XXIV ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – XXIV ENANCIB

ISSN 2177-3688

GT 8 – Informação e Tecnologia

VULNERABILIDADES DIGITAIS DE MULHERES BANIDAS EM APLICATIVOS DE NAMORO

DIGITAL VULNERABILITIES FROM BANNED´S WOMEN IN DATING APP

Thaiz Andraus – Universidade Federal do Paraná (UFPR)
Luiz Rogério Lopes Silva – Universidade Federal do Paraná (UFPR)

Modalidade: Resumo Expandido

Resumo: Os aplicativos de namoro alteraram a maneira de se relacionar, no entanto, são identificadas vulnerabilidades digitais nessas plataformas. Esta pesquisa tem por objetivo comparar as formas de banimento de quatro aplicativos de relacionamento: *Tinder, Happn, Badoo* e *Bumble*, identificando possíveis lacunas em suas políticas e técnicas estabelecidas. O estudo é direcionado especificamente ao banimento de mulheres. A análise documental constatou similaridades nas políticas praticadas pelas plataformas e, complementarmente, serviu de base para a elaboração de uma matriz de análise do conteúdo das diretrizes e das ações realizadas a partir do banimento.

Palavras-chave: vulnerabilidade; banimento; aplicativos de relacionamento.

Abstract: Dating apps have changed the way people interact, however, digital vulnerabilities have been identified on these platforms. This research aims to compare the ways of banned in four dating apps: *Tinder, Happn, Badoo* and *Bumble*, identifying possible gaps in their policies and techniques established. The study is specifically aimed at banning women. The documentary analysis found similarities in the policies practiced by the platforms and, in addition, served as a basis for creating an analyzing matrix of guideline ‘content and the actions taken after the ban.

Keywords: vulnerabilities; banning; dating applications.

1 INTRODUÇÃO

Os aplicativos de namoro (apps) transformaram a maneira como as pessoas se conectam, interagem e formam relacionamentos. Essas plataformas digitais são projetadas para conectar pessoas em busca de relacionamentos românticos ou encontros casuais, funcionando por meio de perfis de usuário que incluem fotos e descrições pessoais (Nunan;

Penido, 2019). Quando há interesse mútuo entre os interagentes, eles podem começar a conversar através do aplicativo, permitindo que manifestem suas vontades e estabeleçam conexões.

Plataformas como *Tinder, Bumble, Badoo* e *Happn* oferecem funcionalidades como geolocalização, configuração de perfis personalizados, mensagens instantâneas e recursos de verificação de fotos, criando um ambiente dinâmico para os interagentes se conhecerem e estabelecerem contatos, facilitando a formação de relações afetivo-sexuais. No entanto, a sistemática algorítmica de moderação destas plataformas não deixa evidente aspectos de privacidade e segurança. A literatura tem revelado vulnerabilidades relacionadas à governança algorítmica potenciais (Courtois; Timmermans, 2018), limitações das *affordances* (Broeker, 2019) e aspectos de segurança e privacidade (Noah; Thakur; Beck; Das, 2024).

Smith e Duggan (2013) indicam que a violência digital realizada através destas plataformas é de gênero, com mulheres que sofrem abusos em taxas mais elevadas do que os homens (42% em comparação com 17%). Adicionalmente, os dados, de 2014 a 2018, de ocorrências policiais relacionadas a aplicativos de namoro em São Paulo aumentaram 253%. No total, foram 338 registros no período. Entre esses, 237 boletins de ocorrência foram classificados como feito pela “vítima” ou “declarante”, e desses dois terços são mulheres. As principais ocorrências registradas por elas são difamação, injúria e ameaça, mas há também estupro, extorsão, furto e lesão corporal (Ferreira, 2029).

