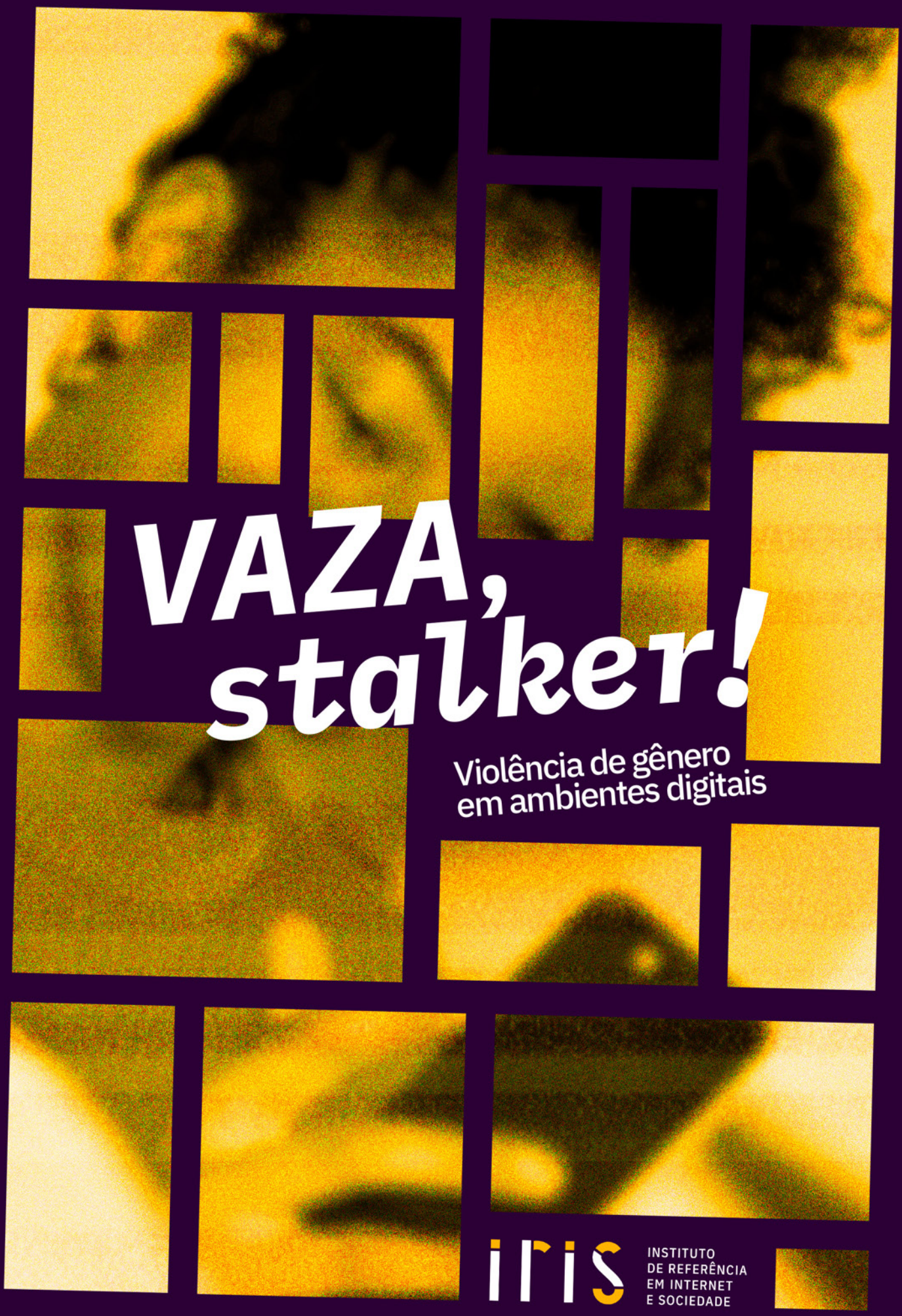


VAZA, stalker!

Violência de gênero em ambientes digitais

iris
INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE

VAZA, stalker!

Violência de gênero em ambientes digitais

AUTORIA
Ana Bárbara Gomes Pereira
Luisa Mello
Luiza Correa de Magalhães Dutra

REVISÃO
Paloma Rocillo
Fernanda Rodrigues

PROJETO GRÁFICO, CAPA, DIAGRAMAÇÃO E FINALIZAÇÃO
Felipe Duarte
Imagem de capa: freepik.com

COMO CITAR EM ABNT
PEREIRA, Ana Bárbara Gomes; MELO, Luisa. DUTRA, Luiza Correa de Magalhães. **Vaza Stalker!** Violência de gênero em ambientes digitais. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2025. Disponível em: https://bit.ly/43bRTHG. Acesso em: dd mmm aaaa.

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

DIREÇÃO

Ana Bárbara Gomes

Paloma Rocillo

MEMBROS

Felipe Duarte | Coordenador de Comunicação

Fernanda Rodrigues | Coordenadora de Pesquisa e Pesquisadora

Luisa Melo | Estagiária de pesquisa

Luiza Correa de Magalhães Dutra | Pesquisadora

Paulo Renâ da Silva Santarém | Pesquisador

Vióría Santos | Pesquisadora

Wilson Guilherme | Pesquisadore

irisbh.com.br

VAZA, stalker!

Esta publicação faz parte do projeto “Vaza, stalker! Proteção de Mulheres da Vigilância Digital”.

Conheça as demais publicações do projeto e saiba mais aqui!

Sumário

Sumário Executivo

- A violência de gênero facilitada pela tecnologia se apresenta enquanto um problema contemporâneo que envolve questões relativas à segurança, privacidade e direitos das mulheres.[1] Em uma sociedade marcada por estruturas patriarcais, as tecnologias digitais podem ser instrumentalizadas para aprofundar formas preexistentes de controle e violência contra corpos femininos. Nesse contexto, o uso de *spyware* e *stalkerware* para acessar dados pessoais e monitorar mulheres configura uma manifestação contemporânea da violência de gênero, cuja dinâmica e implicações demandam investigação crítica e aprofundada.

- *Spywares* são softwares espiões usados para monitorar e controlar o uso de dispositivos, redes ou sistemas eletrônicos. Uma vez instalados, esses softwares maliciosos (*malwares*) permitem acesso a dados pessoais, registros de comunicações e monitoramento de atividades realizadas no dispositivo invadido. Geralmente são usados em contextos cibercriminosos, com finalidades políticas, financeiras ou investigativas. Já os *stalkerwares*, centrais na presente pesquisa, são uma forma específica de *spyware* voltada para o monitoramento íntimo, geralmente em contextos de relacionamentos abusivos. Trata-se do uso de aplicativos aparentemente legítimos com o intuito de vigiar parceiros, ex-companheiros ou familiares.

- Este projeto buscou analisar e explorar de que maneira os dados pessoais coletadas por aplicativos digitais podem ser manipulados e explorados por *stalkerwares* e softwares espiões (*spywares*), evidenciando fragilidades que colocam em risco a privacidade, a autonomia e a liberdade das usuárias, além de compreender como esse tipo de acesso pode ser utilizado como ferramenta para reforçar e ampliar práticas de violência de gênero.Nosso objeto de pesquisa, portanto, foi a violência de gênero online a partir do uso de softwares espiões.

- Nossa metodologia consistiu em uma análise documental envolvendo revisão exploratória sobre o tema e análise das políticas de privacidade de aplicativos frequentemente baixados em dispositivos Android.

- Como resultados, encontramos que a violência de gênero exercida por meio de espionagem e vigilância massiva é perpetrada, frequentemente, por parceiros íntimos, e que tende a ocorrer a partir do uso de dados coletados por aplicativos, como geolocalização, fotos e vídeos do dispositivo, acesso à câmera e ao microfone, trocas de mensagens, nome da usuária, endereço, e-mail, número de telefone, lista de contatos, registro de chamadas, senhas, dados bancários e informações sobre a vida sexual/afetiva da mulher. Nesse âmbito, violências regularmente mencionados pela literatura são assédio, perseguição, stalking, abuso financeiro e monitoramento de comportamentos.

1 Quando falamos de mulheres aqui neste relatório, estamos tratando de indivíduos que se identificam dentro do espectro da performatividade feminina, incluindo mulheres cisgênero, mulheres transgênero, travestis e pessoas não binárias do gênero feminino, entre outras manifestações da feminilidade.

- Outra informação pertinente é que alguns aplicativos desempenham funções que podem ser utilizadas para espionagem, sem a necessidade de recorrer a *spywares*. Esses aplicativos são conhecidos como *dual-use apps*.

- Concluímos que, segundo as políticas de privacidade, muitos aplicativos frequentemente baixados em dispositivos Android coletam uma série de dados sensíveis, que podem ser utilizados para propagação e sofisticação da violência de gênero - se acessados por terceiros maliciosos. Concretiza-se, assim, um cenário no qual perseguições, abusos psicológicos, controle financeiro e violências sexuais são facilitadas pela tecnologia, evidenciando as maneiras pelas quais softwares e aplicativos podem ser manipulados em favor da dominação patriarcal.

Apresentação

O IRIS é um centro de pesquisa independente e interdisciplinar dedicado a produzir e comunicar conhecimento científico sobre os temas de internet e sociedade com o objetivo de fomentar políticas públicas que avancem os direitos humanos na área digital. Há mais de 8 anos o IRIS se dedica em específico às pautas de segurança e privacidade e inclusão de mulheres em ambientes digitais, como por exemplo com pesquisas específicas que criticam o uso de tecnologias digitais alternativas à quebra de criptografia para fins de investigações criminais[2], e ações que defendem a inclusão de mulheres em ambientes digitais.[3]

Buscando aproximar as áreas de segurança digital e de combate à violência de gênero, o presente estudo registra os resultados finais do projeto **VazaStalker: proteção de mulheres em ambientes digitais**[4], realizado com o apoio da Data Privacy Brasil e conduzido de forma independente, com o **objetivo de identificar como os principais aplicativos digitais utilizados por mulheres podem ser uma porta de entrada para uso de *spyware* e vigilância massiva como prática de violência de gênero**.

Buscamos fornecer hipóteses e inferências baseadas em evidências sobre como aplicativos e dados coletados no meio digital podem ser usados para objetivos ilícitos,

2 DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Hacking Governamental: uma revisão sistemática.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponível em: <https://bit.ly/3YdVcIL>.
PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Varredura pelo lado do cliente: uma revisão sistemática.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: <bit.ly/3EAhEDF>.
RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2022. Disponível em: <https://bit.ly/3yLlb0P>.

3 INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE (IP.REC) (Recife, Pernambuco); INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE (Belo Horizonte, Minas Gerais) (org.). **Por Mais #MulheresNaGovernança da Internet.** 2. ed. aum. [S. l.]: IP.rec; IRIS, março 2024. 40 p. Cartilha. Disponível em: https:// bit.ly/3TCW9ts.

4 IRIS-BH. Vaza, Stalker! Proteção de Mulheres da Vigilância Digital. Belo Horizonte, 2024. Disponível em: , https://encr.pw/zWPpe .. Acesso em: 6 maio 2025.

como a violência de gênero. Esta pesquisa é um passo necessário para ampliação do debate sobre violência de gênero online e formas de resistências e enfrentamento a esses atos.

Além deste relatório final, também elaboramos um zine, com objetivo de comunicar sobre os riscos e formas de proteção contra invasões de privacidade e vigilantismo por meio de aplicativos espiões. Em parceria com organizações do terceiro setor que atuam na proteção das mulheres[5], o material será desenvolvido com base em nosso estudo, incorporando contribuições e sugestões dessas organizações. Nosso compromisso com a rigorosidade científica e com a promoção de mudanças sociais, visando à democratização do acesso seguro à internet, também se reflete na construção colaborativa de documentos acessíveis a diversos públicos.

Gostaríamos de expressar nossos mais sinceros agradecimentos ao CodingRights, MariaLab, Coletivo aBertha e Casa Tina Martins. O apoio generoso de vocês e as trocas enriquecedoras ao longo do processo foram fundamentais para a realização do projeto VazaStalker. Seguimos juntas na luta contra a violência de gênero, fortalecendo redes de cuidado, resistência e transformação.

Nosso objetivo não consiste em promover um simples 'denuncismo' em relação às plataformas analisadas, uma abordagem que seria restritiva no contexto científico. Buscamos, ao contrário, contribuir para a formação de um campo crítico que demonstre a sofisticação das novas formas de violência nos ambientes digitais. Nesse sentido, procuramos identificar mecanismos que favoreçam a resistência e o enfrentamento dessas questões, como foco na construção de um ambiente digital verdadeiramente democrático.

Introdução

A violência de gênero facilitada pela tecnologia, conforme definido pela ONU Mulheres,[6] refere-se a qualquer ato de violência cometido, ampliado ou facilitado pelo uso de tecnologias de comunicação e informação, ou outras ferramentas digitais. Esse tipo de violência pode resultar em danos físicos, psicológicos, sexuais, sociais, políticos ou econômicos, ou até em outras violações de direitos. Embora termos como "violência digital" ou "online" sejam comumente usados, a expressão "violência de gênero facilitada pela tecnologia" descreve de maneira mais precisa como a tecnologia pode ser utilizada tanto no ambiente virtual quanto físico para cometer abusos, segundo o mesmo documento.

5

6 UNRIC - CENTRO DE INFORMAÇÃO DAS NAÇÕES UNIDAS EM BRASIL. **Como a violência de gênero facilitada pela tecnologia afeta as mulheres.** UNRIC, 2021. Disponível em: https://unric.org/pt/como-a-violencia-de-genero-facilitada-pela-tecnologia-afeta-as-mulheres/. Acesso em: 9 abr. 2025.

Nesse contexto, o uso de *spywares* contra mulheres se torna uma forma particularmente insidiosa de violência de gênero, pois amplia as possibilidades de vigilância e controle. *Spywares*, ao monitorar as atividades das vítimas sem seu consentimento, não só invadem a privacidade, mas também intensificam a violência psicológica e emocional. O controle de comunicações, localização, e até a coleta de dados bancários podem ser usados por agressores para perseguir, intimidar e controlar suas vítimas de forma constante e inescapável. Essa prática de vigilância digital, portanto, não só agrava a violência de gênero, mas também a torna mais difícil de detectar.

Além disso, o uso de *spyware* como ferramenta de abuso no contexto de violência doméstica complexifica ainda mais o cenário, ao se conectar com tendências de tecnoautoritarismo. Esse fenômeno reflete como a tecnologia, em mãos de indivíduos ou estados, pode ser usada para regular e controlar a vida das pessoas de maneira autoritária, especialmente em grupos vulnerabilizados.[7] Em 2021, a AccessNow[8] revelou que defensoras de direitos humanos no Oriente Médio foram alvo do Pegasus[9], tendo sido suas comunicações privadas usadas para assediá-las. Outro relatório de 2022[10] denunciou o uso de *spyware* para silenciar mulheres na Tailândia, havendo inclusive prejuízos ao exercício das práticas laborais das vítimas. No contexto privado[11], o uso de *spyware* também tem sido extensamente relatado como ferramenta de prática de violência doméstica.

