A EVOLUÇÃO DAS AMEAÇAS DE SEGURANÇA NAS REDES SOCIAIS.

DANIELLE FERNANDA SANTANA FIRMINO[1]
LUCIANO GONÇALVES DE CARVALHO[2]

RESUMO

Este artigo tem como objetivo investigar os principais riscos de segurança associados ao uso de plataformas digitais, com ênfase na evolução das ameaças nas redes sociais ao longo do tempo. A pesquisa utiliza uma metodologia exploratória com abordagem qualitativa para analisar diversos aspectos relacionados ao tema. Os resultados apontam para uma significativa evolução das ameaças, desde a proteção contra hackers e roubo de dados até crimes mais complexos como roubo físico, engenharia social, phishing, disseminação de malware, roubo de identidade, cyberstalking e cybercasing. A pesquisa identificou que a falsa sensação de segurança dos usuários, que confiam na proteção das plataformas, agrava os riscos, uma vez que as informações são frequentemente vendidas para terceiros ou hackeadas. O estudo também revela que crimes tradicionais migraram para o ambiente virtual, utilizando informações sobre localização e atividades dos usuários para fins criminosos. A conclusão enfatiza a necessidade de uma abordagem multifacetada para combater esse cenário. É crucial que os usuários estejam conscientes dos riscos e adotem práticas de segurança, como cautela com as informações compartilhadas, revisão das configurações de privacidade, uso de senhas fortes e softwares de segurança atualizados. As empresas de tecnologia devem implementar medidas robustas de segurança, como autenticação de dois fatores e softwares anti-roubo de identidade, além de promover campanhas de conscientização. A criação de leis específicas para punir crimes cibernéticos também é fundamental para garantir um ambiente digital mais seguro.

Palavras-chave: Ameaças cibernéticas; Prevenção; Redes sociais.

ABSTRACT

This article aims to investigate the main security risks associated with the use of digital platforms, with an emphasis on the evolution of threats on social networks over time. The research uses an exploratory methodology with a qualitative approach to analyze several aspects related to the topic. The results point to a significant evolution of threats, from protection against hackers and data theft to more complex crimes such as physical theft, social engineering, phishing, malware dissemination, identity theft, cyberstalking and cybercasing. The research identified that the false sense of security of users, who trust in the protection of the platforms, aggravates the risks, since the information is often sold to third parties or hacked. The study also reveals that traditional crimes have migrated to the virtual environment,

[1]Graduanda, Tecnologia em Análise e Desenvolvimento de Sistemas pela Faculdade de Tecnologia de Mogi das Cruzes – FATEC-MC. – Mogi das Cruzes-SP. E-mail: danielle.firmino@fatec.sp.gov/br
[2]Docente, Faculdade de Tecnologia de Mogi das Cruzes – FATEC-MC. – Mogi das Cruzes-SP.

using information about users' location and activities for criminal purposes. The conclusion emphasizes the need for a multifaceted approach to combat this scenario. It is crucial that users are aware of the risks and adopt security practices, such as caution with the information shared, reviewing privacy settings, using strong passwords and up-to-date security software. Technology companies must implement robust security measures, such as two-factor authentication and anti-identity theft software, in addition to promoting awareness campaigns. Creating specific laws to punish cybercrimes is also essential to ensure a safer digital environment.

Key words: Cyber threats; Prevention; Social networks.

INTRODUÇÃO

As redes sociais transformaram profundamente nossa maneira de nos conectar e interagir, inaugurando uma nova era de comunicação instantânea e global. Amplamente reconhecido por muitos estudiosos e especialistas, o site SixDegrees.com é a primeira rede social moderna sendo inaugurado em 1997, de acordo com Zampier (2021) o mesmo permitia ao usuários criarem um perfil de usuário, uma lista de amigos para interação e também acessar os amigos de seus amigos. Percorrendo o histórico da rede social, até o ano de 2001, surgiram o Asian Avenue, Black Planet e Mi Gente, que partiam da mesma premissa do Six Degrees. No Brasil, a rede social que introduziu esse novo conceito de interação e alcançou enorme sucesso foi o Orkut, de propriedade do Google Inc., lançado no país em 2004, atualmente extinto. Segundo dados fornecidos pelo We Are Social (2024) relatório de Digital 2024: Global Overview 5,61 bilhões de pessoas possuem pelo menos um perfil ativo em alguma rede, representando 69,4% de toda população mundial.

