Um Mapeamento Sistemático sobre Privacidade em Redes Sociais: Ameaças e Soluções

Andrey Rodrigues[1], **Maria Lúcia Villela**[2], **Eduardo Feitosa** [3]

[1]Instituto de Ciências Exatas e Tecnologia
Universidade Federal do Amazonas (UFAM) – Itacoatiara – AM – Brasil

[2]Departamento de Informática
Universidade Federal de Viçosa (UFV) – Viçosa – MG – Brasil

[3]Instituto de Computação
Universidade Federal do Amazonas (UFAM) – Manaus – AM – Brasil

andrey.rodrigues@ufam.edu.br, maria.villela@ufv.br,

efeitosa@icomp.ufam.edu.br

Resumo. *Este trabalho apresenta um Mapeamento Sistemático da Literatura (MSL) focado em ameaças de privacidade em Redes Sociais Online (RSOs) e nas soluções existentes para mitigá-las. A busca inicial resultou em 904 publicações, que, após a remoção de duplicatas e a aplicação de filtros de inclusão e exclusão, foram reduzidas a 43 artigos relevantes. A análise detalhada desses artigos permitiu a criação de um catálogo das ameaças mais críticas à privacidade dos usuários em RSOs, conforme citadas na literatura. Além disso, foram identificadas diversas soluções acadêmicas destinadas a proteger os usuários dessas ameaças, classificadas principalmente como soluções de prevenção e de medição de riscos. Este estudo contribui para uma melhor compreensão dos desafios e soluções no campo da privacidade em RSOs, oferecendo uma base sólida para pesquisadores e desenvolvedores que buscam aprimorar a proteção dos dados dos usuários nessas plataformas.*

1. Introdução

As Redes Sociais Online (RSOs) surgiram como um dos fenômenos mais significativos da era digital, conquistando uma popularidade eminente entre seus usuários [Abawajy et al. 2016, Grover et al. 2022]. Entretanto, a massiva quantidade de dados pessoais compartilhados nesses perfis ou associada às atividades dos usuários tem gerado diversas ameaças de privacidade [Jain et al. 2021, Bhattacharya et al. 2023].

Uma ameaça de privacidade é um evento indesejável que pode causar danos ao usuário através da exposição e manipulação de seus dados [Joyee De and Imine 2019]. Embora alguns estudos tenham investigado questões de segurança e privacidade nesses sistemas, a pesquisa sobre ameaças de privacidade em RSOs ainda enfrenta muitos desafios. A maioria dos trabalhos se concentra em riscos de segurança [Sahoo and Gupta 2019, Yassein et al. 2019, Yadav et al. 2022]. A segurança tende a focar na integridade e proteção dos sistemas em si, enquanto a privacidade está mais voltada para a proteção dos dados pessoais dos usuários. Nesse sentido, muitos desses estudos não abordam ameaças e soluções de privacidade com um foco direcionado às necessidades e proteção dos usuários.

Neste contexto, este artigo apresenta um Mapeamento Sistemático da Literatura (MSL), que investiga o estado da arte sobre ameaças críticas para a privacidade do usuário existentes em RSOs e uma visão geral das soluções acadêmicas que podem proteger os usuários dessas ameaças. Os resultados desse estudo tem o potencial de auxiliar pesquisadores e especialistas em privacidade, tanto na academia quanto na indústria, a compreenderem as ameaças de privacidade mais relevantes nas RSOs e a trabalharem para mitigá-las de maneira eficaz.

2. Mapeamento Sistemático da Literatura

Um MSL é um tipo de revisão sistemática que visa identificar e classificar os estudos científicos existentes na literatura relacionados a um tópico de interesse de uma área de pesquisa [Kitchenham et al. 2011]. Para a condução do MSL, considerou-se as diretrizes fornecidas por [Kitchenham and Charters 2007]. O protocolo de um MSL especifica os instrumentos que serão utilizados para conduzir o processo específico em torno da execução do MSL [Kitchenham and Charters 2007]. Os elementos que compuseram o protocolo do MSL serão descritos a seguir.