Os dados do Anuário de Segurança Pública evidenciam essa realidade de violência de gênero, revelando que mulheres cis, trans e pessoas não binárias, associadas ao feminino, são frequentemente alvo de violências que vão além do espaço físico; essas informações corroboram o que autoras de referência na pauta de gênero e tecnologia têm demonstrado sobre a crescente violência de gênero online no Brasil[12]. Em 2023, país foi o segundo com mais vítimas de violência digital via *stalkerware*[13].

7 DATA PRIVACY BR. **Defendendo o Brasil do Tecnoautoritarismo**. Disponível em:https://encurtador.com.br/nV4Jr. Acesso em: 31 out. 2024.

8 ACCESS NOW. Unsafe anywhere: attacked by Pegasus, women activists speak out. Publicado em: 17 jan. 2022. Disponível em: https://encurtador.com.br/zXMJ9. Acesso em: 31 out. 2024.

9 O Pegasus é um spyware desenvolvido pela empresa israelense NSO Group, especializada em ferramentas de espionagem cibernética. Desde 2013, o Pegasus tem sido utilizado por governos para monitorar e coletar dados de alvos, incluindo em tempo real. Ele ficou amplamente conhecido em 2016, quando um ativista de direitos humanos dos Emirados Árabes Unidos, Ahmed Mansoor, detectou uma tentativa de infecção em seu iPhone. Esse incidente foi considerado o "ataque de smartphone mais sofisticado de todos os tempos". O uso do Pegasus tem sido associado a violações de direitos humanos, atentados à democracia e à soberania de países. DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Hacking Governamental: uma revisão sistemática.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponível em: <https://bit.ly/3YdVcIL>. Acesso em: 02.04.2025.

10 AMNESTY INTERNATIONAL. Thailand**: State-backed digital abuse used to silence women and LGBTI activists - new report.** Publicado em: 16 mai. 2024. Disponível em:https://encurtador.com.br/v6lDO. Acesso em: 31 out. 2024.

11 CHATTERJEE, Rahul et al. The Spyware Used in Intimate Partner Violence. In: **SYMPOSIUM ON SECURITY AND PRIVACY,** 2018. Anais [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2018. p. 441-458.

12 VALENTE, Mariana. **Misoginia na internet**. 2023. São Paulo: Editora Fósforo.

13 EX PRIME. **Brasil segue como segundo país com mais vítimas de violência digital via stalkerware, aponta Kaspersky.** Publicado em: 1 mar. 2023. Disponível em: https://lexprime.com.br/brasil-segue-como-segundo-pais-com-mais-vitimas-de-violencia-digital-via-stalkerware-aponta-kaspersky/. Acesso em: 31 out. 2024.

Um relatório da Abraji aponta, ainda, que mulheres jornalistas enfrentam ameaças e agressões com o objetivo de silenciá-las, muitas vezes utilizando táticas como intimidação e ameaças a suas famílias.[14] Esse cenário cria um ambiente propício para o uso de *spyware*, que, como ferramenta de vigilância, pode ser empregado para monitorar e controlar as vítimas. O uso de *spyware* é tanto uma invasão de privacidade quanto uma ameaça direta à autonomia e à segurança das mulheres, facilitando práticas como stalking e o acesso a dados íntimos. Esse contexto se torna ainda mais complexo em uma sociedade que historicamente impõe o controle sobre os corpos femininos.

Reconhecer como as tecnologias são projetadas para reforçar essas dinâmicas é essencial para o desenvolvimento de estratégias de prevenção e defesa. Um aspecto central desse processo é a utilização de técnicas de engenharia social, que exploram vulnerabilidades socioemocionais para atingir o alvo. Quando os agressores conhecem os modos de vida, desejos e hábitos das mulheres, tornam-se mais eficazes em identificar suas fraquezas, de modo que o acesso a Tecnologias da Informação e Comunicação (TIC) passa a desempenhar um papel significativo na incidência de violência de gênero, tanto no ambiente online quanto offline.

Em se tratando de formas de violência de gênero online, a partir dos conceitos-chave aqui trabalhados, e que serão melhor explorados em capítulo específico, nossa discussão recai fortemente sobre o que se entende por *stalkerware* - uma forma específica de *spyware* voltada para o monitoramento íntimo, geralmente em contextos de relacionamentos abusivos. Trata-se do uso de aplicativos aparentemente legítimos, como ferramentas de controle parental ou segurança, com a finalidade de vigiar parceiros, ex-companheiros ou familiares. Esses softwares são, muitas vezes, instalados manualmente por alguém com acesso físico ao dispositivo da vítima, e seu principal objetivo é exercer controle e vigilância sobre alguém próximo. Apesar de muitas vezes distribuídos legalmente, o uso do *stalkerware* é um frequentemente um agravante para casos de violência doméstica e de gênero.

Embora o *stalkerware* seja tecnicamente uma subcategoria de *spyware*[15] — ambos são softwares espiões —, há diferenças significativas quanto ao propósito, ao público-alvo e ao contexto de uso. O *spyware* tradicional é amplamente associado a atividades cibercriminosas, sendo utilizado por hackers, empresas ou governos para espionar indivíduos ou organizações em grande escala. Seu foco costuma ser financeiro, político ou estratégico, e a instalação ocorre de maneira remota, geralmente via links maliciosos, phishing ou downloads contaminados. Ao contrário do *stalkerware,* que tem uma vítima específica e um contexto interpessoal, o *spyware* pode vir a operar de forma mais ampla

14 ABRAJI - ASSOCIAÇÃO BRASILEIRA DE JORNALISMO INVESTIGATIVO. **Relatório: violência de gênero contra jornalistas.** ABRAJI, 2021. Disponível em: https://abraji.org.br/publicacoes/relatorio-violencia-de-genero-contra-jornalistas. Acesso em: 9 abr. 2025.

15 KHO, Cynthia; ROBERTSON, Kate; DEIBERT, Ronald. **Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications.** 2019. Electronic version first published by Citizen Lab. Disponível em: https://citizenlab.ca/docs/stalkerware-legal.pdf . Acesso em: 3 abr. 2025.

e impessoal - ainda assim existem situações que o spyware pode ser usado para vigiar e controlar pessoas específicas.[16]

Assim, o objetivo desta pesquisa foi analisar como os dados pessoais já coletados por aplicativos digitais podem ser explorados por *stalkerwares e spyware*, convertendo-se em vulnerabilidades que comprometem a privacidade, autonomia e liberdade das usuárias, e de que forma esse acesso pode ser instrumentalizado para perpetuar e intensificar a violência de gênero. Para isso, partimos da pergunta: De que forma os dados pessoais coletados por aplicativos digitais podem ser explorados por *spyware e stalkerwares*, e como essa exploração contribui para a perpetuação da violência de gênero?

A pesquisa consistiu na análise de dez aplicativos mais populares e amplamente utilizados no Brasil — incluindo plataformas de relacionamento, mobilidade urbana e controle parental — com o intuito de mapear quais dados esses apps coletam, armazenam e compartilham. A partir da leitura de suas políticas de privacidade, buscamos compreender quais informações sensíveis (como localização, redes de contato, interações e comportamentos) estão sendo processadas e como esses dados podem ser explorados por softwares espiões, especialmente *stalkerwares*- isso quando acessados por uma pessoa maliciosa em contexto de violência de gênero,

Nosso foco se volta, particularmente, para os riscos de vigilância digital em contextos de violência de gênero, nos quais o uso desses dados por agressores pode tornar os mecanismos de controle mais sofisticados, invasivos e difíceis de detectar. Ao rastrear hábitos, rotinas e relações pessoais, o uso abusivo dessas tecnologias amplia a capacidade de dominação, coerção e silenciamento das vítimas, mesmo após o fim de relacionamentos ou em situações de distanciamento físico.

Para discutirmos nossos achados de pesquisa, dividimos nosso relatório em 03 partes principais: i) conceitos-chave para nossa pesquisa, buscando apresentar o debate teórico de onde partimos; ii) metodologia das nossas etapas de pesquisa, apresentando os motivos pelos quais decidimos percorrer nosso caminho de pesquisa - passando desde a revisão de literatura, até a escolha pelos aplicativos analisados; iii) apresentação da análise crítica das políticas de privacidade dos aplicativos, com o objetivo de identificar e inferir de que forma os dados coletados, quando acessados por um terceiro malicioso, podem ser explorados em contextos de violência de gênero, especialmente quando associados ao uso de *spywares* e *stalkerwares*. Ainda, dentro de cada categoria de análise iremos apresentar um caso concreto para ilustrar os debates trazidos.

16 ACCESS NOW. Unsafe anywhere: attacked by Pegasus, women activists speak out. Publicado em: 17 jan. 2022. Disponível em: https://encurtador.com.br/zXMJ9. Acesso em: 3 mar. 2025.

1. Conceitos-chave: O que entendemos enquanto violência de gênero facilitada pela tecnologia, violência por parceiro íntimo, *spyware* e vigilância

A fim de delimitar nosso objeto de pesquisa, procuramos definir conceitos basilares para o presente estudo. Nessa fase, leituras exploratórias sobre os temas de violência de gênero, violência de gênero online e uso de *spywares* foram essenciais para a delimitação dos termos. Além disso, também foram trabalhados conceitos necessários a essas análises, como o de violência por parceiro íntimo e vigilância. Abaixo, explicamos cada um deles.

1.1. Violência de gênero

Saffioti tem um entendimento amplo do conceito de violência de gênero, entendendo que ele abrange vítimas de diferentes idades e gêneros, expostos às consequências da concentração de poder nas mãos de figuras masculinas em estruturas patriarcais da sociedade. Como a autora salienta, nesses contextos em que há um projeto de dominação-exploração pelos homens, a subjugação de gênero prescinde da presença física dessas figuras. Refletida em dimensões políticas e econômicas, a violência de gênero seria introjetada e naturalizada pelos indivíduos, compondo ações e formas de pensamento. De acordo com Saffioti, "nenhuma relação social se passa fora da estrutura. Todas elas obedecem às normas que estruturam a sociedade por inteiro". [17]

As discussões sobre gênero também se articulam com os debates foucaultianos acerca da produção de verdades e da constituição das subjetividades. Em especial, essas discussões passam pelo conceito de *dispositivo de sexualidade* — uma rede de saberes, práticas e normas que regulam os corpos e os desejos, funcionando como um mecanismo de controle da população. Nesse contexto, o gênero pode ser compreendido como uma *tecnologia*, isto é, como uma forma de exercício do poder que atua na constituição dos sujeitos a partir da normatização dos corpos.

Para Foucault, em *História da Sexualidade – Volume 1*,[18] o poder não é algo que se possui, mas sim uma relação dinâmica e difusa, presente em toda parte, atravessando

17 SAFFIOTI, Heleieth I.B. Contribuições feministas para o estudo da violência de gênero. **Cadernos Pagu**, Campinas, v. 16, p. 115-136, 2001.

18 FOUCAULT, Michel. **História da sexualidade: volume 1: a vontade de saber.** Tradução de Sérgio Telles. 21. ed. Rio de Janeiro: Graal, 2010.

os indivíduos e suas práticas. As chamadas *tecnologias de poder*, como a de gênero, operam por meio dessas relações, moldando comportamentos e identidades a partir de dispositivos regulatórios que definem o que pode ou não ser dito, feito ou vivido.

Nesse sentido, o gênero, entendido como tecnologia, não é apenas uma identidade ou uma categoria estática, mas um conjunto de práticas performativas e discursivas que organizam os corpos segundo normas sociais específicas. Essa tecnologia estabelece hierarquias entre os corpos, permitindo que alguns se apresentem como legítimos ou universais, enquanto outros são marginalizados ou excluídos. Assim, gênero é uma construção social atravessada por estratégias de poder e dominação.

Para além disso, não se pode falar em qualquer tipo de violência no Brasil, sem se falar sobre marcadores sociais da diferença. A violência de gênero não se coloca de forma similar a todas as pessoas que se identificam mulheres; a raça, por exemplo, é um diferenciador nesta construção violenta. E aqui tratamos de raça não enquanto conceito biológico, mas enquanto categoria social e política que atravessa corpos de forma a criar hierarquias sociais e formas distintas de experiências no mundo - onde a violência também se insere.[19]

A escolha pelo uso do termo "violência de gênero" no lugar de "violência contra a mulher" tem sua justificativa encontrada em outros estudos do campo, focados nas terminologias utilizadas. Azambuja e Nogueira[20] entendem que os termos no campo dos estudos de gênero são histórica e geograficamente situados: o próprio entendimento do que é considerado violência depende do contexto analisado. Tomando a história como fio condutor, as pesquisadoras acompanham, no artigo analisado, o desenvolvimento dos conceitos relativos à violência de gênero no Brasil e suas implicações no campo.

Os termos violência doméstica, sexual e familiar foram inicialmente criados para categorizar agressões físicas e psicológicas em contextos específicos, com o conceito de "violência contra a mulher" surgindo como uma definição mais ampla, centrada na vítima feminina. No entanto, essa abordagem não considerava o sexo do agressor, as dinâmicas de poder e excluía vítimas de outros sexos, como homens, meninos, idosos e pessoas LGBTQIAPN+. A definição de "violência de gênero" surgiu para abarcar essas questões, introduzindo o conceito de gênero como uma abordagem relacional e desafiando a ideia de "mulheres" como um grupo homogêneo.

Debert e Gregori [21]complementam essa discussão, afirmando, ainda, que o conceito de gênero teve fundamental importância na crítica à "vitimização" e à retirada de agência de figuras femininas pelo termo "violência contra a mulher". De acordo com as autoras,

19 MUNANGA, Kabengele. **Rediscutindo a mestiçagem no Brasil - Nova Edição: Identidade nacional versus identidade negra.** 2. ed. São Paulo: Editora XYZ, 2015.

20 AZAMBUJA, Mariana Porto Ruwer de; NOGUEIRA, Conceição. Violência de gênero: uma reflexão sobre a variabilidade nas terminologias. **Saúde em Debate**, Rio de Janeiro, v. 31, n. 75/76/77, p. 97-106, jan./dez. 2007

21 GRIN DEBERT, Guita; GREGORI, Maria Filomena. Violência e gênero: novas propostas, velhos dilemas. **Revista Brasileira de Ciências Sociais**, v. 23, n. 66, 2008.

"violência de gênero" se proporia a ser menos essencialista e a analisar violências conjunturais. Sem limitar-se a aspectos biológicos ou universalizar a categoria "mulher", os estudos de gênero, como propõe Butler,[22] analisam a normatização do masculino e do feminino enquanto performances - como antes explicitado.

Assim, a presente pesquisa propõe-se a analisar a violência de gênero, manifestada como comportamentos que buscam restringir mulheres a papéis de feminilidade nos termos demandados pelo poder e estrutura patriarcal e que buscam puni-las em caso de transgressão a essas normas. Nosso estudo tem como foco o entendimento das ações no campo do poder-saber e o controle de corpos que se entendem enquanto femininos, compreendendo que esses são frequentemente subjugados nas relações pautadas por gênero no cenário estudado: o Brasil. Desse modo, embora esse tipo de violência também possa afetar homens, centramos nossa análise em mulheres. As relações de poder identificadas perpassam questões como vigilância, violência psicológica e controle sobre comportamentos femininos, entendidas como manifestações de assimetrias de gênero, visto que representam tentativas de tolher a liberdade de mulheres e limitá-las a papéis restritos.