O banimento em aplicativos de namoro, como *Tinder, Bumble, Happn* e *Badoo,* é uma medida prevista nos “Termos de Uso” para garantir um ambiente seguro e respeitoso. Essas plataformas estabelecem critérios para o que consideram comportamentos inadequados, que podem resultar na suspensão ou exclusão de contas. As diretrizes incluem a intolerância a assédio, abuso, fraudes, comportamento agressivo, compartilhamento de conteúdo pornográfico ou solicitação de dinheiro. No entanto, apesar de os termos de uso parecerem claros e abrangentes, a aplicação dessas regras muitas vezes peca pela falta de sensibilidade e pela inadequação das ferramentas de denúncia, o que pode levar a banimentos injustos.

Oliveira e Lemos (2023) destacam como esse processo de banimento afeta desproporcionalmente pessoas trans no *Tinder*, devido a vieses algorítmicos presentes nas ferramentas de moderação. As opções de sinalização, genéricas e pouco específicas, são insuficientes para diferenciar situações legítimas de denúncias baseadas em preconceito, especialmente em relação a gênero. Esses vieses podem estimular práticas de vigilantismo

digital, nas quais usuários controlam e denunciam perfis dissidentes, contribuindo para práticas transfóbicas.

Embora os termos de uso sejam pensados para garantir a segurança das interações, na prática, as mulheres estão suscetíveis a banimentos indevidos. Os algoritmos, muitas vezes treinados com dados que refletem preconceitos sociais, podem identificar erroneamente certos comportamentos como inadequados ou perigosos, resultando no bloqueio de perfis femininos de maneira desproporcional (Oliveira; Lemos; Luiz, 2023).

Neste trabalho, a preocupação é com o banimento indevido de mulheres nos aplicativos mais usados nos Brasil (*Tinder, Bumble, Badoo* e *Happn*)[1], visto que há vulnerabilidades associadas à exclusão permanente de um perfil. O objetivo da pesquisa é comparar as formas de banimento dos aplicativos de namoro e identificar as lacunas nas políticas e técnicas das diretrizes que guiam os aplicativos.

2 VULNERABILIDADES DIGITAIS EM APLICATIVOS DE NAMORO

Vulnerabilidade digital é caracterizada pela suscetibilidade de pessoas e sistemas a danos decorrentes do uso de tecnologias digitais. Esses danos podem surgir de várias fontes, incluindo a presença da tecnologia, efeitos secundários do seu uso ou ações maliciosas intencionais (Ransbotham; Fichman; Gopal; Gupta, 2016). Exemplos de danos variam desde estresse tecnológico até invasões de privacidade e perda de dados (Junqueira; Botelho-Francisco, 2021). Para Ransbotham, Fichman, Gopal e Gupta (2016), o ambiente digital amplifica a exposição de entidades e seus atributos e facilita riscos à privacidade e segurança, expondo informações sensíveis e aumentando o risco de violações de dados e roubo de propriedade intelectual, por exemplo.

Autores como Sant'ana (2016) e Song, Chen e Fan (2021) listam uma série de vulnerabilidades no ecossistema das interações no ciberespaço, incluindo vigilância, interrogatório, insegurança, exclusão, violação de confidencialidade, violação à privacidade visível, vazamento malicioso de dados, violação à privacidade invisível, entre outros.

[1] LICHESKI, Kawane. 7 melhores aplicativos de relacionamento. 19 abr. 2024 Disponível em: https://www.bitmag.com.br/7-melhores-aplicativos-de-relacionamento-para-2023-valem-a-pena Acesso em: 15 jun.2024.

No contexto dos aplicativos de namoro, pesquisas apontam vulnerabilidades digitais relacionadas às categorias supracitadas. Mannan e Youssef (2022) demonstram que os aplicativos de namoro transmitem todo o tráfego da rede por meio de HTTP de texto simples, uma falha de segurança que expõe informações confidenciais dos usuários a possíveis interceptações. Nesse mesmo sentido, Chugh e Guggisberg (2020) relatam a exposição de dados privados em mídias sociais e o pouco conhecimento dos interagentes em relação à segurança cibernética.

Informações pessoais, como fotos e mensagens privadas, são frequentemente armazenadas e compartilhadas sem o conhecimento dos usuários, expondo-os a riscos de invasão de privacidade e roubo de dados (Farnden; Kin-Kwang; Choo, 2015; Shetty; Grispos; Choo, 2021; Stenzel; Le-Khac, 2024; Cho; Kim; Sundar, 2020).

