10º Encontro de Ensino Pesquisa e Extensão

Patrocínio, MG, outubro de 2023

DESAFIOS PESSOAIS NOS INCIDENTES DE SEGURANÇA E VAZAMENTOS DE DADOS EM REDES WI-FI PÚBLICAS SOB O ESCOPO DA LGPD

Larissa Hevelyn Santos, Júnio Moreira
<larissa.hevelyn@estudante.iftm.edu.br>,<juniomoreira@iftm.edu.br>
Instituto Federal do Triângulo Mineiro
Modalidade: Pesquisa
Formato: Artigo Completo

Resumo

A Lei Geral de Proteção de Dados (LGPD) estabeleceu regulamentações rigorosas para o tratamento de informações pessoais no contexto empresarial. Este artigo investiga os desafios pessoais enfrentados por indivíduos em incidentes de segurança e vazamentos de dados sob o escopo da LGPD. Tais incidentes representam uma ameaça crescente à privacidade dos dados. Neste contexto, o artigo explora as responsabilidades das empresas de acordo com a LGPD, incluindo a notificação às autoridades e aos indivíduos afetados. Além disso, destaca a importância crítica da implementação de medidas preventivas e planos de resposta em conformidade com os requisitos da LGPD. Os resultados destacam a necessidade de avaliação de impacto à privacidade e práticas de segurança sólidas para garantir a conformidade contínua com a LGPD.

Palavras-chaves: LGPD. Incidentes de Segurança. Vazamentos de Dados. Privacidade de Dados. Medidas Preventivas. Redes Wi-fi Públicas.

Introdução

Ao longo dos séculos, a humanidade tem buscado incessantemente maneiras de aprimorar seu ambiente, ainda que esteja limitada pelas restrições da natureza (GALHARDO, 2022). Contudo, com o avanço tecnológico e a crescente interconexão global proporcionada pela Internet, bem como a disseminação de meios de comunicação,

redes sociais, aplicativos bancários e outras plataformas, a enorme quantidade de dados coletados, transmitidos e compartilhados tornou incontestável a necessidade da Lei Geral de Proteção de Dados (LGPD). Promulgada em setembro de 2020 e em vigor desde setembro de 2021, essa legislação foi concebida com o objetivo primordial de proteger e assegurar a privacidade dos cidadãos, estabelecendo diretrizes rigorosas para o tratamento de informações pessoais.

A LGPD foi uma resposta essencial a uma preocupação global, sendo particularmente urgente no Brasil. De acordo com (GALHARDO, 2022), a tecnologia é uma vitória da humanidade diante das dificuldades impostas pela natureza, e por isso, cada conquista e avanço tecnológico sempre foram amplamente aceitos e valorizados. Mas em decorrência de seu mau uso, o país tem testemunhado inúmeros casos de vazamento de dados, frequentemente vinculados a fraudes bancárias.

Para manterem-se conectadas, muitas pessoas optam por usar redes Wi-Fi públicas, mas ao fazê-lo, muitas vezes ficam vulneráveis. Inúmeras ameaças digitais e cibercriminosos operam por trás dessas redes, muitas vezes disfarçando-se com sites legítimos, o que pode resultar na infiltração de malware. Além disso, existe o risco substancial de que os dados e informações compartilhados por meio dessas redes sejam interceptados e comprometidos, conforme relata (EVAL, 2022).

Neste estudo, examinaremos os riscos associados a essas redes públicas, investigando suas causas e os efeitos resultantes do seu uso. Apresentaremos relatos de experiências de usuários que, lamentavelmente, tiveram seus dados vazados e expostos, incluindo informações sensíveis como o CPF (Cadastro de Pessoa Física), tornando-as acessíveis a qualquer pessoa. Além disso, examinaremos o que a Lei Geral de Proteção de Dados (LGPD) dispõe sobre esse assunto e como ela está sendo aplicada para proteger os usuários.

Nosso objetivo é esclarecer os desafios intrínsecos à proteção de dados em redes Wi-Fi públicas sob o escopo da LGPD e ressaltar a necessidade premente de avaliação de impacto à privacidade e práticas de segurança sólidas para garantir a conformidade contínua com esta legislação. À medida que o cenário de cibersegurança continua a evoluir, é imperativo que empresas e indivíduos estejam preparados para enfrentar os desafios que surgem no contexto da LGPD e das redes Wi-Fi públicas, a fim de

preservar a confidencialidade e integridade das informações pessoais em um mundo cada vez mais conectado.