1.2. Violência de gênero facilitada pela tecnologia

O conceito de "violência de gênero facilitada pela tecnologia", termo definido no contexto da sexagésima sétima sessão da Comissão sobre o Status da Mulher, se refere a qualquer ato que seja cometido, assistido, agravado ou amplificado pelo uso de tecnologias e ferramentas digitais. Os danos desse tipo de ação podem ser físicos, sexuais, psicológicos, sociais, políticos ou econômicos, bem como outras violações de direitos. De acordo com a ONU Mulheres, trata-se de uma forma de violência de gênero, pois mulheres e meninas seriam mais afetadas[23].

No mesmo sentido, a violência de gênero facilitada pela tecnologia, segundo relatório da Unesco, é um problema crescente em uma sociedade informacional e tecnificada, uma vez que abarca práticas como ameaças, assédio, espionagem e invasão de privacidade[24]. Entende-se que, nesses contextos, as tecnologias de comunicação ou ferramentas digitais tratam-se de artifícios para facilitar, potencializar ou reinventar formas de violência já existentes. Ou seja, são maneiras de sofisticar violações marcadamente sexistas, tais quais as agressões verbais dirigidas às mulheres, a vigilância sobre seus comportamentos, a importunação sexual, entre outros.

Considerando que o termo "violência de gênero facilitada pela tecnologia" tem

22 BUTLER, Judith. **Undoing gender**. New York; London: Routledge, 2004.

23 UN Women. **FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women.** 10 fev. 2025. Disponível em: https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women. Acesso em: 3 abr. 2025.

24 UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION (UNESCO). **Your opinion doesn't matter, anyway: Exposing Technology-Facilitated Gender-Based Violence in an Era of Generative AI.** Paris: UNESCO, 2023. (World Trends in Freedom of Expression and Media Development Series). ISBN 978-92-3-100669-2. 2. ed.

especificidades em relação a “violência de gênero online” ou “violência de gênero digital”, como a compreensão nítida de que seus impactos repercutem também fora do mundo das redes, ambos serão utilizados como sinônimos em nossa pesquisa como forma de referência ao mesmo fenômeno: as maneiras pelas quais a tecnologia pode ser mobilizada a fim de perpetuar violências de gênero. No caso específico do nosso objeto de estudo, como aplicativos e softwares podem ser aplicados para controlar e violar mulheres.

1.3. Violência por parceiro íntimo (IPV)

A violência por parceiro íntimo (ou *intimate partner violence*, em inglês) é um conceito utilizado em pesquisas nas áreas de humanidades[25], relacionando-o com estudos no campo de gênero. Como explicado no relatório do Citizen Lab, o termo pode ser usado para se referir a abusos perpetrados tanto por parceiros quanto por ex-parceiros de relacionamentos amorosos[26]. Além disso, as formas de violência são diversas, podendo envolver assédios, agressões físicas, abusos psicológicos, privações econômicas e controle de comportamentos.

Como menciona Abbas Z.Kouzani, a definição de “violência doméstica” para as Nações Unidas, também chamada de “violência entre parceiros íntimos”, consiste em ações recorrentes, dentro de um relacionamento, com o intuito de manter o parceiro sob dominação[27]. Isso abrange abusos e ameaças sexuais, físicas, emocionais, psicológicas ou econômicas, gerando medo, intimidando, manipulando, desonrando ou ferindo o parceiro.

Segundo Gupta e Verma, quando facilitada pela tecnologia, a violência por parceiro íntimo pode encontrar mecanismos para ser potencializada, valendo-se de formas de violência de gênero digital, como hacking, controle ou manipulação de informações, doxxing, disseminação de fotos íntimas ou informações privadas, uso de *spyware*, vigilância, stalking, falsificação de identidade, perseguição na forma de envio de materiais sexuais não solicitados ou indesejados online, e ameaças de estupro. [28] De acordo com as autoras, as TICs podem ser ferramentas manipuladas para que parceiros íntimos exerçam controle

25 **BRANCAGLIONI, Bianca de Cássia Alvarez; FONSECA, Rosa Maria Godoy Serpa da.** Violência por parceiro íntimo na adolescência: uma análise de gênero e geração. *Revista Brasileira de Enfermagem*, Brasília, v. 69, n. 5, p. 940–947, set./out. 2016.
MOREIRA, Alexandro Martins; CECCARELLI, Paulo Roberto. Há múltiplas faces na violência por parceiro íntimo. *Revista Médica de Minas Gerais*, Belo Horizonte, v. 26, supl. 8, p. 351–354, 2016. **MACHADO, Dinair Ferreira; CASTANHEIRA, Elen Rose Lodeiro.** Interseções entre socialização de gênero e violência contra a mulher por parceiro íntimo. *Ciência & Saúde Coletiva*, Rio de Janeiro, v. 26, supl. 3, p. 5003–5012, 2021.

26 KHO, Cynthia; ROBERTSON, Kate; DEIBERT, Ronald. **Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications.** 2019. Electronic version first published by Citizen Lab. Disponível em: https://citizenlab.ca/docs/stalkerware-legal.pdf . Acesso em: 3 abr. 2025.

27 KOUZANI, A. Z. Technological Innovations for Tackling Domestic Violence. **IEEE Access**, v. 11, p. 91293-91311, 2023.

28 VERMA, Rabindra Kumar; GUPTA, Ashish Kumar. Role of Information and Communication Technology in the Digitalization of Violence and Sexual Politics in the Indian Scenario. In: **CYBERFEMINISM AND GENDER VIOLENCE IN SOCIAL MEDIA**, 2023. p. 35-48.

e poder dentro do relacionamento. Nesse sentido, elas facilitariam o monitoramento de atividades da vítima, a manipulação, a coação e a invasão de privacidade pelo acesso a contas pessoais e dispositivos sem consentimento.

Nesse sentido, consideramos, para os fins desta pesquisa, a "violência por parceiro íntimo" como qualquer forma de violência perpetrada por um parceiro ou ex-parceiro em relação à mulher com quem tem ou teve relação afetiva, tendo como intuito sua agressão, manipulação ou controle. É dado enfoque à violação de direitos dessas mulheres, tendo como mediação a tecnologia, principalmente as que possibilitam vigilância.

1.4. Spyware e Stalkerware

Spywares são programas espiões usados para monitorar e controlar o uso de dispositivos, redes ou sistemas eletrônicos. Uma vez instalados, esses softwares permitem acesso a dados pessoais e registros de comunicações, além do monitoramento de atividades realizadas no dispositivo.[29]

Os *spywares* são especialmente desenvolvidos para infiltrar-se em sistemas sem autorização da pessoa afetada e aproveitam vulnerabilidades para isso. Sabe-se que a infecção de um dispositivo pode permitir, por exemplo, ouvir chamadas, fazer capturas de tela, ativar câmeras e microfones, esvaziar informações de um aparelho e captar mensagens antes que sejam criptografadas. [30]

Apesar de haver situações em que o seu uso é entendido por certos especialistas como legítimo (no caso de algumas investigações criminais, por exemplo), há demonstrados riscos à privacidade e outros direitos humanos a partir da utilização de *spywares*.[31]Sem regulamentação e permitindo a invasão de dados sensíveis, esses softwares podem ser utilizados para funções como vigilância em massa, espionagem política e violência por parceiros íntimos.

No que tange à forma de implementação, os *spywares* podem ser inseridos por 5 meios principais: a) ataques *man in the middle* (inglês para "homem no meio"), b) vulnerabilidades *zero-day* ("dia zero"), c) ataques *click-zero* ("zero cliques"); d) *spoofing* ("falsificação") e e) *phishing*.[32] Suas definições são resumidas abaixo:

a. Man in te middle: O atacante se coloca entre a comunicação de duas

29 DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Hacking Governamental: uma revisão sistemática.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponível em: <https://bit.ly/3YdVcIL>. Acesso em: 02/04/2025.

30 ROMÁN SOLTERO, Alberto Rafael et al. Análisis ético de la información en el escándalo Pegasus. Revista de Investigación en Tecnologías de la Información, [S.l.], v. 7, n. 14, p. 22-37, sep. 2019. ISSN 2387-0893. Disponível em https://www.riti.es/ ojs2018/inicio/index.php/riti/article/view/185. DOI: 10.36825/riti.07.14.003. Data de acesso: 13 mai. 2025. p. 28.

31 Ibidem

32 Ibidem

partes, passando-se por uma delas e trocando informações como se tivesse outra identidade.

b. Zero-day: O atacante explora vulnerabilidades no sistema operacional do telefone que são desconhecidas pela empresa e que, portanto, não possuem forma de combate.

c. Click-zero: O atacante encontra uma forma de acessar o dispositivo automaticamente, sem a necessidade de nenhuma ação por parte da vítima.

d. Spoofing: O atacante conquista a confiança da vítima para a obtenção dos seus dados, passando-se por um terceiro confiável ou criando um site falso onde ela deposite essas informações, por exemplo.

e. Phishing: O atacante envia uma mensagem ou link para o alvo, levando-o a acessar um domínio contaminado.

Por outro lado, dentro do campo de discussões sobre o uso de softwares espiões, e aproximando-se do campo da violência de gênero, o termo "*stalkerware*" surge para abarcar os softwares e outras ferramentas digitais que podem ser usadas para monitorar ou acessar dados de um dispositivo alvo. Diferentemente de *spyware*, o termo "*stalkerware*" se refere também a aplicativos que não foram necessariamente projetados para essa funcionalidade, descrevendo, portanto, as suas possibilidades de uso e não sua programação. A literatura do campo também se refere a esses aplicativos como "*dual-use apps*", termo também mobilizado na presente pesquisa.

Além disso, os *stalkerwares* são geralmente utilizados em relações interpessoais abusivas, como em casos de violência doméstica e de gênero. Seu objetivo é monitorar e controlar alguém próximo — geralmente um(a) parceiro(a), ex-companheiro(a) ou familiar. Ele costuma ser instalado manualmente no dispositivo da vítima por alguém com acesso físico ao aparelho, como em um relacionamento íntimo. [33] Esses aplicativos muitas vezes se disfarçam de ferramentas de "controle parental" ou "monitoramento de segurança", o que permite que sejam distribuídos de forma legal, apesar de o uso sem consentimento ser considerado crime.

Os aplicativos de *stalkerware* permitem acesso a uma série de informações que podem ser utilizadas para a violação da segurança da vítima, tais como lista de contatos, fotos e vídeos, interações em redes sociais e, sobretudo, geolocalização.[34] Os softwares de rastreamento e monitoramento são especialmente situados nessa categoria, tendo em

33 FREED, Diana; PALMER, Jackeline; MINCHALA, Diana; LEVY, Karen; RISTENPART, Thomas; DELL, Nicola. "A stalker's paradise": how intimate partner abusers exploit technology. In: **CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS**, 2018, Montreal. New York: ACM, 2018. Paper n. 667, p. 1–13.

34 KHO, Cynthia; ROBERTSON, Kate; DEIBERT, Ronald. I**nstalling Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications.** 2019. Electronic version first published by Citizen Lab. Disponível em: https://citizenlab.ca/docs/stalkerware-legal.pdf . Acesso em: 3 abr. 2025.

vista seu frequente reaproveitamento como ferramenta para violência de gênero - e aqui demonstramos sua proximidade com o campo de discussão sobre violência de gênero online.

2. Metodologia

Para realizar a presente pesquisa, a metodologia dividiu-se em três fases: revisão bibliográfica, a seleção de 10 aplicativos digitais frequentemente baixados e a análise de políticas de privacidade destes aplicativos previamente selecionados. Todas contaram com momentos de coleta, seleção e análise de dados, descritos a seguir.

MÉTODO DE COLETA	OBJETIVO	INSTRUMENTOS UTILIZADOS	ETAPAS DA COLETA	RESULTADOS OBTIDOS
Revisão de literatura exploratória	Acompanhar as discussões que têm sido feitas na academia e responder às perguntas: 1) Como a literatura discute a violência de gênero no ambiente online?; 2) Quais aplicativos e dados coletados são mais utilizados para perpetuar violência de gênero digital?	Repositórios online, Google Forms e Google Sheets	1) Busca por palavras-chave nos repositórios; 2) Análise dos títulos e resumos dos textos encontrados; 3) Leitura dos textos selecionados; 4) Sistematização dos resultados em tabela	1) Dados, serviços e aplicativos frequentemente visados; 2) Tipos de violências perpetradas; 3) Preponderância da violência por parceiro íntimo e papel dos dual-use apps

MÉTODO DE COLETA	OBJETIVO	INSTRUMENTOS UTILIZADOS	ETAPAS DA COLETA	RESULTADOS OBTIDOS
Seleção de 10 aplicativos digitais frequentemente baixados	Identificar aplicativos frequentemente usados que poderiam ser utilizados para violência de gênero	Planilha com resultados da revisão bibliográfica e PlayStore	1) Listagem dos aplicativos mais mencionados pela bibliografia; 2) Busca desses aplicativos na PlayStore e seleção dos que eram mais baixados entre eles; 3) Seleção dos aplicativos mais baixados (top 1) na PlayStore, em cada categoria da loja (Top Geral, Redes Sociais, Estilo de Vida, Comunicação, Esporte e Finanças)	1) 4 aplicativos mais citados pela literatura; 2) 6 aplicativos mais baixados na Play Store
Análise de políticas de privacidade	Mapear as vulnerabilidades dos aplicativos identificados que poderiam ser aproveitadas para violência de gênero	Planilha com resultados da revisão bibliográfica, políticas de privacidade de cada app selecionado e Google Sheets	1) Busca pelas políticas de privacidade de cada app; 2) Registro dos dados coletados pelos apps; 3) Cruzamento de dados, em uma planilha, entre as informações coletadas pelos aplicativos e as possíveis violências citadas pela literatura	Possíveis riscos de violência de gênero em caso de invasão por spyware/ stalkerware em apps frequentemente usados

2.1. Revisão de literatura exploratória

A revisão bibliográfica consistiu em uma busca e análise exploratória de literatura sobre o tema de violência de gênero por uso de *spywares*. Nesse momento, tínhamos como objetivo acompanhar as discussões que têm sido feitas na academia e compreender mais o campo em nossas principais temáticas de estudo. A questão central que norteou essa etapa foi: como a literatura discute a violência de gênero no ambiente online? Além disso, segundo os estudos, quais aplicativos e dados coletados por eles são mais utilizados para perpetuar essas violências digitais, com foco na vigilância massiva e uso de *spywares/stalkwares*?

2.1.1. Como os textos foram coletados e selecionados?

Primeiramente, foram realizadas buscas por palavras-chave em três bases de dados diferentes: **Google Acadêmico, Scopus e Scielo.** Em cada uma delas, foram pesquisados os termos **"violência de gênero" AND "*spyware*"; "violência de gênero" AND "*stalkerware*"; "violência de gênero" AND "espionagem digital"; e "violência de gênero" AND "vigilância digital"**, com o correspondente em inglês de cada um deles.[35] As palavras-chave foram escolhidas pela equipe com base em leituras prévias sobre o tema, as quais foram feitas no intuito de contextualizar as pesquisadoras nos debates acadêmicos sobre a temática em questão. Embora "violência de gênero" e "*spyware*" já fossem termos visados desde a escrita do projeto de pesquisa, outros tornaram-se relevantes a partir dos textos lidos, como "*stalkerware*".