Paralelamente à expansão das redes sociais, proporciona-se uma evolução significativa nas preocupações relativas à segurança digital. Com o contínuo aumento do número de usuários, as vulnerabilidades dessas plataformas tornaram-se alvos cada vez mais abordados pelos cibercriminosos, que se aproveitam de falhas nas configurações de privacidade e nas políticas de segurança. A proteção contra

ameaças cibernéticas, portanto, emerge como uma prioridade tanto para os usuários quanto para as próprias plataformas.

Este artigo tem como objetivo investigar os principais riscos de segurança associados ao uso de plataformas digitais, com ênfase nas redes sociais ao longo do tempo identificando suas causas, impactos e as medidas de mitigação disponíveis.

MATERIAL E MÉTODOS

Este estudo se caracteriza como modelo de pesquisa exploratória e a abordagem de pesquisa utilizada foi através do viés qualitativo. Esse método permite uma maior familiaridade com o problema, ao considerar diversos aspectos relacionados ao fato ou conhecimento estudado, assegurando compreensão mais profunda e holística do tema investigado (Gil, 2010).

Sendo realizada uma ampla pesquisa bibliográfica nas plataformas de artigos acadêmicos Google Acadêmico e IEEE Xplore, buscando trabalhos que abordassem a evolução das ameaças cibernéticas nas redes sociais ao longo do tempo. A pesquisa se concentrou em artigos científicos, livros e relatórios de instituições renomadas na área de segurança da informação e redes sociais. A análise dos dados coletados se baseou em uma revisão sistemática da literatura, buscando identificar os principais tipos de ameaças cibernéticas, suas causas, impactos e medidas de mitigação.

REFERENCIAL TEÓRICO

A evolução das redes e da tecnologia da informação contribui para o desenvolvimento de vários campos, setores e comportamentos de consumo em todo o mundo. De acordo com a pesquisa realizada pela empresa We are social (2024) existem aproximadamente 5,04 bilhões de usuários ativos em mídias sociais, com uma média de 2 horas e 23 minutos por dia usando as plataformas.

Inicialmente, plataformas de mídia social como Facebook e MySpace foram desenvolvidas com o objetivo de serem ferramentas de comunicação voltadas principalmente para jovens. Essas redes ofereciam aos usuários a oportunidade de criar perfis pessoais, compartilhar atualizações e interagir com amigos por meio de mensagens, comentários e compartilhamentos de conteúdo. O foco dessas plataformas era permitir uma forma mais direta e interativa de comunicação, que fosse rápida e acessível para a faixa etária jovem.

Com o passar do tempo, essas plataformas passaram a atrair um público mais amplo, incluindo pessoas de diferentes idades e contextos. Isso se deve, em parte, à adaptação dessas redes às novas necessidades de comunicação, como a integração de funcionalidades de negócios, marketing e outras formas de interação social. Hoje, as redes sociais se tornaram ferramentas multifuncionais, usadas para comunicação pessoal, profissional e empresarial, com plataformas como Facebook, Instagram, LinkedIn e Twitter, sendo utilizadas por uma ampla gama de usuários em todo o mundo. Além disso, novas plataformas, como TikTok e WhatsApp, continuam a expandir as formas de interação social e comunicação online, tornando-se essenciais no cotidiano de indivíduos de todas as idades.

Smith(2012), no artigo *Big Data Privacy Issues in Public Social Media* , mostra como o aumento das capacidades dos dispositivos móveis está relacionado aos problemas de privacidade enfrentados pelos usuários. Eles analisam essa questão no contexto do big data e destacam que, devido à grande quantidade de dados compartilhados diariamente, os usuários têm dificuldade em perceber tanto as consequências imediatas quanto os impactos deste comportamento a longo prazo. Enquanto as redes de internet continuam a se desenvolver, segundo Hiatt e Choi (2016), o principal aspecto para os desenvolvedores terão de lidar é a segurança do uso das redes sociais, tendo em vista, todas os usuários e as informações pessoais e/ou comerciais compartilhadas, tal cenário prepara terceiros para tirarem vantagens das redes sociais tendo acesso não autorizado ou lançando um ataque de phishing

para roubar informações pessoais ou outras formas de hacking. Por exemplo, o LinkedIn teve os endereços de e-mail dos usuários vazados em 2012 e o Facebook foi alvo de ataques em 2016 e 2018, resultando na exposição das informações pessoais de 50 milhões de seus usuários (BBC, 2018; G1, 2016).

