Insegurança do Usuário na Capacidade de Manipulação das Redes: Aplicação do Design Thinking no Contexto da Proteção de Dados

Thiago Reis Diniz Silva
thiiagoreis91@gmail.com

David de Oliveira Costa
dcosta.doc@gmail.com

Resumo

A escolha da temática de insegurança do usuário na capacidade de manipulação das redes digitais foi motivada por incidentes recentes de invasões cibernéticas que expuseram vulnerabilidades significativas. De acordo com um estudo realizado na Universidade Federal do Mato Grosso do Sul, as defasagens envolvendo crimes cibernéticos, falta de privacidade e cibersegurança têm crescido demasiadamente devido ao fácil acesso à tecnologia atual pela maioria dos usuários. A relevância desse tema é destacada pela crescente dependência das tecnologias digitais e a necessidade de proteger dados pessoais e profissionais. O estudo foi conduzido mediante revisão abrangente de evidências e depoimentos recentes pessoais e interpessoais, incluindo análises de artigos acadêmicos sobre crimes cibernéticos, privacidade e cibersegurança aliada à Metodologia *Design Thinking* (DT). A análise enfatizou a importância da educação digital e da conformidade com regulamentações como a LGPD para mitigar riscos e fortalecer a proteção de dados. Os resultados destacam a necessidade de estratégias proativas para criar um ambiente digital mais seguro e confiável. Este estudo buscou utilizar medidas preventivas atreladas à Autenticação de Dois Fatores (2FA), substituição de identificadores pessoais por identificadores únicos, rigidez na regulamentação de empresas e organizações atreladas ao Google, Criptografia de banco de dados (*Database Encryption*), todas focadas na garantia da privacidade dos indivíduos, que vieram a promover um ambiente *online* mais seguro e confiável.

Palavras-chave: Cibersegurança, LGPD

Introdução

A abordagem deste tema visa analisar a insegurança do usuário diante da manipulação de dados por redes digitais, com foco na aplicação do DT para proteção de dados. Destaca-se também a importância de conscientizar os usuários sobre seus direitos e melhores práticas para proteger a privacidade online. Fornecer informações claras e orientações diretas é essencial para capacitar os usuários a tomar decisões informadas e utilizar as redes com mais segurança e confiança, especialmente em um contexto digital em constante destaque na contemporaneidade. Nolasco e Maciel Silva (2022) oferecem *insights* cruciais sobre os riscos que os usuários enfrentam em um cenário digital marcado por crimes cibernéticos.

A proteção de dados tornou-se uma preocupação global, agravada por incidentes de vazamento de informações e pelo uso indevido de dados pessoais por empresas. Esse ambiente incerto afeta diretamente a confiança dos usuários nas plataformas digitais, influenciando sua vontade de compartilhar informações e utilizar serviços online. A insegurança dos usuários

manifesta-se de várias maneiras, desde a desconfiança na utilização de serviços online até o medo de exposições a fraudes e violações de privacidade.

Esses sentimentos são recorrentes devido a frequentes incidentes de vazamentos de dados, ataques cibernéticos e práticas questionáveis de coleta de dados por empresas, destacando a necessidade urgente de abordar estas questões de formas inovadoras e centradas no usuário. Segundo Oliveira, Alhinho, e Lima (2017), a proteção de dados tornou-se uma preocupação central para os usuários de plataformas digitais no Brasil. O estudo revela que a desconfiança em relação à privacidade e segurança online impacta significativamente a disposição dos usuários em compartilhar informações e utilizar serviços na internet. A pesquisa destaca que incidentes de vazamento de dados e práticas inadequadas de coleta de dados por empresas contribuem para o medo de fraudes e violações de privacidade, reforçando a necessidade de soluções inovadoras e centradas no usuário para abordar essas questões.

No contexto atual, a relevância deste tema é inegável. A confiança representa um pilar fundamental para a ampla adoção de tecnologias digitais, bem como para o desenvolvimento e a prosperidade do ecossistema digital. Sem essa confiança, os usuários tendem a ser cada vez menos propensos a compartilhar informações e a se engajar plenamente em serviços online, o que pode limitar significativamente o potencial de inovação e crescimento econômico. Adicionalmente, a ausência de proteção adequada dos dados pessoais pode acarretar em consequências severas, tais como danos financeiros, perda de reputação e impactos negativos tanto na esfera pessoal quanto na profissional dos indivíduos.

