LGPD: UMA ANÁLISE CRÍTICA DA SUA IMPLEMENTAÇÃO E EFETIVIDADE NO COMBATE AO VAZAMENTO DE DADOS

LGPD: a critical analysis of its implementation and effectiveness to combat data leakage

Ana Priscila Gomes Mendes[1]
UniFanor Wyden

Vicente de Paulo Augusto de Oliveira Júnior[2]
UNIFOR

DOI: https://doi.org//10.62140/AMVJ442024

Sumário: Introdução. 1 O alto índice de vazamentos de dados nos últimos anos. 2 Os riscos sobre o vazamento de dados e como eles se tornam públicos dentro da Dark Web. 3 O vazamento de dados após a edição da LGPD no Brasil. Considerações Finais.

Resumo: A Lei Geral de Proteção de Dados (LGPD), inspirada na legislação europeia, foi estabelecida em 2020 no Brasil com o objetivo de proteger os direitos individuais, promovendo liberdade, privacidade e segurança em um ambiente digital em constante evolução e combatendo crimes cibernéticos. A lei atribui responsabilidade às empresas, tanto públicas quanto privadas, sobre os dados pessoais que gerenciam, contribuindo para a adaptação ao cenário digital e assegurando a proteção dos dados das pessoas naturais. A LGPD criou a Autoridade Nacional de Proteção de Dados para supervisionar sua aplicação, porém vários relatórios destacam enormes vazamentos de dados no país, resultando em negligência na proteção dos bancos de dados e exposição de milhões de registros. A lei exige a presença de Encarregados de Proteção de Dados (DPOs) para gerenciar a proteção de dados, mas muitas empresas ainda não estão em conformidade. A falta de conscientização sobre a importância dos dados expõe as pessoas a riscos como sequestro de dados e tráfico humano. A LGPD demanda análise cuidadosa das bases jurídicas, transparência na comunicação com os titulares dos dados e implementação de medidas de segurança. O vazamento de dados representa riscos significativos para as empresas, com ataques de *ransomware* destacando-se, resultando em custos diretos e indiretos graves, além de danos à reputação. A adaptação à LGPD exige medidas proativas, como conscientização e treinamento, apesar dos desafios financeiros e culturais. A implementação da LGPD no Brasil visa proteger os direitos individuais frente às ameaças tecnológicas, impulsionando avanços na conformidade e na cultura de proteção de dados, apesar dos desafios enfrentados.
Palavras-chave: Dados. LGPD. Proteção. Vazamento.

Abstract: The General Data Protection Regulation (LGPD), inspired by European legislation, was created in 2020 in Brazil with the aim of protecting individual rights, promoting freedom, privacy and security in a constantly evolving digital environment and combating crimes cyber. It gives companies, both public and private, responsibility for the people's data that we manage, contributing to the adaptation to the digital world and ensuring the protection of people's data in nature. The LGPD called on the National Data Protection Authority to monitor its application, as several relationships cause huge changes to data in

[1] Graduanda em Direito pelo Centro Universitário Fanor Wyden – UniFanor Wyden. Bolsista do Programa de Iniciação Científica UniFanor Wyden 2023-2024.
[2] Pós-Doutor em Direito pela Universidade de Fortaleza – UNIFOR. Professor do Centro Universitário Christus, campus Parquelândia. Professor do Centro Univeristário Fanor Wyden – UniFanor Wyden. Orientador do Programa de Iniciação Científica UniFanor Wyden 2023-2024.

the country, resulting in negligence in the protection of data meters and the exposure of millions of records. The presence of Data Protection Registers (DPOs) is necessary to ensure data protection, but many companies are currently not compliant. Due to a lack of awareness about the importance of data, people are exposed to the risk of data seizure and human trafficking. The LGPD requires careful analysis of legal bases, transparency in communication with data subjects and implementation of security measures. Data movement represents significant costs for companies, with ransomware attacks being detected, resulting in serious direct and indirect customer losses, resulting in reputational damage. Adapting to the LGPD requires proactive measures such as awareness and training, as well as financial and cultural considerations. The implementation of LGPD in Brazil will protect individual rights vis-à-vis technology industries, boosting compliance and a culture of data protection, without compromising security concerns.
Keywords: Data. LGPD. Protection. Leak.