Outro aspecto preocupante é o uso de *bots* e perfis falsos em aplicativos de namoro para enganar e manipular usuários, gerando interações fraudulentas e potencialmente perigosas. Esses *bots,* muitas vezes ocultos nos termos e condições dos aplicativos, podem enganar usuários desavisados, fazendo-os acreditar que estão interagindo com pessoas reais (Light, 2014).

Há o risco de interceptação de dados, onde é possível acessar mensagens e imagens compartilhadas, como também descobrir todos os dados de identidade do interagente (Puglisi, 2017). Falhas de segurança nos códigos dos aplicativos podem comprometer sua integridade e gerar riscos para a saúde mental dos interagentes, uma vez que o uso excessivo pode aumentar as chances de ansiedade e depressão (Capelotti; Pelizzon, 2020; Mosley; Lancaster; Parker; Campbell, 2020).

2.1 O banimento enquanto vulnerabilidade digital

Para ser banido do aplicativo, um usuário deve violar os termos de uso estabelecidos ou ser denunciado devido a mal comportamento por outros usuários, que posteriormente são revisados pelas equipes de moderação. Em casos graves ou recorrentes, a conta do infrator pode ser permanentemente banida.

Os banimentos, embora necessários para a manutenção de um ambiente seguro, podem representar uma vulnerabilidade digital, especialmente quando ocorrem de forma indevida. Erros nos algoritmos de detecção de comportamento inadequado, denúncias falsas

ou motivadas por vingança podem levar ao banimento injusto de usuários (Walker, 2023). Isso não só prejudica a experiência dos usuários legítimos, como também levanta questões sobre a eficácia e a justiça dos processos de moderação dessas plataformas.

Além disso, os mecanismos de banimento nem sempre são transparentes. Muitos interagentes não são informados adequadamente sobre os motivos específicos de seu banimento ou sobre os procedimentos para contestar a decisão (Walker, 2023). Essa falta de clareza pode levar a frustrações e a uma percepção negativa da plataforma, impactando a confiança na aplicação. Este cenário é agravado pela falta de transparência nos processos de revisão e apelação, deixando as pessoas sem recursos claros para contestar banimentos injustos.

Para evitar banimentos indevidos, o *Tinder* e outras plataformas estão considerando alternativas antes de excluir um perfil. Uma dessas alternativas pode incluir etapas de validação de perfil do usuário, garantindo que a infração realmente tenha sido cometida pela pessoa denunciada (Loubak, 2024). Além disso, há propostas para que a plataforma ofereça a possibilidade de justificativa por parte do denunciado antes da exclusão definitiva de um perfil. No caso de um banimento acidental, existem duas formas de revertê-lo: enviando um recurso diretamente para a empresa ou criando uma nova conta desvinculada da anterior (Bozovic, 2021). Segundo as plataformas, as iniciativas visam aumentar a justiça e a precisão dos processos de banimento.

De toda sorte, a literatura sobre banimento indevido e vulnerabilidade digitais de mulheres em aplicativos de namoro indica que os mecanismos mal calibrados acabam perpetuando desigualdades e reforçando estereótipos de gênero, prejudicando a experiência digital das mulheres em plataformas que, paradoxalmente, se propõem a facilitar conexões e promover interações seguras.

3 PROCEDIMENTOS METODOLÓGICOS

Os procedimentos metodológicos desta pesquisa entrelaçam dois métodos clássicos de análise: a análise documental e a análise de conteúdo. A análise documental tem como objetivo a condensação da informação para facilitar sua consulta e armazenagem. Já a análise de conteúdo se fundamenta em procedimentos sistemáticos e intersubjetivamente validados,

que permitem descrever, quantificar ou interpretar fenômenos com base em conteúdos verbais, visuais ou escritos (Sampaio; Lycarião, 2021).