2.1. Questões de Pesquisa

As questões de pesquisa definidas neste MSL são apresentadas a seguir:

- QP-1. Quais ameaças de privacidade têm sido consideradas relevantes e precisam ser tratadas no contexto de RSOs?
- QP-2. Quais soluções têm sido adotadas para lidar com as ameaças de privacidade em RSOs?
- QP-3. Que procedimentos metodológicos foram adotados para avaliar as soluções propostas?

2.2. Estratégia de busca dos artigos

As bibliotecas digitais *Elsevier Scopus*, *Engineering Village* e *ACM* foram escolhidas para a busca das publicações. A estratégia de busca também incluiu a definição da *string* de busca a ser utilizada nas bases de dados selecionadas. Para estruturar os termos da *string*, foram utilizados os parâmetros PIO *(Population, Intervention e Output*) [Petticrew and Roberts 2008]. Os termos utilizados que formam a *string* de busca são apresentados na Tabela 1.

Tabela 1. *Strings* de busca utilizadas no MSL

Critério PICOC	*Strings* de busca
População	"online social network" **OR** "social network" **OR** "social software" **OR** "social application" **OR** "social system" **OR** "social interaction") **AND**
Intervenção	"language" **OR** "tool" **OR** "framework" **OR** "technique" **OR** "method" **OR** "mechanism" **OR** "model" **OR** "guideline" **OR** "approach" **OR** "algorithm" **OR** "aspect" **OR** "heuristic") **AND**
Resultado	"privacy threat modelling" **OR** "privacy threat evaluation" **OR** "privacy modeling" **OR** "privacy threat" **OR** "threat modeling" **OR** "privacy risk" **OR** "privacy vulnerability"

2.3. Critérios para seleção dos artigos

Os critérios de seleção servem para definir se um artigo será incluído ou excluído do MSL, visando garantir a relevância desses artigos para o contexto da pesquisa. A Tabela 2 apresenta os critérios de seleção definidos neste MSL.

Tabela 2. Critérios de seleção do artigos

Critérios	Critérios de inclusão
CI-1	O artigo descreve técnicas de modelagem de ameaças de privacidade em RSOs
CI-2	O artigo descreve uma linguagem ou notação para modelagem de ameaças de privacidade em RSOs
CI-3	O artigo descreve soluções para tratar ameaças de privacidade em RSOs
CI-4	O artigo descreve ameaças específicas de privacidade em RSOs
Critérios	**Critérios de exclusão**
CE-1	O artigo não atende nenhum dos critérios de inclusão
CE-2	A versão completa do artigo não está disponível para download ou nas fontes de busca
CE-3	A publicação não é um artigo científico, por exemplo, é um capítulo de um livro, portanto, não garantindo que houve revisão por pares (*peer review*)
CE-4	O artigo não está em inglês
CE-5	O artigo está duplicado, ou seja, foi retornado em outro mecanismo de busca

2.4. Execução do Mapeamento Sistemático

Para a execução da busca dos artigos, o pesquisador responsável pelo MSL aplicou as *strings* de busca nas bases de dados definidas. Para garantir a confiabilidade dos resultados obtidos, cada artigo retornado foi analisado por outros dois pesquisadores. Inicialmente, foram retornadas 904 publicações como resultado da busca inicial nas bibliotecas selecionadas (primeiro filtro). Após a aplicação dos critérios de inclusão e exclusão nessas publicações, 149 artigos foram selecionados para a aplicação do segundo filtro. Todas as 149 publicações foram lidas por meio da leitura diagonal (introdução, tópicos principais, conclusão), e apenas 55 publicações atenderam aos critérios de inclusão. Por fim, após a leitura completa desses artigos (terceiro filtro), um total de 43 artigos foram selecionados para a extração de dados.

3. Resultados

Esta seção apresenta de forma resumida os resultados obtidos para cada questão de pesquisa do MSL. Os resultados completos podem ser conferidos em [Rodrigues et al. 2024].

3.1. QP-1. Quais ameaças de privacidade têm sido consideradas relevantes e precisam ser tratadas no contexto de RSOs?

Para identificar e extrair as ameaças mais críticas de privacidade existentes na literatura, realizou-se uma análise minuciosa nos artigos encontrados no MSL. Cada artigo foi analisado e as ameaças abordadas neles foram extraídas. Após esse levantamento inicial, criou-se um diagnóstico de ameaças de privacidade. Com base no diagnóstico extraído a partir do mapeamento, criou-se um catálogo de ameaças (Figura 1) registrando as ameaças de privacidade mais críticas no contexto de RSOs, citadas na literatura. Essas ameaças podem impactar fortemente a privacidade do usuário na forma de divulgação, manipulação ou uso indevido de dados privados.