Dessa etapa, foram selecionados materiais que continham em sua centralidade as discussões a partir dos termos "*spyware*" ou "*stalkerware*" e que, após análise do resumo e de uma leitura dinâmica das pesquisadoras, correspondiam ao tema de pesquisa, resultando em 14 textos para análise. Por outro lado, também foram selecionados, de forma discricionária, outros 5 textos identificados como pertinentes pelas pesquisadoras, paralelamente aos encontrados nas bases de dados.

Ao final, um total de 17 textos entraram efetivamente no escopo do projeto, pois abordavam diretamente os temas de *spyware*, violência de gênero, aplicativos e dados usados para vigilância massiva em contextos de violência de gênero online e possíveis aplicações de *spywares/stalkwares* para fins de vigilância massiva.

2.1.2. Como os textos foram analisados?

Os textos selecionados foram analisados a partir de um Google Forms que possuía perguntas como o nome da pesquisadora responsável, o título do texto, os autores, a plataforma em que foi encontrado, ano de publicação e tipo de texto (artigo, capítulo de livro ou monografia), a fim de identificação. Também foram feitas perguntas a

35 Correspondentes em inglês, na ordem respectiva: "gender violence" AND "spyware"; "gender violence" AND "stalkerware"; "gender violence" AND "digital espionage"; e "gender violence" AND "digital surveillance"

respeito do conteúdo dos textos: quais tipos de violência de gênero estavam envolvidas, quais as tecnologias visadas pelos *spywares* segundo o texto (ou seja, quais apps e funcionalidades digitais eram alvo de *spywares*), quais as vulnerabilidades mais visadas por esses softwares (fragilidades aproveitadas), quais os dados mais intencionados (informações que os perpetradores da violência pretendiam conseguir), citações e comentários (veja o formulário completo no Anexo I).

As respostas geraram uma planilha que foi analisada pelas pesquisadoras. A partir dela, foram criadas novas planilhas para a organização das informações: 1) quais os dados mais visados pelos *spywares* e para quais finalidades, segundo a bibliografia; 2) quais os apps mencionados nominalmente são visados para vigilância massiva e uso de *spywares*, e para quais finalidades, de acordo com a bibliografia; 3) quais os apps mencionados genericamente (como categoria) são visados para fins de espionagem e respectiva motivação segundo a bibliografia - todos dentro da discussão de gênero.

2.2. Aplicativos selecionados

A segunda fase da pesquisa consistiu em identificar aplicativos que poderiam ser utilizados para violência de gênero. Inicialmente, procuramos quais eram os aplicativos mais baixados por mulheres; no entanto, como não obtivemos êxito, dada a dificuldade de encontrar dados sobre a quantidade de downloads feita por mulheres, tanto em pesquisas sobre o tema quanto nas próprias lojas de apps, além do curto período para execução do projeto, que impediria a realização de um *survey* com o público-alvo, foram seguidos outros dois caminhos:

1. Identificação de aplicativos citados nominalmente nos textos da revisão bibliográfica;

2. Identificação dos aplicativos mais baixados segundo a loja de aplicativos Play Store.

O sistema Android e sua respectiva loja de aplicativos foram os escolhidos em detrimento do iOS e a Apple Store levando-se em conta sua preponderância de uso no Brasil[36]. Considerando os dois caminhos distintos para coleta de aplicativos, foram realizadas etapas diferentes para sua seleção. Ambas, no entanto, seguiram o mesmo padrão de considerar a quantidade de downloads de um app como indicativo de sua maior usabilidade pela população, da qual inferiu-se uma presença feminina igualmente considerável. As seleções de aplicativos seguiram os seguintes passos:

36 LARICCHIA, Federica**. Market share of mobile operating systems in Brazil from January 2019 to October 2024.** Statista, 22 out. 2024. Disponível em: https://www.statista.com/statistics/262167/market-share-held-by-mobile-operating-systems-in-brazil/. Acesso em: 26 fev. 2025.

1. Busca pelos apps mencionados nominalmente nos artigos analisados:

A partir das respostas obtidas no formulário de resultados da revisão bibliográfica à pergunta “Quais as tecnologias mais visadas para uso de *spywares*?”, foram listados todos os apps mencionados nominalmente nos textos (veja a lista completa no Anexo II). Em seguida, foi feita uma busca na Play Store, a fim de identificar quais, entre eles, eram os aplicativos mais baixados.

Essa informação foi encontrada na loja de apps na forma de menção à quantidade de downloads (ex. “+50 mil downloads). A partir desse dado, foram selecionados os 4 primeiros aplicativos mais baixados.

Quando não era possível encontrar os apps citados nos textos exatamente com o mesmo nome na Play Store, foi considerado o primeiro resultado da busca pelo nome sugerido nos artigos. Dentre os aplicativos selecionados, isso ocorreu somente com o app “Mlite rastreador de celular”, que foi selecionado por ser o primeiro resultado quando se buscava por “Location tracker”.

A partir dessa metodologia, os apps selecionados foram os seguintes: Gmail/ Google Maps, Tinder, Mlite rastreador de celular e Controle Parental MM Guardian.

2. Seleção dos apps mais utilizados na Play Store:

Para a seleção dos apps mais utilizados segundo a Play Store, foram levadas em conta as categorias da loja de apps: Top Geral, Redes Sociais, Estilo de Vida, Comunicação, Esporte e Finanças. Foram selecionados os aplicativos considerados Top 1 em cada categoria, tendo em vista sua colocação pelo maior número de downloads.

A partir dessa metodologia, foram selecionados os seguintes 6 apps: Genius IA Editor de fotos, Instagram, Pinterest, Whatsapp, Flashcore e Nubank.

2.3. Políticas de Privacidade

Na terceira fase da pesquisa, foram mapeados dados gerados a partir do uso de aplicativos que poderiam ser aproveitados para refinamento da violência de gênero e espionagem digital/vigilância massiva. Isso foi feito a partir da análise das políticas de privacidade dos apps à luz da revisão de literatura.

As escolhas pela análise das políticas de privacidade se dão por dois motivos centrais: a) as política de privacidade são documentos que devem ser disponibilizados de forma aberta e gratuita para todos os usuários; b) as política de privacidade, em regra, apresentam quais dados são tratados por determinado app, os motivos por eles serem tratados, seguindo a Lei Geral de Proteção de Dados, bem como informações adicionais sobre o tratamento de dados. A partir desta escolha foi possível ter uma visão inicial dos motivos de tratamento de dados trazidos pelas plataformas, adentrando no jogo do "dito X não-dito"; ou seja, nem sempre o "dito" sinaliza a realidade, uma vez que também a constrói.

Existe, neste termos, uma representação social que demonstra uma relação de estruturação. Representações sociais são entendidas como as crenças e valores compartilhados pelos indivíduos dentro de um contexto social. Elas surgem das interações e transformações sociais, refletindo as diversas camadas, grupos e etnias presentes na sociedade. Essas representações funcionam como instrumentos metodológicos que ajudam a compreender as ações e condutas, já que estão ligadas às ideias de valor e à forma como os indivíduos interpretam e respondem à estrutura social. Segundo Porto,[37] as representações sociais são influenciadas pela relação dialética entre o indivíduo e a sociedade, reconhecendo o papel ativo do indivíduo, que, embora condicionado por essa estrutura, ainda possui capacidade de fazer escolhas e tomar decisões, mesmo que limitadas.

A análise das políticas de privacidade, assim, podem nos dar pistas sobre as narrativas das plataformas, as narrativas das bibliografias lidas e criar espécies de inferências sobre como a vigilância massiva e uso de *spywares* podem ser utilizados a partir do acesso indevido por terceiros maliciosos a esses dados, a partir de um aplicativo espião em contexto de violência de gênero. Cabe salientar que, para essa análise, foram considerados tanto dados de conteúdo quanto dados de acesso coletados pelos aplicativos. No entanto, priorizamos a análise de dados de conteúdo, visto que não nos propomos a fazer estudos e verificações sobre a qualidade dos códigos dos aplicativos. Nossa análise centra-se, portanto, não na probabilidade de determinados dados serem invadidos, mas sim nos malefícios que o acesso a eles, através de um ente malicioso, pode provocar.

Dada a relevância desse tipo de informação, foram selecionadas as políticas de

37 PORTO, Maria Stela Grossi. **Crenças, valores e representações sociais da violência.** Sociologias, Porto Alegre, v. 16, p. 1-21, dez. 2006. DOI: https://doi.org/10.1590/S1517-45222006000200010.

privacidade de todos os aplicativos indicados na fase anterior. Esses documentos foram encontrados na internet, por busca no Google ou na Play Store, e baixados entre os dias 7 e 14 de março de 2025. Cabe salientar que, como a Google segue a mesma política de privacidade para todos os seus aplicativos, dois apps da empresa foram considerados como um único caso (Gmail e Google Maps).

Para a análise das políticas de privacidade, foram consideradas categorias inspiradas nos achados da revisão bibliográfica. Os dados que poderiam ser utilizados para violência de gênero, segundo a literatura, foram sistematizados em uma tabela com suas respectivas possibilidades de uso para fins de agressão e controle apresentadas nos textos. Esses dados foram mobilizados como categorias de análise para verificação das políticas de privacidade, a fim de promover um cruzamento de informações. Nosso objetivo era encontrar quais apps coletavam determinados tipos de dados sensíveis e quais as justificativas que suas políticas davam para essas coletas.

2.4. Limitações de Pesquisa

Como qualquer pesquisa científica, nossas análises possuem escolhas metodológicas e, por este motivo, limitações de pesquisa. Na escolha dos aplicativos, nossa intenção era identificar aplicativos que pudessem ser usados para perpetrar violência de gênero, se acessados por terceiros mal intencionados a partir de softwares espiões. Inicialmente, buscamos informações sobre os aplicativos mais baixados por mulheres, mas nos deparamos com uma limitação significativa: a dificuldade de obter dados confiáveis sobre a quantidade de downloads feitos especificamente por mulheres. Essa informação não estava facilmente disponível nem nas pesquisas sobre o tema nem nas próprias lojas de aplicativos. Além disso, o curto período disponível para a execução do projeto dificultava a realização de uma pesquisa direta com o público-alvo, como um survey, para coletar esses dados de forma mais precisa. Optamos, então, por realizar a identificação de aplicativos mencionados nominalmente nos textos da revisão bibliográfica; e, em segundo lugar, a análise dos aplicativos mais baixados na Play Store, para entender quais são os mais populares, independentemente do gênero dos usuários.

Uma outra limitação importante do nosso trabalho é que não realizamos nenhuma análise de código para aferir vulnerabilidades na infraestrutura de aplicativos e sistemas operacionais que poderiam ser exploradas por spywares. Essa foi uma escolha adequada à expertise das pesquisadoras envolvidas e, ainda, ao fato de estarmos falando de softwares proprietários, cujo acesso ao seu código não está disponível de forma aberta.

É importante mencionar que não nos propomos, neste relatório, a realizar uma análise de compliance em relação às políticas de privacidade dos aplicativos selecionados. O uso das políticas de privacidade como material de referência para o mapeamento dos dados utilizados pelos aplicativos se deu por ser um documento que o sintetiza, mas uma análise da adequação à lei vigente não é objeto deste trabalho.

Por fim, esta foi uma pesquisa realizada em 06 meses. Devido a necessidade de um aprofundamento teórico e outras possibilidades metodológicas a serem percorridas, e que não nos foi possível pelo curto período de tempo, sabemos que novas pesquisas poderão surgir, e merecem surgir, a partir de nossos achados. Da mesma forma, a amostra dos aplicativos se restringiu aos 10 mais utilizados, também em razão do cronograma do projeto.

3. Quais serviços podem ser mais vulneráveis a aplicativos de stalkerware e spyware?

Antes de apresentarmos a análise dos aplicativos específicos e dos tipos de dados suscetíveis à manipulação indevida, identificamos, com base na literatura consultada, uma série de serviços que tendem a ser mais visados por aplicativos espiões. Essa maior exposição se deve tanto à vulnerabilidade desses serviços quanto à natureza sensível das informações que armazenam durante o uso. Quando comprometidos, esses serviços podem fornecer dados valiosos a agentes mal-intencionados, facilitando a prática de diversas formas de violência mediada por tecnologia.

A seguir, reunimos os principais serviços identificados e os motivos pelos quais eles costumam ser alvos frequentes de espionagem. Para facilitar a compreensão, organizamos duas tabelas: a primeira apresenta os títulos dos textos analisados, com a numeração correspondente (por exemplo, Texto 1: “SELECT GENDER-BASED VIOLENCE LITERATURE REVIEWS – THE IMPACT OF INFORMATION COMMUNICATION TECHNOLOGIES ON GENDER-BASED VIOLENCE”); a segunda relaciona os serviços identificados, os dados aos quais eles têm acesso e os riscos associados ao eventual acesso indevido dessas informações por meio de aplicativos espiões.

NUMERAÇÃO	TEXTOS
1	SELECT GENDER-BASED VIOLENCE LITERATURE REVIEWS THE IMPACT OF INFORMATION COMMUNICATION TECHNOLOGIES ON GENDER-BASED VIOLENCE
2	Role of Information and Communication Technology in the Digitalization of Violence and Sexual Politics in the Indian Scenario

NUMERAÇÃO	TEXTOS
3	"So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums
4	An OutlineOn IncreasingOnline Gender Violence Against Women In India And The Role Of Cyber Security
5	The Urgency of Regulation in the Case of Online Gender-Based Violence in Indonesia
6	“A Stalker’s Paradise”: How Intimate Partner Abusers Exploit Technology
7	Gender-Specific Election Violence: The Role of Information and Communication Technologies
8	Technological Innovations for Tackling Domestic Violence
9	“Is my phone hacked?” Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence
10	Can Prosuming Become Perilous? Exploring Systems of Control and Domestic Abuse in the Smart Homes of the Future
11	Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review
12	EFETIVIDADE DA CRIMINALIZAÇÃO DO CYBERSTALKING (LEI 14.132/2021)

NUMERAÇÃO	TEXTOS
13	The Nature, Patterns and Consequences of Technology-Facilitated Domestic Abuse: A Scoping Review
14	The Spyware Used in Intimate Partner Violence
15	Gender, Violence and Technology: At a Conceptual and Empirical Crossro
16	INSTALLING FEAR A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications
17	A Global Survey of Android Dual-Use Applications Used in Intimate Partner Surveillance

Os números entre parênteses na tabela a seguir apresentada se referem aos números dos textos da tabela acima já apresentada:

SERVIÇOS	DADOS	RISCOS
Redes Sociais (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16)	Nome (2, 16)	Envio de ameaças (2)
Redes Sociais (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16)	Telefone (7)	Exposição para terceiros (7); Envio de ameaças (1, 2, 5, 7, 11); Assédio (1, 2, 5, 6, 7, 10, 11, 12); Envio de conteúdo sexual não solicitado (1, 3, 11)