De forma prática, os objetos de pesquisa deste estudo são os aplicativos de namoro mais populares e amplamente utilizados por mulheres no Brasil: *Tinder, Bumble, Badoo* e *Happn.* A escolha desses aplicativos se deve a sua vasta base de interagentes e a relevância de suas políticas de uso e de privacidade. Entende-se que a análise destes documentos serve a fase inicial de identificação de possíveis vulnerabilidades em aplicativos de namoro, sobretudo no que se refere a banimento indevido.

O processo de coleta de dados envolveu a reunião dos termos de uso e políticas de privacidade de cada um desses aplicativos[2][3][4][5]. A leitura preliminar, ou leitura flutuante, desses documentos resultou em dois achados principais: primeiro, as similaridades entre as políticas dos apps, incluindo a dissociação dos locais e empresas que coletam, tratam e armazenam os dados; segundo, o desenvolvimento de categorias de análise, sistematizadas em uma matriz, para examinar as políticas referentes ao banimento indevido. Neste trabalho, a matriz é apresentada como resultado de pesquisa.

Como se trata de uma pesquisa em andamento, não se descarta a ampliação dos documentos analisados para uma análise comparativa mais completa. Isso é relevante considerando que as políticas de uso e privacidade atuais não tratam profundamente da questão do banimento indevido.

4 RESULTADOS PARCIAIS

A partir da análise dos termos de uso das plataformas de namoro, bem como da literatura existente sobre banimentos indevidos e vulnerabilidades digitais nestes ambientes, foram identificadas fragilidades no contexto brasileiro, especialmente em relação a questões de infraestrutura e governança. Embora as empresas responsáveis por plataformas como *Bumble, Badoo, Happn* e *Tinder* aleguem seguir a Lei Geral de Proteção de Dados (LGPD), não

[2] BADOO. **Diretrizes da comunidade badoo**. 2024. Disponível em: https://badoo.com/guidelines#guidelines Acesso em: 14 jun. 2024.
[3] BUMBLE. Termos e condições do bumble. 2024. Disponível em: https://bumble.com/pt/terms Acesso em 16 jun. 2024.
[4] HAPPN. **Condições gerais de utilização**: definição dos termos. 2023. Disponível em: https://support.happn.fr/hc/pt-br/p/terms Acesso em: 14 jun. 2024.
[5] TINDER. **Termos de uso do tinder**. Dallas, 2024. Disponível em: https://policies.tinder.com/terms/intl/pt-br/ Acesso em: 19 jun. 2024.

se pode afirmar com certeza que essas diretrizes são plenamente implementadas e adequadas à realidade brasileira. A ausência de servidores locais e de um controle de dados regional, por exemplo, dificulta a fiscalização e o cumprimento integral das exigências da LGPD, o que pode comprometer a proteção dos dados dos interagentes e aumentar o risco de violações de privacidade.

Além disso, o Brasil enfrenta um histórico de racismo algorítmico e discriminação de gênero, que impacta diretamente o funcionamento dessas plataformas. A literatura aponta que algoritmos de moderação podem excluir desproporcionalmente perfis de mulheres, especialmente aquelas que pertencem a minorias raciais ou à comunidade LGBTQIAPN+. Essas exclusões, geralmente motivadas por denúncias automatizadas ou outros interagentes, ocorrem sem uma investigação adequada ou a possibilidade de defesa, perpetuando um ambiente digital injusto e excludente.

Outro ponto crítico, tanto nos termos de uso quanto na literatura especializada, é a ausência de mecanismos eficazes para que interagentes contestem banimentos indevidos. Quando uma mulher é excluída de uma plataforma, muitas vezes não há um canal acessível para que ela defenda seu caso, o que gera uma sensação de arbitrariedade que pode ser comparada à experiência de ser expulsa de um bar sem justificativa aparente, impedindo que a interagente concretize potenciais interações, novas conexões e possíveis encontros, prejudicando diretamente a experiência.

