REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO COMBATE AOS CRIMES DIGITAIS

THE IMPORTANCE OF THE GENERAL DATA PROTECTION LAW IN COMBATING DIGITAL CRIMES

Ciências Sociais Aplicadas • 15/05/2026

REGISTRO DOI: 10.70773/revistatopicos/778730899

Lucas Zanette Marquese[1]

Giulliano Ivo Batista Ramos[2]

RESUMO

Com o avanço da era digital no Brasil, a necessidade de regulamentar a privacidade no ambiente virtual tornou-se cada vez mais urgente. Em resposta a essa demanda, foi promulgada a Lei Geral de Proteção de Dados (LGPD), que se destaca por sua abrangência e especificidade. Seu principal objetivo é proteger direitos fundamentais, como a liberdade, a privacidade e o desenvolvimento das pessoas naturais, além de exercer papel essencial no combate a crimes virtuais. A lei introduz novos direitos que garantem maior transparência no tratamento de dados e conferem mais controle ao titular sobre seu uso, dificultando ações maliciosas como fraudes e roubos de identidade. A proteção dos dados pessoais, conforme prevista na LGPD, contribui para a prevenção de crimes virtuais ao impor normas rigorosas de segurança da informação e responsabilizar as organizações por violações. Este trabalho analisa a implementação e a relevância da LGPD no Brasil, com metodologia baseada em uma análise detalhada da legislação e de seus impactos sociais, destacando a importância de uma regulamentação eficaz para proteger dados pessoais e prevenir crimes virtuais.

Palavras-chave: Lei Geral de Proteção de Dados; Privacidade; Brasil.

ABSTRACT

With the advancement of the digital era in Brazil, the need to regulate privacy in the virtual environment has become increasingly urgent. In response to this demand, the General Data Protection Law (LGPD) was enacted, standing out for its breadth and specificity. Its main objective is to protect fundamental rights such as freedom, privacy, and the development of natural persons, as well as to play an essential role in combating cybercrimes. The law introduces new rights that ensure greater transparency in data processing and grant

individuals more control over their personal information, hindering malicious actions such as fraud and identity theft. The protection of personal data, as established by the LGPD, contributes to preventing cybercrimes by imposing strict information security standards and holding organizations accountable for violations. This study analyzes the implementation and relevance of the LGPD in Brazil, using a methodology based on a detailed examination of the legislation and its social impacts, highlighting the importance of effective regulation to protect personal data and prevent cybercrimes.
Keywords: General Data Protection Law; Privacy; Brazil.

1. INTRODUÇÃO

Para que a Lei Geral de Proteção de Dados (LGPD) tenha uma aplicação efetiva, é crucial entender o contexto da sociedade informacional. A Internet e os avanços tecnológicos proporcionaram uma gama vasta de oportunidades e inovações para a sociedade. No entanto, esse progresso muitas vezes ultrapassa certos limites, resultando em uma invasão da privacidade individual.

Com frequência, ao pesquisar um produto ou serviço na Internet, observa-se que várias empresas começam a oferecer exatamente o que foi pesquisado. Não é incomum que, após conversas informais sobre um assunto de interesse, ao acessar plataformas como o Google, surjam anúncios relacionados ao que foi discutido. Essa situação revela uma forma de monitoramento que muitos consideram intrusiva.

Além disso, aposentados frequentemente recebem ligações de instituições financeiras oferecendo empréstimos consignados, muitas vezes antes mesmo de a aposentadoria ser oficialmente

deferida. Isso ocorre porque empresas como Google e Facebook empregam técnicas de filtragem e análise de palavras-chave para oferecer produtos e serviços com base nas informações que coletam sobre os usuários. Este fenômeno ressalta a necessidade urgente de regulamentação, como a LGPD, para proteger a privacidade dos indivíduos em um ambiente digital cada vez mais invasivo.

2. A LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) representa um marco significativo na transformação da cultura e do comportamento no que diz respeito à proteção de dados pessoais, promovendo benefícios para todos os envolvidos. Esta legislação surge como uma resposta necessária às frequentes ocorrências de invasão de privacidade e vazamentos de dados, que se tornaram cada vez mais comuns e preocupantes.