SERVIÇOS	DADOS	RISCOS
Redes Sociais (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16)	Conteúdo das mensagens de texto (1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 16, 17)	Monitoramento sobre as comunicações (1, 2, 3, 6, 8, 11, 14); Manipulação da comunicação (6, 11)
Redes Sociais (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16)	Câmera (1, 8, 9, 11, 12, 14, 15)	Monitoramento da vítima (9, 10, 11, 14, 16)
Redes Sociais (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16)	Fotos e vídeos (2, 3, 4, 5, 6, 7, 9, 11, 12, 14, 15, 16, 17)	Manipulação de imagem, sobretudo sexuais (4, 5, 7, 8 ,10); Compartilhamento de imagens íntimas (1, 2, 5, 7, 8, 10, 16); Realização de chantagem (2); Exposição (4, 5, 7, 11, 16); Monitoramento (1, 3, 11, 16)
Redes Sociais (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16)	Lista de contatos (6, 16)	Remoção de amigos (6)
Redes Sociais (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16)	Microfone (8, 12, 14, 16, 17)	Monitoramento da vítima (14, 16)
Redes Sociais (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16)	Senhas (11, 16, 17)	Invasão de outros sistemas e controle sobre o acesso (16)
Mensageria (1, 2, 3, 4, 5, 6, 7, 9, 12, 16)	Nome (2, 16)	Envio de ameaças (2)

SERVIÇOS	DADOS	RISCOS
Mensageria (1, 2, 3, 4, 5, 6, 7, 9, 12, 16)	Endereço de email (1, 2, 4, 7, 8, 9, 11, 12, 15, 16)	Assédio (7, 8, 11) ; Envio de ameaças (2, 7, 8, 11, 12) ; Envio de conteúdo sexual não solicitado (7, 12); Envio de vírus (7); Sobrecarga do sistema para que deixe de funcionar (7, 12);
Mensageria (1, 2, 3, 4, 5, 6, 7, 9, 12, 16)	Conteúdo dos e-mails (2, 3, 7, 8, 10, 11, 15, 16)	Controle de comportamentos (2, 3, 6, 8, 11); Manipulação da comunicação (7); Acesso a outras contas (6)
Mensageria (1, 2, 3, 4, 5, 6, 7, 9, 12, 16)	Telefone (7, 11)	Exposição para terceiros (7) ; Envio de ameaças (1, 2, 5, 7, 11); Assédio (1, 2, 5, 6, 7, 10, 11, 12); Envio de conteúdo sexual não solicitado (1, 3, 11);
Mensageria (1, 2, 3, 4, 5, 6, 7, 9, 12, 16)	Conteúdo das mensagens de texto (1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 16, 17)	Monitoramento sobre as comunicações (1, 2, 3, 6, 8, 11, 14); Manipulação da comunicação (6, 11)
Mensageria (1, 2, 3, 4, 5, 6, 7, 9, 12, 16)	Lista de contatos (6, 16)	Remoção de amigos (6)
Mensageria (1, 2, 3, 4, 5, 6, 7, 9, 12, 16)	Ligações/Registro de chamadas (2, 3, 6, 8, 9, 14, 16, 17)	Controle de comportamentos (3, 6)

SERVIÇOS	DADOS	RISCOS
Mensageria (1, 2, 3, 4, 5, 6, 7, 9, 12, 16)	Microfone (8, 12, 14, 16, 17)	Monitoramento da vítima (14, 16)
Mensageria (1, 2, 3, 4, 5, 6, 7, 9, 12, 16)	Fotos e vídeos (2, 3, 4, 5, 6, 7, 9, 11, 12, 14, 15, 16, 17,	Manipulação de imagem, sobretudo sexuais (4, 5, 7, 8 ,10); Compartilhamento de imagens íntimas (1, 2, 5, 7, 8, 10, 16); Realização de chantagem (2); Exposição (4, 5, 7, 11, 16); Monitoramento (1, 3, 11, 16)
Mensageria (1, 2, 3, 4, 5, 6, 7, 9, 12, 16)	Câmera (1, 8, 9, 11, 12, 14, 15,	Monitoramento da vítima (9, 10, 11, 14, 16)
Rastreamento e GPS (1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17)	Geolocalização (1, 2, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16)	Violência física (1,); Violência psicológica pela sensação de constante monitoramento (10); Controle de comportamentos (1, 2, 3, 8, 10, 11, 12, 13, 14); Perseguição (2, 8, 10, 13)
Rastreamento e GPS (1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17)	Endereço (2, 5, 7, 12, 16)	Envio de ameaças (11); Exposição para terceiros (5, 7)
Controle Parental (1, 2, 6, 9, 10, 11, 14, 17)	Geolocalização (1, 2, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16)	Violência física (1,); Violência psicológica pela sensação de constante monitoramento (10); Controle de comportamentos (1, 2, 3, 8, 10, 11, 12, 13, 14); Perseguição (2, 8, 10, 13)

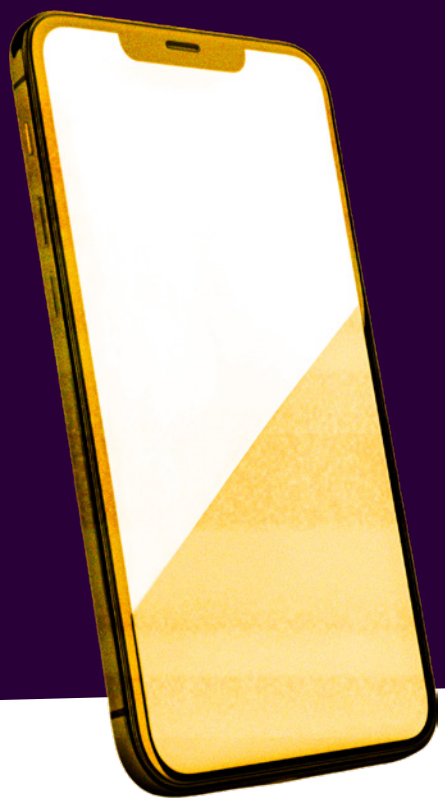
SERVIÇOS	DADOS	RISCOS
Controle Parental (1, 2, 6, 9, 10, 11, 14, 17)	Conteúdo das mensagens de texto (1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 16, 17)	Monitoramento sobre as comunicações (1, 2, 3, 6, 8, 11, 14); Manipulação da comunicação (6, 11)
Controle Parental (1, 2, 6, 9, 10, 11, 14, 17)	Câmera (1, 8, 9, 11, 12, 14, 15)	Monitoramento da vítima (9, 10, 11, 14, 16)
Financeiro (3, 9, 11)	Senhas (11, 16, 17)	Invasão de outros sistemas e controle sobre o acesso (16)
Financeiro (3, 9, 11)	Registro de compras e atividades bancárias (3, 6, 8, 9, 11)	Controle de comportamentos (3, 6, 8) ; Impedimento de que a vítima tenha recursos para buscar ajuda (11)
Relacionamento (3, 10, 16)	Vida sexual/afetiva (1, 3, 4, 16)	Discriminação (1, 2, 7); Controle de comportamentos (3, 10); Agressão sexual (1, 2, 7)
Saúde (10)	Informações sobre saúde (10)	Não foram encontradas informações sobre violências associadas a esse tipo de dado na literatura*
Não consta*	Calendário e eventos (16)	Não foram encontradas informações sobre violências associadas a esse tipo de dado na literatura*

*A ausência de dados sobre esses campos não diz sobre a inexistência desses serviços ou violências, apenas indica que não foram tratados na literatura analisada.

As tabelas demonstram como tecnologias amplamente utilizadas no cotidiano podem ser convertidas em instrumentos de vigilância e controle quando exploradas por meio de spywares e stalkerwares. Observa-se uma preocupante sobreposição entre funcionalidades legítimas e práticas abusivas, especialmente em contextos de relacionamentos marcados por violência. Aplicativos de redes sociais, serviços de rastreamento, comunicação, cuidados pessoais e relacionamento, quando acessados por terceiros mal-intencionados, tornam-se ferramentas eficazes de monitoramento. A introdução de um spyware potencializa ainda mais esses riscos, permitindo ao agressor acessar informações altamente sensíveis — como localização em tempo real, comunicações privadas, conteúdos íntimos e dados de saúde — com o objetivo de manipular, ameaçar ou isolar a vítima, intensificando o controle coercitivo e a violência psicológica.

Além disso, muitos dos aplicativos analisados são classificados como **dual-use apps**, ou seja, softwares com finalidades legítimas que podem ser facilmente convertidos em instrumentos de espionagem. Esses aplicativos frequentemente operam de maneira autônoma, sem que a vítima perceba ou que o agressor precise interagir diretamente com o dispositivo após a instalação. Essa característica os torna ainda mais perigosos, pois ampliam o alcance do controle abusivo e invisibilizam a violência digital, especialmente em contextos de violência por parceiro íntimo.

Os dados contam uma história, e aqueles que você cria, produz, armazena e registra no seu celular de forma mais ou menos intencional poderá contar uma história sobre você. Na próxima seção, desenvolvemos como os dados podem enredar essas narrativas e serem instrumentalizadas de forma indevida.



Aplicativos de redes sociais e mensageria

É comum que as pessoas compartilhem dados sobre a sua rotina, os lugares que frequenta, as relações que cultiva e como. Também é usual que as plataformas ofereçam interfaces para compartilhamento de áudio, vídeo, localização. Em alguns casos pode parecer que você está construindo um diário digital da sua vida. Através de invasão de terceiros não autorizados, esse conteúdo pessoal pode se converter em chantagem, em isolamento de redes de proteção, em ameaças, envio de conteúdo sexual não solicitado, assédio, exposição, manipulação de imagens.

4. Quais dados podem ser mais visados para aplicativos de *stalkerware e spyware*?

Nesta parte de nosso relatório, vamos analisar os cruzamentos que fizemos a partir das coletas de dados realizada em nosso caminho metodológico: políticas de privacidade dos apps; revisão da literatura e bibliografia sobre os conceitos-chave.

Os dados identificados, conforme a revisão bibliográfica, que podem ser utilizados para fins de vigilância massiva e refinamento de violência de gênero se acessados por aplicativos espiões são: **gênero, nome, endereço, e-mail, telefone, geolocalização, registro de comunicações (mensagens), foto/vídeo, câmeras, contatos/registros de chamadas, microfone/voz, senhas, informações bancárias, vida sexual/afetiva, monitoramento de saúde, agenda/rotina.**

Como já sinalizado, esses dados, quando coletados em grande escala, e sendo passíveis de serem acessados por estes terceiros maliciosos, possuem um potencial significativo para monitoramento e vigilância em nível massivo, podendo impactar a privacidade e segurança das mulheres, ainda mais em se tratando de contexto de violência de gênero.

Para a análise, dividimos os dados em **04 categorias principais: a) dados pessoais de identificação** (gênero; nome; endereço; telefone; vida sexual/afetiva; monitoramento de saúde; e-mail); **b) dados de interações/comunicações** (registro de comunicações de mensagens, foto/vídeo, câmeras, contatos/registros de chamadas; microfone/voz; email); **c) dados de localização e finanças** (geolocalização; agenda/rotina; informações bancárias; senhas); **d) dados de/para controle parental.**

4.1. Dados coletados pelos aplicativos: quais usos indevidos podem ser feitos?

Neste ponto, apresentaremos quais os dados tratados e coletados, segundo as políticas de privacidade, pelos diferentes aplicativos analisados e quais possíveis implicações do seu uso para vigilância a partir do uso de *spyware/stalkware* podemos inferir a partir das leituras realizadas.

4.1.1. Dados Pessoais e de Identificação

Com base nas categorias de análise adotadas, classificamos como dados pessoais de identificação aqueles que permitem, direta ou indiretamente, reconhecer uma pessoa específica. Dentro desse escopo, consideramos como relevantes os seguintes elementos: gênero; nome; endereço físico; número de telefone; aspectos da vida sexual

e/ou afetiva; e informações provenientes de monitoramento de saúde. Esses dados, ainda que aparentemente cotidianos ou rotineiramente compartilhados em ambientes digitais, adquirem uma dimensão sensivelmente crítica quando inseridos no contexto da violência contra a mulher — especialmente em situações de invasão de privacidade por meio de spywares, aplicativos espiões ou outras tecnologias de vigilância abusiva.

DADOS PESSOAIS

Gênero; nome; endereço físico; número de telefone; aspectos da vida sexual e/ou afetiva; informações provenientes de monitoramento de saúde

RISCOS

Agravamento de situações de abuso, assédio ou coerção; localização ou identificação de uma mulher dentro de redes sociais, banco de dados públicos ou plataformas digitais, muitas vezes sem o seu consentimento; perseguição; assédio contínuo e sistemático; manipulação emocional; ameaças; humilhação; controle

Quando esses dados são acessados por terceiros mal-intencionados, como agressores, perseguidores ou operadores de tecnologias de controle, o risco de agravamento de situações de abuso, assédio ou coerção aumenta de forma significativa. O nome da usuária, por exemplo, combinado com o dado de gênero (especialmente se identificado entre as chamadas "informações demográficas"), pode ser utilizado para localizar ou identificar uma mulher dentro de redes sociais, bancos de dados públicos ou plataformas digitais, muitas vezes sem o seu consentimento.[38] Da mesma forma, o endereço IP — que permite rastrear a localização geográfica aproximada de um dispositivo — pode ser explorado para fins de perseguição, aumentando a vulnerabilidade da mulher à violência física, emocional ou psicológica.[39]

Além disso, o número de telefone e o endereço de e-mail, frequentemente coletados por aplicativos e serviços digitais, podem ser utilizados para promover formas de assédio contínuo e sistemático.[40] Por meio desses canais, a vítima pode receber mensagens invasivas, ameaças ou tentativas de manipulação emocional, o que caracteriza o chamado assédio online. [41]A persistência e a facilidade com que essas mensagens podem ser enviadas — a qualquer momento, por diferentes meios — faz com que os impactos dessa violência não se limitem ao ambiente digital, afetando também a saúde mental, o bem-estar e a sensação de segurança da mulher em sua vida cotidiana.

38 VERMA, Rabindra Kumar; GUPTA, Ashish Kumar. *Role of Information and Communication Technology in the Digitalization of Violence and Sexual Politics in the Indian Scenario*. In: *Cyberfeminism and Gender Violence in Social Media*. 2023. Cap. 3.

39 MADIWALE, A. R.; KUMAR, S. An outline on increasing online gender violence against women in India and the role of cyber security. **Journal of Positive School Psychology**. 2022.

40 IQBAL, Muhammad; CYPRIEN, Genie. The urgency of regulation in the case of online gender-based violence in Indonesia. Sawwa: *Journal Studi Gender,* Semarang, v. 16, n. 2, p. 173-190, out. 2021.

41 ZERAI, Assata. Select gender-based violence literature reviews: gender-based violence in the MENA among religious and other minorities in conflict settings. [S.l.]: United States Agency for International Development (USAID), maio 2020. Relatório n. GS-10F-0033M / ORDER NO. 7200AA18M00016 / DRG-LER II TASKING N008.