INTRODUÇÃO

Nas palavras de Klaus Schwab "A Quarta Revolução Industrial gera um mundo no que os sistemas de fabricação virtuais e físicos cooperam entre si de uma maneira flexível a nível global".

Com os incríveis avanços das novas tecnologias e as inúmeras atualizações constantes do mundo digital, a chamada "quarta revolução industrial", surgiu junto a inúmeros riscos à segurança em relação a proteção de dados. Como meio de proteger as pessoas, o direito brasileiro está caminhando no meio legislativo para proteger e assegurar os direitos coletivos e individuais das pessoas naturais.

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, foi inspirada diretamente na RGPD (Regulamento Geral Sobre a Proteção de Dados 2016/679, União Europeia), que de acordo com pesquisadora de LGPD na USP Selma Carloto[1], é o regulamento do Direito europeu que versa sobre a privacidade e a proteção de dados para todos os indivíduos residentes na referida união econômica e política.

A LGPD foi criada para garantir a liberdade e a privacidade, bem como os dados da pessoa natural e isso fica claro em seu artigo 1º. A fim de tentar se adequa ao novo mundo digital garantindo segurança, e com o objetivo de evitar os "cibercrimes" evoluído muitas vezes de crimes comuns. A LGPD foi criada para que as pessoas jurídicas públicas e privadas tenham responsabilidade em relação as informações pessoais tratadas sob seu domínio.

O método de pesquisa utilizado é o qualitativo, sustenta-se em técnicas de coleta de dados. De acordo com Neves (1996, p.1), a pesquisa qualitativa não busca enumerar ou medir eventos. Ela serve para obter dados descritivos, a pesquisa tem o objetivo de analisar o contexto geral proporcionando maiores informações sobre o referido tema. Para que o estudo seja possível, houve um levantamento bibliográfico, com o uso de doutrinas

renomadas pelo Direito brasileiro, notícias jornalísticas e produções audiovisuais acerca da relação entre a aplicação e eficácia da LGPD.

1 O ALTO ÍNDICE DE VAZAMENTOS DE DADOS NOS ÚLTIMOS ANOS

Diante da quantidade de dados disponíveis na internet, as pessoas se tornaram a parte frágil e prejudicada das relações de forma geral. Apesar de o Brasil ter sido um país que sempre teve um alto índice de democratização digital ao longo dos anos, se formos comparar com os países vizinhos da américa latina, o Brasil agiu de forma muito tardia em relação a proteção de dados pessoais.

Sobre os riscos de vazamentos de dados, passados quase dois anos de sua vigência, a LGPD passou por algumas modificações ao longo desses anos. Criando-se no ano de 2020 a Autoridade Nacional de Proteção de Dados (ANPD), a ANPD tem a função de fiscalizar o cumprimento da LGPD. Diante do aumento dos cibercrimes e da grande exposição de dados vazados ao longo dos anos. veja o que diz as matérias apuradas entre os anos de 2020 à 2022.

"Os casos de phishing não param de crescer. 2020 foi o ano da pandemia e do tão falado aumento da superfície de ataque. Nosso relatório anual registrou um recorde de identificação em casos de phishing: 48.137 casos em 2020, observando um aumento de 99,23% em relação aos 24.161 casos registrados em 2019." (Hugo Moura, Relatório Axur: phishing cresce 99,23% em um ano, site: Blog Axur,).

"Este ano, infelizmente, o Brasil ficou no topo de vazamento de informação, de invasões, no mundo todo. Tivemos nesse ano de 2021 mais de 227 milhões de dados de brasileiros expostos". (CAMBRAIA, em 2021, Brasil ficou no topo de vazamento de informação no mundo, diz especialista, site: CNN Brasil, 2021).