Na era da sociedade informacional, onde a internet e a tecnologia avançam rapidamente, a privacidade individual frequentemente é comprometida. A coleta e análise de dados têm se expandido exponencialmente, levando a um cenário em que informações pessoais são frequentemente usadas para fins comerciais, muitas vezes sem o consentimento adequado dos indivíduos. A LGPD visa exatamente corrigir essa situação, promovendo um ambiente onde os dados pessoais sejam tratados com o devido respeito e segurança.

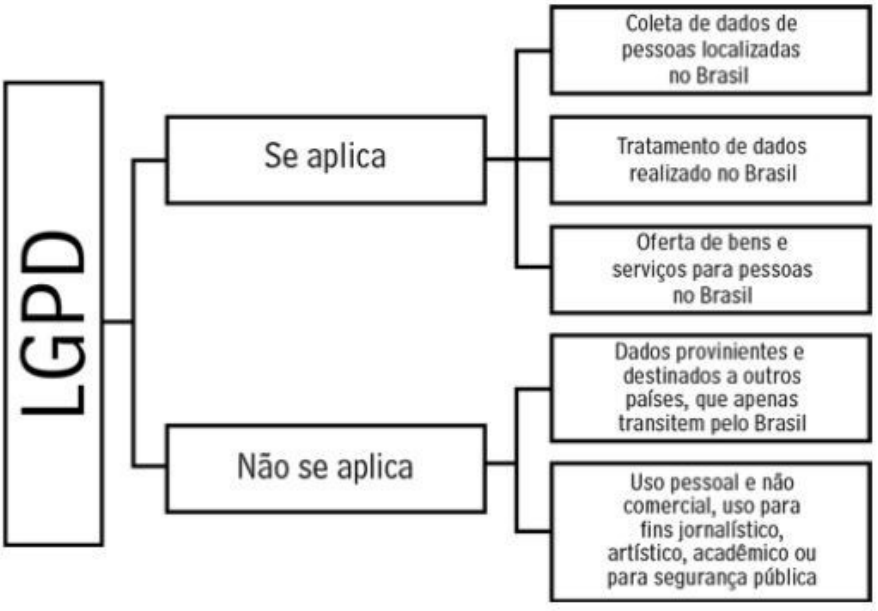
“A LGPD é uma resposta necessária às crescentes preocupações com a privacidade e segurança dos dados pessoais no Brasil. Sua implementação é crucial para proteger os direitos dos cidadãos e

promover um ambiente digital seguro e confiável.” (PINHEIRO, 2020).

A legislação estabelece que a proteção dos dados pessoais deve ser um princípio fundamental, proporcionando aos titulares dos dados o controle sobre suas informações e garantindo que o tratamento desses dados observe critérios de segurança adequados.

A legislação adota princípios como transparência, boa-fé e respeito à privacidade, refletindo a necessidade de um tratamento ético e responsável das informações.

Figura 1 – Organograma da LGPD.



Fonte: Viviane Porto. Descomplicando a Lei Geral de Proteção de Dados, 2023.

Inspirada na regulamentação europeia, contempla uma série de princípios, conceitos, direitos e deveres que orientam o tratamento de dados pessoais.

A Lei não busca obstruir o desenvolvimento econômico, tecnológico ou a inovação, mas sim garantir que essas atividades sejam

conduzidas de acordo com os princípios de proteção de dados, promovendo segurança jurídica e criando um ambiente propício ao crescimento sustentável.

E aplica-se a qualquer operação de tratamento realizada por pessoas naturais ou jurídicas, independentemente do meio ou local de operação, abrangendo dados pessoais coletados no território nacional.