Adicionalmente, dados considerados mais íntimos, como aqueles relacionados à vida afetiva ou sexual,[42] ou ainda registros de saúde[43] (monitoramentos hormonais, ciclos menstruais, dados de anticoncepcionais, entre outros), quando expostos ou explorados por aplicativos espiões, podem ser usados como instrumentos de humilhação, chantagem ou controle. A coleta e o tratamento desses dados, especialmente sem transparência, consentimento informado e medidas de segurança eficazes, perpetuam dinâmicas de poder assimétrico e contribuem para a manutenção de estruturas opressoras e violentas, tanto no meio digital quanto fora dele.[44]

4.1.2. Dados de Interações/Comunicações

No que diz respeito à categoria de interações e comunicações pessoais, a análise é direcionada à coleta de um conjunto sensível de dados que inclui: **registros de mensagens de texto e de voz, conteúdo multimídia (fotos e vídeos), acesso à câmera e microfone, lista de contatos, registros de chamadas telefônicas e e-mails.** Esses elementos, quando acessados por terceiros mal-intencionados por meio de aplicativos espiões (*spywares* ou *stalkerwares*), representam sérias ameaças à privacidade, à integridade e à segurança das vítimas, sobretudo em contextos de violência de gênero.[45]

DADOS DE COMUNICAÇÃO

Registros de mensagens de texto e de voz, conteúdo multimídia (fotos e vídeos), acesso à câmera e microfone, lista de contatos, registros de chamadas telefônicas e e-mails

RISCOS

Monitoramento constante; isolamento de redes de apoio; exploração de fotos e vídeos; Cyber grooming; roubo de identidade; difamação online

Esses dados podem ser explorados de diferentes formas pelo agressor. O registro de mensagens e e-mails, por exemplo, permite o monitoramento constante da vítima, favorecendo práticas de vigilância abusiva e controle coercitivo.[46] A simples leitura

42 BELLINI, Rosanna et al. “So-called privacy breeds evil”: Narrative Justifications for Intimate Partner Surveillance in Online Forums. Proceedings of the ACM on Human-Computer Interaction, v. 4, n. CSCW3, art. 210, p. 1-27.

43 SOVACOOL, Benjamin; FURSZYFER-DEL RIO, Dylan D.; MARTISKAINEN, Mari. Can prosuming become perilous? Exploring systems of control and domestic abuse in the smart homes of the future. Frontiers in Energy Research, [s.l.], v. 9, 04 nov. 2021. Disponível em: https://doi.org/10.3389/fenrg.2021.765817.

44 ZERAI, Assata. Select gender-based violence literature reviews: gender-based violence in the MENA among religious and other minorities in conflict settings. [S.l.]: United States Agency for International Development (USAID), maio 2020. Relatório n. GS-10F-0033M / ORDER NO. 7200AA18M00016 / DRG-LER II TASKING N008.

45 KOUZANI, A. Z. Technological Innovations for Tackling Domestic Violence. **IEEE Access**, v. 11, p. 91293-91311, 2023.

46 FREED, Diana; PALMER, Jackeline; MINCHALA, Diana; LEVY, Karen; RISTENPART, Thomas; DELL, Nicola. “A stalker’s paradise”: how intimate partner abusers exploit technology. In: **CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS**, 2018, Montreal. New York: ACM, 2018. Paper n. 667, p. 1–13.

das mensagens trocadas pode oferecer ao perpetrador informações íntimas sobre amizades, vínculos familiares, relações afetivas, rotinas diárias, preferências pessoais e vulnerabilidades emocionais.[47] Com isso, o agressor pode manipular ou isolar a vítima dos seus sistemas de apoio,[48] criando um cenário de dependência emocional ou até mesmo financeira.

O acesso a fotos e vídeos armazenados no dispositivo da vítima amplia ainda mais o potencial de danos. Esses arquivos podem ser usados para difamar a vítima nas redes sociais, chantageá-la com ameaças de divulgação ou até mesmo para forjar situações, criando narrativas falsas ou enganosas.[49] Além disso, a ativação remota da câmera e do microfone do dispositivo, sem o consentimento da usuária, configura uma grave violação de privacidade, podendo resultar na produção de conteúdo íntimo não consensual – o que, em muitos casos, caracteriza violência sexual digital.

A utilização de e-mails e chamadas telefônicas como canais para envio de mensagens abusivas também reforça práticas de assédio e perseguição, facilitando o acesso do agressor à vítima.[50] Esses dados, quando expostos, podem também ser utilizados como ponto de partida para invasões a outras plataformas digitais utilizadas pela vítima,[51] como redes sociais e contas bancárias, por meio da instalação de programas espiões ainda mais sofisticados.

Importante destacar que a própria política de privacidade de alguns aplicativos pode reconhecer a existência de brechas que facilitam o uso indevido dessas informações, o que expõe ainda mais as usuárias a riscos. Em um cenário de violência digital, a coleta e o vazamento desses dados por terceiros representa uma ameaça real e contínua à segurança da vítima, podendo alimentar estratégias de coerção e silenciamento.

Além disso, os dados visuais – como fotos da vítima – podem ser utilizados para fins de roubo de identidade, montagem de perfis falsos ou manipulação de imagens com o uso de tecnologias como a inteligência artificial.[52] É possível, por exemplo, que imagens sejam

47 ROGERS, Michaela; FISHER, Colleen; ALI, Parveen Azam; ALLMARK, Peter. Technology-facilitated abuse in intimate relationships: a scoping review. Trauma, Violence & Abuse, [S.l.], v. 24, n. 202, maio 2022. DOI: https://doi.org/10.1177/15248380221090218.

48 VERMA, R. K.; GUPTA, A. K. Role of Information and Communication Technology in the Digitalization of Violence and Sexual Politics in the Indian Scenario. In: **Cyberfeminism and Gender Violence in Social Media**. 2023.

49 SOVACOOL, Benjamin; FURSZYFER-DEL RIO, Dylan D.; MARTISKAINEN, Mari. Can prosuming become perilous? Exploring systems of control and domestic abuse in the smart homes of the future. Frontiers in Energy Research, [s.l.], v. 9, 04 nov. 2021. Disponível em: https://doi.org/10.3389/fenrg.2021.765817.

50 BARDALL, Gabrielle. Gender-specific election violence: the role of information and communication technologies. Stability: International Journal of Security and Development, [s.l.], v. 2, n. 3, art. 60, 2013. DOI: https://doi.org/10.5334/sta.cs.

51 FREED, Diana; PALMER, Jackeline; MINCHALA, Diana; LEVY, Karen; RISTENPART, Thomas; DELL, Nicola. "A stalker's paradise": how intimate partner abusers exploit technology. In: *CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS*, 2018, Montreal. New York: ACM, 2018. Paper n. 667, p. 1–13.

52 KOUZANI, A. Z. Technological Innovations for Tackling Domestic Violence. IEEE Access, v. 11, p. 91293-91311, 2023.

inseridas em vídeos falsos (*deepfakes*), ampliando as possibilidades de constrangimento e humilhação pública. Essas ações, além de violentas, têm efeitos devastadores sobre a autoestima e o bem-estar psicológico da vítima.[53]

Por fim, informações sobre a vida pessoal da vítima, quando acessadas por pessoas com intenções violentas, podem ser utilizadas para a prática de crimes motivados por preconceito, ódio ou intolerância, especialmente quando se trata de mulheres, pessoas LGBTQIAPN+ ou outros grupos historicamente marginalizados. [54]

Nesse contexto de coleta e uso indevido de dados de interações e comunicações, a presença de **spywares** se revela especialmente preocupante, pois atua como facilitador direto de diversas formas de violência digital. A instalação desses aplicativos cria um ambiente propício para a prática de ameaças por mensagem,[55] incluindo casos de ***cyber grooming*** ou **assédio cibernético**, nos quais o perpetrador busca intimidar, ferir, invadir a privacidade ou difamar a vítima por meio de conteúdos compartilhados de forma abusiva.[56] Além disso, o uso desses dados pode resultar em **divulgação não consensual de imagens íntimas**, prática muitas vezes realizada por parceiros ou ex-parceiros como forma de vingança ou controle.[57] Em situações ainda mais sofisticadas, o material capturado pode ser manipulado digitalmente — por meio de técnicas como o ***morphing*** — para criar conteúdos falsos e difamatórios com o objetivo de extorquir, constranger ou desacreditar a vítima.[58] Soma-se a isso a **difamação online**, que se vale de informações falsas disseminadas na internet para destruir reputações, sendo frequentemente alimentada por dados obtidos por meio de *stalkerwares*.

4.1.3. Dados de Localização e Finanças

A exposição da geolocalização dos usuários pode também configurar um risco significativo à privacidade, especialmente para mulheres em situação de vulnerabilidade.[59]

53 SILVA, Lucas Gonçalves da; CARDOSO, Henrique Ribeiro; FARIA, Lucas Ribeiro. Deepfake pornográfico na sociedade de risco contemporânea: os desafios de regulamentação e controle da inteligência artificial. ***Fluxo Contínuo***, v. 9, n. 3, 2024.

54 VERMA, Rabindra Kumar; GUPTA, Ashish Kumar. Role of Information and Communication Technology in the Digitalization of Violence and Sexual Politics in the Indian Scenario. In: Cyberfeminism and Gender Violence in Social Media. 2023. Cap. 3.

55 BARDALL, Gabrielle. Gender-specific election violence: the role of information and communication technologies. Stability: International Journal of Security and Development, [s.l.], v. 2, n. 3, art. 60, 2013. DOI: https://doi.org/10.5334/sta.cs.

56 KOUZANI, A. Z. Technological Innovations for Tackling Domestic Violence. IEEE Access, v. 11, p. 91293-91311, 2023.

57 SOVACOOL, Benjamin; FURSZYFER-DEL RIO, Dylan D.; MARTISKAINEN, Mari. Can prosuming become perilous? Exploring systems of control and domestic abuse in the smart homes of the future. Frontiers in Energy Research, [s.l.], v. 9, 04 nov. 2021. Disponível em: https://doi.org/10.3389/fenrg.2021.765817.

58 MADIWALE, Ranjita; KUMAR, Sona. An outline on increasing online gender violence against women in India and the role of cyber security. Journal of Positive School Psychology, [S.l.], v. 6, n. 6, p. 3920-3927, 2022. Disponível em: http://journalppw.com.

59 BUKHTEYEV, Alexey. The illusion of privacy: geolocation risks in modern dating apps. **Checkpoint Researc***h*, 4 abr. 2024. Disponível em: https://research.checkpoint.com/2024/the-illusion-of-privacy-geolocation-risks-in-modern-

Embora muitas das políticas de privacidade dos aplicativos analisados justifiquem a coleta de dados de localização como medida de segurança ou para oferecer serviços personalizados, notamos que, quando cruzamos com a literatura analisada, o acesso a esse tipo de informação pode ser facilmente instrumentalizado como ferramenta de vigilância, controle e perseguição quando feita por um terceiro malicioso ou por um aplicativo espião.

DADOS FINANCEIROS

Movimentações financeiras; senhas de bancos; histórico de transação bancária; informações financeiras de terceiros; localização de compras

RISCOS

Abuso e controle financeiro; monitoramento de transações; chantagem financeira; cruzamento de dados financeiros com localização

DADOS DE LOCALIZAÇÃO

Geolocalização; GPS; endereço IP

RISCOS

Vigilância em tempo real; rastreamento indireto; possibilidade de vigilância presencial

A coleta de dados de geolocalização não se restringe ao acesso direto ao GPS autorizado pelo usuário nas configurações do dispositivo. Diversas estratégias indiretas podem ser utilizadas para inferir a localização de uma pessoa, como a análise do endereço IP, metadados de imagens (que indicam onde uma foto foi tirada), e até mesmo a ativação da câmera do celular para obter indícios do ambiente. Essas práticas, que podem estar ocultas nos termos de uso de determinado aplicativo, tornam possível o rastreamento contínuo mesmo quando o compartilhamento de localização está desativado, levantando sérias preocupações sobre consentimento, transparência e controle sobre os próprios dados. Quando acessado por um *spyware* esse tipo de dado pode ser utilizado para monitorar os deslocamentos da vítima em tempo real, possibilitando formas sofisticadas de vigilância e controle que, muitas vezes, ocorrem sem o seu conhecimento. Isso agrava ainda mais os riscos associados à violência de gênero, ao permitir que agressores utilizem essas informações para ameaçar, intimidar ou restringir a liberdade da pessoa monitorada.

O acesso não autorizado à localização de uma mulher por parte de um agressor — frequentemente um parceiro íntimo ou ex-companheiro — pode facilitar episódios de perseguição, assédio, ameaças, sequestro e até violência física, gerando um estado constante de medo e insegurança por parte da vítima.

dating-apps/. Acesso em: 15 abr. 2024.

Paralelamente, os dados financeiros coletados por aplicativos também representam uma dimensão crítica da exposição digital. Muitas plataformas acessam, armazenam e até compartilham informações como histórico de transações bancárias, hábitos de consumo, senhas, localização de compras e perfis de gastos. Embora esse acesso seja frequentemente descrito como necessário para o funcionamento dos serviços, ele pode ser explorado para práticas de abuso financeiro.

Ao monitorar movimentações financeiras, um agressor pode exercer controle sobre os gastos da vítima, limitando sua autonomia e reforçando uma dependência econômica que a impede de sair da situação de violência. O controle financeiro silencioso — por meio de notificações de gastos, análise de saldos, bloqueio de acessos ou até ameaças ligadas à exposição de dívidas ou transações — pode ser tão invasivo quanto outras formas de abuso físico ou emocional. [60]

Além disso, alguns aplicativos extrapolam a coleta de dados do usuário individual, estendendo o monitoramento a pessoas que mantêm algum vínculo com ele, como contatos frequentes, parceiros de transações ou representantes legais. Isso permite que um agressor, mesmo após o fim de uma relação, continue acessando informações sensíveis por meio de conexões indiretas, como uma antiga conta conjunta ou histórico de transferências. Esse tipo de vigilância indireta amplia o alcance do controle e da manipulação, tornando ainda mais difícil a ruptura total entre vítima e agressor.

A possibilidade de cruzamento entre dados de localização e informações financeiras potencializa os riscos, permitindo que um agente mal-intencionado, utilizando de um *stalkerware*, mapeie toda a rotina da vítima: onde ela esteve, o que comprou, com quem interagiu e quanto gastou. Essa vigilância minuciosa pode ser empregada como tática de intimidação, chantagem, retaliação ou coerção, especialmente em contextos onde a vítima já enfrenta isolamento e fragilidade emocional.

4.1.4. Dados de/para controle parental

Aplicativos de controle parental podem ser facilmente reconfigurados para exercer formas de vigilância abusiva, especialmente em contextos de violência de gênero.[61] Essas ferramentas, ao oferecerem funcionalidades como rastreamento de localização em tempo real, acesso a mensagens, histórico de chamadas, ativação remota de câmeras e microfones, entre outras, criam oportunidades para que o monitoramento de outra pessoa aconteça sem o seu conhecimento ou consentimento.

60 SANTOS, Maria Joelma Alves. **Violência doméstica: a permanência da mulher em relacionamento abusivo**. 2022. Trabalho de Conclusão de Curso (Bacharelado em Serviço Social) – Centro Universitário Internacional – UNINTER, Brasília, 2022.

61 WITTHOFT, Brandy; POOLE, Dani. **Select gender-based violence literature reviews: the impact of information communication technologies on gender-based violence**. 2020.