Fundamentação Teórica

A privacidade é um conceito amplamente discutido e abrange elementos fundamentais, como a dignidade humana, liberdade e independência individual, bem como o controle sobre o uso e abuso de informações pessoais (SAAD, 2021). A Lei Geral de Proteção de Dados (LGPD) foi estabelecida com o propósito duplo de proteger nossas informações pessoais e reafirmar nosso direito à privacidade, ao mesmo tempo em que conscientiza sobre os crescentes crimes cibernéticos. Essa abordagem está alinhada com a visão do professor Tarcísio Teixeira, que enfatiza a importância da proteção da intimidade do titular, especialmente quando se trata de dados pessoais sensíveis (TEIXEIRA, 2020).

Este capítulo se propõe a explorar os fatores que transformam uma rede Wi-Fi pública em uma armadilha potencialmente perigosa, especialmente para ataques bancários. Conectar-se a uma rede Wi-Fi não segura, a redes com software de roteador desatualizado ou a roteadores Wi-Fi configurados inadequadamente pode representar uma séria ameaça à segurança (EVAL, 2022). Usuários que negligenciam medidas de segurança, redes sem senhas ou com proteções fracas estão oferecendo oportunidades ideais para cibercriminosos invadirem a privacidade e vazarem dados sensíveis.

De acordo com a pesquisa de (EVAL, 2022), para garantir sua segurança, é altamente recomendável o uso de um aplicativo de VPN (Rede Virtual Privada). Essa ferramenta tem a capacidade de mascarar o endereço IP e criptografar todos os dados transmitidos, aumentando significativamente a segurança. Além disso, é aconselhável contar com um programa antivírus capaz de proteger contra uma variedade de malwares. A ativação de um firewall também é essencial, pois impede o acesso não autorizado ao seu dispositivo pessoal.

No entanto, ao se conectar a uma rede pública, é fundamental evitar o acesso a aplicativos que contenham informações sigilosas, especialmente relacionadas a transações bancárias (EVAL, 2022). Um exemplo notável de vulnerabilidade de segurança

foi o ataque à empresa americana SolarWinds, que desenvolve softwares para a gestão de redes, sistemas e infraestrutura de TI de outras empresas. Este ataque, atribuído a hackers russos, afetou cerca de 18 mil clientes e se tornou um dos incidentes mais impactantes na história da cibersegurança (TECHTUDO, 2020).

Mesmo no contexto da pandemia de COVID-19, até o Ministério da Saúde enfrentou vulnerabilidades de segurança e incidentes de segurança (TECHTUDO, 2020). Dados de mais de 243 milhões de brasileiros foram expostos, incluindo informações pessoais até dados cadastrais.

Diante deste cenário alarmante de comprometimento e violação da privacidade, com milhares de incidentes de segurança e vazamentos de dados, até mesmo em grandes empresas, torna-se imperativo adotar medidas preventivas. A LGPD (Lei nº 13.709), conforme destacado por (RAPÔSO et al., 2019), foi promulgada para assegurar e garantir a privacidade dos dados de terceiros.

A LGPD nivelou o Brasil com nações que já adotaram medidas semelhantes, solucionando problemas críticos, uma vez que antes não havia regulamentação clara para a proteção da privacidade dos cidadãos e a aplicação da jurisdição em casos de solicitação de informações (GALHARDO, 2022).

Neste contexto, diversas pesquisas têm sido conduzidas com o objetivo de compreender e abordar a complexa questão da segurança cibernética. No trabalho de (SANTOS, 2023), argumenta-se que a segurança de rede não é apenas uma questão técnica, mas também uma preocupação de governança empresarial, dada a vulnerabilidade das empresas a ataques cibernéticos. A pesquisa de (CANALTECH, 2021) destaca experiências negativas de usuários em redes públicas, reforçando a importância da proteção de dados. O artigo 5º, parágrafos I, IV, VII (REPÚBLICA, 2018) ressalta o respeito à privacidade e direitos humanos. O autor (FERREIRA, 2022) enfatiza a relevância crescente da LGPD em casos específicos, enquanto (CHAVES, 2022) destaca a importância da LGPD na imposição de penalidades para crimes cibernéticos.

Proposta

Este artigo se propõe a analisar os desafios e as implicações pessoais enfrentadas pelos indivíduos em incidentes de segurança e vazamentos de dados ocorridos em redes Wi-Fi públicas, dentro do contexto regulatório estabelecido pela Lei Geral de Proteção de Dados (LGPD) no Brasil. Abordaremos as questões relacionadas ao uso cada vez mais difundido dessas redes Wi-Fi públicas e os riscos associados a elas, com foco na exposição de informações pessoais e sensíveis dos usuários.

Neste estudo, adota-se uma abordagem baseada em métodos documentais para coletar e analisar os dados necessários para alcançar os objetivos de pesquisa. A coleta de dados concentrou-se em artigos acadêmicos e relatórios relacionados aos resultados de incidentes de segurança e vazamentos de dados que ocorreram no contexto da Lei Geral de Proteção de Dados (LGPD). O objetivo é investigar os desafios pessoais enfrentados por organizações e profissionais de segurança de dados ao lidar com tais incidentes.