De acordo com levantamento da Tenable 2,29 bilhões de registros foram expostos em 2022, enquanto mais de 800 milhões foram vazados devido à negligência na proteção dos bancos de dados. O relatório anual da companhia sobre o cenário de ameaças no ano passado também destacou que foram expostos 257 terabytes de dados ao redor do planeta, desse número, 112 terabytes apenas no Brasil. (Bruno Silva, 2,29 bilhões de registros foram expostos em 2022 e Brasil lidera ranking de vazamentos, site: Security Report).

Observa-se que devido a quantidade de dados disponíveis na web e nos bancos de dados das empresas, os usuários estão cada vez mais suscetíveis a ter sua privacidade invadida devido ao vazamento de dados. O professor israelense Yuval Noah Harari[2], disse a seguinte frase sobre a privacidade no mundo atual "Hoje, muitos de nós já abrimos mão de nossa

privacidade e individualidade, registramos cada uma de nossas ações, conduzimos nossa vida on-line e ficamos histéricos se nossa conexão com a rede se interrompe mesmo que por alguns minutos."

O que o professor Harari, pontua em sua reflexão é que a sociedade como um todo se vende muitas vezes de forma completa, por apenas alguns minutos de conexão para continuar se expondo para o mundo sem ao menos se dar conta dos riscos que podem ocorrer consigo.

Para entender melhor a complexidade do problema é importante destacar alguns pontos importantes sobre a lei 13.709/2018, o art. 7º, discorre sobre os requisitos para o tratamento de dados pessoais. Veja o que diz os parágrafos quarto e quinto:

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

Esses parágrafos em específicos são de extrema importância para a análise da tratativa de dados pessoais, entende-se em um primeiro momento que os controladores de dados não são obrigados a cumprir os requisitos para o tratamento de dados desde que o titular dos dados torne-os públicos. Dessa forma ao baixar um aplicativo ou se inscrever em um site que exige o fornecimento de dados e cadastro de conta, o usuário precisa concordar com os termos do controlador.

É importante ressaltar que a maior parte das empresas ainda não estão em conformidade com a lei, não tendo nem DPO (Data Protection Officer, Encarregado pelo Tratamento de Dados Pessoais) e muito menos um controlador. Que são os agentes responsáveis que a LGPD obriga as empresas a terem em seu quadro de funcionários para poder gerir melhor a proteção de dados pessoais.

2 OS RISCOS SOBRE O VAZAMENTO DE DADOS E COMO ELES SE TORNAM PÚBLICOS DENTRO DA DARK WEB

O momento que os dados pessoais entram em risco, se dá principalmente pela falta de conhecimento sobre a importância dos dados por parte das empresas e das próprias

pessoas físicas. Por não saberem os níveis dos riscos que sofrem, as pessoas acabam concordando com os termos de uso do controlador e os seus dados tornam-se públicos.

Podendo serem vendidos para outras empresas ou acabando públicos na "dark web" por descuido dos controladores, a dark web é um elo alternativo da internet chamada visível ou comum. Os dados encontrados na dark web são vendidos a preços exorbitantes, incluindo desde a localização da residência das pessoas até dados bancários. A problemática desse descuido é importante pois o navegador utilizado é anônimo dificultando a investigação da polícia nessas situações.

Os crimes derivados dos vazamentos de dados também podem ser atingidos de forma coletiva para atender melhor às necessidades dos criminosos, eis aqui um exemplo:

Para os criminosos conseguirem concluir seus crimes da melhor forma possível eles estão se utilizando de "Malwares" (termo genérico para qualquer tipo de "malicious software" ou "software malicioso") para sequestrar dados que geralmente são administrados por pessoas jurídicas tanto públicas como privadas.

Os dados vazados na dark web, podem ser utilizados para uma variedade de atividades maliciosas. Como o roubo de identidade, no qual os criminosos utilizam as informações pessoais para cometer fraudes financeiras, abrir contas fraudulentas ou até mesmo obter acesso a serviços confidenciais. Além disso, os dados podem ser vendidos a terceiros interessados em explorá-los para diversos fins, como chantagem, extorsão, espionagem industrial, pornografia infantil até mesmo tráfico humano. Os crimes de tráficos humano em especial são um dos mais complexos, por exemplo, ao sequestrar os dados escolares de uma determinada escola, os cibercriminosos criam uma espécie de banco de dados, lá eles podem armazenar informações do tipo: idade, nome, país, residência etc. Trançando esse perfil os criminosos podem criar um mercado virtual para os "compradores" da *dark web* que escolhem de forma personalizada o seu "produto".