Convém ainda ressaltar, a necessidade de que os usuários compreendam os conceitos fundamentais de cibersegurança para poder identificar tentativas de ciberataques e adotar medidas adequadas para proteger suas informações pessoais. A segurança da informação nas redes sociais envolve três objetivos principais: integridade, disponibilidade e privacidade dos dados. A integridade assegura que os dados não sejam alterados sem permissão, enquanto a disponibilidade garante o acesso autorizado às informações a qualquer momento. Por fim, a privacidade protege os dados dos usuários, restringindo o acesso indevido a eles. Para que os usuários possam identificar possíveis ameaças, é fundamental que entendam esses conceitos e como os ataques cibernéticos, como man-in-the-middle e negação de serviço (DoS), podem comprometer a segurança das informações (Stergiou, 2018).

De acordo com a National White Collar Crime Centre (NW3C) (2013), existem 6 principais tipos de cibercrimes associados às atividades nas redes sociais, esses crimes podem ser praticados diretamente pelas redes sociais ou através de informações obtidas por ela serem praticados na vida real.

Roubo via rede social: Criminosos utilizam as redes sociais para buscar potenciais alvos para roubo, aproveitando informações sobre a localização e atividades dos usuários. Por exemplo, postagens sobre jantares fora ou viagens de férias podem indicar aos criminosos que uma casa está vazia e vulnerável a roubos. Um exemplo notável desse tipo de crime foi o roubo de joias no valor de 10 milhões de dólares de Kim Kardashian em Paris, onde suspeita-se que os criminosos obtiveram informações sobre sua localização através de suas postagens no Twitter.
Engenharia social e phishing: A engenharia social usa manipulação psicológica para obter informações pessoais. Criminosos podem se passar por amigos ou instituições

confiáveis, como bancos, para enganar os usuários e fazê-los fornecer dados confidenciais, como senhas e números de cartão de crédito. O phishing, uma técnica comum de engenharia social, utiliza e-mails falsos que parecem ser de fontes legítimas para induzir as vítimas a clicar em links maliciosos ou fornecer informações pessoais.

Malware: As redes sociais são plataformas propícias para a disseminação de malware, como vírus e adware. Criminosos podem esconder programas maliciosos em links, anexos e mensagens, infectando os computadores dos usuários que interagem com esses conteúdos. A proliferação de malware através das redes sociais representa um risco significativo para a segurança dos usuários e das empresas, que podem ter suas redes corporativas comprometidas.

Roubo de identidade: O roubo de identidade ocorre quando um criminoso obtém informações pessoais de uma vítima, como número de CPF, data de nascimento e endereço, para fins criminosos. Essas informações podem ser usadas para abrir contas bancárias fraudulentas, fazer compras online ou obter crédito em nome da vítima. O roubo de identidade é um crime crescente, com um número significativo de vítimas e perdas financeiras consideráveis a cada ano.

Cyberstalking: O cyberstalking envolve o uso da internet e das redes sociais para perseguir e assediar uma vítima. O cyberstalker pode enviar mensagens ameaçadoras, espalhar rumores falsos, monitorar as atividades online da vítima ou usar informações pessoais para intimidá-la. As vítimas de cyberstalking podem sofrer danos psicológicos e emocionais significativos, incluindo ansiedade, medo e depressão.

Cybercasing: O cybercasing utiliza informações disponíveis online, como geolocalização em fotos e postagens de redes sociais, para identificar a localização física de um alvo. Criminosos podem usar essas informações para planejar roubos, assaltos ou outros crimes. Com o aumento do uso de aplicativos de geolocalização, o

cybercasing se tornou uma ameaça crescente para a segurança dos usuários de mídias sociais.

Em função da evolução dos cibercrimes, as empresas e os órgãos governamentais foram, ao longo do tempo, desenvolvendo medidas preventivas e legislações cujo objetivo principal é garantir aos usuários a utilização segura das redes sociais, prevenindo crimes e garantindo a liberdade de direitos.