Para atingir esses objetivos, adotaremos uma abordagem metodológica abrangente, combinando técnicas de pesquisa qualitativa e quantitativa. Nossa metodologia engloba as seguintes etapas fundamentais:

- Análise dos Riscos em Redes Wi-Fi Públicas: Estudaremos a compreensão dos riscos específicos que os usuários enfrentam ao utilizar redes Wi-Fi públicas. Este aspecto envolverá uma investigação de ameaças cibernéticas, como ataques de interceptação de dados e exposição a potenciais cibercriminosos.

- Exploração dos Impactos Pessoais e Sociais: Será realizada uma análise dos impactos pessoais, sociais e emocionais que indivíduos enfrentam quando têm seus dados pessoais comprometidos em incidentes de segurança. Além disso, examinaremos as implicações legais e financeiras que recaem sobre as empresas envolvidas nesses incidentes.

- Avaliação da Eficácia da LGPD: A eficácia da LGPD como marco regulatório de proteção de dados será avaliada. Isso incluirá a análise das disposições da LGPD relacionadas à proteção de dados em redes Wi-Fi públicas e a investigação das

responsabilidades que as empresas tem no que diz respeito à notificação das autoridades e dos indivíduos afetados.

- Destaque de Medidas de Prevenção e Resposta: Abordaremos estratégias para prevenir incidentes de segurança em redes Wi-Fi públicas e apresentaremos planos de resposta que as empresas podem implementar em conformidade com os requisitos da LGPD. Nosso foco é fornecer diretrizes claras para a minimização de riscos e para a eficaz proteção dos dados dos usuários.

Essa abordagem metodológica nos permitirá obter uma visão holística dos desafios e das soluções relacionados à proteção de dados em redes Wi-Fi públicas sob o escopo da LGPD. Ao combinar métodos qualitativos e quantitativos, estaremos melhor preparados para analisar a complexidade do cenário atual de cibersegurança e privacidade, oferecendo recomendações valiosas para empresas, formuladores de políticas e a comunidade em geral interessada na segurança dos dados pessoais.

Resultados

Apresentaremos os resultados de nossa pesquisa, que se concentrou em analisar os desafios pessoais enfrentados por indivíduos em incidentes de segurança e vazamentos de dados em redes Wi-Fi públicas sob o escopo da Lei Geral de Proteção de Dados (LGPD). A seguir, destacamos os principais resultados obtidos em cada uma dessas áreas:

Análise dos Riscos em Redes Wi-Fi Públicas

Nossa pesquisa revelou que as redes Wi-Fi públicas continuam sendo um terreno fértil para uma variedade de ameaças cibernéticas. Entre os principais riscos identificados estão: (1) Interceptação de Dados: Ficou evidente que os dados transmitidos por meio de redes Wi-Fi públicas estão suscetíveis a interceptações por parte de cibercriminosos; (2) Malware e Phishing: Observamos um aumento na disseminação de malware e ataques de phishing por meio de redes Wi-Fi públicas. Os usuários frequentemente são enganados para acessar sites falsos que visam roubar suas credenciais e dados pessoais;

e (3) Exposição a Redes Não Seguras: Muitas redes Wi-Fi públicas não implementam medidas de segurança adequadas, o que torna os usuários vulneráveis a ataques.

Exploração dos Impactos Pessoais e Sociais

Os impactos pessoais e sociais de incidentes de segurança e vazamentos de dados em redes Wi-Fi públicas são significativos: (1) Estresse e Ansiedade: Indivíduos afetados por vazamentos de dados relataram altos níveis de estresse e ansiedade, resultantes da perda de privacidade e da incerteza sobre o uso futuro de suas informações pessoais; (2) Prejuízos Financeiros: Algumas vítimas enfrentaram prejuízos financeiros significativos devido a fraudes bancárias e compras não autorizadas realizadas por terceiros; e (3) Desconfiança nas Tecnologias Digitais: Os incidentes abalaram a confiança dos usuários nas tecnologias digitais e nas empresas que coletam e armazenam seus dados.

Avaliação da Eficácia da LGPD

Ao analisar a eficácia da LGPD em proteger os dados dos usuários em redes Wi-Fi públicas, identificamos os seguintes pontos: (1) Responsabilidades das Empresas: A LGPD estabeleceu claramente as responsabilidades das empresas na proteção de dados pessoais. As organizações têm a obrigação de notificar as autoridades e os indivíduos afetados em caso de violação de dados; e (2) Desafios na Aplicação: No entanto, nossa pesquisa também apontou desafios na aplicação efetiva da LGPD, incluindo a falta de conscientização sobre a legislação e a capacidade limitada das autoridades para lidar com um grande número de violações.