No contexto da LGPD, as empresas devem conduzir uma minuciosa análise das bases jurídicas que justificam o tratamento de dados pessoais. É crucial para as empresas identificarem e classificarem os dados pessoais sob sua responsabilidade, com atenção especial aqueles que requerem tratamento diferenciado, incluindo informações sensíveis e dados relacionados a crianças e adolescentes.

A transparência é um pilar importante para a LGPD. As empresas devem informar de forma clara aos titulares dos dados a finalidade do tratamento, os tipos de dados, quem são os destinatários que receberam esses dados e os direitos dos titulares sobre a proteção

dos dados. Essa comunicação com o titular deve ser feita de forma que o indivíduo compreenda plenamente a finalidade do uso de suas informações pessoais.

A LGPD demanda a implementação de medidas técnicas, políticas internas e diretrizes que garantam a aderência aos requisitos legais. Isso abrange a elaboração de regulamentações de segurança, a revisão de procedimentos internos e o estabelecimento de políticas de proteção de dados que estejam alinhadas com os princípios fundamentais da Lei Geral de Proteção de Dados. Ademais, é importante que as empresas possam demonstrar de forma clara o procedimento usado na tratativa de dados quando requisitado pelos titulares dos dados ou pela Autoridade Nacional de Proteção de Dados (ANPD).

3 O VAZAMENTO DE DADOS APÓS A EDIÇÃO DA LGPD NO BRASIL

Ao longo do artigo foi possível ver que a quantidade de dados vazados foram enormes e que os riscos são inimaginaveis para as pessoas. Mas nesse momento iremos discorrer sobre os problemas que são gerados as empresas quando ocorre negligência em seu tratamento de dados.

Um dos principais problemas são os incidentes ocasionados por ransomwares que é uma espécie de malwere[3]. O ransomware emergiu como uma das ameaças cibernéticas mais devastadoras enfrentadas pelas organizações atualmente, deixando um rastro de prejuízos financeiros e operacionais em seu caminho. Os danos causados por esse tipo de ataque são vastos e impactam profundamente a capacidade das empresas de operar de maneira eficiente e segura.

Os custos diretos associados a um ataque de ransomware são significativos. O pagamento de resgate é apenas uma parte desse quadro, e os valores exigidos pelos cibercriminosos podem variar de milhares a dezenas de milhões de dólares, dependendo da sofisticação do ataque e da capacidade financeira da empresa-alvo. O exemplo do pagamento de US$ 70 milhões exigido pelo grupo REvil à fornecedora de software Kaseya ilustra a magnitude desses custos. Mesmo se a empresa se recusar a pagar o resgate, ela ainda enfrentará despesas substanciais para conter e recuperar os sistemas afetados, podendo incorrer em perdas de receita durante semanas ou meses.

Além dos custos diretos, há também os custos indiretos, que podem ser ainda mais devastadores. A perda de produtividade e receita devido ao tempo de inatividade, danos à reputação da empresa, multas por violação de conformidade e despesas legais aumentam

[3] Neste caso o Ransomware é um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo.

significativamente o ônus financeiro. O tempo de recuperação após um ataque de ransomware é extenso, com empresas enfrentando em média 22 dias de tempo de inatividade para retomar as operações. Essa paralisação não apenas resulta em perdas imediatas, mas também pode levar a oportunidades de vendas perdidas e produção reduzida de produtos ou serviços, ampliando ainda mais os prejuízos.

Além dos impactos financeiros, os ataques de ransomware expõem as vulnerabilidades nas defesas de segurança cibernética das empresas. Identificar e corrigir essas lacunas requer investimentos adicionais em tecnologia e processos de segurança cibernética, aumentando ainda mais os custos a longo prazo.