2.1. Princípios Fundamentais da LGPD e a Governança de Dados

A eficácia da LGPD reside na aplicação de seus dez princípios, que devem nortear todo e qualquer tratamento de dados pessoais. Estes princípios não são meras diretrizes, mas sim pilares que estabelecem o padrão de governança de dados que as organizações devem seguir. Além da finalidade, adequação e necessidade, que garantem que o tratamento será restrito ao propósito informado ao titular, destacam-se:

Livre acesso no Direito dos titulares de consultar, de forma facilitada e gratuita, a integralidade de seus dados, bem como a forma e a duração do tratamento. Qualidade dos dados na garantia de que os dados sejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Transparência no fornecimento de informações claras, precisas e acessíveis sobre a realização do tratamento e os agentes de tratamento, observados os segredos comercial e industrial. SegurançaUtilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração,

comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Não discriminação: Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Responsabilização e prestação de contas (*Accountability*): Dever dos agentes de tratamento de demonstrar a adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. O princípio da Responsabilização e Prestação de Contas (*Accountability*) é particularmente relevante, pois exige que as empresas não apenas cumpram a lei, mas que sejam capazes de demonstrar esse cumprimento de forma proativa. Isso implica a criação de políticas internas, relatórios de impacto à proteção de dados (RIPD) e a manutenção de registros detalhados das operações de tratamento.

2.2. Atores da LGPD: Controlador, Operador e Encarregado

A LGPD define claramente os papéis e responsabilidades dos agentes de tratamento, estabelecendo uma cadeia de responsabilidade que visa garantir a proteção dos dados em todas as etapas do ciclo de vida da informação.

Controlador: É a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O Controlador é o principal responsável pela

conformidade com a lei e por definir a finalidade e os meios do tratamento.

Operador: É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador, seguindo suas instruções. O Operador responde solidariamente em caso de descumprimento das obrigações da LGPD se agir em desconformidade com as instruções lícitas do Controlador ou se a lei for descumprida por sua culpa exclusiva.

Encarregado de Proteção de Dados (DPO - *Data Protection Officer*): Atua como o principal canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Sua indicação é obrigatória para a maioria das organizações, e suas funções incluem orientar os funcionários sobre as práticas de proteção de dados e receber reclamações e comunicações dos titulares.

A clareza na definição desses papéis é crucial para a aplicação das sanções e para a responsabilização em caso de incidentes de segurança, como vazamentos de dados.

2.3. A Autoridade Nacional de Proteção de Dados

A Autoridade Nacional de Proteção de Dados (ANPD) é a entidade responsável pela implementação, regulamentação e fiscalização da LGPD no Brasil. Com autonomia técnica e decisória, a ANPD possui a incumbência de zelar pela conformidade com a legislação, aplicar sanções e promover a educação sobre proteção de dados. A entidade também regulamenta e fiscaliza o cumprimento da Lei, disponibilizando guias e outros documentos técnicos, e realizando

consultas públicas para obter contribuições sobre temas a serem regulamentados.

Desde março de 2023, a ANPD tem publicado uma lista de processos sancionatórios, detalhando as condutas e status dos processos em andamento. O encarregado de proteção de dados, ou Data Protection Officer (DPO), é a pessoa responsável por gerenciar a proteção de dados dentro da empresa, garantindo comunicação eficaz com a autoridade e com os titulares dos dados.

A identidade e os dados de contato do encarregado devem ser divulgados de forma clara e acessível, nesse sentido, a Lei Geral de Proteção de Dados, ao promover a proteção dos dados pessoais, não visa restringir a livre iniciativa ou a concorrência, mas assegurar que o tratamento de dados seja realizado de maneira legítima e transparente. Este princípio está alinhado com o Código de Defesa do Consumidor, que já destacava a importância da transparência e da harmonia nas relações de consumo, harmonizando a proteção do consumidor com o desenvolvimento econômico e tecnológico. Assim, a Lei representa um avanço crucial para a proteção de dados pessoais, estabelecendo uma base sólida para um ambiente digital mais seguro e respeitoso com a privacidade dos indivíduos.