DADOS DE/PARA CONTROLE PARENTAL

Rastreamento de localização em tempo real, acesso a mensagens, histórico de chamadas, ativação remota de câmeras e microfones

RISCOS

Monitoramento sem consentimento; funcionalidades invasivas; geofencing para controle de mobilidade; rastreamento de uso de aplicativos; controle de comunicação; monitoramento indireto de terceiros

A coleta massiva de dados pessoais por esses aplicativos — incluindo informações bancárias, geolocalização, comunicações, fotos e vídeos — torna-se especialmente problemática quando utilizada para fins distintos dos quais a ferramenta foi publicamente destinada.[62] Em casos de relacionamentos abusivos, por exemplo, essas informações podem ser manipuladas para impor restrições, estabelecer dependência financeira ou controlar a rotina da vítima. Segundo as políticas de privacidade, estes aplicativos ainda possuem opções como: “gravação de ambiente”; ”câmera ao vivo”, para obter acesso à câmera do celular de terceiro, a qualquer momento; “apps de mensagens”, para monitoramento de mensagens; “contatos”, em que abre a possibilidade de se saber quando alguma nova pessoa é adicionada ao aplicativo móvel; e “localização ao vivo” e “alerta de localização”, em que se consegue receber um alerta caso o terceiro monitorado saia de alguma área específica.

De acordo com a bibliografia analisada, e com as políticas de privacidade dos aplicativos também analisados, diversos aplicativos classificados como ferramentas de uso duplo - que englobam os aplicativos de controle parental e de localização de pessoas, como familiares e amigos - apresentam funcionalidades que podem ser utilizadas para fins de vigilância indevida, configurando práticas associadas ao uso de *stalkerware*.[63] Entre essas funcionalidades estão o rastreamento contínuo da localização de uma pessoa, o acesso a mensagens trocadas em aplicativos de terceiros, como WhatsApp e Facebook, a leitura de SMS e registros de chamadas, a visualização do histórico de navegação na internet, o monitoramento de listas de contatos e a criação de *geofences*.

As *geofences* — ou cercas geográficas — são limites virtuais definidos com base em coordenadas geográficas, como latitude e longitude, que permitem o monitoramento da entrada ou saída de um dispositivo em determinada área.[64] Essa funcionalidade, embora tecnicamente neutra, pode ser instrumentalizada por agressores para exercer vigilância

62 FREED, Diana; PALMER, Jackeline; MINCHALA, Diana; LEVY, Karen; RISTENPART, Thomas; DELL, Nicola. “A stalker’s paradise”: how intimate partner abusers exploit technology. In: ***CHI ‘18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems***. Montreal, Canadá: ACM, 2018. Paper n. 667, p. 1–13. Disponível em: https://doi.org/10.1145/3173574.3174241. Acesso em: 23 abr. 2025.

63 ALMANSOORI, Majed; GALLARDO, Andrea; POVEDA, Julio; AHMED, Adil; CHATTERJEE, Rahul. A global survey of Android dual-use applications used in intimate partner surveillance. Proceedings on Privacy Enhancing Technologies, v. 2022, n. 4, p. 120–139, 2022. Disponível em: https://doi.org/10.56553/popets-2022-0092. Acesso em: 23 abr. 2025.

64 AWATI, RAUL. Geofencing. **TechTarget.** Disponível em: https://www.techtarget.com/whatis/definition/geofencing. Acesso em: 23 abr.2025.

constante sobre os deslocamentos da vítima, intensificando dinâmicas de controle e violação de privacidade.[65]

Além disso, alguns desses aplicativos acessam dados de pessoas conectadas ao usuário principal, como contatos e familiares, o que amplia significativamente o alcance da coleta de informações. Assim, uma pessoa pode ser monitorada indiretamente, mesmo que não tenha instalado ou consentido com o uso do aplicativo. Isso cria um ambiente de vigilância invisível e persistente, dificultando a identificação da violação e tornando mais complexa a sua interrupção.

Alguns aplicativos de controle parental, ainda, possibilitam um nível de monitoramento altamente detalhado das atividades realizadas no dispositivo monitorado. Entre as funcionalidades disponíveis, está a capacidade de acompanhar em tempo real quando novos contatos são adicionados ou removidos do telefone, bem como acessar os nomes que aparecem nos registros de chamadas e mensagens. Tais recursos permitem que a pessoa responsável — ou, em situações de uso indevido, um terceiro mal-intencionado — visualize, autorize ou bloqueie interações com determinados contatos, exercendo um controle direto sobre as redes de comunicação da pessoa monitorada.[66]

Além disso, esses aplicativos coletam informações sobre os aplicativos instalados no dispositivo, incluindo dados sobre o momento da instalação, remoção e utilização de cada app. Quando ativada a funcionalidade de monitoramento de mensagens, também são registrados detalhes de comunicações via SMS e MMS, como conteúdo textual, horários e contatos envolvidos. Embora essas funcionalidades sejam, em tese, voltadas à proteção de crianças e adolescentes, elas também abrem espaço para usos abusivos.

Neste sentido, um aspecto preocupante é como esses aplicativos são frequentemente apresentados sob um discurso de cuidado ou proteção — muitas vezes usando termos como “monitoramento de entes queridos” ou “segurança da família”. Essa narrativa mascara o potencial de uso abusivo dessas ferramentas e normaliza práticas de controle que violam direitos fundamentais, como a privacidade e a autonomia individual. Esse tipo de retórica é recorrente em relações marcadas por dinâmicas de poder e pode reforçar justificativas emocionais para a invasão da vida privada do outro.[67]

O acesso a dados financeiros, em particular, pode ser explorado para exercer controle econômico — uma das formas mais recorrentes e difíceis de romper em casos de violência

65 KHO, Cynthia; ROBERTSON, Kate; DEIBERT, Ronald. **Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications.** 2019. Electronic version first published by Citizen Lab. Disponível em: https://citizenlab.ca/docs/stalkerware-legal.pdf . Acesso em: 3 abr. 2025.

66 KHO, Cynthia; ROBERTSON, Kate; DEIBERT, Ronald. **Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications.** 2019. Electronic version first published by Citizen Lab. Disponível em: https://citizenlab.ca/docs/stalkerware-legal.pdf . Acesso em: 3 abr. 2025.

67 FREED, Diana; PALMER, Jackeline; MINCHALA, Diana; LEVY, Karen; RISTENPART, Thomas; DELL, Nicola. “A stalker’s paradise”: how intimate partner abusers exploit technology. In: **Proceedings of the 2018 ACM SIGCHI Conference on Human Factors in Computing Systems.** ACM Digital Library, 2018. Disponível em: https://dl.acm.org/doi/10.1145/3234548.3234573. Acesso em: 7 abr. 2025.

doméstica. Saber quanto a vítima ganha, onde gasta, ou com quem realiza transações permite ao agressor exercer vigilância sobre sua autonomia financeira, dificultando sua saída da situação de violência.[68]

Outro ponto crítico é o uso desses aplicativos mesmo após o término de uma relação. Ex-companheiros, com acesso anterior ao dispositivo ou às credenciais da vítima, podem manter o monitoramento por longos períodos. Isso perpetua o controle mesmo à distância, impedindo a reconstrução segura e autônoma da vida da pessoa afetada.

Relatos de usuários dessas ferramentas, disponíveis em plataformas de avaliação pública, revelam explicitamente esse uso indevido. Muitos descrevem como utilizaram os aplicativos para "investigar" parceiros, invadir dispositivos e acessar mensagens pessoais — atitudes que ultrapassam qualquer noção legítima de cuidado e configuram práticas invasivas, que atentam contra a segurança e a dignidade da pessoa vigiada.[69]

5. Pontos conclusivos

As políticas de privacidade dos aplicativos analisados evidenciam que os dados coletados, quando acessados por meio de aplicativos espiões, podem ser utilizados de forma indevida, gerando riscos significativos quando examinados à luz de conceitos como privacidade, vigilância e violência de gênero em contextos digitais — especialmente em sua relação com práticas de spyware e *stalkerware.*

Aplicativos que coletam uma vasta gama de informações sensíveis, como localização, comunicações pessoais, fotos, vídeos, dados bancários e históricos de navegação, possuem, segundo a bibliografia analisada, risco de serem instrumentalizadas e exploradas para vigilância não autorizada, assédio, chantagem e até controle financeiro.

Esses aplicativos, se invadidos por um terceiro que acessa os dados sensíveis coletados, podem ser usados para criação de um espaço de controle e perseguição de vítimas, especialmente mulheres em situações de abuso.

A relação entre vigilância e gênero, especialmente no contexto de violência digital, se

68 SANTOS, Maria Joelma Alves. **Violência doméstica: a permanência da mulher em relacionamento abusivo**. 2022. Trabalho de Conclusão de Curso (Bacharelado em Serviço Social) – Centro Universitário Internacional – UNINTER, Brasília, 2022.

69 "Eu suspeitava que meu cônjuge estava me traindo, mas nunca tive nenhuma evidência, apesar de ter minhas dúvidas e ela também estava agindo de maneira suspeita e escondendo segredos. Isso continuou por meses e eu me sentia completamente desconfortável até que decidi tomar a iniciativa de fazer minhas próprias investigações com alguns aplicativos de rastreamento, até que encontrei uma avaliação positiva sobre um investigador privado, o qual entrei em contato através do e-mail fornecido: XXXXX Expliquei cuidadosamente e passei as informações que ele solicitou e, em poucas horas, o dispositivo da minha esposa foi hackeado e eu consegui acessar suas mensagens, WhatsApp, Facebook e e-mails. Também pude monitorar a localização dela em tempo real, além de ouvir suas chamadas telefônicas. Fiquei muito machucado quando todas essas informações vieram à tona. Me senti totalmente decepcionado, pois sempre fui honesto com ela e detesto a infidelidade." Disponível em: https://apps.apple.com/us/app/mspy-find-my-friends-phone/id1182397829?mt=8. Acesso em: 17 abr. 2025.

reflete nas práticas de uso de *spyware* e *stalkerware*, que monitoram de forma invasiva as vítimas e as controlam por meio do acesso aos dados coletados por aplicativos legítimos, em muitos casos, como localização, comunicações e até dados bancários. Esses mecanismos de vigilância não apenas têm o objetivo de observar, mas de influenciar, controlar e regular as ações das vítimas, muitas vezes de maneira coercitiva, reforçando relações de poder desiguais. Assim, a vigilância digital pode vir a atuar como uma ferramenta de controle social e, no caso de mulheres em situações de violência, um instrumento de opressão.

Importante lembrar que esses *spywares* exploram falhas de segurança em aplicativos e sistemas operacionais para coletar dados e perpetuar violências. Vulnerabilidades podem estar no código do aplicativo ou no dispositivo da vítima. O *spyware* pode se infiltrar disfarçado de uma atualização legítima ou ser distribuído por links. Ao acessar um aplicativo, o *spyware* monitora atividades em tempo real, capturando mensagens, transações bancárias, senhas e localizações.

Além das falhas nos aplicativos, sistemas operacionais, como Android e iOS, também podem ter vulnerabilidades em sua infraestrutura que permitem ao *spyware* obter controle total do dispositivo, coletando dados de qualquer aplicativo. Com essas informações, as violências aqui mapeadas, podem ser instrumentalizadas com o uso não autorizado dos dados.

A violência de gênero é compreendida como um fenômeno estrutural, vinculado à manutenção de relações de poder desiguais em sociedades patriarcais, afetando de maneira diferenciada indivíduos com base em marcadores como gênero, raça e classe. Essa violência não se limita ao âmbito físico, mas está profundamente enraizada em estruturas simbólicas e subjetivas que regulam comportamentos, corpos e identidades, reforçando papéis de gênero normativos. A concepção contemporânea, apoiada por autoras como Saffioti, Butler e Foucault, entende o gênero como uma construção performativa e estratégica de poder, que organiza hierarquias e legitima práticas de dominação. Nesse sentido, a violência de gênero não se resume a agressões físicas ou sexuais, mas se manifesta também como vigilância, controle, manipulação e tentativas de restringir a autonomia de mulheres e pessoas dissidentes de normas de gênero.

Quando essas relações de poder são mediadas por tecnologias digitais, elas se intensificam e ganham novas formas. A chamada “violência de gênero facilitada pela tecnologia” inclui práticas como espionagem, assédio, invasão de privacidade e disseminação de conteúdo íntimo, frequentemente realizadas por parceiros ou ex-parceiros abusivos. Softwares como *spywares* e *stalkerwares* desempenham um papel central nesse tipo de violência, pois permitem o acesso não autorizado a dados extremamente sensíveis, como mensagens, localização, fotos e registros de chamadas, a partir da invasão de um dispositivo digital da vítima que contenha seus dados sensíveis, seja no próprio dispositivo, seja em um aplicativo baixado e instalado em seu dispositivo. Muitos desses aplicativos operam de forma invisível e exploram falhas de segurança

nos dispositivos, possibilitando o monitoramento constante das vítimas sem seu conhecimento. Ao capturar e armazenar dados íntimos de aplicativos digitais legítimos, a partir da sua exploração, esses softwares podem se tornar um tipo ferramenta de dominação, transformando a coleta de dados em uma oportunidade para a perpetuação da violência.

Mas, então, o que fazer?

Produzir e divulgar guias de segurança digital acessíveis, especialmente voltados a mulheres e ativistas

Não compartilhar senhas e aplicativos com terceiros

Barrar o uso e comercialização de aplicativos espiões

Boas práticas de segurança digital, como uso de senhas fortes, autenticação em dois fatores

6. Referências bibliográficas:

ACCESS NOW. ***Unsafe anywhere: attacked by Pegasus, women activists speak out***. Publicado em: 17 jan. 2022. Disponível em: https://encurtador.com.br/zXMJ9. Acesso em: 31 out. 2024.

AMNESTY INTERNATIONAL. ***Thailand: State-backed digital abuse used to silence women and LGBTI activists - new report***. Publicado em: 16 mai. 2024. Disponível em: https://encurtador.com.br/v6lDO. Acesso em: 31 out. 2024.

AZAMBUJA, Mariana Porto Ruwer de; NOGUEIRA, Conceição. Violência de gênero: uma reflexão sobre a variabilidade nas terminologias. ***Saúde em Debate***, Rio de Janeiro, v. 31, n. 75/76/77, p. 97-106, jan./dez. 2007.

BARDALL, Gabrielle. Gender-specific election violence: the role of information and communication technologies. Stability: International Journal of Security and Development, [s.l.], v. 2, n. 3, art. 60, 2013. DOI: https://doi.org/10.5334/sta.cs.

BELLINI, Rosanna et al. "So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums. ***Proceedings of the ACM on Human-Computer Interaction***, v. 4, n. CSCW3, art. 210, p. 1-27.

BRANCAGLIONI, Bianca de Cássia Alvarez; FONSECA, Rosa Maria Godoy Serpa da. Violência por parceiro íntimo na adolescência: uma análise de gênero e geração. 2016. MOREIRA, Alexandro Martins; CECCARELLI, Paulo Roberto. Há múltiplas faces na violência por parceiro íntimo. 2016. MACHADO, Dinair Ferreira; CASTANHEIRA, Elen Rose Lodeiro. Interseções entre socialização de gênero e violência contra a mulher por parceiro íntimo. 2021.

BRODEALĂ, Elena; JELIĆ, Ivana; ȘUTEU, Silvia. ***Introduction to violence against women under European human rights law***. In: ***Violence against women under human rights law: the ongoing need for further action and research***. 2024.

BUTLER, Judith. ***Undoing gender***. New York; London: Routledge, 2004.