Pagar o resgate não garante a eliminação do risco, já que os cibercriminosos podem continuar a acessar os sistemas e dados da empresa ou lançar novos ataques. Além disso, o pagamento de resgate pode incentivar outros grupos de criminosos cibernéticos a mirarem na empresa, aumentando ainda mais a probabilidade de futuros ataques.

Diante desses custos substanciais e da ameaça contínua representada pelo ransomware, é essencial que as empresas adotem medidas proativas para fortalecer suas defesas cibernéticas e desenvolver planos de resposta a incidentes robustos. Investir em segurança cibernética adequada e educação do pessoal, bem como implementar práticas de backup e recuperação de dados sólidas, são passos cruciais para mitigar os riscos e proteger os ativos das empresas contra essa crescente ameaça digital.

Os incidentes de vazamento de dados representam uma séria ameaça para as organizações, trazendo consigo consequências financeiras e de reputação devastadoras. O "Relatório do Custo de uma Violação de Dados 2021", elaborado pelo Ponemon Institute e pela IBM, oferece uma visão detalhada dos impactos econômicos desses eventos, revelando um cenário alarmante para empresas em todo o mundo, inclusive no Brasil.

De acordo com o relatório, os custos associados aos negócios perdidos e ao dano reputacional representam uma parcela significativa do custo total médio de uma violação de dados, chegando a aproximadamente 38%. Esses custos refletem não apenas a perda de clientes e receita decorrente do tempo de inatividade dos sistemas, mas também o aumento dos custos de aquisição de novos negócios devido à reputação prejudicada da empresa.

Os dados revelam que, após um vazamento ou violação, as organizações enfrentam desafios financeiros que vão além das sanções administrativas impostas pelas autoridades reguladoras. O custo médio de uma violação de dados atingiu um novo recorde, aumentando 10% em relação ao ano anterior, alcançando US$ 4,24 milhões. Esse aumento é atribuído

principalmente às falhas de conformidade, com empresas que apresentam alto nível de não conformidade enfrentando custos médios de violação de dados 51,1% acima da média.

Os custos associados a uma violação de dados são diversos e incluem detecção, notificação, resposta pós-violação, despesas legais e multas das autoridades reguladoras. Além disso, o tempo necessário para identificar e conter uma violação é significativo, com uma média de 287 dias entre o incidente e sua contenção adequada, o que representa um sério desafio para as organizações em termos de recuperação e mitigação de danos.

O relatório também destaca dados específicos, como o fato de que 44% das violações continham dados pessoais e que 20% foram inicialmente causadas por credenciais comprometidas. Além disso, o setor de assistência médica registrou um aumento de 29,5% no custo médio de uma violação de dados em 2021, mantendo sua posição como o setor mais afetado por violações há 11 anos consecutivos.

Diante dessas conclusões alarmantes, fica evidente a necessidade urgente de as empresas se adequarem à LGPD (Lei Geral de Proteção de Dados) como um investimento essencial. A contratação de assessoria especializada e a implementação de uma cultura de proteção de dados são fundamentais para mitigar os riscos e reduzir significativamente os custos em caso de incidentes de violação de dados. Em um cenário cada vez mais digital e interconectado, a proteção dos dados dos clientes e a preservação da reputação da empresa são imperativos de mercado que não podem ser negligenciados

As empresas devem seguir alguns meios para evitar que o vamento de dados ocorra. Primeiramente deve-se ter um controlador e nomear um DPO, para lidar com a demanda de privacidade de dados.

Foi compreendido que a estratégia bem-sucedida para a adaptação à LGPD inclui a implementação de um plano abrangente de conscientização e treinamento destinado aos colaboradores da empresa. Esse plano visa promover a compreensão coletiva da importância da privacidade dos dados pessoais entre funcionários, colaboradores terceirizados e demais partes envolvidas. O entendimento compartilhado das práticas adequadas de tratamento de dados é fundamental para manter a conformidade contínua.