3. A LEI Nº 14.155/2021: O REFORÇO PENAL NO COMBATE AOS CRIMES CIBERNÉTICOS

A Lei nº 14.155, promulgada em 2021, representa um marco crucial no endurecimento da legislação penal brasileira contra os crimes cibernéticos, atuando como um complemento direto à abordagem preventiva e sancionatória da LGPD. Enquanto a LGPD foca na proteção dos dados e na responsabilização administrativa das

empresas por falhas de segurança, a Lei 14.155 atua na esfera penal, punindo de forma mais rigorosa os indivíduos que praticam as fraudes. As principais alterações introduzidas pela Lei 14.155/2021 no Código Penal (Decreto-Lei nº 2.848/1940) foram:

Invasão de Dispositivo Informático (art. 154-A): A lei alterou a redação do Art. 154-A, que trata da invasão de dispositivo informático de uso alheio. A pena foi aumentada para reclusão de 1 (um) a 4 (quatro) anos, e multa, se a invasão for com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário, ou de instalar vulnerabilidades para obter vantagem ilícita. A pena é ainda maior (reclusão de 2 a 5 anos) se a invasão resultar em prejuízo econômico.

Furto Mediante Fraude Eletrônica (Art. 155, § 4º-B): Foi introduzida uma nova modalidade de furto qualificado: o furto mediante fraude eletrônica. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto for cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso. A lei prevê ainda um aumento de pena de 1/3 (um terço) a 2/3 (dois terços) se o crime for praticado mediante a utilização de servidor mantido fora do território nacional, o que visa combater a impunidade de criminosos que utilizam a infraestrutura internacional para cometer delitos no Brasil.

Estelionato praticado por meio eletrônico (ART. 171, § 2º-A): A Lei 14.155/2021 criou a figura do estelionato praticado por meio eletrônico, com pena de reclusão de 4 (quatro) a 8 (oito) anos, e multa. Este crime ocorre quando a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro

induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento (*phishing*), ou por qualquer outro meio fraudulento análogo.

A combinação da LGPD e da Lei 14.155/2021 estabelece um duplo mecanismo de proteção: a LGPD exige que as empresas adotem medidas preventivas e as responsabiliza administrativamente por falhas, enquanto a Lei 14.155/2021 pune criminalmente os indivíduos que exploram essas falhas ou que agem diretamente contra os titulares de dados.

A governança de dados e a cultura de privacidade: A simples existência de leis como a LGPD e a Lei 14.155/2021 não garante, por si só, a segurança dos dados. É fundamental que as organizações desenvolvam uma cultura de privacidade e implementem um robusto programa de governança de dados.

A governança de dados refere-se ao conjunto de processos, políticas, padrões e métricas que garantem que os dados sejam gerenciados de forma eficaz e segura em toda a organização. No contexto da LGPD, isso significa:

Mapeamento de Dados: Identificar quais dados pessoais são coletados, onde são armazenados, como são tratados e por quanto tempo são mantidos.

Avaliação de Risco: Realizar o Relatório de Impacto à Proteção de Dados (RIPD) para avaliar os riscos de privacidade e segurança inerentes às operações de tratamento.

Medidas de Segurança: Implementar medidas técnicas (como criptografia, *firewalls* e sistemas de detecção de intrusão) e

administrativas (como treinamento de funcionários e políticas de acesso) para proteger os dados.

Resposta a Incidentes: Estabelecer um plano de resposta a incidentes de segurança, que inclua a notificação rápida à ANPD e aos titulares dos dados em caso de vazamento.

A cultura de privacidade, por sua vez, é a internalização dos princípios da LGPD por todos os colaboradores da empresa. Ela transforma a proteção de dados de uma obrigação legal em um valor organizacional, reduzindo significativamente o risco de incidentes causados por erro humano.

4. O IMPACTO DA INTELIGÊNCIA ARTIFICIAL E OS DESAFIOS PARA A LGPD

A ascensão da Inteligência Artificial (IA) generativa e de outros sistemas algorítmicos apresenta novos e complexos desafios para a proteção de dados, exigindo uma reinterpretação dos princípios da LGPD.

Modelos de IA são treinados com volumes massivos de dados, muitas vezes coletados da internet, o que levanta questões sobre a legalidade dessa coleta e o cumprimento dos princípios da LGPD, como a finalidade e a transparência. O uso de dados pessoais para treinar algoritmos sem o consentimento explícito dos titulares é uma área de grande debate jurídico.