Figura 1. Catálogo de ameaças da PTMOL
Fonte: Próprio autor.

3.2. QP-2. Quais soluções têm sido adotadas para lidar com as ameaças de privacidade em RSOs?

Os resultados apresentados nessa subseção respondem a questão de pesquisa (QP-2). Diversos trabalhos propuseram soluções acadêmicas para proteger os usuários contra inúmeras ameaças de privacidade. A maioria das soluções identificadas direcionam o foco da sua proposta principalmente para a prevenção e medição de riscos associados a ameaças de privacidade. No entanto, observou-se que ainda existem limitações e algumas lacunas não cobertas pelas soluções existentes, que podem ser relevantes para a proposta de novas soluções.

3.3. QP-3. Que procedimentos metodológicos foram adotados para avaliar as soluções propostas?

Esta questão de pesquisa teve como principal objetivo apresentar quais os principais procedimentos metodológicos que foram adotados para avaliar as soluções identificadas no MSL. Observou-se que a maioria das soluções foram avaliadas por meio de simulações, não sendo testadas ou utilizadas em projetos reais na indústria ou em outras organizações. Além disso, nota-se que há uma carência na adoção de instrumentos de coleta de dados qualitativos, como entrevistas ou grupos focais.

4. Conclusões

Este trabalho apresentou um Mapeamento Sistemático sobre ameaças de privacidade em RSOs e soluções existentes para mitigá-las. Com base no MSL executado, criou-se um catálogo, que indica as ameaças mais críticas no contexto de RSOs, citadas na literatura. Esse catálogo foi gerado a partir de uma análise minuciosa realizada nos artigos identificados no MSL. Os resultados do MSL também revelaram diversos estudos propondo soluções acadêmicas para proteger os usuários contra inúmeras ameaças de privacidade. Tais soluções são classificadas principalmente como soluções de prevenção e medição de riscos associados às ameaças em RSOs.

Referências

Abawajy, J., Ninggal, M., and Herawan, T. (2016). Privacy preserving social network data publication. *IEEE Communications Surveys and Tutorials*, 18(3):1974–1997. cited By 37.

Bhattacharya, M., Roy, S., Chattopadhyay, S., Das, A. K., and Shetty, S. (2023). A comprehensive survey on online social networks security and privacy issues: Threats, machine learning-based solutions, and open challenges. *Security and Privacy*, 6(1):e275.

Grover, P., Kar, A. K., and Dwivedi, Y. (2022). The evolution of social media influence-a literature review and research agenda. *International Journal of Information Management Data Insights*, 2(2):100116.

Jain, A. K., Sahoo, S. R., and Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, 7(5):2157–2177.

Joyee De, S. and Imine, A. (2019). On consent in online social networks: Privacy impacts and research directions (short paper). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11391 LNCS:128–135. cited By 0.

Kitchenham, B. and Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering.

Kitchenham, B. A., Budgen, D., and Brereton, O. P. (2011). Using mapping studies as the basis for further research–a participant-observer case study. *Information and Software Technology*, 53(6):638–651.

Petticrew, M. and Roberts, H. (2008). *Systematic reviews in the social sciences: A practical guide*. John Wiley & Sons.

Rodrigues, A., Villela, M. L., and Feitosa, E. (2024). A systematic mapping study on social network privacy: Threats and solutions. *ACM Computing Surveys*, 56(7):1–29.

Sahoo, S. R. and Gupta, B. B. (2019). Classification of various attacks and their defence mechanism in online social networks: a survey. *Enterprise Information Systems*, 13(6):832–864.

Yadav, U. S., Gupta, B. B., Peraković, D., Peñalvo, F. J. G., and Cvitić, I. (2022). Security and privacy of cloud-based online online social media: A survey. In *Sustainable management of manufacturing systems in industry 4.0*, pages 213–236. Springer.

Yassein, M. B., Aljawarneh, S., and Wahsheh, Y. A. (2019). Survey of online social networks threats and solutions. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pages 375–380. IEEE.