De acordo com Soomro (2019), as práticas de conscientização e vigilância são essenciais na prevenção de cibercrimes. É crucial estar informado sobre os diferentes tipos de ameaças online, como roubo via redes sociais, engenharia social, phishing, malware, roubo de identidade, cyberstalking e cybercasing. Os usuários devem ser cautelosos com as informações que compartilham publicamente online, especialmente dados sensíveis como localização, endereço residencial e informações financeiras. A revisão regular das configurações de privacidade e a limitação das permissões de aplicativos em mídias sociais também são medidas importantes. A vigilância constante sobre extratos bancários e de cartão de crédito pode ajudar a detectar atividades suspeitas precocemente. A destruição de documentos de identidade expirados e a abstenção de compartilhá-los online são medidas preventivas adicionais. É fundamental ter softwares de segurança, como antivírus, sempre atualizados e prestar atenção aos URLs de sites, certificando-se de que sejam legítimos antes de inserir informações pessoais. A verificação da autenticidade de e-mails suspeitos, a utilização de senhas fortes e únicas para cada conta e a cautela ao abrir anexos de remetentes.

Além da conscientização, a implementação de medidas de segurança robustas é crucial para fortalecer a proteção contra cibercrimes. A autenticação de dois fatores (2FA) adiciona uma camada extra de segurança às contas online, dificultando o acesso não autorizado. Softwares anti-roubo de identidade, como o LifeLock da Symantec, podem ajudar a monitorar e proteger informações pessoais. Ferramentas online que verificam e removem a geolocalização de imagens são úteis para evitar o

cybercasing. Medidas de segurança física, como câmeras de segurança, fechaduras de portas e iluminação com sensor de movimento, também podem dissuadir criminosos. As empresas devem adotar políticas de segurança cibernética abrangentes, realizar campanhas de conscientização para funcionários, manter os dados apenas pelo tempo necessário e preparar planos de resposta a incidentes. A realização de avaliações de vulnerabilidade de rotina e a verificação da validade das credenciais de login são práticas essenciais. A utilização de técnicas de detecção de malware e anti-phishing, como senhas de uso único (OTP), CAPTCHAs e certificados digitais, pode fortalecer a segurança online. A implementação de medidas para prevenir fraude de cartão de crédito, como a verificação de endereço (AVS) e o valor de verificação do cartão (CVV), é crucial para proteger as transações financeiras.

Finalmente, a segurança de plataformas em nuvem pode ser aprimorada com criptografia baseada em Petri net e outros mecanismos de segurança.

Em contrapartida, o papel dos programadores e desenvolvedores nas plataformas de mídia social é crucial para garantir que os sistemas ofereçam mecanismos eficazes para proteger os dados dos usuários. Isso inclui a criação de dispositivos de segurança, como criptografia de dados para proteger a integridade das informações durante a transmissão, protocolos de autenticação robustos para garantir o acesso autorizado e sistemas de detecção de intrusão para impedir acessos não autorizados.

Além disso, os programadores têm a responsabilidade de desenvolver ferramentas educacionais que ajudem os usuários a entender como proteger suas informações pessoais, como alertas de segurança e orientações sobre as melhores práticas de privacidade (National Cybersecurity Centre, 2020).

RESULTADOS E DISCUSSÃO

Durante os estudos realizados durante a pesquisa, nota-se que as ameaças à segurança nas redes sociais evoluíram significativamente desde o seu surgimento. O

foco inicial era a proteção contra hackers e roubo de dados, mas com o aumento da popularidade das plataformas e a mudança de comportamento dos usuários, ameaças surgiram. De acordo com Hiatt e Choi (2016) os usuários têm uma falsa sensação de confiança em seu provedor de rede social para proteger suas informações, quando muitas vezes elas são vendidas a terceiros ou hackeadas por ladrões de identidade.

A tabela 1 apresenta técnicas de prevenção relacionadas às redes sociais e às ameaças associadas.

Tabela 1. Relação de Técnicas de Prevenção e Ameaças.

REDE SOCIAL	AMEAÇAS	TÉCNICAS DE PREVENÇÃO
Facebook, Twitter	Roubo, Cybercasing	Configuração de privacidade, evitar publicação de localização, restrição de compartilhamento de dados pessoais
Instagram	Engenharia Social, Phishing	Verificar autenticidade de mensagens, evitar compartilhamento de informações sensíveis, uso de OTP e CAPTCHA
YouTube	Malware, Roubo de Identidade	Instalação de antivírus, vigilância do usuário, atenção aos URLs suspeitos
LinkedIn	Roubo de Identidade, Cyberstalking	Uso de configurações de privacidade, separação de e-mails profissionais e pessoais, uso de pseudônimos
Redes sociais em geral	Intrusão de Dados e Fraudes em Desastres	Campanhas de conscientização, políticas de segurança cibernética, uso de sistemas de detecção e prevenção de intrusões, checagem de legitimidade de doações

Fonte: Soomro, (2019).