Além disso, a utilização de sistemas de IA para tomada de decisões automatizadas que afetam os indivíduos (como análise de crédito, seleção de candidatos a vagas de emprego ou sentenças judiciais) exige uma atenção especial. A LGPD garante aos titulares o direito à

revisão de decisões tomadas unicamente com base em tratamento automatizado de dados. A complexidade dos algoritmos (o chamado “problema da caixa-preta”) pode dificultar a explicação sobre como uma decisão foi tomada, tornando o cumprimento desse direito um desafio técnico e jurídico.

4.1. A Regulamentação da IA e a LGPD

A regulamentação do uso da IA, que já está em discussão no Congresso Nacional, deverá dialogar com a LGPD para garantir que a inovação tecnológica não ocorra em detrimento dos direitos fundamentais. A futura legislação de IA no Brasil deverá estabelecer diretrizes para a minimização de dados, a garantia de *fairness* (justiça) e a auditabilidade dos sistemas de IA, complementando o arcabouço legal da LGPD.

5. EVOLUÇÃO DOS CRIMES DIGITAIS

A evolução dos crimes digitais no Brasil tem sido marcada por um aumento significativo tanto em volume quanto em sofisticação. Inicialmente, as infrações digitais no país eram relativamente simples, focando principalmente em fraudes bancárias e invasões de sistemas para obtenção de informações pessoais. No entanto, com o avanço da tecnologia e a maior disseminação da internet, os criminosos digitais passaram a utilizar métodos mais complexos.

Nos últimos anos, houve uma intensificação nos esforços governamentais e privados para combater esses crimes. A promulgação do Marco Civil da Internet, em 2014, e a Lei Geral de Proteção de Dados (LGPD), em 2018, são exemplos de marcos legais importantes que visam regulamentar e proteger os dados dos usuários, além de estabelecer penalidades para infrações digitais.

Esses esforços têm sido complementados por iniciativas de conscientização e educação sobre segurança digital para a população.

Sobre a evolução dos crimes digitais e a LGPD, Danilo Doneda:

> *A evolução dos crimes digitais tem desafiado constantemente as estruturas de segurança cibernética. A LGPD, ao estabelecer normas rigorosas de proteção de dados, busca mitigar esses desafios e oferecer um framework para a prevenção e resposta a incidentes de segurança. (DONEDA, 2021)*

Apesar dessas medidas, os criminosos digitais continuam a inovar e adaptar suas táticas, o que exige uma vigilância constante e uma adaptação contínua das estratégias de segurança cibernética no Brasil. Nesse sentido, Laura Schertel Mendes afirma: "A LGPD estabelece um marco regulatório fundamental para a segurança da informação no Brasil, servindo como uma ferramenta crucial na prevenção de crimes digitais ao impor rigorosos requisitos de proteção de dados." (MENDES, 2019).

Os crimes digitais relacionados ao roubo de dados são uma preocupação crescente na era digital. Esses delitos podem ter consequências significativas tanto para indivíduos quanto para organizações. Entre eles, destacam-se os crimes de phishing e ransomware.

5.1. Phishing

Trata-se de uma técnica de engenharia social na qual criminosos enganam as vítimas para obter informações sensíveis, como senhas e dados bancários, geralmente por meio de emails fraudulentos ou sites falsificados. O objetivo é roubar credenciais de login e informações pessoais para realizar fraudes financeiras ou obter acesso não autorizado a contas.

Neste contexto, ressalta-se a importância da conscientização e da educação dos indivíduos em relação à proteção de seus próprios dados.

5.2. Ransomware

O *ransomware* é um tipo de malware que criptografa os dados da vítima, tornando-os inacessíveis, e exige um resgate em dinheiro para sua liberação. O objetivo é extorquir dinheiro das vítimas em troca da recuperação dos dados comprometidos. Esse contexto destaca a importância de investir em sistemas de segurança robustos.