Destaque de Medidas de Prevenção e Resposta

Identificamos medidas eficazes de prevenção e resposta que as empresas podem adotar para proteger os dados dos usuários em redes Wi-Fi públicas: (1) Implementação de Criptografia: A criptografia robusta nas redes Wi-Fi públicas é fundamental para proteger as comunicações dos usuários; (2) Educação e Conscientização: Promover a educação e a conscientização dos usuários sobre os riscos e as práticas seguras ao utilizar redes Wi-Fi públicas é crucial; e (3) Planos de Resposta a Incidentes: As

empresas devem desenvolver planos de resposta a incidentes bem elaborados para lidar eficazmente com violações de dados e garantir a conformidade com a LGPD.

Estes resultados destacam a complexidade dos desafios enfrentados por indivíduos em incidentes de segurança e vazamentos de dados em redes Wi-Fi públicas e enfatizam a necessidade contínua de medidas de proteção de dados e conscientização, bem como o fortalecimento da aplicação da LGPD para garantir a segurança e a privacidade dos usuários nesse cenário digital em constante evolução.

Considerações Finais

Ao longo deste estudo, presenciamos tristes relatos de usuários cuja privacidade foi violada, resultando em uma gama de emoções negativas, desconfiança e prejuízos para as empresas envolvidas. A entrada em vigor da LGPD (Lei Geral de Proteção de Dados) colocou o Brasil em sintonia com outros países, dada a urgência de uma legislação mais clara e proativa nesse domínio. No entanto, a implementação da LGPD ainda enfrenta inúmeros desafios, embora tenha trazido a promessa de um futuro mais promissor em relação às sanções para crimes cibernéticos, conforme enfatizado por (CHAVES, 2022) em seu artigo.

Neste contexto, é imperativo que medidas preventivas sejam adotadas, com um foco especial na conscientização da população, particularmente entre os idosos, sobre como proteger sua presença no mundo virtual em constante expansão. Como perspectiva futura, almejamos contribuir para o reforço da criptografia em redes Wi-Fi públicas, utilizando técnicas de inteligência artificial, como um passo adicional na promoção da segurança digital.

Esta pesquisa destaca a importância de se enfrentar os desafios da privacidade e da segurança cibernética no cenário brasileiro, e, ao abordar essas questões, esperamos que este estudo possa fornecer recomendações valiosas para aqueles envolvidos na proteção dos dados pessoais e na promoção de um ambiente virtual mais seguro para todos os usuários.

REFERÊNCIAS BIBLIOGRÁFICAS

CANALTECH. **Sistema de gerenciamento de Wi-Fi público expõe dados de 2 milhões de pessoas**. [S.l.: s.n.], 2021. Acessado em 26/09/2023. Disponível em: <https://canaltech.com.br/seguranca/sistema-de-gerenciamento-de-wi-fi-publico-expos-dados-de-2-milhoes-de-pessoas-202305/>.

CHAVES, M. E. d. A. O vazamento de dados sob a perspectiva da LGPD e sua correlação com os crimes cibernéticos., 2022.

EVAL. **Perigos da WiFi pública: dados de 2 milhões de usuários são vazados**. [S.l.: s.n.], 2022. Acessado em 26/09/2023. Disponível em: <https://eval.digital/perigos-da-wifi-publica-dados-de-2-milhoes-de-usuarios-sao-vazados/>.

FERREIRA, M. P. S. A responsabilidade civil no vazamento de dados pessoais, 2022.

GALHARDO, J. A. F. Lei geral de proteção de dados pessoais: desafios e perspectivas de sua implementação no Brasil, 2022.

RAPÔSO, C. F. L. et al. Lgpd-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. **RACE-Revista de Administração do Cesmac**, v. 4, p. 58–67, 2019.

REPÚBLICA, P. da. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. [S.l.: s.n.], 2018. Acessado em 27/09/2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>.

SAAD, C. d. O. A lei geral de proteção de dados pessoais e incidentes de segurança: regulação e prática de vazamento de dados, 2021.

SANTOS, I. Segurança de rede no ambiente corporativo, 2023.

TECHTUDO. **Relembre os oito maiores vazamentos de dados em 2020**. [S.l.: s.n.], 2020. Acessado em 26/09/2023. Disponível em: <https://www.techtudo.com.br/listas/2020/12/relembre-os-oito-maiores-vazamentos-de-dados-em-2020.ghtml>.

TEIXEIRA, T. **Direito digital e processo eletrônico**. [S.l.]: Saraiva Educação SA, 2020.