A Lei Geral de Proteção de Dados, não está isenta de desafios como foi demonstrado ao longo deste artigo, destacasse alguns pontos que incluem a necessidade de reformular processos internos, manter a conformidade constante e enfrentar possíveis violações de segurança. Apesar dos obstáculos, uma implementação eficaz da LGPD pode levar a uma maior confiança dos internautas, além de promover uma abordagem responsável sobre tratamento de dados pessoais.

A implementação da LGPD, no âmbito empresarial tem se revelado uma jornada permeada por uma série de desafios. Entre os principais obstáculos encontrados, destacam-se:

A Restrição de Recursos Financeiros ao processo de adequação à LGPD envolve um conjunto complexo de atividades que demandam recursos financeiros substanciais. Desde a contratação de consultorias especializadas até a implementação de sistemas de segurança e plataformas adequadas, os custos envolvidos podem representar um entrave, especialmente para as pequenas e médias empresas. Contudo, é imperativo enxergar esses investimentos como estratégicos, uma vez que a conformidade com a LGPD não apenas evita penalidades, mas também confere melhorias à reputação e uma vantagem competitiva.

O estabelecimento de uma cultura sólida de proteção de dados ainda não é uma realidade presente na maioria das organizações no Brasil. A privacidade, embora reconhecida como benéfica, não permeia integralmente a cultura organizacional. Para garantir a integridade dos dados tratados durante as operações, é imprescindível que as empresas desenvolvam uma cultura de governança de dados, incorporando medidas operacionais e de segurança da informação.

A maturidade no setor de serviços em relação à adequação. Fois registrado que cerca de 45% das empresas desse segmento relatam a aderência a apenas de 0% a 20% dos requisitos legais. Além disso, as empresas de pequeno porte, por dependerem de recursos especializados e envolverem investimentos substanciais, muitas vezes não priorizam a conformidade com a LGPD.

Como resposta a essa realidade, a Autoridade Nacional de Proteção de Dados (ANPD) emitiu a Resolução CD/ANPD N° 2/2022, proporcionando certas flexibilizações na aplicação da LGPD para agentes de tratamento de pequeno porte. Embora permaneçam vinculados ao cumprimento da LGPD, essas organizações desfrutam de benefícios, como prazos estendidos para atender às solicitações dos titulares de dados e a possibilidade de não indicar um encarregado de proteção de dados (DPO), desde que ofereçam um canal de comunicação alternativo com os titulares.

CONSIDERAÇÕES FINAIS

O Brasil, ciente das ameaças decorrentes dos avanços tecnológicos, implementou a Lei Geral de Proteção de Dados (LGPD) para proteger os direitos individuais e coletivos. No entanto, uma jornada rumo à conformidade com a LGPD tem sido complexa e repleta de desafios.

A LGPD, apesar de ainda enfrentar desafios e obstáculos, oferece um arcabouço legal essencial para a proteção dos direitos individuais e a promoção da transparência no tratamento de dados pessoais. No entanto, a implementação eficaz da LGPD requer não apenas conformidade legal, mas também uma mudança cultural dentro das organizações, visando uma verdadeira conscientização sobre a importância da privacidade e da segurança dos dados.

Os dados pessoais, uma vez comprometidos, podem ser explorados de diversas maneiras pelos criminosos, desde sua venda para terceiros até a utilização em atividades ilícitas, como pornografia infantil e tráfico humano. A existência de mercados clandestinos na chamada "dark web" amplifica esses riscos, dificultando a identificação dos responsáveis e a recuperação dos dados.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) surge como um marco regulatório fundamental para garantir a segurança e a privacidade das informações pessoais. A LGPD estabelece diretrizes claras para o tratamento de dados pessoais, exigindo transparência por parte das empresas e estabelecendo medidas técnicas e políticas internas para garantir a conformidade com a legislação.

É essencial que as empresas conduzam uma análise detalhada das bases jurídicas que justificam o tratamento de dados pessoais, identificando e classificando as informações sob sua responsabilidade. A transparência com os titulares dos dados é um princípio fundamental da LGPD, exigindo uma comunicação clara sobre a finalidade do tratamento, os tipos de dados envolvidos e os direitos dos titulares.