A situação é ainda mais agravada quando se considera o impacto financeiro dessas exclusões. Mulheres que pagam por serviços *premium* nas plataformas podem ser banidas sem explicação, perdendo o acesso às funcionalidades pelas quais pagaram, sem direito a reembolso ou compensação. Essa prática levanta preocupações sobre a transparência e equidade dessas plataformas, que não oferecem garantias de proteção adequadas.

Também é resultado parcial deste trabalho a criação de uma matriz destinada a avaliar as possíveis vulnerabilidades técnicas e operacionais das plataformas no que diz respeito a banimentos indevidos. A implementação dessa matriz busca investigar como a governança algorítmica, a infraestrutura de dados e as práticas de moderação dessas plataformas impactam as mulheres brasileiras que utilizam os aplicativos.

QUADRO 1 – Análise de banimento

CATEGORIA	ASPECTOS	PERGUNTAS
Critérios de Banimento	Comportamentos proibidos	Quais comportamentos são explicitamente proibidos nas diretrizes?
	Exemplos específicos	Quais são os exemplos específicos fornecidos para cada comportamento proibido?
Procedimentos de Apelação	Processo de apelação	Qual é o processo de apelação disponível para os usuários?
	Tempo de resposta	Qual é o tempo estimado para uma resposta após a apelação?
	Níveis de revisão	Quantos e quais são os níveis de revisão envolvidos no processo de apelação?
Transparência e Comunicação	Comunicação de banimento	Como os usuários são informados sobre seu banimento?
	Detalhamento da razão	Até que ponto as razões para o banimento são detalhadas aos usuários?
	Acesso às políticas	Quão acessíveis e compreensíveis são as políticas de banimento e uso?
Uso de Algoritmos	Tipo de algoritmo	Que tipo de algoritmos são utilizados para detectar comportamentos proibidos?
	Mitigação de vieses	Quais medidas são tomadas para mitigar vieses nos algoritmos?
	Ajustes e atualizações	Com que frequência os algoritmos são ajustados e atualizados?

Fonte: Os autores (2024).

A continuidade da pesquisa prevê observar como o banimento indevido atinge as mulheres sem que elas tenham infringido as regras de maneira objetiva, ou seja, as vulnerabilidades que os sistemas de denúncia e moderação automatizada carregam em si mesmos.

Outro aspecto que a continuidade da pesquisa prevê é de que forma as plataformas oferecem ou não canais de apelação e o quão eficazes eles podem ser. Além disso, será observado aspectos de resposta e comunicação que os aplicativos usam na tratativa com as interagentes com potencial de banimento.

5 CONSIDERAÇÕES FINAIS

A fase inicial desta pesquisa revelou vulnerabilidades relacionadas à exclusão permanente de perfis em aplicativos de namoro, que podem ocorrer devido a falhas nos algoritmos responsáveis por detectar comportamentos inadequados, denúncias falsas ou motivadas por vingança. Ao analisar e comparar a documentação dos termos de uso e privacidade desses aplicativos, foi identificado que as políticas de privacidade apresentavam grande similaridade entre as plataformas avaliadas. Como parte dos resultados preliminares, foi elaborada uma matriz de análise específica para os processos de banimento.

Os primeiros achados corroboram o que a literatura já tem evidenciado: os mecanismos de banimento em aplicativos de namoro nem sempre são transparentes para os interagentes. O objetivo dos próximos experimentos é confirmar ou refutar a hipótese de que as pessoas não recebem informações claras e detalhadas sobre os motivos exatos de seus banimentos, nem são devidamente orientadas sobre os procedimentos para contestar essas decisões. Em trabalhos futuros, busca-se comprovar empiricamente que essa falta de transparência é intensificada pela complexidade e opacidade dos processos de revisão e apelação, tornando ainda mais difícil para os interagentes recorrerem contra banimentos injustos e obterem uma resolução adequada. A continuidade da pesquisa permitirá expandir a comparação entre aplicativos de namoro em relação às suas regras de exclusão.

REFERÊNCIAS

BOZOVIC, Novak. How to get unbanned from tinder. **TechNadu**, 20 nov. 2021. Disponível em: https://www.technadu.com/get-unbanned-from-tinder/313158/. Acesso em: 19 jun. 2024.