Com a implementação da Lei Geral de Proteção de Dados (LGPD), criminosos têm se aproveitado de empresas com sistemas de segurança pouco eficazes para realizar chantagens, eles expõem falhas na segurança, mostrando a desconformidade com as exigências da Lei o que implica em multas pela Agência Nacional de Proteção de Dados (ANPD).

Dessa forma, a empresa se torna refém do criminoso, que inicia a chantagem. Dada a gravidade das multas previstas pela LGPD, que podem atingir até R$ 50 milhões, muitas empresas, em desespero, acabam optando por ceder às exigências dos criminosos e pagar um valor menor como forma de evitar maiores prejuízos. Sobre as

implicações dos ataques de ransomware e a LGPD, Eduardo Pereira Maroso:

> *Os ataques de ransomware destacam a importância de uma conformidade robusta com a LGPD. As organizações precisam implementar medidas de segurança adequadas para proteger dados pessoais e evitar as graves consequências legais que podem advir de falhas na segurança. (MAROSO, 2021).*

Além disso, os ataques de *ransomware* evidenciam a necessidade de uma cultura organizacional voltada à proteção de dados. Não basta apenas investir em tecnologia; é fundamental que as empresas promovam a conscientização e o treinamento contínuo de seus colaboradores, garantindo que todos compreendam a importância da segurança da informação e do cumprimento das normas estabelecidas pela LGPD.

6. E SE A EMPRESA NÃO SEGUIR A LGPD?

As organizações que não cumprirem os requisitos estabelecidos pela Lei Geral de Proteção de Dados (LGPD) estarão sujeitas a penalidades financeiras rigorosas. As empresas podem ser multadas em até 2% do faturamento total da pessoa jurídica, com um limite de R$ 50 milhões por infração. As organizações também podem sofrer outras sanções, como o bloqueio ou a perda de acesso aos seus dados. As penalidades previstas pela LGPD são severas e as multas substanciais, com o intuito de assegurar que as empresas se adaptem e cumpram integralmente a legislação.

As empresas também ficarão sujeitas à fiscalização e eventual responsabilização pelo Ministério Público e Procon, que podem, até mesmo, ajuizar ações judiciais para a apuração de dados coletivos. Nesses casos, as penalidades podem ser extremamente altas, uma vez que visam a indenização da comunidade afetada.

Sobre o impacto financeiro das multas: "As sanções financeiras impostas pela LGPD, com limites significativos para as infrações, servem como um mecanismo de coação para garantir que as organizações adotem práticas rigorosas de proteção de dados." (MENDES, 2020). E, no que concerne a importância da conformidade, Laura Schertel Mendes:

> *A não conformidade com a LGPD não só expõe a empresa a penalidades financeiras, mas também pode resultar em perda de reputação e confiança dos consumidores. A adequação à lei é fundamental para a proteção dos dados pessoais e a continuidade dos negócios. (MENDES, 2020).*

Dessa forma, observa-se que a conformidade com a LGPD vai além do simples cumprimento legal — trata-se de uma estratégia essencial para a sustentabilidade empresarial. Ao investir em políticas de governança e segurança da informação, as organizações não apenas evitam penalidades severas, mas também fortalecem sua credibilidade no mercado e consolidam a confiança dos consumidores.

6.1. Netshoes Sofre Novo Ataque Hacker e Exposição de Dados de Clientes

Recentemente, a Netshoes, adquirida pela Magazine Luiza, sofreu um novo ataque cibernético que resultou na exposição de dados de clientes. Na publicação relacionada ao incidente, um usuário anexou uma captura de tela que revela dados pessoais de pelo menos 100 brasileiros, incluindo nome completo, CPF, número de telefone, endereço completo, e informações sobre pedidos e entregas.

A Netshoes confirmou o vazamento de dados ao jornal Valor Econômico, mas não divulgou o volume total de dados expostos. A empresa informou que está conduzindo uma investigação forense em colaboração com a Autoridade Nacional de Proteção de Dados (ANPD) para elucidar as circunstâncias do ataque. A companhia também afirmou que o incidente não impactou as operações e que os dados sensíveis não foram comprometidos.

