de privacidade e até mesmo uso indevido de informações pessoais.

É importante ressaltar que a LGPD não é apenas uma obrigação legal, mas também uma oportunidade para as empresas estabelecerem uma relação de confiança com seus clientes. Ao adotar medidas eficazes para proteger os dados pessoais, as empresas demonstram seu compromisso com a privacidade e a segurança dos usuários, o que pode resultar em uma imagem positiva e na fidelização aos clientes.

Além disso, a fiscalização por parte das agências reguladoras é essencial para garantir o cumprimento da LGPD. A abertura de canais de denúncia possibilita que os sujeitos afetados reportem possíveis violações, contribuindo para a identificação e punição dos responsáveis. A constante fiscalização também desempenha um papel importante na conscientização das empresas sobre a importância de se adequarem às diretrizes da LGPD, Somente dessa forma será possível garantir a privacidade e a segurança dos dados pessoais dos cidadãos, promovendo uma sociedade mais justa e transparente.

Uma solução presente para se verificar a titularidade dos dados do cadastro, seria implementar em seu sistema de atendimento, na operação de coleta de dados o sistema de 3 fatores, que no caso seria: Nome Completo, CPF e Data de nascimento. Muitas das vezes, as pessoas que se passam pelos titulares nem sempre têm acesso a todos os dados do titular, com isso, para completar solicitam estes dados à empresa detentora, onde a implementação dessa regra facilitaria na conferência da titularidade do cliente, pois, como sabemos nenhuma pessoa responde por outra, o que seria uma resposta penal a essa

tentativa de sabotagem, podendo implicar ao sabotador o crime de Falsidade Ideológica, sendo responsabilizado criminalmente.

## REFERÊNCIAS BIBLIOGRÁFICAS

ÁVILA, A. P- Canterji, R. B- Azevedo, R. **Os riscos e as responsabilidades do encarregado de dados**. Revista: Conjur, publicado em 19/12/2021- Disponível em: https://www.conjur.com.br/2021-dez-19/opiniao-riscosresponsabilidades-encarregado-dados?imprimir=1.

CABRAL, B. F. **"The righttobeletalone": considerações sobre o direito ao esquecimento.** Revista: Jus.com.br, publicado em 15/06/2014 Disponível em: https://us.com.br/artigos/28362/the-right-to-be-let-alone-consideracoes-sobreo-direito-ao-esquecimento.

CALIL, J. H. M. **A Lei Geral de Proteção de Dados no contexto histórico global - Um novo conjunto normativo sobre um direito não muito novo**. Publicado por: Comissão de Direito Digital Aba Rio: 2022, texto produzido 2020. Disponível em: https://www.jusbrasil.com.br/artigos/a-lel-geral-deprotecao-de-dados-no-contexto-historico-global-um-novo-conjunto-normativosobre-um-direito-nao-muito-novo/1414685352.

DONEDA, DANILO. **A proteção dos dados pessoais como um direito Fundamental.** 2011. Disponível em: https://portalperiodicos.unoeso.edu.br/espacojuridico/article/view/1315/658.

GOMES, M. C. O. **Lei Geral de Proteção de Dados e GDPR: Histórico, análise e Impactos - 1.1 Os primeiros passos da proteção de dados no mundo**. Revista: Academia, publicado em 2018 - Disponível em: https://www.academia.edu/38940887/Lel_GeraldeProteção_de_Dados_e_GDPR_histórico_análise_e_impactos.

MENKE, F. **Spiros Simitis e a primeira lei de proteção de dados**. Revista: Migalhas, publicado em 19/01/2021-Disponívelem: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-protecao-de-dados-do-mundo.

PEIXOTO, E. L. C, E MARCOS EHRHARDT JÚNIOR, E. J. **Os desafios da compreensão do direito à privacidadeno sistema jurídico brasileiro em face das novas, 2.1A privacidade segundo warren e brandeis, O Direito de Ser Deixado em Paz" (The RighttoPrivacy), de Warren e Brandeis**, publicada em 1890 -Artigo científico, publicado em 2020, Disponível em: https://www.cidp.pt/revistas/rjlb/2020/2/2020_02_0389_0418.pdf

PINHEIRO, P. P., LEANDRO. S. R. **Segurança Cibernética: Novas Regras e Paradigmas. Direito Digital aplicado 4.0. 1**. Ed. São Paulo: Thomsom Reuters Brasil. 2020.

POETA, V. S. **Inteligência artificial e a proteção de dados pessoais: reflexos do regulamento geral de proteção de dados europeu - GDPR, no âmbito da garantia de direitos fundamentais no direito brasileiro. Dissertação para obtenção de Mestrado,** Publicado em: abril de 2020, Disponível em: A INTELIGÊNCIA ARTIFICIAL E A PROTEÇÃO DE DADOS PESSOAIS https://www.univali.br/Lists/TrabalhosMestrado/Attachments/3015/DISSERTA%C3%87%C3%83O%20-%20VITOR%20SARDAGNA%20POETA.pdf

PREIS, F. **Bundesdatenschutzgesetz (BDSG) – Como funciona a proteção de dados na Alemanha**, publicado em 2021, Disponível em: https://www.alemanhacast.com.br/datenschutz-como-funciona-a-protecao-de-dados-na-alemanha/

WARREN, S. D.; BRANDEIS, L. D. **The Right to Privacy**. Harvard Law Review. Cambridge Harvard University Press. V, IV, n. 05, pg. 193-217.