Considerando a contribuição de Sales Sarlet e Linden Ruaro (2021), vale ressaltar os *insights* abordados sobre a importância da legislação na proteção dos dados sensíveis dos usuários contra manipulações indevidas. Ao explorar o arcabouço legal e regulatório relacionado à proteção de dados pessoais, o artigo enriquece a discussão sobre a necessidade de garantir a segurança e privacidade dos usuários no ambiente digital.

O presente projeto visa não só identificar os principais fatores que contribuem para a insegurança dos usuários, mas também propor soluções práticas e centradas no usuário para mitigar esses problemas. Santos (2019) e Sêmola (2003) destacam que a confiabilidade garante que toda informação deve ser protegida e seu acesso é de uso apenas das pessoas para quem são destinadas. A principal problemática reside na forma como os dados dos usuários são coletados, armazenados e utilizados por empresas como o Google. A coleta massiva de dados pessoais é essencial para a personalização de serviços e para o direcionamento de publicidade, mas essa prática levanta preocupações significativas sobre privacidade e segurança.

Muitos usuários não possuem conhecimento suficiente sobre segurança digital e privacidade, o que os deixa vulneráveis a práticas inseguras e à exposição desnecessária de seus dados pessoais. A desinformação é um problema significativo, pois muitos usuários não estão cientes dos riscos ou das melhores práticas para proteger seus dados. Segundo Furnell e Thomson (2009), a educação digital é crucial para capacitar os usuários a protegerem seus dados, e programas educacionais específicos podem melhorar significativamente a segurança dos usuários online.

No contexto digital contemporâneo, o crescente poder das empresas de tecnologia como o Google tem gerado preocupações substanciais sobre a privacidade e a segurança dos dados dos usuários. Um estudo recente de Moss (2019), publicado na *Harvard Business Review*, ressalta como as empresas de tecnologia enfrentam um dilema ético ao equilibrar a inovação com a proteção da privacidade. O artigo destaca que, embora a inovação tecnológica traga benefícios significativos para a sociedade, ela também pode representar uma ameaça à privacidade dos indivíduos, especialmente quando se trata da coleta e do uso de dados pessoais.

As políticas de coleta de dados do Google são frequentemente vistas como invasivas. A empresa coleta vastas quantidades de dados para fins publicitários e de personalização de serviços, o que levanta preocupações sobre a extensão da vigilância e a invasão da privacidade dos usuários. Zuboff (2020) argumentou que as práticas de coleta de dados do Google podem violar princípios de privacidade e sugeriu a necessidade de regulamentos mais rígidos para proteger os direitos dos usuários. Cumprir regulamentações como o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia tem sido desafiador para o Google. A empresa foi multada em diversas ocasiões por não aderir plenamente aos requisitos de proteção de dados. Em 2019, a *Commission Nationale de l'Informatique et des Libertés* (CNIL) multou o Google em 50 milhões de euros por falta de transparência e informação inadequada sobre políticas de consentimento de dados. Este caso ilustra os desafios contínuos na conformidade regulatória e a necessidade de maior clareza nas práticas de proteção de dados.

Fundamentação Teórica

A era digital trouxe consigo um mundo de oportunidades e conveniências, mas também apresentou novos desafios à segurança e privacidade dos usuários. A manipulação nas redes digitais, muitas vezes favorecida pela falta de controle sobre os dados pessoais, é um problema crescente que exige atenção e medidas eficazes. Neste contexto, os artigos selecionados para revisão abordam temas relevantes para a compreensão da insegurança do usuário na manipulação das redes.

Conforme Nolasco e Silva (2022), a cibersegurança refere-se às práticas e tecnologias empregadas para proteger sistemas, redes e dados de acessos não autorizados e ataques maliciosos. A evolução constante das ameaças cibernéticas exige uma abordagem proativa e adaptativa e as organizações devem adotar uma postura de segurança em camadas, implementando firewalls, sistemas de detecção e prevenção de intrusões, além de políticas robustas de gerenciamento de riscos.

Sugerido por Sarlet e Ruaro (2021), a privacidade no contexto digital envolve a proteção das informações pessoais contra coleta, uso e divulgação não autorizados. Com a proliferação de dispositivos conectados e a coleta massiva de dados, garantir a privacidade tornou-se um desafio significativo. Os indivíduos frequentemente não têm controle sobre como suas informações são utilizadas, levando a potenciais abusos e violações de privacidade. É essencial que políticas claras e transparentes sejam implementadas para assegurar que os dados pessoais sejam tratados com o devido respeito e proteção.