BROEKER, Fabian. The evolving digital dynamics of intimacy: affordances and dating apps. **New media society?** 2019. Disponível em: Doi: 10.26650/B/SS07SS49.2023.009.05. Acesso em: 19 jun. 2024.

CAPELOTTI, João Paulo; PELIZZON, Thiago Conceição. Apontamentos sobre proteção de dados pessoais em aplicativos de namoro que usam a geolocalização. **Revista Fórum de Direito na Economia Digital,** Belo Horizonte, v. 7, p. 127-145, 2020. Disponível em: https://www.academia.edu/109727841/Apontamentos_sobre_prote%C3%A7%C3%A3o_de_dados_em_aplicativos_de_namoro_que_usam_a_geolocaliza%C3%A7%C3%A3o. Acesso em: 30 jun. 2024.

CHO, Eugene; KIM, Jinyoung; SUNDAR, Shyman S. Will you log into tinder using your facebook account?: Adoption of single sign-on for privacy-sensitive apps. **Association for computing machinery**. p. 1-7, 2020. Disponível em: https://dl.acm.org/doi/10.1145/3334480.3383074. Acesso em: 19 jun. 2024.

CHUGH, Ritesh; GUGGISBERG, Marika. Stalking and other forms of dating violence: lessons learned from you in relation to cyber safety **Journal of interpersonal violence**, v. 37, p. 9-10, 2020. Disponível em: https://doi.org/10.1177/0886260520966674. Acesso em: 29 jun. 2024.

COURTOIS, Cédric; TIMMERMANS, Elisabeth. Decifrando o código do *Tinder*: uma abordagem de amostragem de experiência para a dinâmica e o impacto dos algoritmos de governança da plataforma. **Journal of computer-mediated communication**, v. 23, p. 1-16, 2018. Disponível em: https://doi.org/10.1093/jcmc/zmx001. Acesso em: 29 jun. 2024.

DUGGAN, Maeve; SMITH, Aaron. Online Dating and Relationships. **Pew Research Centre and the American Life Project**. v. 18, n. 2, p. 99–122, 2013. Disponível em: https://www.pewresearch.org/internet/wp-content/uploads/sites/9/media/Files/Reports/2013/PIP_Online-Dating-2013.pdf. Acesso em: 17 set. 2024.

FARNDEN, Jody; KIM-KWANG, Ben Martini; CHOO, Raymond. Privacy risks in mobile dating apps. *In*: AMERICAS CONFERENCE ON INFORMATION SYSTEMS, 21, 2015. **Proceedings**… p. 13-15, 2015. Disponível em: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2017/10/21180944/1505.02906.pdf. Acesso em: 30 jun. 2024.

FERREIRA, Lola. A punição pelo desejo: registros de crimes relacionados a apps de relacionamento aumentaram mais de 250% em cinco anos. **Gênero e Número**. Disponível em: https://www.generonumero.media/reportagens/punicao-desejo-crimes-apps-tinder-relacionamento/. Acesso em: 15 jul.2024.

JUNQUEIRA, Antonio Hélio; BOTELHO-FRANCISCO, Rodrigo. Raça: dimensão interseccional das vulnerabilidades digitais. **Contemporanea**, v. 19, n. 3, p. 63–78, 2021.

LIGHT, Ben. **Disconnecting with social networking sites**. Basingstoke: Palgrave Macmillan, 2014.

LOUBAK, Ana Letícia. Tinder: app de namoro expande verificação de segurança no Brasil, EUA, Reino Unido e México. **CBN Tecnologia**, 23 fev. 2024. Disponível em: https://cbn.globoradio.globo.com/media/audio/431855/tinder-app-de-namoro-expande-sistema-de-verificaca.htm. Acesso em: 14 jun. 2024.

MANNAN, Mohammad; YOUSSEF, Amr. Privacy report card for online solutions targeting seniors. In: FINAL report for OPC contributions program 2021-2022. Montreal: Concordia Institute for Information Systems Engineering, 2022. Disponível em: https://madiba.encs.concordia.ca/reports/OPC-2021/OPC-2021-report.pdf. Acesso em: 29 jun. 2024.