Segundo Mcgovern e Milivojevic (2019) A mídia social tem gerado novas oportunidades para as autoridades de justiça criminal. O acesso rápido e direto à informação proporcionado por plataformas como Facebook e Twitter tem se mostrado fundamental tanto para as forças de segurança quanto para o público, especialmente durante situações de emergência ou no dia a dia local. Além disso, a mídia social se tornou uma ferramenta relevante nas investigações, como exemplificado pelo caso de Jill Meagher, em que a divulgação das imagens de câmeras de segurança nas redes sociais ajudou na captura de seu assassino. A transmissão de processos judiciais por meio dessas plataformas também tem favorecido a transparência nos tribunais.

Contudo, a mídia social também apresenta aspectos negativos, que merecem atenção, principalmente no que diz respeito à segurança dos usuários e ao comportamento criminoso. As redes sociais têm sido utilizadas para facilitar crimes como a pornografia de vingança, o roubo de identidade e o assédio virtual, além de servir como ferramenta para criminosos que buscam rastrear suas vítimas. Crimes antigos, como fraudes e ameaças, estão sendo cometidos de maneiras inovadoras por meio dessas plataformas. Além disso, a natureza dos comportamentos pós-crime tem se alterado, com criminosos frequentemente se vangloriando de suas ações nas redes sociais, o que tem gerado o fenômeno dos chamados "crimes performáticos".

Segundo İsa (2022), as motivações para a prática de ataques cibernéticos podem variar significativamente, sendo categorizadas em diferentes tipos, como emoções, ganhos financeiros, entre outros. No caso das emoções, por exemplo, hackers podem atacar plataformas de mídia social para expressar raiva ou vingança, impactando tanto a reputação online quanto a confiança dos usuários. Em relação aos ganhos financeiros, os cibercriminosos buscam acessar informações sensíveis, como dados bancários, para explorar recursos financeiros. Já no hacktivismo, o ataque é motivado por causas políticas ou sociais, como a defesa de direitos humanos ou a liberdade de expressão, demonstrando como as intenções por trás dos ataques

podem ser variadas, desde questões pessoais até objetivos mais amplos de mudança social e política.

CONCLUSÃO

A evolução das ameaças de segurança nas redes sociais tem sido uma constante desde o seu surgimento. Inicialmente, as preocupações se concentravam em hackers e roubo de dados, mas com a popularização das plataformas, surgiram novas ameaças. A falsa sensação de segurança dos usuários, que confiam na proteção das plataformas enquanto suas informações são vendidas ou hackeadas, intensifica os riscos. Crimes tradicionais migraram para o ambiente virtual, como roubo, engendrado por informações sobre localização e atividades dos usuários.

Técnicas como engenharia social e phishing, que se aproveitam da manipulação psicológica para obter dados confidenciais, tornaram-se comuns. A disseminação de malware através de links e anexos maliciosos compromete a segurança individual e corporativa. O roubo de identidade, para fins criminosos como abertura de contas fraudulentas, e o cyberstalking, com mensagens ameaçadoras e monitoramento online, causam danos psicológicos e emocionais nas vítimas. O cybercasing, utilizando geolocalização de fotos e postagens para planejar crimes, representa uma ameaça crescente. A desinformação e a manipulação algorítmica também se tornaram graves problemas, impactando a democracia e o debate público. Para combater esse cenário, medidas de segurança robustas, educação digital e leis específicas são essenciais. A conscientização dos usuários sobre os riscos e a adoção de práticas de segurança individuais, como cautela com informações compartilhadas, senhas fortes e softwares atualizados, também são cruciais.

REFERÊNCIAS BIBLIOGRÁFICAS

BBC NEWS BRASIL; **Facebook admite uso indevido de dados de 87 milhões de usuários, 443 mil no Brasil.** Publicado em: 4 abr. 2018. Disponível em: https://www.bbc.com/portuguese/geral-43646687. Acesso em: 16/10/2024.

BORUP, M.; BROWN, N.; KONRAD, K.; VAN LENTE, H. **The sociology of expectations in science and technology. Technology analysis & strategic management,** v. 18, n. 3-4, pp. 285-298, 2006.