Além disso, a implementação eficaz da LGPD requer a adoção de medidas técnicas e organizacionais que garantam a conformidade com os requisitos legais. Isso inclui a elaboração de regulamentos de segurança, a revisão de procedimentos internos e o estabelecimento de políticas de proteção de dados alinhadas com os princípios da legislação.

Em suma, a LGPD representa um avanço significativo na proteção dos dados pessoais no Brasil, exigindo uma mudança de cultura e práticas por parte das empresas e uma maior conscientização por parte dos cidadãos. Somente com o cumprimento rigoroso da legislação e o fortalecimento das medidas de segurança cibernética podemos garantir a integridade e a privacidade dos dados no ambiente digital em constante evolução.

Diante do exposto, torna-se inegável a magnitude dos prejuízos ocasionados pelos vazamentos de dados às empresas, sobretudo quando se observa os impactos devastadores dos ataques de ransomware. Estes não apenas acarretam custos diretos expressivos, como os pagamentos de resgate exigidos pelos cibercriminosos, mas também desencadeiam uma

cascata de despesas indiretas, que incluem perda de produtividade, danos à reputação corporativa, multas e despesas legais.

Além dos custos financeiros, os ataques de ransomware expõem fragilidades nas defesas cibernéticas das organizações, demandando investimentos adicionais em tecnologia e processos de segurança. Vale ressaltar que pagar o resgate não garante a eliminação do risco, podendo até mesmo incentivar novos ataques.

Por outro lado, os vazamentos de dados também impõem sérios desafios às empresas, refletidos em custos substanciais que ultrapassam as sanções regulatórias. A detecção, notificação e resposta pós-violação demandam recursos significativos, enquanto o tempo necessário para contenção e mitigação do incidente prolonga ainda mais o impacto financeiro e reputacional.

Diante desse panorama alarmante, é imperativo que as empresas adotem medidas proativas para fortalecer suas defesas cibernéticas, cumprindo rigorosamente as disposições da LGPD e investindo em cultura de proteção de dados. Somente assim poderão mitigar os riscos e reduzir os custos associados aos incidentes de violação de dados, garantindo a proteção dos dados dos clientes e preservando sua reputação no mercado cada vez mais digital e interconectado.

A referida pesquisa buscou mostrar de forma clara uma análise concisa e os desafios da LGPD ao longo dos anos. Entre os obstáculos enfrentados pelas organizações, destaca-se a compreensão completa dos princípios e abrangência da LGPD. Muitas empresas ainda lutam para entender a extensão do termo "tratamento de dados pessoais", o que é essencial para garantir a conformidade.

A necessidade de estabelecer uma cultura forte em relação a proteção de dados é outro desafio destacado, uma vez que a privacidade ainda não está totalmente enraizada na cultura organizacional de muitas empresas. Para garantir a integridade dos dados, é fundamental desenvolver uma cultura de governança de dados, incorporando medidas operacionais e de segurança da informação.

Na última análise, uma jornada rumo à conformidade com a LGPD é essencial para proteger a privacidade e os direitos dos indivíduos em um mundo digital em constante evolução. As empresas enfrentam desafios complexos, mas ao superá-los, podem construir confiança com os internautas, melhorar sua confiança e obter uma vantagem competitiva. A adaptação à LGPD não é apenas uma obrigação legal, mas também uma oportunidade para promover práticas responsáveis de tratamento de dados.

Os reflexos da implementação da LGPD são evidentes no cotidiano, manifestando-se principalmente nas constantes solicitações de autorização em sites e aplicativos. Frequentemente, nos deparamos com a necessidade de consentir novamente com as políticas de privacidade atualizadas ou com o uso de cookies por essas plataformas. Essa abordagem tornou-se comum, e hoje já estamos familiarizados com essa prática em diversas páginas e aplicativos que utilizamos. Um dos impactos mais notáveis da LGPD é a introdução da possibilidade de solicitar a exclusão de dados. Antigamente, a internet era comparada a um espaço onde as informações eram gravadas a caneta, dada a dificuldade de remover dados uma vez inseridos nas plataformas digitais. No entanto, essa realidade mudou com a nova legislação. Agora, o titular tem o direito de remover suas informações a qualquer momento, uma prerrogativa que os sites devem facilitar, proporcionando aos usuários maior controle sobre seus dados pessoais. Essa mudança representa uma significativa evolução no respeito à privacidade online.