MOSLEY, Marissa A.; LANCASTER, Morgan; PARKER, M. L.; CAMPBELL, Kelly. Adult attachment and online dating deception: a theory modernized. **sexual and relationship**

therapy, v. 35, n. 2, p. 227-43, 2020. Disponível em: https://doi.org/10.1080/14681994.2020.1714577. Acesso em: 19 jun. 2024.

NOAH, Naheem; THAKUR, Supriya; BECK, Jason; DAS, Sanchari. Evaluating privacy and security of online dating applications with a focus on older adults. *In*: WORKSHOP on accessible security and privacy. [S.l.]: IEEE, 2024. Disponível em: http://dx.doi.org/10.2139/ssrn.4828190. Acesso em 19 jun. 2024.

NUNAM, Adriana; PENIDO, Maria Amélia. **Relacionamentos Amorosos na Era Digital**. 1. ed. São Paulo: Editora dos Editores, 2019.

OLIVEIRA, Amanda Nogueira de; LEMOS, André Luiz Martins. Banida por ser trans? Enviesamentos algorítmicos, plataformas e denúncia no Tinder. **C&S,** São Bernardo do Campo, v. 45, n. 2, p. 129-160, maio-ago. 2023. Disponível em: https://core.ac.uk/download/599335072.pdf. Acesso em: 30 jun. 2024.

PUGLISI, Silvia. Analysis, modelling and protection of online private data. 2017. Tese (Doutorado) - Universitat Politècnica de Catalunya, España, 2017. Disponível em: https://www.tdx.cat/handle/10803/456205. Acesso em: 19 jun. 2024.

RANSBOTHAM, Sam; FICHMAN, Robert G.; GOPAL, Ram; GUPTA, Alok. special section introduction: ubiquitous it and digital vulnerabilities. **Information systems research**, v. 27, n. 4, p. 834-847, 2016. Disponível em: http://www.jstor.org/stable/26652532. Acesso em: 19 jun. 2024.

SANT'ANA, Ricardo César Gonçalves. Ciclo de vida dos dados: uma perspectiva a partir da Ciência da Informação. **Informação & Informação**, Londrina, v. 21, n. 2, p. 116–142, 2016. Disponível em: https://doi.org/10.5433/1981-8920.2016v21n2p116. Acesso em: 17 mar. 2024.

SAMPAIO, Rafael Cardoso; LYCARIÃO. **Análise de conteúdo categorial**: manual de aplicação. 1. ed. Brasília: Escola Nacional de Administração Pública, 2021.

SHETTY, Rushank; GRISPOS, George; CHOO, Kim Kwang-Raymond. Are you dating danger? an interdisciplinary approach to evaluating the (in)security of android dating apps. **IEEE transactions on sustainable computing,** v. 6, n. 2, p. 197-207, 2021. Disponível em: https://ieeexplore.ieee.org/document/8207632. Acesso em: 18 jun. 2024.

SONG, Dacheng; CHEN, Ming; FAN, Sheng. The study of privacy protection of scientific data sharing based on data life cycle. **Journal of Physics**: conference series, v. 1952, n. 4, p. 042142, 2021. Disponível em: https://iopscience.iop.org/article/10.1088/1742-6596/1952/4/042142#:~:text=10.1088/1742%2D6596,Artigo%20PDF. Acesso em: 20 jun. 2024.

STENZEL, Paul; LE-KHAC, Nhien-An. Users on dating applications: a forensic perspective. **Digital forensics and cyber crime**, v. 570, p. 58-77, 2024. Disponível em: https://doi.org/10.1007/978-3-031-56580-9_4. Acesso em: 19 jun. 2024.

WALKER, Chris Stokel. I’ve have been banned from almost every dating app. **Vice**. 25 set. 2023. Disponível em: https://www.vice.com/en/article/banned-from-dating-apps/. Acesso em: 16 set. 2024.