Este não é o primeiro episódio de vazamento de dados envolvendo a Netshoes. Em 2019, a empresa havia fechado um acordo com o Ministério Público do Distrito Federal para pagar R$ 500 mil ao Fundo de Defesa de Direitos Difusos (FDD) devido ao vazamento de dados de quase 2 milhões de clientes no ano anterior.

A aquisição da Netshoes pela Magazine Luiza, ocorrida em 2019 por US$ 62 milhões, seguiu-se à queda significativa de valor da empresa. Originalmente, a Netshoes havia alcançado uma avaliação de US$ 1 bilhão em 2017, após sua abertura de capital, mas dois anos depois, seu valor despencou para aproximadamente US$ 65 milhões.

A repercussão do vazamento de dados em 2018 prejudicou a imagem da empresa, que acabou sendo vendida tanto no Brasil

quanto na Argentina, onde estava sediada. Essa é uma consequência direta que uma empresa pode sofrer ao não investir em padrões elevados de segurança. "A não conformidade com a LGPD pode resultar em danos significativos à reputação da empresa, afetando sua capacidade de manter e atrair clientes" (MAROSO, 2021).

6.2. Apagão Cibernético

No dia 19 de julho de 2024, um incidente significativo evidenciou a vulnerabilidade da economia global e sua dependência crítica de sistemas de computação. Esse evento desencadeou um apagão que afetou uma ampla gama de serviços, incluindo aplicativos bancários, aeroportos, sistemas ferroviários e diversos outros serviços dependentes da internet em escala global. E embora o colapso não tenha sido causado por um agente malicioso, seu impacto foi significativo.

O cenário caótico ressaltou a interconexão e a fragilidade dos sistemas tecnológicos modernos, levando autoridades governamentais ao redor do mundo a refletirem sobre as possíveis consequências de um ataque cibernético efetivo.

A internet, que inicialmente se apresentou como uma ferramenta facilitadora no cotidiano, tornou-se indispensável para a sociedade atual, um entendimento que se fortaleceu diante dos numerosos impactos resultantes do apagão.

7. CONCLUSÃO

A Lei Geral de Proteção de Dados (LGPD) consolidou-se como um pilar fundamental na defesa dos direitos de personalidade na era

digital brasileira. Sua importância transcende a mera regulamentação do tratamento de dados, estabelecendo-se como um instrumento de prevenção e combate aos crimes cibernéticos. Ao impor rigorosos padrões de segurança, transparência e accountability às organizações, a LGPD atua na raiz do problema, dificultando a coleta e o uso indevido de informações que alimentam fraudes como phishing, ransomware e outros delitos digitais que ameaçam a integridade informacional.

A LGPD, em conjunto com o endurecimento da legislação penal promovido pela Lei nº 14.155/2021, cria um arcabouço jurídico robusto e coerente que aborda a segurança de dados em múltiplas esferas: administrativa, civil e penal. Essa interação entre as normas permite não apenas a punição de condutas ilícitas, mas também a construção de um ambiente digital mais ético, seguro e orientado à responsabilidade. Nesse contexto, a atuação da Autoridade Nacional de Proteção de Dados (ANPD) ganha relevância ao exercer o poder fiscalizatório e sancionador, além de promover a conscientização e o desenvolvimento de boas práticas nas empresas e órgãos públicos, fortalecendo a cultura da proteção de dados no Brasil.

A consolidação dessa cultura demanda não apenas a adequação técnica das instituições, mas também uma transformação comportamental, na qual o respeito à privacidade e à segurança da informação se torne parte essencial da gestão organizacional. Os desafios impostos pela evolução tecnológica, como a ascensão da Inteligência Artificial, da Internet das Coisas (IoT) e do Big Data, exigem uma constante atualização da legislação e dos mecanismos de controle. Ainda assim, a base normativa e principiológica estabelecida pela LGPD constitui o alicerce indispensável para que o

avanço tecnológico ocorra de forma ética, transparente e em conformidade com os direitos fundamentais dos cidadãos.