G1. **Vazamento do LinkedIn ressurge com 167 milhões de senhas.** Por Altieres Rohr. Publicado em: 24 maio 2016. Disponível em: https://g1.globo.com/tecnologia/blog/seguranca-digital/post/vazamento-do-linkedin-ressurge-com-167-milhoes-de-senhas.html. Acesso em: 16/10/2024

GIL, A. C. **Como Elaborar Projetos de Pesquisa.** 5° Edição. São Paulo: Atlas, 2010.

HIATT, D. ; CHOI, YB.. **"Papel da segurança em redes sociais."** 2016Revista internacional de ciência da computação avançada e aplicações 7.Publicado em 2016. Disponível em: https://thesai.org/Publications/ViewPaper?Volume=7&Issue=2&Code=ijacsa&SerialNo=2

İSA, AVCI. 2022. **"ANÁLISE de SEGURANÇA DE DADOS e MÉTODOS DE ATAQUE CIBERNÉTICO em MOEDA DIGITAL**." Mühendislik Bilimleri e Tasarım Dergisi 10 (3): 1000–1013.

KRAUSE, J. M.; NALCA, A**. Social Engineering: The Science of Human Hacking**. John Wiley & Sons, Inc., Indianapolis, 2018. ISBN 978-1-119-43338-5.

KOFFERMANN, M.; AGUADED, I. **A influência das redes sociais sobre os adolescentes: ciberconsumo e educação crítica**. Revista do Programa de Pós-graduação em Comunicação - Universidade Federal de Juiz de Fora , Juiz de Fora, v. 123-139, jan./abr. 2023. e-ISSN 1981-4070.

LIMA, F. H.; OLIVEIRA, C. C. **Uma análise das estratégias de defesa contra ataques automatizados em redes sociais de marketing digital.** Instituto Federal do Triângulo Mineiro/Campus Patrocínio, v. 10, n. 1, 2023. Publicado em: 22 nov. 2023.

MCGOVERN, A.; MILIVOJEVIC, S. **Social media and crime: the good, the bad and the ugly**. ***The Conversation*****,** 16 out. 2016. Disponível em: https://theconversation.com/social-media-and-crime-the-good-the-bad-and-the-ugly-66397. Acesso em: 30 out. 2024.

NATIONAL CYBERSECURITY CENTRE. **Mídias sociais: como usá-las com segurança**. 2020 Disponível em: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely. Acessado em 28 de janeiro de 2021

NATIONAL WHITE COLLAR CRIME CENTRE (NW3C). **Criminal use of social media**. 2013. Disponível em: https://www.nw3c.org/docs/training/nw3c-training-catalog.pdf. Acesso em: 31 out. 2024.

NEIVA, L. **O direito à privacidade no tempo do big data: narrativas profissionais na União Europeia**. Rev. Tecnol. Soc., Curitiba, v. 16, n. 45, p. 1-20, out/dez. 2020. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/11439

SMITH, M.; SZONGOTT, C.; HENNE, B.; VON VOIGT, G. 2012. **Big Data Privacy Issues in Public Social Media.** Em IEEE International Conference on Digital Ecosystems and Technologies. Apresentado na IEEE International Conference on Digital Ecosystems and Technologies, IEEE, Itália. 10.1109/DEST.2012.6227909

SOOMRO, T. R.; HUSSAIN, M. **Social media-related cybercrimes and techniques for their prevention**. *Applied Computer Systems*, v. 24, n. 1, Riga Technical University, 2019, p. 9-17. DOI: https://doi.org/10.2478/acss-2019-0002.

STERGIOU, C.; PSANNIS, K. E.; PLAGERAS, A.P.; GUPTA, B. B. 2018. **Segurança e privacidade de Big Data para serviços de redes sociais na nuvem,** apresentado no IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, Honolulu, HI, pp. 438–443. 10.1109/INFCOMW.2018.8406831

UNIÃO EUROPEIA. Lei n.º 2016.679 de 27 de abril de 2016. **Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Regulamento Geral sobre a Proteção de Dados. Jornal Oficial da União Europeia, v. 3, pp. 1-88.

WE ARE SOCIAL LTD. Digital 2024: **5 bilhões de usuários de mídia social.** Disponível em: https://wearesocial.com/uk/blog/2024/01/digital-2024-5-billion-social-media-users/. Publicado em 2024. Acesso em: 30 out. 2024.

ZAMPIER, B. **Bens digitais: cybercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais**. 2. ed. Indaiatuba, SP: Editora Foco, 2021. 296 p. ePUB. ISBN 978-65-5515-133-6.