De acordo com Apocalypse e Vicentini Jorente (2022), a proteção de dados está intimamente ligada à privacidade e envolve a implementação de medidas para garantir a integridade, confidencialidade e disponibilidade das informações. A proteção de dados não só previne o acesso não autorizado, mas também assegura que os dados sejam utilizados de maneira ética e conforme as leis vigentes. Ferramentas como criptografia, controle de acesso e auditorias regulares são fundamentais para manter a segurança dos dados.

Reiterado por Rosa e Bertoncini (2022), a intervenção do Estado na regulação e proteção do ambiente digital é crucial para estabelecer normas e diretrizes que protejam os cidadãos e promovam a segurança. Políticas governamentais devem equilibrar a inovação tecnológica com a proteção dos direitos individuais. Leis específicas para combater crimes cibernéticos, proteger dados pessoais e garantir a privacidade são essenciais. A cooperação internacional também é vital, dado o caráter global das ameaças digitais.

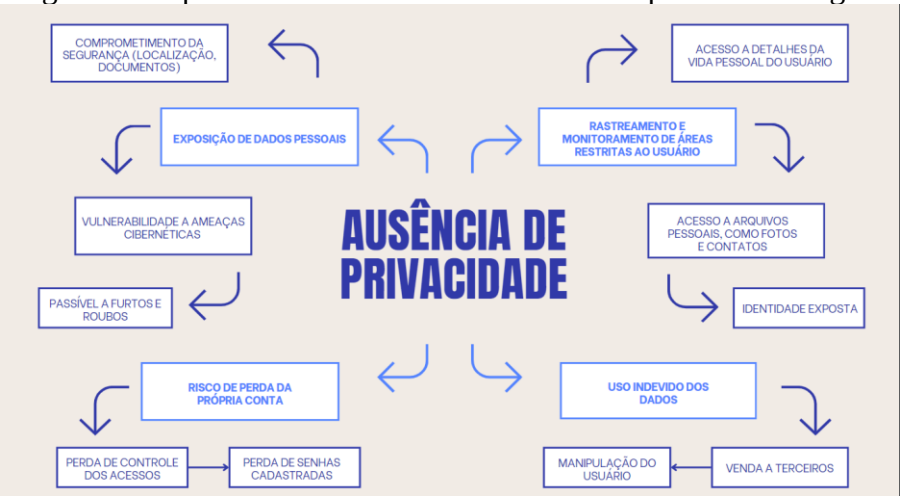
Segundo Junior e Souza (2023), a Lei Geral de Proteção de Dados (LGPD) do Brasil é uma legislação abrangente que regula o tratamento de dados pessoais e fortalece os direitos dos indivíduos sobre suas informações. A LGPD estabelece princípios e obrigações para organizações que processam dados, impondo sanções rigorosas em caso de não conformidade. A implementação da LGPD representa um avanço significativo na proteção da privacidade e dos

dados no Brasil, alinhando-se com práticas internacionais como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia.

Metodologia

A referida pesquisa utilizou das 6 etapas de *Rockower*, que se inicia pelo entendimento do sistema e definição do objetivo ao abordá-lo. Posteriormente foram definidas métricas de análise da eficácia operacional, limitando a causa a um determinado escopo (recorte geográfico) com uma base de dados adequada e confiável. As constantes melhorias do modelo utilizado foram analisadas e postas em prática na busca por alternativas realistas para cada problema envolvido.

Figura 1: Mapa Mental descritivo na ausência de privacidade digital



Autores (2024)

O projeto consiste no desenvolvimento de um aplicativo móvel e *web* chamados *Segurança+*. Este aplicativo será uma plataforma abrangente que oferece diversas funcionalidades focadas na segurança digital e na privacidade dos usuários. A proposta ideal é oferecer tutoriais intuitivos sobre práticas de segurança digital, como a criação de senhas fortes. Todas as informações armazenadas no aplicativo serão criptografadas utilizando algoritmos avançados para garantir a privacidade dos dados dos usuários. O aplicativo também disponibilizará ferramentas que apresentem as ameaças cibernéticas de forma clara e compreensível. Essa proposta de solução prevê um aumento na confiança dos usuários, melhora na conscientização e educação sobre segurança digital, além de auxiliar as empresas a seguirem as regulamentações de segurança e privacidade.

Referências

CNIL. CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. CNIL, 2019.