Percebe-se que a implementação da LGPD, está gradualmente se instalando no país surtindo seus efeitos de forma lenta porém constante, a implementação está sendo mais efetifiva no âmbito privado devido ao orgão fiscalizador ANPD, e apesar de apenas uma pequena quantidade realmente estar em conformidade com a lei geral de proteção de dados é importante analizar que tanto o executivo como o judiciário estão começando a terem mais atuação nessa área, o que se espera é que nos próximos cinco anos a lei já consiga atingir um número maior de empresas para que assim possamos ir vendo os pontos positivos e negativos da lei.

REFERÊNCIAS BIBLIOGRÁFICAS:

CAMBRAIA, Duda. Em 2021, Brasil ficou no topo de vazamento de informação no mundo, diz especialista, site: CNN Brasil, 2021, disponível em: https://www.cnnbrasil.com.br/tecnologia/em-2021-brasil-ficou-no-topo-de-vazamento-de-informacao-no-mundo-diz-especialista/. Acessado em: 29/08/2023).

KASPERSKY, O que é a Deep Web e a Dark Web?, disponível em: https://www.kaspersky.com.br/resource-center/threats/deep-web, acessado:03/09/2023.

LORENZETTI, Paola Luongo; CUNHA, Heloísa Helena de Paula. Desafios das empresas com a LGPD. Tech Compliance. Disponível em: https://techcompliance.org/desafios-das-empresas-com-a-lgpd/. Acessado: 28/08/2023

MINISTÉRIO DA ECONOMIA. (2020). Como se adequar à LGPD? Serpro. Disponivel em: https://www.serpro.gov.br/lgpd/governo/como-se-adequar-lgpd . Acessado: 28/08/2023

MORAES, Alexandre de. Direito constitucional. 30.ª edição. São Paulo: Atlas, 2014.

MOURA, Hugo. Relatório Axur: phishing cresce 99,23% em um ano, site: Blog Axur, disponível em: https://blog.axur.com/pt/relat%C3%B3rio-da-atividade-criminosa-online-no-brasil-q4-2020. Acessado em: 29/08/2023).

SCHWAB, Klaus. The Fourth Industrial Revolution**,** disponível em: https://www.foreignaffairs.com/world/fourth-industrial-revolution, acessado: 28/08/2023.
SILVA, Bruno. 2,29 bilhões de registros foram expostos em 2022 e Brasil lidera ranking de vazamentos, site: Security Report, disponível em: https://www.securityreport.com.br/229-bilhoes-de-registros-foram-expostos-em-2022-e-brasil-lidera-ranking-de-vazamentos/. Acessado em:29/08/2023).
HARARI, Yuval Noah. Homo Deus: uma breve história do amanhã. São Paulo. Editora Companhia das Letras, 2016.
Procon Estadual multa rede de farmácias por infração à Lei de Proteção de Dados Pessoais, site: Procon Mato Grosso, disponível em: https://www.procon.mt.gov.br/-/17501890-procon-estadual-multa-rede-de-farmacias-por-infracao-a-lei-de-protecao-de-dados-pessoais. Acessado em: 15/01/2024.

AGRADECIMENTOS

"O melhor mestre é aquele que mostra onde olhar, mas não te diz o que ver." – Alexandra K. Trenfor. É com essa frase que eu gostaria de iniciar agradecendo ao meu orientador Vicente Augusto, por todo o apoio que ele tem dado, cada incentivo e comentário foram importantes para a minha caminhada até este momento. Agradecer também aos meus pais que sempre me ajudaram e torceram por todos os meus sonhos.