Assim, a conformidade com a LGPD não deve ser vista apenas como uma obrigação legal, mas como um investimento estratégico que protege a reputação institucional, assegura a confiança dos consumidores e garante a sustentabilidade das operações no ambiente digital. A observância dessa legislação representa, portanto, um compromisso com a cidadania digital, a inovação responsável e o fortalecimento do Estado Democrático de Direito na era da informação.

REFERÊNCIAS BIBLIOGRÁFICAS

CANTO DE LIMA, Ana Paula Moraes; ALMEIDA, Dionice; MAROSO, Eduardo Pereira. **LGPD - Lei Geral de Proteção de Dados: sua empresa está pronta?** Literare Books, 2023.

CNN BRASIL. **Apagão cibernético: como a tecnologia mundial caiu de uma só vez.** Disponível em: https://www.cnnbrasil.com.br/internacional/apagao-cibernetico-como-atecnologia-mundial-caiu-de-uma-so-vez/. Acesso em: 24 jul. 2024.

CONVERGÊNCIA DIGITAL. **Crimes na web: Brasil teve seis contas violadas por minuto em 2023.** Disponível em: https://www.convergenciadigital.com.br/Seguranca/Crimes-na-Web%3A-Brasil-teve-seis-contas-violadas-por-minuto-em-2023-65329.html?UserActiveTemplate=mobile#:~:text=O%20mais%20recente%20estudo%20da,progressivamente%20ao%20longo%20dos%20anos. Acesso em: 24 jul. 2024.

CONVERGÊNCIA DIGITAL. **Netshoes, da Magazine Luiza, sofre novo ataque hacker: Milhares de dados de clientes são expostos.** Disponível em: https://www.convergenciadigital.com.br/Seguranca/Netshoes%2C-da-Magazine-Luiza%2Csofre-novo-ataque-hacker.-Milhares-de-dados-de-clientes-sao-expostos66518.html?UserActiveTemplate=mobile. Acesso em: 24 jul. 2024.

DONEDA, Danilo. **Proteção de Dados e Privacidade: Aspectos Jurídicos e Práticos.** São Paulo: Editora Revista dos Tribunais, 2021.

FLOWTI. **A importância da LGPD no combate aos cibercrimes.** Disponível em: https://flowti.com.br/blog/a-importancia-da-lgpd-no-combateaoscibercrimes#:~:text=tudo%20neste%20artigo.-,A%20LGPD%20também%20está%20relacionada20ao%20combate%20aos%20cibercrimes.,ao%20vazamento%20de%20dados%20pessoais. Acesso em: 24 jul. 2024.

MAROSO, Eduardo Pereira. **Lei Geral de Proteção de Dados: Comentários e Análises.** Curitiba: Juruá Editora, 2021.

MENDES, Laura Schertel. P**rivacidade e Proteção de Dados Pessoais: A LGPD e a Constituição.** Brasília: XYZ Editora, 2019.

MENDES, Laura Schertel. **Privacidade e Proteção de Dados Pessoais: Comentários à Lei Geral de Proteção de Dados.** Rio de Janeiro: Editora Forense, 2020.

NAKAMURA, J. **E-commerce brasileiro perdeu R$ 65 milhões em vendas na madrugada do apagão cibernético, diz Neotrust.** Disponível em: https://www.cnnbrasil.com.br/economia/negocios/e-commerce-brasileiro-perdeu-r-65milhoes-em-vendas-na-

madrugada-do-apagao-cibernetico-diz-neotrust/. Acesso em: 25 jul. 2024.

PINHEIRO, Patrícia Peck. P**roteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD).** 2. ed. São Paulo: Saraiva Jur, 2020.

PORTO, Viviane de Araujo. **Descomplicando a Lei Geral de Proteção de Dados.** 1. ed. Goiânia: OM Edições, 2019. p. 12.

Trabalho de conclusão de curso, apresentado ao curso de Direito do Centro Universitário de Santa Fé do Sul- SP – UNIFUNEC.

[2] Discente do curso de Direito da UNIFUNEC, Centro Universitário de Santa Fé do Sul – SP. RM: 40147 - E-mail: acesse o artigo original para visualizar o e-mail

[3] Docente do Centro Universitário de Santa Fé do Sul – SP, UNIFUNEC