COSTA, L. A. C. da; BARRETO, R. M. Construindo pontes entre o Design Thinking e a aprendizagem criativa: possibilidades para o ensino tecnológico. Educitec - Revista de Estudos e Pesquisas sobre Ensino Tecnológico, Manaus, Brasil, v. 10, n. jan./dez., p. e232424, 2024. DOI: 10.31417/educitec.v10.2324. Disponível em: <https://sistemascmc.ifam.edu.br/educitec/index.php/educitec/article/view/2324>. Acesso em: 27 maio 2024.

DOS SANTOS, B. C.; FERRAZ SANTOS, L. C.; GUERRA, M. S.; STOCKER, F. Vulnerabilidade de dados e a percepção de privacidade dos usuários de redes sociais. Brazilian Journal of Business, [S. l.],

v. 1, n. 4, p. 1728–1742, 2019. Disponível em: <https://ojs.brazilianjournals.com.br/ojs/index.php/BJB/article/view/4836>. Acesso em: 28 maio 2024.

ELECTRONIC FRONTIER FOUNDATION. Empowering Users: The Importance of Data Ownership in the Digital Age, 2021.

FURNELL, S.; THOMSON, K. L. From culture to disobedience: Recognising the varying user acceptance of IT security. Computer Fraud & Security, v. 2009, n. 2, p. 5-10, 2009. DOI: 10.1016/S1361-3723(09)70019-3.

JUNIOR, N. F.; DE SOUZA, V. J. S. Proposta de novos estereótipos na modelagem de bancos de dados no contexto da LGPD. Pensar Acadêmico, v. 21, n. 1, 2023. Disponível em: <https://pensaracademico.unifacig.edu.br/index.php/pensaracademico/article/view/3491>. Acesso em: 27 maio 2024.

MARCOS APOCALYPSE, Simão; JOSÉ VICENTINI JORENTE, Maria. O método Design Thinking e a pesquisa em Ciência da Informação. Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação, [S. l.], v. 27, n. 1, 2022. DOI: 10.5007/1518-2924.2022.e87281. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/87281>. Acesso em: 24 maio 2024.

MOSS, Emanuel; METCALF, Jacob. The Ethical Dilemma of Big Tech: Balancing Innovation and Privacy. Harvard Business Review, 2019. Disponível em: <https://store.hbr.org/product/the-ethical-dilemma-at-the-heart-of-big-tech-companies/H05967>. Acesso em: 29 maio 2024.

NOLASCO, Loreci Gottschalk; MACIEL SILVA, Bruno Dutra. Crimes cibernéticos, privacidade e cibersegurança. Revista Quaestio Iuris, [S. l.], v. 15, n. 4, p. 2353–2389, 2022. DOI: 10.12957/rqi.2022.67976. Disponível em: <https://www.e-publicacoes.uerj.br/quaestioiuris/article/view/67976>. Acesso em: 22 maio 2024.

OLIVEIRA, T.; ALHINHO, M.; LIMA, A. Percepções de privacidade e segurança no uso da internet. Revista Brasileira de Gestão de Negócios, v. 19, n. 64, p. 206-228, 2017. DOI: 10.7819/rbgn.v19i64.3369. Acesso em: 27 maio 2024.

RADER, E.; WASH, R.; BROOKS, B. Stories as informal lessons about security. Proceedings of the ACM on Human-Computer Interaction, v. 2, n. CSCW, p. 1-24, 2018.

ROSA, B. M. H. DA; BERTONCINI, M. E. S. N. Intervenção do Estado em matéria consumerista e a LGPD. Revista de Direito Globalização e Responsabilidade nas Relações de Consumo, v. 8, n. 1, 2022. Disponível em: <https://indexlaw.org/index.php/revistadgrc/article/view/8794>. Acesso em: 27 maio 2024.

SALES SARLET, G. B.; LINDEN RUARO, R. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. Revista Direitos Fundamentais & Democracia, [S. l.], v. 26, n. 2, p. 81–106, 2021. DOI: 10.25192/issn.1982-0496.rdfd.v26i22172. Disponível em: <https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172>. Acesso em: 22 maio 2024.

TECHSEC. The Data Dilemma: Balancing Convenience and Privacy in a Connected World. TechSec, 2023. Disponível em: <https://techsec.com/data-dilemma>. Acesso em: 29 maio 2024.

UNIVERSIDADE DE OXFORD. Ethical Guidelines for Data Collection and Use in the Digital Age, 2020.

UNIVERSIDADE DE STANFORD. Transparency and Trust: The Key to Ethical Data Practices, 2022.

ZUBOFF, S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Journal of Information Technology, v. 35, n. 1, 2020.