CHATTERJEE, Rahul; DOERFLER, Periwinkle; ORGAD, Hadas; HAVRON, Sam; PALMER, Jackeline; FREED, Diana; LEVY, Karen; DELL, Nicola; McCOY, Damon; RISTENPART, Thomas. The Spyware Used in Intimate Partner Violence. In: ***Proceedings - 2018 IEEE Symposium on Security and Privacy, SP 2018***. San Francisco, United States: Institute of Electrical and Electronics Engineers Inc., 2018. p. 441-458. ISBN 9781538643525. Disponível em: https://ieeexplore.ieee.org/document/8476695. Acesso em: 7 abr. 2025.

DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. ***Hacking Governamental: uma revisão sistemática***. Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponível em: https://bit.ly/3YdVcIL. Acesso em: 02 abr. 2025.

DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. ***Varredura pelo lado do cliente: uma revisão sistemática***. Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: <bit.ly/3EAhEDF>.

EX PRIME. ***Brasil segue como segundo país com mais vítimas de violência digital via stalkerware, aponta Kaspersky***. Publicado em: 1 mar. 2023. Disponível em: https://lexprime.com.br/brasil-segue-como-segundo-pais-com-mais-vitimas-de-violencia-digital-via-stalkerware-aponta-kaspersky/. Acesso em: 31 out. 2024.

FREED, Diana; PALMER, Jackeline; MINCHALA, Diana; LEVY, Karen; RISTENPART, Thomas; DELL, Nicola. "A stalker's paradise": how intimate partner abusers exploit technology. In: ***CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS***, 2018, Montreal. New York: ACM, 2018. Paper n. 667, p. 1–13.

FOUCAULT, Michel. ***História da sexualidade: volume 1: a vontade de saber***. Tradução de Sérgio Telles. 21. ed. Rio de Janeiro: Graal, 2010.

FOUCAULT, Michel. ***Segurança, território, população: palestras no Collège de France (1977-1978)***. Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2008.

FOUCAULT, Michel. ***O nascimento da biopolítica: curso dado no Collège de France (1978-1979)***. Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2008.

GRIN DEBERT, Guita; GREGORI, Maria Filomena. Violência e gênero: novas propostas, velhos dilemas. ***Revista Brasileira de Ciências Sociais***, v. 23, n. 66, 2008.

INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE (IP.REC) (Recife, Pernambuco); INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE (Belo Horizonte, Minas Gerais) (org.). ***Por Mais #MulheresNaGovernança da Internet***. 2. ed. aum. [S. l.]: IP.rec; IRIS, março 2024. 40 p. Cartilha. Disponível em: https://bit.ly/3TCW9ts.

KHO, Cynthia; ROBERTSON, Kate; DEIBERT, Ronald. ***Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications***. 2019. Electronic version first published by Citizen Lab. Disponível em: https://citizenlab.ca/docs/stalkerware-legal.pdf. Acesso em: 3 abr. 2025.

KOUZANI, A. Z. ***Technological Innovations for Tackling Domestic Violence***. IEEE Access, v. 11, p. 91293-91311, 2023.

LARICCHIA, Federica. ***Market share of mobile operating systems in Brazil from January 2019 to October 2024***. Statista, 22 out. 2024. Disponível em: https://www.statista.com/statistics/262167/market-share-held-by-mobile-operating-systems-in-brazil/. Acesso em: 26 fev. 2025.

MADIWALE, A. R.; KUMAR, S. ***An outline on increasing online gender violence against women in India and the role of cyber security***. ***Journal of Positive School Psychology***, 2022.

MUNANGA, Kabengele. ***Rediscutindo a mestiçagem no Brasil - Nova Edição: Identidade nacional versus identidade negra***. 2. ed. São Paulo: Editora XYZ, 2015.

PORTO, Maria Stela Grossi. ***Crenças, valores e representações sociais da violência***. ***Sociologias***, Porto Alegre, v. 16, p. 1-21, dez. 2006. DOI: https://doi.org/10.1590/S1517-45222006000200010.

PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. ***Varredura pelo lado do cliente: uma revisão sistemática***. Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: <bit.ly/3EAhEDF>.

RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. ***Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas***. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2022. Disponível em: https://bit.ly/3yLlb0P.

ROGERS, Michaela; FISHER, Colleen; ALI, Parveen Azam; ALLMARK, Peter. Technology-facilitated abuse in intimate relationships: a scoping review. ***Trauma, Violence & Abuse***, [S.l.], v. 24, n. 202, maio 2022. DOI: https://doi.org/10.1177/15248380221090218.

SAFFIOTI, Heleieth I.B. ***Contribuições feministas para o estudo da violência de gênero***. ***Cadernos Pagu***, Campinas, v. 16, p. 115-136, 2001.

SANTOS, Maria Joelma Alves. ***Violência doméstica: a permanência da mulher em relacionamento abusivo***. 2022. Trabalho de Conclusão de Curso (Bacharelado em Serviço Social) – Centro Universitário Internacional – UNINTER, Brasília, 2022.

SILVA, Lucas Gonçalves da; CARDOSO, Henrique Ribeiro; FARIA, Lucas Ribeiro. ***Deepfake pornográfico na sociedade de risco contemporânea: os desafios de regulamentação e controle da inteligência artificial***. ***Fluxo Contínuo***, v. 9, n. 3, 2024.

SOVACOOL, Benjamin; FURSZYFER-DEL RIO, Dylan D.; MARTISKAINEN, Mari. Can prosuming become perilous? Exploring systems of control and domestic abuse in the smart homes of the future. Frontiers in Energy Research, [s.l.], v. 9, 04 nov. 2021. Disponível em: https://doi.org/10.3389/fenrg.2021.765817.

UN Women. ***FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women***. 10 fev. 2025. Disponível em: https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women. Acesso em: 3 abr. 2025.

UNRIC - CENTRO DE INFORMAÇÃO DAS NAÇÕES UNIDAS EM BRASIL. ***Como a violência de gênero facilitada pela tecnologia afeta as mulheres***. UNRIC, 2021. Disponível em: https://unric.org/pt/como-a-violencia-de-genero-facilitada-pela-tecnologia-afeta-as-mulheres/. Acesso em: 9 abr. 2025.

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION (UNESCO). ***Your opinion doesn't matter, anyway: Exposing Technology-Facilitated Gender-Based Violence in an Era of Generative AI***. Paris: UNESCO, 2023. (World Trends in Freedom of Expression and Media Development Series). ISBN 978-92-3-100669-2. 2. ed.

VALENTE, Mariana. ***Misoginia na internet***. 2023. São Paulo: Editora Fósforo.

VERMA, Rabindra Kumar; GUPTA, Ashish Kumar. ***Role of Information and Communication Technology in the Digitalization of Violence and Sexual Politics in the Indian Scenario***. In: ***Cyberfeminism and Gender Violence in Social Media***. 2023. Cap. 3.

ZERAI, Assata. Select gender-based violence literature reviews: gender-based violence in the MENA among religious and other minorities in conflict settings. [S.l.]: United States Agency for International Development (USAID), maio 2020. Relatório n. GS-10F-0033M / ORDER NO. 7200AA18M00016 / DRG-LER II TASKING N008.

ANEXO I

Perguntas do Formulário - Revisão Bibliográfica

1) Quem está respondendo o formulário?
2) Título do artigo
3) Autores
4) Plataforma: ( ) Google Acadêmico ( ) Scielo ( ) Scopus ( ) Outro
5) Ano de publicação
6) Tipo de texto: ( ) Artigo ( ) Monografia ( ) Dissertação ( ) Tese ( ) Capítulo de Livro
7) Quais violência de gênero mencionadas?
8) Quais as tecnologias mais visadas pelos Spywares?
9) Quais as vulnerabilidades mais visadas pelos Spywares?
10) Quais os dados mais visados por Spywares?
11) Citações
12) Comentários

7. ANEXO II

Gmail/ google maps	apps citados nominalmente lit.	serviço de e-mail gratuito do Google/aplicativo de mapas que permite encontrar locais, traçar rotas, obter informações de trânsito e muito mais
Tinder	apps citados nominalmente lit.	aplicativo de namoro online e rede social que permite conhecer pessoas novas

Mlite rastreador de celular	apps citados nominalmente lit.	aplicativo de controle parental que permite aos pais monitorar a localização do celular de seus filhos e suas atividades online
Controle Parental MM guardian	apps citados nominalmente lit.	aplicativo de controle parental que monitora o uso do celular de crianças
Genius: AI Editor de fotos	Mais baixados geral	AI art photo editor
Instagram	Redes sociais	Aplicativo de redes sociais
Pinterest	Estilo de vida	plataforma de descoberta visual para encontrar ideias como receitas, inspiração para sua casa e estilo, e muito mais
Whatsapp	comunicação	aplicação de mensagens instantâneas
Flashcore	esporte	aplicativo que fornece informações sobre resultados de desportos, como futebol, basquete, tênis, entre outros
Nubank	finanças	plataforma de serviços financeiros digitais

Tabela IRIS

ANEXO III - Aplicativos

APPS MENCIONADOS NOMINALMENTE	MOTIVO PARA SEREM VISADOS
Facebook	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; O spyware pode coletar dados sobre com quem a vítima está se comunicando, o que pode ser usado para isolá-la ainda mais dos sistemas de apoio; Permite acesso a fotos e vídeos; pode permitir acesso à localização;
Instagram	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; O spyware pode coletar dados sobre com quem a vítima está se comunicando, o que pode ser usado para isolá-la ainda mais dos sistemas de apoio; Permite acesso a fotos e vídeos; pode permitir acesso à localização;
Twitter	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; O spyware pode coletar dados sobre com quem a vítima está se comunicando, o que pode ser usado para isolá-la ainda mais dos sistemas de apoio;
WhatsApp	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; pode coletar o número de telefone, que pode ser usado para perseguir ou assediar indivíduos; O spyware pode coletar dados sobre com quem a vítima está se comunicando, o que pode ser usado para isolá-la ainda mais dos sistemas de apoio;
Snapchat	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; O spyware pode coletar dados sobre com quem a vítima está se comunicando, o que pode ser usado para isolá-la ainda mais dos sistemas de apoio; Permite acesso a fotos e vídeos; pode permitir acesso à localização;

APPS MENCIONADOS NOMINALMENTE	MOTIVO PARA SEREM VISADOS
TikTok	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; O spyware pode coletar dados sobre com quem a vítima está se comunicando, o que pode ser usado para isolá-la ainda mais dos sistemas de apoio; Permite acesso a fotos e vídeos;
Track family	plicativos usados para rastrear a localização de crianças podem ser aproveitados para acessar mensagens de texto ou gravar vídeos, além de permitir acesso à localização
Track kids/ children	aplicativos usados para rastrear a localização de crianças podem ser aproveitados para acessar mensagens de texto ou gravar vídeos.
Track friends	permite acesso à localização do dispositivo em tempo real
Track phone	permite acesso à localização do dispositivo em tempo real
Track your devices	permite acesso à localização do dispositivo em tempo real
Find My Friends	permite acesso à localização do dispositivo em tempo real
MMGuardian	permite acesso à localização do dispositivo em tempo real
Location Tracker	permite acesso à localização do dispositivo ou veículo em tempo real

APPS MENCIONADOS NOMINALMENTE	MOTIVO PARA SEREM VISADOS
Life360	permite acesso à localização do dispositivo em tempo real
SMS	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; O spyware pode coletar dados sobre com quem a vítima está se comunicando, o que pode ser usado para isolá-la ainda mais dos sistemas de apoio
Rastreador GPS em veículo	permite monitorar a localização do indivíduo em tempo real
Apple AirTags	permite monitorar a localização do indivíduo em tempo real via bluetooth
Gmail	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; O spyware pode coletar dados sobre com quem a vítima está se comunicando, o que pode ser usado para isolá-la ainda mais dos sistemas de apoio; também possibilita monitorar conversas pessoais e compromissos
Google maps	permite monitorar a localização do indivíduo e os trajetos que fez
WebCam	permite acesso à câmera do dispositivo e, assim, à imagem da vítima; também é possível monitorar os contatos feitos e ligar remotamente a câmera
Gravador de áudio	o spyware pode ser usado para ter acesso às gravações e à voz do indivíduo, além de ativar remotamente a gravação, permitindo ouvir conversas

APPS MENCIONADOS NOMINALMENTE	MOTIVO PARA SEREM VISADOS
Câmera do dispositivo	pode ser ligada remotamente, permitindo que o indivíduo tenha sua imagem monitorada em tempo real
Calendário/ Agenda	é possível ter acesso à rotina do indivíduo, com detalhamento sobre horários e locais
Tinder	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; controle sobre a vida sexual do indivíduo; por meio das conversas, também pode ser possível monitorar seus encontros/compromissos e localização

APPS MENCIONADOS DE MODO GENÉRICO	MOTIVOS PARA SEREM VISADOS
Apps de aplicativos de relacioamento e "matrimonial websites"	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; controle sobre a vida sexual do indivíduo; por meio das conversas, também pode ser possível monitorar seus encontros/ compromissos e localização
App de social media	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; O spyware pode coletar dados sobre com quem a vítima está se comunicando, o que pode ser usado para isolá-la ainda mais dos sistemas de apoio; Permite acesso a fotos e vídeos; pode permitir acesso à localização

APPS MENCIONADOS DE MODO GENÉRICO	MOTIVOS PARA SEREM VISADOS
Apps de mensageria	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; pode coletar o número de telefone, que pode ser usado para perseguir ou assediar indivíduos; O spyware pode coletar dados sobre com quem a vítima está se comunicando, o que pode ser usado para isolá-la ainda mais dos sistemas de apoio
E-mail	permite acesso a interações online, que podem ser usadas para intimidar ou chantagear as vítimas; O spyware pode coletar dados sobre com quem a vítima está se comunicando, o que pode ser usado para isolá-la ainda mais dos sistemas de apoio; também possibilita monitorar conversas pessoais e compromissos
Site de busca	Permite acessar o histórico de navegação
Aplicativos anti-furto	permite localizar o dispositivo em tempo real e, assim, localizar o usuário
Aplicativos usados para rastrear a localização de crianças	permite localizar o dispositivo em tempo real e, assim, localizar o usuário
Software de espelhamento de tela	permite monitorar todas as atividades realizadas no dispositivo
Aplicativos da apple e google	os aplicativos tendem a estar conectados e sincronizados por uma conta, o que permite acesso a múltiplas funções e informações de outros apps, como email, agenda, localização, etc

APPS MENCIONADOS DE MODO GENÉRICO	MOTIVOS PARA SEREM VISADOS
Tecnologias de prosuming	de modo geral, por meio dessas tecnologias é possível monitorar imagens e sons da casa, além de controlar as condições do ambiente (como temperatura)
Salas de bate-papo	é possível monitorar as conversas do indivíduo
Femtech: aplicativos relacionados à gravidez e menstruação	é possível monitorar informações sobre a saúde do indivíduo, como atividade sexual, uso de métodos contraceptivos, sintomas, etc
Aplicativos de monitoramento parental/ contas de crianças com guarda compartilhada	é possível monitorar a localização em tempo real, além de acessar mensagens, ligações e a câmera
Alto-falantes de casa inteligente	é possível escutar o que ocorre no ambiente, como conversas
Recording call	por meio desse tipo de app é possível escutar conversas telefônicas

iris

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE