

EXPONDO STALKERWARE

um panorama das produções científicas
sobre o uso de stalkerware como tecnologia
facilitadora de violência de gênero no Brasil



Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Expondo stalker(ware) [livro eletrônico] : um
panorama das produções científicas sobre o uso
de stalkerware como tecnologia facilitadora de
violência de gênero no Brasil / Anicely
Santos...[et al.]. -- Recife, PE : IP.rec, 2025.
PDF

Outros autores: Carolina Branco, Luana Batista
Araújo, Mariana Canto, Raquel Saraiva, Rhaiana
Valois.

ISBN 978-65-982630-3-4

1. Software de aplicação 2. Tecnologia -
Aspectos sociais 3. Violência de gênero I. Santos,
Anicely. II. Branco, Carolina. III. Araújo, Luana
Batista. IV. Canto, Mariana. V. Saraiva, Raquel.
VI. Valois, Rhaiana.

25-284171

CDD-005.8

Índices para catálogo sistemático:

1. Stalkerware : Crimes digitais : Ciência da
computação 005.8

Eliete Marques da Silva - Bibliotecária - CRB-8/9380



FICHA TÉCNICA

Realização:

Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec

Equipe:**Coordenação:**

Mariana Canto

Autores:

Anicely Santos

Carolina Branco

Luana Batista Araújo

Mariana Canto

Raquel Saraiva

Rhaiana Valois

Projeto Gráfico:

Estúdio Puya!

Apoio:

Programa de Acesso Digital da Embaixada do Reino Unido no Brasil

Como citar:

IP.REC - INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE. Expondo stalker(ware): um panorama das produções científicas sobre o uso de stalkerware como tecnologia facilitadora de violência de gênero no Brasil. Recife: IP.rec, 2025.

Essa publicação é distribuída através de licença Creative Commons Atribuição-NãoComercial Compartilhaigual CC BY-NC-SA



Sumário

Sumário Executivo

Considerações Terminológicas e Escolhas Linguísticas

Metodologia

1. Evolução terminológica

2. Questões jurídicas, invisibilização legal e lacunas normativas

3. Questões técnicas relacionadas a stalkerware ou tecnologias de uso duplo

4. Questões psicossociais acerca do uso de ferramentas de monitoramento em relações íntimas

5. Estratégias de resistência e proteção das vítimas

6. Abordagens interseccionais

Conclusão

Apêndice I

Apêndice II



Sumário Executivo

O projeto de pesquisa *Expondo stalker(ware)* desenvolvido pelo Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec com apoio do Programa de Acesso Digital da Embaixada do Reino Unido no Brasil busca endereçar a violência de gênero facilitada por tecnologias. Ao se debruçar sobre essa temática, a iniciativa colabora para diminuir as desigualdades digitais, promovendo ambientes virtuais mais seguros e acolhedores.

A primeira publicação de uma série de estudos realizados a partir deste projeto busca compreender o estado da arte da produção científica brasileira sobre o uso de aplicativos espiões (*spyware*) e tecnologias de uso duplo (*dual-use apps*) como facilitadores de violência de gênero entre os anos de 2020 e 2025. Por meio da presente análise, buscamos identificar avanços, lacunas e disputas conceituais no campo, com o intuito de contribuir para o fortalecimento de respostas acadêmicas, políticas e sociais frente a esse fenômeno.

A pesquisa realizada identificou que o *stalkerware*, como tecnologia de monitoramento íntimo não consensual, tornou-se, ao longo dos últimos anos, um tema de crescente relevância na produção acadêmica brasileira, especialmente à medida que suas implicações jurídicas e psicossociais passaram a ser mais bem compreendidas. Entretanto, ainda que o tema tenha ganhado atenção nos últimos anos, ainda há significativa escassez de pesquisas sistemáticas no Brasil que abordem a complexidade dessa forma de violência, em especial no que se refere às suas dimensões técnicas e interseccionais.

Principais achados

- 1. O setor acadêmico e organizações da sociedade civil enfatizam que o *stalkerware* não se define apenas por suas características de programação, mas, sobretudo, pelo contexto e pela finalidade de seu uso. O termo é profundamente situado nos debates sobre vigilância e opressão digital.**



2. Há uma tensão entre a lenta consolidação de marcos legais e a precariedade das respostas institucionais no Brasil, evidenciando a contínua invisibilização das tecnologias como instrumentos de perpetuação da violência de gênero.
3. O setor privado, a academia e a sociedade civil brasileira alertam para um ecossistema de abuso digital cada vez mais sofisticado, que inclui o uso de softwares de uso duplo (*dual-use apps*), *cyberstalking* e *doxxing* como formas de controle e vigilância digital associadas à violência de gênero.
4. A produção acadêmica brasileira tem aprofundado a compreensão da violência digital como expressão de relações de gênero desiguais, em que o controle tecnológico se legitima por meio de discursos afetivos e normas culturais que naturalizam a vigilância como forma de cuidado.
5. Durante o período analisado, observa-se uma evolução gradual e não linear nas estratégias de proteção às vítimas, com respostas distintas entre os setores. Enquanto empresas focam em soluções tecnológicas para detecção e remoção de softwares maliciosos, o governo prioriza a orientação às vítimas e a sociedade civil e a academia propõem medidas mais humanizadas e estruturais, como redes de apoio, capacitação e políticas públicas.
6. Abordagens voltadas ao enfrentamento dessa violência de gênero no Brasil muitas vezes carecem de uma perspectiva interseccional robusta e aprofundada que vá além da questão da violência contra mulheres cis de uma forma geral.

Considerações Terminológicas e Escolhas Linguísticas

Durante a análise, foram adotados de forma intencional e crítica os termos **agressor**, **perpetrador** e **abusador** para se referir àquele que pratica atos de violência digital por meio do uso de tecnologias como o *stalkerware*. A escolha pela alternância desses termos visa refletir a variedade de enfoques presentes na



literatura, respeitando os contextos específicos em que cada um se apresenta. Já o termo **vítima** foi mantido por sua consolidação tanto nos textos jurídicos quanto acadêmicos, reconhecendo, no entanto, a complexidade do termo e os debates existentes em torno de sua centralidade. Optou-se por sua utilização neste trabalho por razões de clareza e aderência ao vocabulário predominante na bibliografia analisada.

Em relação à grafia, optou-se por utilizar o termo *cyberstalking* com “y”, conforme padrão consolidado na literatura internacional e adotado pela maior parte dos estudos acadêmicos brasileiros. Cabe ainda esclarecer que, ao longo da revisão, os termos de origem inglesa como *spywares*, *stalkerwares* e *malwares* foram mantidos no plural com a adição do “s”, embora tal flexão não exista na língua inglesa. Essa escolha estilística reflete uma prática cada vez mais comum na literatura brasileira sobre tecnologia, que pluraliza esses termos segundo a lógica gramatical do português, permitindo maior fluidez e familiaridade na leitura.

Metodologia

O presente estudo tem como objetivo investigar “*Qual é o estado da arte da produção científica brasileira sobre o uso de spyware e aplicativos de uso duplo como tecnologias facilitadoras de violência de gênero no contexto de relações interpessoais?*” a partir de uma análise qualitativa e interdisciplinar da bibliografia científica brasileira produzida entre 2020 e 2025.

A seleção do material foi realizada por meio de buscas sistemáticas nas plataformas *Google Acadêmico* e *Google Web*, utilizando *strings* de pesquisa desenvolvidas previamente pela equipe de pesquisa (conforme detalhado no Apêndice I), que combinam termos em português e inglês relacionados a cinco focos:

- (i) Violência de gênero a partir da utilização de *spywares* no Brasil;
- (ii) A utilização de *stalkerwares* no Brasil;
- (iii) A relação entre *cyberstalking* e *spywares* no Brasil;
- (iv) A associação entre *cyberstalking* e violência de gênero no Brasil; e
- (v) Violência de gênero a partir da utilização de aplicativos de uso duplo (*dual-use apps*) no Brasil.



Foram incluídos em nosso levantamento artigos científicos, teses, capítulos de livros, documentos técnico-orientadores publicados por membros do setor governamental e materiais produzidos por empresas e organizações da sociedade civil, desde que assinados por autores vinculados a instituições de ensino e pesquisa brasileiras ou organizações com sede e/ou escritórios no país (Apêndice II). Os critérios de inclusão envolveram, além da afiliação institucional, a pertinência temática ao objeto da pesquisa e a disponibilidade pública dos textos.

Ao final do processo de levantamento e sistematização do material, foi realizada uma análise temática qualitativa, com foco na identificação e categorização dos principais eixos de debate presentes na produção científica brasileira sobre o tema entre 2020 e 2025. Essa análise foi organizada a partir de seis vertentes analíticas definidas pela equipe de pesquisa:

(i) **evolução terminológica**, que buscou mapear como os conceitos de *stalkerware*, *spyware* e tecnologias de uso duplo foram sendo nomeados, definidos e utilizados;

(ii) **questões jurídicas, invisibilização legal e lacunas normativas**, que examinou os debates em torno da ausência ou insuficiência de regulamentação específica sobre essas tecnologias e sua interface com a legislação sobre violência de gênero;

(iii) **questões técnicas relacionadas a *stalkerware* ou tecnologias de uso duplo**, com atenção às características operacionais, formas de instalação, rastreamento e detecção desses aplicativos;

(iv) **questões psicossociais acerca do uso de ferramentas de monitoramento em relações íntimas**, centrando-se nos impactos emocionais, simbólicos e relacionais associados ao controle tecnológico;

(v) **estratégias de resistência e proteção das vítimas**, com ênfase em iniciativas de enfrentamento, denúncia e suporte institucional ou comunitário; e

(vi) **abordagens interseccionais**, analisando como marcadores sociais como gênero, raça, classe, território e idade atravessam as experiências e análises sobre o uso dessas tecnologias;

Essa categorização permitiu não apenas organizar o *corpus*, mas também evidenciar as complexidades e tensões que estruturam o debate acadêmico nacional sobre o uso de tecnologias de monitoramento íntimo como instrumento de violência de gênero.



1. Evolução terminológica

A evolução terminológica do termo *stalkerware* no Brasil ao longo da primeira metade da década de 2020 reflete não apenas o amadurecimento técnico e jurídico da sociedade em relação ao entendimento das tecnologias de vigilância digital, mas também uma mudança epistêmica mais ampla, que envolve disputas semânticas, apropriações político-sociais e redefinições normativas acerca da violência facilitada por tecnologias. Trata-se de um conceito cuja consolidação reflete a interseção entre dinâmicas tecnológicas, transformações legais e discussões sobre o controle, a vigilância e a violência digital nas relações sociais contemporâneas.

A análise da evolução terminológica do termo - fundamentada em fontes que abrangem desde relatórios técnicos de empresas de cibersegurança e pesquisas acadêmicas até materiais informativos e educativos de organizações do terceiro setor - revela uma trajetória que acompanha, quase que paralelamente, o avanço dos mecanismos de vigilância digital. Essa evolução evidencia como o léxico em torno do *stalkerware* transitou de uma compreensão difusa para uma conceituação mais precisa, articulada a áreas como segurança cibernética, violência de gênero, direitos digitais e privacidade.

A presente análise da bibliografia brasileira sobre o termo tem início em 2020, ano em que o termo *stalkerware* começou a ganhar visibilidade internacional e nacional, impulsionado pela pandemia de COVID-19. O confinamento forçado que ocorreu nesse período contribuiu para o aumento expressivo do uso de tecnologias de monitoramento em ambientes domésticos, intensificando situações de abuso e vigilância íntima. Relatórios de empresas como a Avast apontaram um crescimento de 51% na instalação desses aplicativos durante a quarentena¹, revelando a estreita relação entre o isolamento social e o fortalecimento de práticas abusivas facilitadas pela tecnologia.

Embora ainda incipiente no vocabulário popular e jurídico, o termo *stalkerware* já aparecia em documentos técnicos como sinônimo de "*softwares*

¹ Marcela Franco, "Uso de app espião para vigiar parceiro cresce 51% na pandemia", TechTudo, 11 de julho de 2020, <https://www.techtudo.com.br/noticias/2020/07/uso-de-app-espiao-para-vigiar-parceiro-cresce-51percent-na-pandemia.ghtml>.



antiéticos que permitem o rastreamento da localização de uma pessoa, acesso a seus arquivos e comunicações sem consentimento"². Também era descrito como uma subcategoria de *spyware* voltada à vigilância íntima não consensual³, frequentemente comercializada de forma aberta e acessível, o que agravava seu impacto sobre as vítimas. Na produção acadêmica brasileira, prevalecia o uso da expressão *cyberstalking*, entendida como forma de perseguição reiterada e obsessiva por meios digitais⁴ ⁵. Apesar de reconhecerem as dinâmicas relacionais e abusivas da vigilância digital, os estudos ainda não distinguiam com precisão o uso de *stalkerware*, tratando ambas as práticas de forma sobreposta e generalista.

Nesse cenário, organizações da sociedade civil desempenharam um papel central na visibilização do problema. Iniciativas do MariaLab⁶ como o Mapa do Acolhimento⁷ alertavam para o uso de celulares como instrumentos de controle em contextos de violência doméstica. Termos como "aplicativos espiões" e idéias relacionadas a monitoramento e vigilância eram comuns nesses materiais, evidenciando o esforço de nomear e combater um fenômeno ainda carente de uma definição consolidada. Essa fase inicial revela um campo em disputa, no qual diferentes setores contribuíam, ainda que de forma fragmentada, para a formulação de um conceito emergente.

Já em 2021, o termo *stalkerware* passou por um processo de definição conceitual. No campo acadêmico, pesquisadoras como Roberta Paiva⁸ passaram a empregar o termo com maior precisão, analisando sua relação com a violência baseada em gênero e a vigilância íntima não consensual. Apesar disso, ainda era comum que se observasse nos trabalhos uma terminologia centrada no

² Ibidem.

³ "O Estado do Stalkerware em 2020", Kaspersky, 2020, https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2020/03/25175214/PT_BR_The-State-of-Stalkerware-2020.pdf.

⁴ Carlos Henrique Mota, "Cyberstalking: A necessidade de tipificação no Direito Penal Brasileiro", *Faculdade Damas*, 2020, <https://revistas.faculdedamas.edu.br/index.php/academico/article/view/1931>.

⁵ Amanda Arruda, "A conduta do stalking sob o paradigma do ordenamento jurídico brasileiro" (Monografia, Salvador, Universidade Católica do Salvador, 2020), <https://ri.ucs.br/handle/123456789/5335>.

⁶ "Como Evitar Que Agressores Tenham Acesso Ao Seu Celular", MariaLab, *MariaLab* (blog), 16 de maio de 2020, <https://www.marialab.org/como-evitar-que-agressores-tenham-acesso-ao-seu-celular/>.

⁷ "Quarentena Sem Violência" (Mapa do Acolhimento, 2020), https://oab-brusque.org.br/wp-content/uploads/2020/07/Cartilha-Mapa-do-Acolhimento_QuarentenaSemViole%CC%82ncia_BR.pdf.

⁸ Roberta Paiva, "Inovações digitais no combate à violência contra a mulher: iniciativas durante a pandemia da Covid-19 no Brasil" (Dissertação, Rio de Janeiro, Brazil, Pontifícia Universidade Católica do Rio de Janeiro, 2021), <https://doi.org/10.17771/PUCRio.acad.55652>.



cyberstalking como no trabalho de Edilayne Brito⁹, compreendendo-o como uma forma reiterada de perseguição online, envolvendo o uso de redes sociais, camadas profundas da internet e técnicas de intrusão informática.

No âmbito da sociedade civil, organizações como o NIC.br, passaram a adotar o termo com mais clareza, ampliando a conscientização pública sobre os riscos dos *stalkerwares* e os definindo como aplicativos instalados em dispositivos móveis com o objetivo de espionar vítimas em contextos de abuso¹⁰. Nesse mesmo contexto, a Secretaria de Estado de Desenvolvimento Social de Minas Gerais (SEDS MG) também passou a reconhecer o problema institucionalmente, caracterizando os *stalkerwares* como aplicativos de espionagem online projetados para operar de forma oculta, permitindo acesso remoto a celulares e computadores sem o conhecimento das vítimas¹¹.

Simultaneamente, ainda no ano de 2021 ocorreu a promulgação da Lei nº 14.132/2021¹², que tipificou o crime de *stalking* (perseguição), incluindo o meio digital, embora a lei não mencione explicitamente o *stalkerware*, ela criou uma base normativa para responsabilizar o uso dessas tecnologias em práticas de assédio e vigilância abusiva, sinalizando um avanço na articulação entre discurso técnico e regulação legal.

Analisando o ano de 2022, o termo passou a ser abordado com maior rigor técnico e jurídico. No âmbito acadêmico, pesquisadores como Almir Junior et. al.¹³, com base nas definições da *Coalition Against Stalkerware*, descreveram o *stalkerware* como um tipo de *software* disponibilizado diretamente para indivíduos, permitindo o monitoramento remoto de outro dispositivo sem consentimento ou notificação explícita. Essa definição destaca o papel do *stalkerware* na facilitação de práticas de assédio, controle coercitivo, espionagem e violência, mesmo quando

⁹ Edilayne Brito, “Cyberstalking: uma análise do crime de perseguição contra mulheres na internet, sob o olhar do art. 147 – a, CP inserido pela nova lei 14.132/2021” (Monografia, Mossoró, Universidade Estadual do Rio Grande do Norte, 2021), <https://repositorio.apps.uern.br/jspui/handle/123456789/351>.

¹⁰ *Segurança digital: uma análise de gestão de risco em empresas brasileiras* (Núcleo de Informação e Coordenação do Ponto BR, 2021), <https://cetic.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras>.

¹¹ “Referências técnicas para atuação profissional nos Centros de Referência de Atendimento às Mulheres em Situação de Violência” (Secretaria de Estado de Desenvolvimento Social, 2020), <https://serdh.mg.gov.br/serdh-start/ser-dh/serdh-backend/public/storage/uploads/2021/03/08/RXK7zBfzKvYjOdTyzhJJddtc82WPgkO5v3jsL9Q.pdf>.

¹² “Lei nº 14.132, de 31 de março de 2021”, Pub. L. No. 14.132 (2021), https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm.

¹³ Almir Junior et al., *Clínica Criminal a Tutela das Vulnerabilidades*, vol. 3 (Thoth, 2022).



utilizado de forma aparentemente não intencional. A ênfase recai sobre a intimidade da vigilância e sua sutileza técnica, o que a torna particularmente insidiosa e difícil de detectar pelas vítimas.

Ainda nesse campo, a autora Líliam Vasconcelos¹⁴ reforçou a ideia de que o *stalkerware* constitui uma subcategoria específica de *spyware*, voltada ao monitoramento clandestino da localização, comunicações e dados de navegação da vítima, associando o uso desse tipo de *software* ao crime de perseguição. Evidenciando uma integração crescente entre o discurso técnico e o marco jurídico inaugurado no ano anterior com a Lei nº 14.132/2021¹⁵.

Além disso, outros trabalhos como de Marjorie Andrade¹⁶ apontam que o crime de *stalking*, quando mediado por tecnologias digitais, é compreendido como *cyberstalking*, neologismo que, em 2022, aparece articulado ao uso de ferramentas específicas como o *stalkerware* como visto no trabalho de Vasconcelos¹⁷. Essa diferenciação entre *cyberstalking* como conduta e *stalkerware* como ferramenta representa um amadurecimento conceitual e normativo, aproximando o debate técnico da legislação recém-promulgada.

Em 2023, o termo foi empregado de maneira ainda mais elaborada. Mariana Valente¹⁸ destacou em sua pesquisa o caráter relacional e interpessoal do *stalkerware*, enfatizando que sua distinção frente ao *spyware* tradicional não está apenas na funcionalidade, mas no contexto de uso. Nesse contexto, aplicativos de monitoramento passaram a ser analisados também sob a ótica da intencionalidade abusiva, ampliando o escopo da discussão sobre consentimento e privacidade.

O termo *stalkerware* passou a ser definido de forma multidisciplinar, incorporando aspectos técnicos (sendo descrito como um tipo de *malware* que

¹⁴ Líliam Vasconcelos, “A criminalidade na sociedade da era digital: uma reflexão acerca das presenças digitais e o cyberstalking” (Monografia, Salvador, Faculdade Baiana de Direito, 2022), <https://monografias.faculdadebaianadedireito.com.br/tcc/a-criminalidade-na-sociedade-da-era-digital-uma-reflexao-acerca-das-presencas-digitais-e-o-cyberstalking/>.

¹⁵ Lei nº 14.132, de 31 de março de 2021.

¹⁶ Marjorie Andrade, “Stalking e cyberstalking: percepções incipientes acerca da criminalização da prática no Brasil” (Monografia, Brasília, Centro Universitário de Brasília, 2022), <http://repositorio.uniceub.br/jspui/handle/prefix/16415>.

¹⁷ Vasconcelos, “A criminalidade na sociedade da era digital”.

¹⁸ Mariana Valente, *Misoginia na internet: uma década de disputa por direitos* (Fósforo, 2023).



permite o monitoramento remoto de dispositivos infectados^{19 20 21}), aspectos legais (relacionados ao uso não consensual dessas tecnologias e à sua configuração como violação de direitos fundamentais) e aspectos sociais (ao ser reconhecido como uma ferramenta de violência baseada em gênero²²). Essa convergência de perspectivas reforça o entendimento de que o termo não é neutro, mas profundamente situado nos debates sobre vigilância e opressão digital.

O setor empresarial também teve papel relevante ao qualificar o *stalkerware* como uma forma específica de espionagem íntima, operando de modo furtivo e, muitas vezes, disfarçada sob a aparência de aplicativos legítimos, como ferramentas de controle parental ou segurança digital. Empresas como a Kaspersky, a Avast e a Perallis Security alertaram para os riscos dessas tecnologias, enfatizando que, embora aparentemente inofensivos, tais programas são frequentemente usados para monitorar localização, comunicações e histórico de navegação sem o conhecimento da vítima^{23 24 25 26}.

Essa ambiguidade funcional levantou preocupações éticas e jurídicas quanto ao uso indevido de tecnologias originalmente projetadas para fins legítimos. Ainda que o termo *dual-use apps* não apareça explicitamente nas fontes consultadas, a ideia de que um mesmo *software* pode ser apropriado para vigilância abusiva está presente de forma implícita nos relatos e análises. Esse reconhecimento reforça a necessidade de regulações mais claras sobre o desenvolvimento e o uso de tecnologias de monitoramento.

¹⁹ *Reflexões sobre direito e sociedade: fundamentos e práticas*, vol. 7 (Aya Editora, 2023), <https://doi.org/10.47573/aya.5379.2.170>.

²⁰ Aline Costa, “Juventudes e direitos humanos: redes, violências e representações na era digital” (Tese, Salvador, Universidade Católica do Salvador, 2023), <https://ri.ucsal.br/handle/123456789/5400>.

²¹ Ana Carolyne Gonçalves, “Crime de perseguição (stalking) nova Lei nº 14.132, de 31 de março de 2021” (Monografia, Goiânia, Pontifícia Universidade Católica de Goiás, 2023), <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/6804>.

²² Valente, *Misoginia na internet: uma década de disputa por direitos*.

²³ Claudio Yuge, “Stalkerware: apps espiões instalados na surdina crescem 358% no Brasil”, Canaltech, 16 de março de 2023, <https://canaltech.com.br/espionagem/stalkerware-apps-espioes-instalados-na-surdina-crescem-358-no-brasil-243436/>.

²⁴ “Crescem casos de stalkerware no Brasil; saiba como identificá-los e removê-los”, Perallis Security, 2023, <https://www.perallis.com/news/crescem-casos-de-stalkerware-no-brasil-saiba-como-identifica-los-e-re-move-los>.

²⁵ “Como detectar e remover spyware em um celular Android”, Kaspersky, 27 de novembro de 2023, <https://www.kaspersky.com.br/resource-center/preemptive-safety/spyware-on-android>.

²⁶ “El estado del stalkerware en 2022”, Securelist | Kaspersky, 8 de março de 2023, <https://securelist.lat/the-state-of-stalkerware-in-2022/97693/>.



No ano de 2024, não foram identificadas produções relevantes que contribuíssem para o desenvolvimento terminológico do conceito de *stalkerware* no Brasil. Embora algumas publicações tenham mencionado o fenômeno do stalking e suas manifestações digitais²⁷ ²⁸, essas referências não trouxeram avanços conceituais ou reflexões específicas sobre o uso e a consolidação do termo *stalkerware*. Essa ausência pode ser interpretada como uma fase de estabilidade na literatura nacional, após o processo de consolidação ocorrido nos anos anteriores. Ao mesmo tempo que evidencia a necessidade de maior continuidade na produção acadêmica nacional voltada à interseção entre tecnologia, vigilância íntima e violência digital.

Por fim, em 2025, o termo *stalkerware* aparenta estar consolidado no vocabulário técnico e político brasileiro, sendo empregado em diferentes contextos institucionais como uma categoria que articula dimensões técnicas, jurídicas e sociais. Observa-se também um aprofundamento nas discussões sobre os chamados *dual-use apps* — aplicativos originalmente desenvolvidos para finalidades legítimas, como controle parental ou rastreamento de dispositivos, mas que podem ser apropriados para fins abusivos. Relatórios e estudos provenientes do setor acadêmico e de organizações da sociedade civil passaram a enfatizar que o *stalkerware* não se define apenas por suas características de programação, mas, sobretudo, pelo contexto e pela finalidade de seu uso²⁹ ³⁰.

Essa trajetória terminológica, portanto, não é apenas uma mudança de nomenclatura ou um refinamento técnico. Trata-se de um processo epistemológico que envolve a produção de sentido, a visibilização de práticas antes ocultas e a possibilidade de intervenção política e jurídica. O termo *stalkerware* não apenas descreve uma tecnologia: ele contribui para delimitar responsabilidades e ampliar a compreensão sobre formas específicas de violência digital. Sua evolução é, por

²⁷ Priscilla Danille, “Stalking: as implicações da incorporação do tipo penal de perseguição no ordenamento jurídico brasileiro” (Dissertação, Universidade do Estado do Rio de Janeiro, 2024), <https://www.bdtd.uerj.br:8443/handle/1/22422>.

²⁸ Evelin Silva, Gabrielle Silva, e Andreia Almeida, “Stalking e cyberstalking contra a mulher”, *Revista ft* 29, nº 140 (16 de novembro de 2024), <https://doi.org/10.69849/revistaft/ni10202411161620>.

²⁹ Bruno Carvalho, Ana Maria Barros, e Roberta Aline Guimarães, “Lei n.º 11.340 de 07 de agosto de 2006: Patrulha Maria da Penha - guardiões da vida”, *Revista Eletrônica do Curso de Direito* 11, nº 1 (16 de abril de 2025): 48–63, <https://doi.org/10.52397/recdubm.v11i1.2327>.

³⁰ Luiza Dutra, Luisa Melo, e Ana Bárbara Gomes, “Vaza, Stalker! Proteção de Mulheres da Vigilância Digital”, *IRIS-BH* (blog), 2024, <https://irisbh.com.br/projetos/vaza-stalker-protacao-de-mulheres-da-vigilancia-digital/>.



isso, um espelho das lutas contemporâneas por soberania informacional, justiça de gênero e proteção de dados.

2. Questões jurídicas, invisibilização legal e lacunas normativas

A produção acadêmica e institucional sobre o crime de perseguição e suas derivações digitais entre 2020 e 2025, como o *stalkerware*, revela uma tensão constante entre a emergência da normatização penal e a persistente precariedade regulatória em torno da proteção das vítimas, especialmente mulheres. A partir de uma análise cronológica, observam-se três grandes vetores analíticos que atravessam os textos: a lenta consolidação de marcos legais, a fragilidade das respostas institucionais e a insistente invisibilização das tecnologias como formas de perpetuação da violência de gênero.

O ano de 2020 apresenta um retrato de apagamento normativo em relação à violência de gênero mediada por tecnologias, com destaque para a ausência de uma legislação específica que trate do *cyberstalking* ou do uso de *stalkerware* no Brasil. Como apontado por Carlos Henrique Mota³¹, a inexistência de um marco legal adequado cria um vácuo normativo que obriga o uso de legislações imprecisas e insuficientes, como o art. 65 da Lei de Contravenções Penais e dispositivos da Lei Maria da Penha. Ainda que esta última preveja formas de violência psicológica, como controle, vigilância e perseguição, seu escopo é limitado pela exigência de relações afetivas pregressas, o que exclui casos de assédio e perseguição por desconhecidos ou em âmbito profissional.

Esse contexto se agrava pela dificuldade de fixação de competência jurídica e jurisdicional, especialmente em crimes transnacionais ou que envolvem servidores localizados em outros países, como destacado por Edilayne Brito³². Soma-se a isso a ausência de capacitação dos profissionais que atuam na persecução penal, fator que impede a efetividade das respostas institucionais. A invisibilidade do problema também se revela na ausência de jurisprudência sobre a aplicação da LGPD em

³¹ Mota, “Cyberstalking: A necessidade de tipificação no Direito Penal Brasileiro”.

³² Brito, “Cyberstalking: uma análise do crime de perseguição contra mulheres na internet”.



casos de violência de gênero, apesar de seu potencial protetivo em relação à privacidade das mulheres.

Destaca-se ainda a análise da Secretaria de Estado de Desenvolvimento Social de Minas Gerais³³, que aborda o *cyberstalking* sob a ótica da Lei Maria da Penha. O texto sugere uma interpretação ampliada da legislação de gênero, incluindo a chantagem e a exposição de imagens como formas de violência psicológica e sexual. Apesar disso, não há menção a responsabilizações institucionais para além do agressor direto, mantendo a centralidade na figura do autor individual do crime.

Em 2021, a produção acadêmica começa a delinear com mais nitidez as limitações estruturais e institucionais na abordagem jurídica do *cyberstalking*, aprofundando a relação entre violência tecnológica e marcadores sociais como raça, classe e território. As contribuições de Mirela Silva e Daniela Oliveira³⁴ são decisivas nesse sentido, ao evidenciarem a situação de extrema vulnerabilidade das mulheres nas favelas, cuja exposição à violência é agravada pela ausência de recursos institucionais e pela desconfiança nas forças policiais. O medo de retaliações de traficantes e a conivência de agentes do Estado com redes criminosas tornam as soluções jurídicas inviáveis, deslocando a regulação da violência para instâncias extralegis como os próprios grupos armados locais. Nessa perspectiva, o sistema de justiça aparece não apenas como ineficaz, mas como agente de perpetuação da violência.

Outros estudos de 2021 apontam que a legislação penal brasileira ainda carece de instrumentos para lidar com o *cyberstalking*. Embora leis como a "Lei Carolina Dieckmann" (2012) e a "Lei Lola" (2018) representem avanços pontuais, sua área de incidência é limitada. Milena Gomes³⁵, citando Castro e Sydow demonstra que a tipificação penal exige a comprovação de conduta reiterada, estado mental do autor e resposta da vítima, o que gera barreiras probatórias significativas. O novo crime de perseguição, introduzido em 2021, ainda depende da

³³ "Referências técnicas para atuação profissional nos Centros de Referência de Atendimento às Mulheres em Situação de Violência".

³⁴ Mirela Silva e Daniela Oliveira, "Brazilian Favela Women: How Your Standard Solutions for Technology Abuse Might Actually Harm Them", 22 de janeiro de 2021, <https://doi.org/10.48550/arXiv.2101.09257>.

³⁵ Milena Gomes, "O stalking como forma de violência de gênero e sua previsão legal no ordenamento jurídico pátrio", Jusbrasil, 9 de fevereiro de 2021, <https://www.jusbrasil.com.br/artigos/o-stalking-como-forma-de-violencia-de-genero-e-sua-previsao-legal-no-ordenamento-juridico-patrio/1165160015>.



reiteração da conduta, diferentemente do art. 65 da Lei das Contravenções Penais, que permitia a punição mesmo por ato único, o que pode representar retrocesso na proteção da liberdade individual.

A literatura também destaca a ausência de articulação entre a Lei Geral de Proteção de Dados e os casos de violência de gênero, embora autores como José Luiz Júnior³⁶ reconheçam seu potencial de fortalecimento da proteção à privacidade feminina. No entanto, a falta de divulgação e conhecimento dessa legislação entre mulheres inviabiliza sua utilização como instrumento efetivo de defesa. A falha institucional se soma a uma lacuna cognitiva, evidenciando que o problema não é apenas jurídico, mas também pedagógico e informacional.

A abordagem do NIC.br³⁷, por sua vez, propõe um deslocamento importante ao destacar o papel das empresas de tecnologia na perpetuação da violência por meio do *stalkerware*. A discussão sobre o lucro obtido com esses dispositivos, bem como a necessidade de aplicar a Lei Geral de Proteção de Dados para responsabilização civil e institucional dessas corporações, é colocada como urgência. A violência é aqui compreendida como externalidade de um modelo de negócio que capitaliza sobre a vigilância interpessoal, deslocando a discussão da esfera penal para a mercadológica e regulatória.

Em 2022, o debate sobre o *cyberstalking* está atravessado pela incipiência legislativa e pela dificuldade em distinguir entre condutas lícitas e ilícitas, como apontado por Vasconcelos³⁸. A percepção de impunidade e a falta de compreensão sobre a ilicitude das ações denunciam não apenas lacunas normativas, mas também uma crise de inteligibilidade jurídica frente à velocidade das transformações tecnológicas.

Autoras como Andrade³⁹ (citando Marques e Maciel) problematizam a ausência de regulações consolidadas, o que aponta para um descompasso entre a produção normativa e as práticas sociais. A preocupação com a tipificação excessiva também é recorrente ainda em 2021⁴⁰, indicando o risco de se criminalizar condutas sociais

³⁶ José Luiz Júnior, “O direito a privacidade da mulher no mundo digital, e a aplicação da Lei Geral de Proteção de Dados (LGPD) como instrumento de enfrentamento à violência de gênero no país” (Monografia, Natal, Universidade Estadual do Rio Grande do Norte, 2021), <https://repositorio.apps.uern.br/jspui/handle/123456789/592>.

³⁷ *Segurança digital: uma análise de gestão de risco em empresas brasileiras*.

³⁸ Vasconcelos, “A criminalidade na sociedade da era digital”.

³⁹ Andrade, “Stalking e cyberstalking”.

⁴⁰ Gomes, “O stalking como forma de violência de gênero e sua previsão legal no ordenamento jurídico pátrio”.



banais sob o pretexto da perseguição reiterada. Tal posição revela uma tensão clássica do direito penal: o desafio de atuar sem se tornar um instrumento de controle normativo desproporcional.

Paralelamente, Barbosa e Braga⁴¹ propõem uma leitura mais pragmática e pedagógica da Lei Maria da Penha no contexto digital, sinalizando um movimento de expansão das interpretações legais para abarcar as novas formas de violência mediadas por tecnologia. Ainda que a proposta não aprofunde a responsabilização de plataformas, ela marca um deslocamento do debate para o campo da violência de gênero, ainda que limitado pela insistência em soluções de ordem penal.

No ano seguinte, os textos analisados expressam certa consolidação da tipificação penal, mas também surgem críticas mais densas ao alcance efetivo da legislação. Carvalho⁴², por exemplo, denuncia a baixa ocorrência de casos nos tribunais, mesmo com a frequência do fenômeno. Seu argumento, que questiona o reconhecimento social da ilicitude da perseguição, ressoa com leituras feministas que apontam a naturalização da violência simbólica contra mulheres.

A preocupação de Valente⁴³ com o "caráter aberto" do tipo penal revela um risco intrínseco à tipificação vaga: a possibilidade de uso instrumental da norma penal. Em sintonia, a autora problematiza a tendência de se apoiar em figuras jurídicas genéricas, o que denuncia uma forma de regulação imprecisa que se esquia da responsabilidade de nomear a violência tecnológica em sua especificidade.

A ausência de distinção entre *stalking* físico e digital, como argumenta Carvalho⁴⁴, é apresentada como um ganho de eficácia normativa. No entanto, essa homogeneização também pode ser lida como uma omissão frente às especificidades tecnológicas do *cyberstalking*, como o uso de ferramentas de

⁴¹ Márcio Barbosa e Romulo Braga, "Stalking: uma nova forma do crime de perseguição habitual e implacável sofrido pelas mulheres no Brasil", *Mnemosine Revista* 13, n° 1 (16 de dezembro de 2022): 118–31, <https://www.mnemosinerevista.com.viverleve.org/index.php/revista/article/view/83>.

⁴² Luana Carvalho, "Crimes cibernéticos: evolução e perseguição contra privacidade feminina e infantil" (Monografia, Goiânia, Pontifícia Universidade Católica de Goiás, 2022), <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/6123>.

⁴³ Valente, *Misoginia na internet: uma década de disputa por direitos*.

⁴⁴ André Carvalho, "A Responsabilidade Civil em casos de Stalking e Cyberstalking: Um estudo comparado entre os ordenamentos jurídicos do Brasil e do Estados Unidos da América." (Dissertação, São Paulo, Pontifícia Universidade Católica de São Paulo, 2022), <https://repositorio.pucsp.br/jspui/bitstream/handle/39278/1/Andr%c3%a9%20Furegate%20de%20Carvalho.pdf>.



monitoramento invisível, apontadas por Marques e Santos⁴⁵. Estes, por sua vez, enfatizam os desafios probatórios e a necessidade de medidas cíveis para suspensão imediata da conduta, indicando um deslocamento discursivo da esfera penal para formas de responsabilização mais acessíveis às vítimas.

Em 2024, a produção acadêmica adquire um tom ainda mais crítico, questionando a eficácia real da legislação penal. Gonçalves⁴⁶, por exemplo, alerta para a insuficiência das penas atribuídas ao crime de *cyberstalking*, que permitem a aplicação de medidas como a suspensão condicional do processo. Esse tipo de resposta, embora tecnicamente adequada, revela-se inócua na proteção da vítima e contribui para uma sensação de impunidade institucional.

Essa perspectiva é reforçada por autores como Danille⁴⁷, ao discutir a habitualidade como elemento do tipo penal. A exigência de reiteração de condutas, ainda que juridicamente justificável, pode inviabilizar a responsabilização de comportamentos graves quando isolados. O argumento, implícito, denuncia uma arquitetura normativa que exige que a violência se acumule para se tornar visível, colocando a vítima em um ciclo de exposição prolongada.

No ano mais recente, emerge uma pluralidade discursiva que, no entanto, ainda não rompe com o paradigma da responsabilização individualizada. Pithon⁴⁸ introduz a noção de controle coercitivo, já tipificado em outros países, mas ainda ausente do ordenamento jurídico brasileiro. A menção à legislação internacional aponta para um referencial comparado relevante, mas que permanece como horizonte e não como prática normativa concreta.

Carvalho, Dinardi e Guimarães⁴⁹ reforçam a importância da Lei Maria da Penha, enquanto Rivelli⁵⁰ destaca a natureza onipresente da violência digital. Ainda que reconheçam a especificidade da violência tecnológica, os textos permanecem

⁴⁵ Mateus Marques e Vanessa Santos, *Crime de Stalking: Uma análise sobre a subjetividade do tipo penal* (Papel da Palavra, 2023).

⁴⁶ Letícia Gonçalves, “Efetividade da criminalização do cyberstalking (Lei 14.132/2021)” (Monografia, Fortaleza, Universidade Federal do Ceará, 2024), <http://repositorio.ufc.br/handle/riufc/78997>.

⁴⁷ Danille, “Stalking: as implicações da incorporação do tipo penal de perseguição no ordenamento jurídico brasileiro”.

⁴⁸ Fabiana Pithon, “Jungian clinical approach with women in abusive relationships and post-divorce abuse: challenges and coping”, *Cadernos Junguianos*, 2024, https://www.ajb.org.br/wp-content/uploads/2025/01/18-edicao-Cadernos-Junguianos-versao-final-2024_AJB-EN.pdf#page=116.

⁴⁹ Carvalho, Barros, e Guimarães, “Lei n.º 11.340 de 07 de agosto de 2006: Patrulha Maria da Penha - guardiões da vida”.

⁵⁰ Fabio Rivelli, “A violência digital e seus efeitos nas vítimas: desafios contemporâneos e perspectiva do ser humano digital”, *Revista Internacional de Vitimologia e Justiça Restaurativa* 3, nº 1 (27 de fevereiro de 2025), <https://doi.org/10.58725/rivjr.v3i1.100>.



centrados em soluções legislativas tradicionais. A contribuição do terceiro setor, representado pelo Instituto de Referência em Internet e Sociedade (IRIS)⁵¹ aponta para a urgência de considerar o *stalkerware* como agravante em casos de violência de gênero.

A trajetória analítica entre os anos de 2020 a 2025 revela uma lenta, fragmentada e, em muitos casos, ineficaz consolidação jurídico-política da problemática do *stalkerware*, sobretudo quando imbricada às dimensões de gênero, privacidade e violência tecnológica. O que se observa, ao longo dos seis anos analisados, é menos uma progressiva normatização do tema e mais uma manutenção da negligência estrutural, tanto legal quanto institucional, com relação a formas digitais de controle e perseguição. As respostas jurídicas, quando existentes, foram majoritariamente orientadas por uma lógica penal, centrada no agressor individual e esvaziada de um enfrentamento das estruturas que tornam o *cyberstalking* um fenômeno social e de gênero amplamente disseminado e pouco responsabilizado.

Comparando os anos, nota-se um deslocamento importante entre 2020 e 2025: de uma quase ausência de discussão jurídica sobre o tema nos primeiros anos para uma crítica mais contundente à resposta penal nos últimos. Os anos de 2022 e 2023 são decisivos nesse processo, pois marcam a transição de uma abordagem meramente descritiva para uma formulação mais crítica da invisibilização legal e de seus efeitos. A partir de 2024, algumas análises ensaiam caminhos alternativos à punição tradicional, mas ainda sem força suficiente para gerar ruptura com o modelo punitivo dominante.

Apesar da mudança discursiva, o foco nas respostas penais permanece como eixo estruturante da abordagem institucional. A insistência nesse caminho, mesmo diante das evidências reiteradas de sua insuficiência, não é neutra. Como apontam os trabalhos de 2024 e 2025, ela revela uma adesão a soluções que deixam intactas as estruturas que permitem e sustentam a vigilância interpessoal. O direito penal aparece, aqui, como uma espécie de espantalho jurídico: sinaliza enfrentamento, mas não ameaça os interesses que lucram com a violência.

Esse ponto é particularmente sensível quando se observa o papel do setor privado, que permanece intocado pela responsabilização. A análise dos seis anos

⁵¹ Dutra, Melo, e Gomes, “Vaza, Stalker! Proteção de Mulheres da Vigilância Digital”.



demonstra que as plataformas e empresas que desenvolvem, distribuem ou hospedam *spywares* e serviços similares seguem atuando impunemente. A Kaspersky se destaca como uma das poucas empresas a reconhecer publicamente os riscos associados ao uso de *stalkerwares*, contribuindo para o debate e a conscientização sobre o tema. No entanto, esse tipo de posicionamento ainda é raro e insuficiente diante da ausência de medidas concretas de responsabilização. A omissão regulatória, portanto, funciona como blindagem mercadológica: ao não propor medidas de responsabilização civil ou administrativa, o Estado legitima o lucro corporativo obtido com práticas de controle e vigilância abusiva, frequentemente dirigidas a mulheres.

Trata-se de um pacto silencioso entre setores: enquanto o direito penal é mobilizado para punir sujeitos individuais, quase sempre em respostas tardias e ineficazes, o mercado da vigilância cresce livre, produzindo e vendendo dispositivos cuja principal finalidade é o controle coercitivo. A violência tecnológica, nesse sentido, não é um efeito colateral, mas uma externalidade lucrativa.

Ao longo do período, não há qualquer produção que trate de auditorias independentes, exigência de transparência algorítmica ou sanções econômicas às plataformas envolvidas na circulação de aplicativos de espionagem. Essa ausência não é casual: ela escancara a escolha institucional de manter o foco na punição individual, protegendo os interesses empresariais em jogo. O singelo antipunitivismo que começa a emergir na literatura mais recente não representa uma recusa da responsabilização, mas um esforço de deslocamento, da culpabilização do infrator isolado para a responsabilização sistêmica dos agentes que lucram com o dano.

A principal constatação que emerge da análise comparativa dos seis anos é que o vácuo normativo não decorre de ignorância, mas de uma escolha política. Ele opera como estratégia de manutenção da impunidade, sobretudo para os setores que mais se beneficiam da ausência de regulação. A retórica da neutralidade tecnológica e a resposta penal simbólica são, juntas, os dispositivos que sustentam esse cenário. Romper com essa lógica exige pensar para além do direito penal, instituindo mecanismos que responsabilizem quem lucra com o ciclo da violência, e isso passa, necessariamente, por enquadrar as plataformas como agentes ativos na cadeia de danos.



3. Questões técnicas relacionadas a stalkerware ou tecnologias de uso duplo

A disseminação de tecnologias de vigilância acessíveis transformou a segurança digital e a privacidade pessoal. Com base em pesquisas realizadas entre 2020 e 2025, esta seção explora os aspectos técnicos do stalkerware e dos aplicativos de uso duplo, ferramentas que, embora distintas de *spyware* tradicionais (focados em instalação remota, objetivando ganhos financeiros e roubo de dados) e *infostealers* (*malware* que roubam dados já armazenados no dispositivo), representam uma ameaça direta à liberdade e segurança das vítimas⁵², em especial aquelas inseridas em contextos de violência de gênero e relacionamentos abusivos^{53 54}.

O *stalkerware* configura-se como uma ferramenta de vigilância invasiva, projetada para roubar a liberdade física e online da vítima⁵⁵. Seu uso expressa uma problemática de dimensão global. Em 2020, período em que o tema ainda era pouco discutido no Brasil, já se contabilizavam 6.523 usuários afetados por este tipo de software no país, número equivalente a pouco mais da metade dos casos registrados na Federação da Rússia, então líder mundial em ocorrências⁵⁶. Em 2023, embora o Brasil tenha permanecido na segunda posição, o número de dispositivos infectados caiu para 4.186, evidenciando um progresso nas medidas de segurança para mitigar a propagação dos riscos inerentes a esse software.

Um dos aspectos técnicos mais relevantes é o modo de instalação. Em geral, esse tipo de software requer, na maioria dos casos, acesso físico direto ao dispositivo da vítima para ser instalado. Este processo, relativamente simples e rápido, pode ser concluído em poucos minutos. No entanto, sua execução envolve uma violação concreta da esfera privada no espaço físico, o que muitas vezes distingue o stalkerware de outras formas de vigilância digital. Essa característica evidencia uma vulnerabilidade estrutural: a confiança depositada em indivíduos do

⁵² Franco, “Uso de app espião para vigiar parceiro cresce 51% na pandemia”.

⁵³ Rivelli, “A violência digital e seus efeitos nas vítimas”.

⁵⁴ “Ciberviolencia y cyberacoso contra las mujeres y niñas en el marco de la Convención Belém do Pará”, Iniciativa Spotlight, 2022, [https://lac.unwomen.org/sites/default/files/2022-11/MUESTRA%20Informe%20Violencia%20en%20linea%202021%20\(2\)_Aprobado%20\(Abril%202022\)_0.pdf](https://lac.unwomen.org/sites/default/files/2022-11/MUESTRA%20Informe%20Violencia%20en%20linea%202021%20(2)_Aprobado%20(Abril%202022)_0.pdf).

⁵⁵ Franco, “Uso de app espião para vigiar parceiro cresce 51% na pandemia”.

⁵⁶ “O Estado do Stalkerware em 2020”.



círculo íntimo, especialmente parceiros e ex-parceiros, que configuram o perfil mais recorrente na grande maioria dos casos⁵⁷.

Uma vez instalado, o *stalkerware* opera de forma oculta, sem exibir notificações ou ícones na lista de aplicativos⁵⁸, impossibilitando a vítima de perceber que está sendo observada, mas permitindo ao agressor um monitoramento completo e contínuo. Para funcionar plenamente, esse tipo de software pode depender de permissões como acesso ao GPS, à câmera, ao microfone e a dados armazenados, permissões que, em muitos casos, são concedidas automaticamente ou aceitas sem a devida atenção pelo usuário. Essa combinação entre invisibilidade e permissões amplas torna os dispositivos móveis especialmente vulneráveis, oferecendo ao agressor uma base de ataque mais ampla do que por meio de computadores tradicionais⁵⁹. Esta vigilância, inclui^{60 61}:

- **Rastreamento de localização** em tempo real;
- **Acesso a mensagens** de redes sociais e aplicativos de comunicação;
- **Visualização de fotos, vídeos** e outros arquivos armazenados no dispositivo.
- **Escuta de conversas telefônicas** e gravação de áudio ambiente através do microfone;
- **Captura de tela e de tudo o que é digitado (*keylogging*)**, incluindo senhas e códigos de autenticação de dois fatores.

Alguns aplicativos de monitoramento podem ser encontrados em lojas oficiais de aplicativos, mas na maioria dos casos o agressor obtém o *link* diretamente nos sites dos desenvolvedores⁶². Em alguns países, como o Estados Unidos, é possível inclusive contratar serviços especializados para a instalação desses aplicativos⁶³, o que evidencia a existência de um mercado estruturado em torno da vigilância íntima.

⁵⁷ Costa, “Juventudes e direitos humanos: redes, violências e representações na era digital”.

⁵⁸ Julia Glazova, “Stalkerware ainda é um problema em 2020”, Kaspersky, 24 de março de 2021, <https://www.kaspersky.com.br/blog/stalkerware-in-2020/17192/>.

⁵⁹ *Segurança digital: uma análise de gestão de risco em empresas brasileiras*.

⁶⁰ Ibidem.

⁶¹ “Referências técnicas para atuação profissional nos Centros de Referência de Atendimento às Mulheres em Situação de Violência”.

⁶² “O Estado do Stalkerware em 2020”.

⁶³ Ibidem.



A plataforma do dispositivo também é um fator técnico determinante quanto a facilidade de instalação. O Android, por ser um sistema de código aberto, é o alvo principal^{64 65}, já que permite o escalonamento de privilégios⁶⁶, como o acesso ao *root*, que concede controle total sobre o dispositivo. Apesar da presença do *Google Play Protect* (sistema de segurança integrado e padrão de todos os dispositivos Android), a desativação dessa proteção é simples e pouco eficaz diante de um agressor com acesso físico ao aparelho.

O iOS, sistema operacional do iPhone, por adotar uma arquitetura mais restrita, impõe barreiras mais robustas. No entanto, essa proteção pode ser contornada se o *iPhone* sofrer um processo de "*jailbreak*" (remoção das restrições de software impostas pela Apple), que também exige acesso físico para ser executado^{67 68}.

Um estudo realizado por Flach e Deslandes identificou 40 aplicativos classificados como *stalkerware* disponíveis para os sistemas operacionais Android e iOS. A análise discursiva desses aplicativos revelou um padrão preocupante: 12 dos 14 participantes deste estudo associaram o rastreamento e o controle à ideia de cuidado e afeto. Nessa linha, Taylor et al. argumentam que comportamentos de controle por meios tecnológicos estão presentes nas relações íntimas da maioria dos jovens brasileiros e que seu uso explícito pode indicar uma "colaboração" entre parceiros como estratégia para evitar a escalada de conflitos envolvendo medos de infidelidade e ciúmes⁶⁹.

O ecossistema comercial que sustenta o desenvolvimento deste software malicioso tem se tornado progressivamente mais sofisticado, permitindo a replicação e personalização de softwares, a partir de uma amostra inicial. Esse modelo de negócio é conhecido como "*stalkerware as a service*". Nesta modalidade, é alugado a infraestrutura do aplicativo móvel e do servidor de controle para

⁶⁴ Ibidem.

⁶⁵ Paiva, "Inovações digitais no combate à violência contra a mulher".

⁶⁶ Do inglês *privilege escalation*, é um conceito de segurança digital que se refere ao processo que o indivíduo (no caso aqui o agressor) ganha mais permissão ou acesso do que deveria ter em um sistema.

⁶⁷ "O Estado do Stalkerware em 2020".

⁶⁸ "O que é Stalkerware? Como encontrar e remover stalkerware", Kaspersky, 21 de maio de 2024, <https://www.kaspersky.com.br/resource-center/definitions/what-is-stalkerware>.

⁶⁹ Gisella Ferreira, "Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence: Perspectives from Advocates in the Global-South", em *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (Emerald Publishing Limited, 2021), 427–46, <https://doi.org/10.1108/978-1-83982-848-520211032>.



terceiros que podem então renomear o produto com sua própria marca e vendê-lo de forma independente.

Um exemplo proeminente é a amostra *Nidb*, identificada pela *Kaspersky* como a mais utilizada em 2020⁷⁰ (afetando cerca de 8.100 usuários globalmente), e 2021⁷¹. Aplicativos como *iSpyoo*, *TheTruthSpy* e *Copy9* são, na essência, variações do *Nidb*, o que explica sua ampla disseminação⁷².

Em versões mais avançadas de monitoramento, o *Kaspersky* identificou o *Track My Phone*, baseado na amostra *Agent.af*. Outro caso relevante é o *Cerberus*, um *spyware* amplamente utilizado que se apresenta como uma solução antifurto para *smartphones*, mas opera de forma oculta, evitando ser detectado. Similar aos aplicativos legítimos de rastreamento de dispositivos, ele tem acesso à localização por GPS, além de poder capturar imagens, fazer prints de tela e gravar áudios.

Apesar de seu potencial uso abusivo, muitos desses aplicativos permanecem disponíveis na *Google Play Store*, uma vez que, formalmente, atendem às diretrizes da plataforma. Isso revela limitações nas políticas de moderação e fiscalização da loja, que, embora promovam medidas contra o *stalkerware*, ainda permitem a circulação de softwares com funcionalidades invasivas sob a justificativa de finalidades legítimas⁷³.

Talvez o desafio técnico e ético mais complexo seja o dos "*dual-use apps*" (aplicativos de uso duplo). Trata-se de softwares desenvolvidos com finalidades legítimas, mas que possuem funcionalidades que podem ser facilmente adaptadas para fins de vigilância e controle⁷⁴. Exemplos comuns incluem:

- **Aplicativos de controle parental**⁷⁵: ferramentas desenvolvidas para ajudar pais e responsáveis a monitorar e gerenciar o uso da internet e de dispositivos eletrônicos por crianças e adolescentes;
- **Ferramentas antifurto**⁷⁶: softwares projetados para prevenir ou dificultar o roubo de bens, como veículos, dispositivos eletrônicos ou outros itens de valor, como o *Cerberus*;

⁷⁰ "O Estado do Stalkerware em 2020".

⁷¹ Glazova, "Stalkerware ainda é um problema em 2020".

⁷² "O Estado do Stalkerware em 2020".

⁷³ Glazova, "Stalkerware ainda é um problema em 2020".

⁷⁴ Dutra, Melo, e Gomes, "Vaza, Stalker! Proteção de Mulheres da Vigilância Digital".

⁷⁵ Yuge, "Stalkerware: apps espiões instalados na surdina crescem 358% no Brasil".

⁷⁶ Glazova, "Stalkerware ainda é um problema em 2020".



- **Localizadores familiares**⁷⁷: são aplicativos ou dispositivos que permitem aos membros de uma família compartilhar suas localizações em tempo real uns com os outros. São projetados com o objetivo de aumentar a segurança e facilitar a coordenação entre os membros da família, como o *Life360*.

Embora vendidos com descrições inofensivas, seu potencial para abuso é enorme⁷⁸. Além disso, esses aplicativos muitas vezes recorrem a estratégias de *marketing* que incentivam o uso como forma de controle interpessoal, sugerindo que o monitoramento pode trazer "paz de espírito" e controle total no relacionamento. Propagandas como "ninguém pode escapar de você agora [...] nem mesmo seu namorado", "Você pode namorar em paz...", "...pergunte ao seu namorado se ele te ama, se ele disser 'sim', então pede para baixar [...] app de rastreamento" exemplificam o discurso que normaliza a vigilância no contexto das relações afetivas, disfarçando práticas invasivas sob a lógica do cuidado e da confiança⁷⁹.

Essa ambiguidade entre funcionalidade legítima e uso abusivo não se restringe aos *dual-use apps*. Mesmo aplicativos considerados inofensivos ou amplamente utilizados podem contribuir para a criação de um ambiente propício à vigilância e ao controle, especialmente quando envolvem a coleta massiva e contínua de dados sensíveis. As políticas de privacidade revelam que muitos apps populares coletam dados sensíveis (geolocalização, contatos, hábitos de uso e rotina diária, etc.) que, se acessados por um agressor, refinam e potencializam a violência de gênero⁸⁰.

Além da coleta direta de dados, a sofisticação das práticas de abuso digital tem avançado, incorporando táticas que extrapolam o uso isolado de *stalkerware*. Entre essas estratégias, destacam-se o *cyberstalking by proxy* (onde o agressor usa terceiros, como simpatizantes, redes sociais ou bots, para assediar e vigiar a vítima) e o doxxing (vazamento deliberado de informações pessoais, como endereço, contatos, rotina ou dados financeiros)⁸¹ ⁸², demonstrando que o *stalkerware* é apenas uma peça em um ecossistema de abuso digital mais amplo e complexo.

⁷⁷ Junior et al., *Clínica Criminal a Tutela das Vulnerabilidades*.

⁷⁸ Ibidem.

⁷⁹ Ibidem.

⁸⁰ Dutra, Melo, e Gomes, "Vaza, Stalker! Proteção de Mulheres da Vigilância Digital".

⁸¹ Danille, "Stalking: as implicações da incorporação do tipo penal de perseguição no ordenamento jurídico brasileiro".

⁸² Brito, "Cyberstalking: uma análise do crime de perseguição contra mulheres na internet".



4. Questões psicossociais acerca do uso de ferramentas de monitoramento em relações íntimas

Entre 2020 e 2025, os estudos revisados sobre *stalkerware* e vigilância digital em relações íntimas revelam não apenas a consolidação de um campo emergente, mas o aprofundamento de interpretações sobre os efeitos subjetivos e sociais da violência digital. Um dos achados mais consistentes é que o controle tecnológico exercido por parceiros ou ex-parceiros se ancora em discursos afetivos e relações desiguais de gênero, em que a vigilância se disfarça de cuidado. Esse tipo de controle não depende apenas da ferramenta utilizada, mas da permissividade cultural que ainda associa ciúmes à prova de amor e monitoramento à atenção romântica.

Os estudos em 2020 centraram-se em identificar e descrever o fenômeno emergente do *cyberstalking* em relações amorosas, muitas vezes atravessadas por históricos de domínio emocional e assimetria de poder. Carlos Henrique Mota⁸³ enfatiza que um grande percentual dos casos de *cyberstalking* decorre de relações amorosas presentes ou passadas, em que o conhecimento íntimo sobre a rotina da vítima é instrumentalizado para sua vigilância. Os dispositivos digitais tornam-se então extensões do poder afetivo-patriarcal, não apenas por fornecerem meios técnicos, mas por ativarem discursos simbólicos que naturalizam o controle.

Ainda em 2020, Amanda Arruda⁸⁴ problematizou como o uso das plataformas eletrônicas amplia a capacidade de aproximação não consentida, o que reitera que a tecnologia não inaugura a violência, mas a potencializa. As condições pandêmicas, como destacaram autores vinculados ao setor privado como a Avast⁸⁵, agravaram esse cenário ao promover isolamento social e dependência digital, criando um terreno ainda mais vulnerável para a adoção de stalkerwares por parceiros abusivos.

Em 2021, a literatura avança para a análise dos efeitos psicossociais do monitoramento, com foco nas dimensões emocionais que estruturam as relações

⁸³ Mota, “Cyberstalking: A necessidade de tipificação no Direito Penal Brasileiro”.

⁸⁴ Arruda, “A conduta do stalking sob o paradigma do ordenamento jurídico brasileiro”.

⁸⁵ Franco, “Uso de app espião para vigiar parceiro cresce 51% na pandemia”.



abusivas. Estudos de Gisella Ferreira⁸⁶, Pâmela Pedruzzi e Agnaldo Garcia⁸⁷, e Edilayne Brito⁸⁸ evidenciam o papel do medo, da vergonha e da dependência afetiva como elementos que dificultam o reconhecimento da violência e a busca por ajuda. Ao identificar que muitas mulheres não percebem o controle como agressão, esses autores apontam para uma gramática relacional perversa, na qual o ciúmes é confundido com cuidado, e a insistência, com afeto. Tal confusão é alimentada por uma cultura midiática e afetiva que romantiza comportamentos abusivos como expressões de amor verdadeiro. A perspectiva da SEDS-MG⁸⁹ aprofunda essa análise ao relacionar o medo das vítimas de romper com o agressor às armadilhas do "dispositivo amoroso" que aprisiona mulheres em vínculos violentos.

O ano de 2022 marca uma inflexão analítica com a consolidação da perspectiva interseccional. Pesquisas coordenadas por Almir Junior et al.⁹⁰ revelam que 70% das mulheres vigiadas por *stalkerware* já haviam sido vítimas de violência doméstica, reiterando que a violência digital é parte de um ciclo estrutural e não um evento isolado. Daniel Nascimento⁹¹ critica a ideia de que o *cyberstalking* afeta apenas pessoas famosas, ressaltando que mulheres comuns, especialmente em relações afetivas heterossexuais, constituem o principal alvo dessa forma de abuso. Esse deslocamento analítico permite superar leituras individualizantes ou espetacularizadas da violência, favorecendo a compreensão da vigilância digital como parte de dinâmicas sociais mais amplas, com raízes estruturais que ainda precisam ser enfrentadas.

Estudos de Fornasier, Spinato e Ribeiro⁹² aprofundam a discussão sobre os padrões de gênero nas formas de perseguir, apontando que homens tendem a adotar táticas mais reiteradas e invasivas, enquanto mulheres, quando perpetradoras, operam por vias mais sutis. Tais observações, embora não se

⁸⁶ Ferreira, "Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence".

⁸⁷ Pâmela Pedruzzi e Agnaldo Garcia, "Violência contra a mulher por parceiro íntimo: contextos online e offline", *Interação em Psicologia* 25, n° 2 (31 de agosto de 2021), <https://doi.org/10.5380/riep.v25i2.72061>.

⁸⁸ Brito, "Cyberstalking: uma análise do crime de perseguição contra mulheres na internet".

⁸⁹ "Referências técnicas para atuação profissional nos Centros de Referência de Atendimento às Mulheres em Situação de Violência".

⁹⁰ Junior et al., *Clínica Criminal a Tutela das Vulnerabilidades*.

⁹¹ Daniel Nascimento, "Criminalização do stalking no Brasil: análise do artigo 147-A do código penal em face do direito à privacidade" (Monografia, Fortaleza, Universidade Federal do Ceará, 2022), <http://repositorio.ufc.br/handle/riufc/73074>.

⁹² Mateus Fornasier, Tiago Spinato, e Fernanda Ribeiro, "Cyberstalking: perseguição, privacidade e suas consequências no ambiente de rede", *Revista do Mestrado em Direito da UCB*, 2022, <https://portalrevistas.ucb.br/index.php/rvmd/article/view/12116>.



prestem a essencialismos, abrem espaço para interpretações sobre as distintas manifestações do domínio simbólico em contextos marcados por desigualdades estruturais.

Em 2023, a literatura acadêmica volta-se com mais rigor à análise das sequelas psicossociais geradas pelo monitoramento contínuo. Jair Ilídio da Silva⁹³ demonstra como o acesso íntimo da vítima, tanto a dispositivos quanto à sua estrutura emocional, permite ao agressor manipular mesmo após o rompimento da relação. Os efeitos são devastadores: desorganização da rotina, retração do convívio social, sensação de perseguição constante. Ferreira⁹⁴ retoma o caso de jovens para discutir o abuso digital no namoro, categorizando-o em quatro dimensões: controle, humilhação, ameaça e coerção sexual. Essa tipologia contribui para ampliar a compreensão da violência digital como um fenômeno multidimensional, que afeta não apenas a privacidade, mas também a autoestima, o desejo e a própria percepção de realidade das vítimas.

No mesmo ano, Mateus Marques e Vanessa Santos⁹⁵ observam que a ignorância da população sobre o caráter criminoso da conduta e o despreparo das autoridades constituem barreiras críticas à efetividade das denúncias. Assim, a violência se perpetua tanto por via simbólica quanto por omissão institucional.

Em 2024, o foco recai sobre a dificuldade de reconhecimento da violência por parte das vítimas. Jessica Rebouças⁹⁶ demonstra que muitas mulheres encaram o comportamento do *stalker* como "chato" ou incômodo, mas não como uma ameaça real, o que retarda a reação e agrava os efeitos do abuso, além de reforçar que as consequências da perseguição (como mudanças drásticas de rotina, paranoia constante e perda de vínculos sociais) permanecem mesmo após o encerramento da relação afetiva. Letícia Gonçalves⁹⁷ reforça que esse tipo de perseguição pode levar ao isolamento, ao medo constante de contato social e a sintomas severos de ansiedade. A vigilância íntima, nessa etapa, é reconhecida como uma forma de coerção indireta, capaz de disciplinar o comportamento da vítima mesmo na ausência do agressor.

⁹³ *Reflexões sobre Direito e Sociedade*.

⁹⁴ Ferreira, "Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence".

⁹⁵ Marques e Santos, *Crime de Stalking: Uma análise sobre a subjetividade do tipo penal*.

⁹⁶ Jéssica Rebouças, "A criminalização do stalking: abordagens legais para prevenir o feminicídio e combater a violência de gênero" (Monografia, Fortaleza, Universidade Federal do Ceará, 2024), <http://repositorio.ufc.br/handle/riufc/79017>.

⁹⁷ Gonçalves, "Efetividade da criminalização do cyberstalking (Lei 14.132/2021)".



Por fim, 2025 consagra a compreensão do *stalkerware* como tecnologia de permanência da violência. Fabio Rivelli⁹⁸ destaca que o monitoramento após o término da relação representa uma continuidade simbólica do domínio, operando silenciosamente por meio de acessos preexistentes aos dispositivos. O Instituto de Referência em Internet e Sociedade (IRIS)⁹⁹ complementa essa leitura ao mostrar que a dificuldade de reconstruir uma vida autônoma e segura é uma das consequências mais danosas da violência digital, pois aprisiona a vítima em um tempo relacional que já deveria ter se encerrado, mas continua a produzir efeitos concretos.

A investigação desse período de 6 anos nos leva a compreender que é evidente o contraste entre a densidade interpretativa da produção acadêmica e a superficialidade das respostas institucionais e empresariais. O setor privado, mesmo quando reconhece os riscos dos *stalkerwares*, como é o caso da Kaspersky¹⁰⁰, raramente vincula essas práticas à estrutura de gênero ou à lógica do patriarcado afetivo. As políticas de prevenção ainda estão baseadas em uma visão tecnocrática da segurança digital, sem enfrentar as condições simbólicas e relacionais que sustentam a vigilância como expressão de poder.

Comparativamente, observa-se que o período de 2020 e 2021 ainda estava fortemente voltado ao reconhecimento do fenômeno e às suas formas mais evidentes. A partir de 2022, no entanto, emerge uma virada interpretativa com maior sensibilidade aos atravessamentos de gênero, classe, geração e subjetividade, que permite conectar o uso do *stalkerware* às formas contemporâneas de controle e dominação nas relações afetivas. Nos anos seguintes, a literatura se dedica a mapear as sequelas emocionais e sociais do monitoramento, assim como os entraves institucionais à sua prevenção e repressão.

Essa evolução revela não apenas um amadurecimento teórico, mas também um aprofundamento da escuta sobre as vítimas e suas experiências, produzindo uma compreensão mais fina e situada dos efeitos da vigilância digital. Ao mesmo tempo, evidencia a necessidade de respostas que não se limitem à regulação técnica, mas que enfrentem as bases simbólicas e afetivas que sustentam essas práticas.

⁹⁸ Rivelli, “A violência digital e seus efeitos nas vítimas”.

⁹⁹ Dutra, Melo, e Gomes, “Vaza, Stalker! Proteção de Mulheres da Vigilância Digital”.

¹⁰⁰ “O Estado do Stalkerware em 2020”.



A investigação dessa literatura permite afirmar que a vigilância íntima mediada por tecnologia não é um desvio, mas uma expressão coerente de uma cultura que ainda tolera, e em certos contextos celebra, a dominação romântica. A desnaturalização dessas práticas requer não apenas dispositivos legais, mas também uma transformação das narrativas afetivas e das formas de educação para as relações. A vigilância que adoece, isola e destrói subjetividades não é menos violenta por ser invisível, ela é, na verdade, uma das mais eficazes expressões do controle patriarcal em tempos de hipermediatização da intimidade.

5. Estratégias de resistência e proteção das vítimas

Durante o período analisado, observa-se um progressivo adensamento das estratégias de resistência e proteção às vítimas. Mesmo que predominantemente centradas em ações individuais e no uso de soluções tecnológicas específicas, essas estratégias evoluíram para abordagens mais amplas e intersetoriais. Isso não significa que essa evolução tenha ocorrido de maneira estanque, com o abandono das conquistas anteriores e sem regressões ou que não tenham sido identificadas, nos primeiros anos examinados, medidas voltadas à conscientização e ao fortalecimento de redes de apoio. Ao contrário, trata-se de um processo complexo e não linear, no qual novas estratégias são gradualmente incorporadas conforme avançam tanto o desenvolvimento tecnológico quanto a compreensão mais ampla e contextualizada do problema.

No que se refere às medidas de proteção às vítimas, é possível observar que as publicações analisadas seguem padrões distintos, de acordo com o setor que as elaborou. Nesse sentido, o setor empresarial concentra-se em soluções tecnológicas de detecção e remoção de aplicativos de *stalkerware*. O governo, por sua vez, tende a focar na orientação às vítimas sobre como reconhecer o crime e em identificar possíveis sinais da presença de *stalkerware*. Já a sociedade civil e a academia propõem um olhar mais humanizado para a situação, propondo, a formação de redes de apoio multidisciplinares, a capacitação de profissionais envolvidos na investigação desses crimes, a construção de campanhas educativas, bem como a elaboração de políticas públicas para o combate do crime e o acolhimento das vítimas.



Em 2020, a Kaspersky, por exemplo, anunciou a criação da *TinyCheck*, uma ferramenta gratuita e de código aberto utilizada para detecção de *stalkerware* em celulares. A solução foi desenvolvida especificamente para uso por organizações e unidades policiais que trabalham com vítimas de violência doméstica¹⁰¹, sendo esta a única publicação identificada sobre o tema naquele ano.

No ano seguinte, a empresa continuou reforçando essas recomendações, apontando a importância de notar sinais de alerta como o consumo incomum de bateria do dispositivo, o uso elevado de dados móveis e a presença de permissões excessivas concedidas a aplicativos instalados, especialmente no que diz respeito ao acesso à geolocalização e a recursos de acessibilidade¹⁰². A Kaspersky, no entanto, advertiu sobre a possibilidade de que a instalação de antivírus em um dispositivo já comprometido pode notificar o agressor, agravando a situação da vítima¹⁰³.

De forma semelhante, em 2023, foram identificadas empresas como a Perallis Security que também reforçam orientações sobre a detecção e remoção de *stalkerware*. A empresa explica que aplicativos espiões geralmente são difíceis de identificar, pois costumam operar de forma oculta. Por isso, recomenda, em caso de suspeita, a verificação manual nas configurações do dispositivo para identificar aplicativos suspeitos instalados e, em caso de dúvida, a remoção imediata desses itens¹⁰⁴. A Perallis também orienta o uso de antivírus confiáveis, capazes de detectar e remover esses softwares automaticamente, e, como último recurso, sugere a restauração do aparelho aos padrões de fábrica¹⁰⁵.

No mesmo ano, também encontramos recomendações da Avast (2023), abordando tanto os sinais de possível infecção quanto formas de prevenção. Como formas de proteção, a empresa destacou a importância de impedir acessos físicos não autorizados ao dispositivo, utilizar autenticação de dois fatores e instalar programas antivírus confiáveis¹⁰⁶. Além disso, apresentou orientações sobre como remover manualmente o *stalkerware* de um telefone. No entanto, informou que a

¹⁰¹ Ibidem.

¹⁰² Glazova, "Stalkerware ainda é um problema em 2020".

¹⁰³ Ibidem.

¹⁰⁴ "Crescem casos de stalkerware no Brasil; saiba como identificá-los e removê-los".

¹⁰⁵ Ibidem.

¹⁰⁶ Yuge, "Stalkerware: apps espiões instalados na surdina crescem 358% no Brasil".



remoção do *software* espião pode ser perigosa, pois pode acarretar riscos à segurança física da vítima¹⁰⁷.

Nesse aspecto, é importante observar que a remoção do aplicativo espião, diferente do que sugere a Perallis, pode trazer consequências negativas para as vítimas, algo que já tinha sido alertado em publicações anteriores. Isso porque, em casos em que o agressor percebe a perda de controle sobre o dispositivo da vítima, pode ocorrer a escalada da violência. A própria Kaspersky (2023) orienta que a remoção do aplicativo só deve ser feita com cautela, após uma avaliação do risco para a vítima, uma vez que podem ser alvos de um ciclo maior de violência¹⁰⁸.

Além disso, a remoção do *stalkerware* pode destruir provas importantes para investigações futuras e possível responsabilização do abusador. Nesse cenário, tem-se recomendado entrar primeiramente em contato com as autoridades competentes e parar de usar o dispositivo infectado até que o *software* espião seja removido¹⁰⁹. Dessa forma, evita-se que provas sejam perdidas e, principalmente, que a vítima fique exposta a uma possível retaliação por parte do abusador.

No âmbito governamental, foram encontradas poucas publicações sobre o tema. Um exemplo é a cartilha divulgada em 2023 pela Secretaria de Estado de Desenvolvimento Social do Governo de Minas Gerais, que apresenta diretrizes técnicas e operacionais destinadas a profissionais dos Centros de Referência de Atendimento às Mulheres em Situação de Violência. O objetivo é qualificar o acolhimento e o atendimento prestados a mulheres em contextos de violência doméstica e intrafamiliar¹¹⁰.

No entanto, o material limita-se a reconhecer os tipos penais comumente aplicáveis nesses casos e a oferecer orientações básicas às vítimas, como as já mencionadas acima. Mesmo que importantes, as considerações trazidas pela cartilha ainda demonstram um foco predominante em situações de violência doméstica física e ações individuais, em detrimento da abordagem mais aprofundada e coletiva da violência online.

Almir Junior et al., mencionando Townsend, ressaltam que apesar da adoção alternativas que impeçam o acesso físico dos dispositivos aos agressores ou o uso

¹⁰⁷ Ibidem.

¹⁰⁸ “El estado del stalkerware en 2022”.

¹⁰⁹ Ibidem.

¹¹⁰ “Referências técnicas para atuação profissional nos Centros de Referência de Atendimento às Mulheres em Situação de Violência”.



de soluções como antivírus e até mesmo a busca por ajuda em delegacias, a situação é mais complexa do que parece¹¹¹.

Isso porque a vigilância pode ocorrer por outros meios além do celular e do computador, como por meio de câmeras instaladas na residência ou, ainda, por formas menos óbvias, a exemplo de mecanismos de controle parental¹¹². Soma-se a isso o fato de que, muitas vezes, a vítima está inserida em um relacionamento abusivo, caracterizado por práticas de controle e violência exercidas por um parceiro que geralmente convive com ela. Nessas circunstâncias, a dependência financeira e emocional também pode dificultar e até impedir a busca por ajuda especializada, até porque a comunicação pode estar sendo monitorada, dificultando o acesso a redes de apoio e canais de denúncia.

Em 2021, destacou-se no levantamento acadêmico o uso de tecnologia no combate e na prevenção à violência de gênero. O artigo de Gisella Ferreira, em que ela descreve a violência entre parceiros íntimos (intimate partner violence - IPV) entre jovens do sul global, é um deles. Utilizando uma metodologia de pesquisa qualitativa e exploratória, ela realizou entrevistas com 14 defensores e advogados brasileiros e 5 australianos e concluiu que a tecnologia pode ser uma aliada para ajudar jovens mulheres a falar sobre o relacionamento abusivo que vivem, destacando que o uso de inteligência artificial, em forma de chatbots¹¹³. Ela ressalta, entretanto, que é importante verificar as políticas de privacidade desses aplicativos, para que eles não coletem dados das usuárias e possam expô-las, considerando a sensibilidade das situações em que vivem.

Ainda nesse sentido, a autora destaca que participantes brasileiros da pesquisa explicitaram como estão engajando os jovens a produzir filmes curtos sobre violência contra mulheres e meninas e disponibilizando-os no Youtube para conhecimento geral. Os entrevistados destacaram a qualidade do conteúdo dos vídeos, concluindo que a iniciativa é, portanto, bem sucedida, demonstrando mais uma vez o benefício do uso da tecnologia neste âmbito.

Autores como Pâmela Pedruzzi e Agnaldo Garcia também destacam o papel da Internet em contextos de violência de gênero. Segundo os autores, a Internet tem possibilitado o compartilhamento de experiências, a construção de redes de apoio e

¹¹¹ Junior et al., *Clínica Criminal a Tutela das Vulnerabilidades*.

¹¹² Ibidem.

¹¹³ Ferreira, "Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence".



a criação de um espaço no qual as vítimas podem se expressar e desabafar¹¹⁴. Além disso, os autores ressaltam como aspecto positivo o uso da Internet e das redes sociais na produção de provas, destacando que recursos como o *backup* permitem preservar mensagens trocadas entre vítimas e agressores, o que pode ser fundamental, por exemplo, para fundamentar pedidos de medidas protetivas com base na Lei Maria da Penha¹¹⁵.

Mirela Silva e Daniela Oliveira também explicam como a própria tecnologia pode ser usada para proteger a privacidade e a localização das vítimas, criando uma espécie de "capa de invisibilidade" a partir de recursos como a adição de ruídos aleatórios à comunicação real e a implementação de recursos para mensagens instantâneas em aplicativos populares¹¹⁶. Roberta Paiva também reforça que a tecnologia pode contribuir para a prevenção e combate da violência contra a mulher, através de iniciativas que acolhem, informam e ampliam o acesso à ajuda. Entretanto, ela ressalta, que há um risco de monitoramento dos dispositivos por seus parceiros, inclusive por meio de *stalkerware*, razão pela qual as ferramentas devem garantir privacidade e segurança¹¹⁷.

Este ponto é primordial: ferramentas utilizadas para proteção de meninas e mulheres contra violência de gênero devem manter uma coleta mínima de dados e, de preferência, não sensíveis, a fim de realmente ajudá-las e não causar exposição desnecessária, que pode inclusive causar sua revitimização. E, mais ainda, o uso deve levar em consideração o contexto social em que vivem, de forma a não ser mais uma possibilidade de violência por seus parceiros, através de aplicativos de monitoramento, por exemplo, pois, nestes casos, a violência pode inclusive escalar e se tornar mais grave.

Como já observado, o *stalkerware* é desenvolvido intencionalmente para não ser visto pela vítima, de modo que muitas vezes é difícil de identificar a presença de um software espião¹¹⁸. Isso talvez explique porque grande parte das publicações encontradas fazem recomendações parecidas entre si no que diz respeito a como se proteger desses aplicativos espiões. As mesmas recomendações se repetem nas publicações do ano de 2022, que também traz, no trabalho de Almir Junior et

¹¹⁴ Pedruzzi e Garcia, "Violência contra a mulher por parceiro íntimo: contextos online e offline".

¹¹⁵ Ibidem.

¹¹⁶ Silva e Oliveira, "Brazilian Favela Women: How Your Standard Solutions for Technology Abuse Might Actually Harm Them".

¹¹⁷ Paiva, "Inovações digitais no combate à violência contra a mulher".

¹¹⁸ Vasconcelos, "A criminalidade na sociedade da era digital".



al., a mesma conclusão anteriormente mencionada sobre o uso da tecnologia como aliada no combate da violência de gênero, incluindo vários exemplos de sucesso desta natureza, tanto do Brasil quanto de outros países¹¹⁹.

Os autores destacam neste âmbito o sistema do Reino Unido chamado “Saia Agora”, presente no *National Domestic Abuse Helpline*, que impossibilita que o espião saiba qual site o usuário está acessando pelo histórico. O que fica registrado, segundo os autores, é um histórico de acesso com letras e números aleatórios, e o link apresentado leva à página inicial do Google, sem deixar rastros¹²⁰.

Nesse mesmo ano, Lucélia Afonso et al., citando Emezue, destacaram algumas formas de mitigar a vigilância e o abuso digital online. A adoção de medidas de segurança e design mais robustas, como autenticação secreta; bloqueio de aplicativos; e protocolos de verificação, associadas a ferramentas voltadas ao apoio às vítimas de violência e que possibilitem distinguir agressores de vítimas a partir da análise comportamental, o que inclui métricas a partir do pressionamento de teclas e pistas contextuais, são algumas delas¹²¹. Todavia, é preciso, conforme exposto, ter cautela no desenvolvimento de tecnologias que envolvem a coleta de dados para não vulnerabilizar ainda mais essas vítimas.

A partir de 2023, observa-se uma maior complexificação nas estratégias propostas para o enfrentamento da violência de gênero digital, com a incorporação de medidas mais estruturais, especialmente (mas não só) no meio acadêmico e pela sociedade civil. Ana Carolyne Gonçalves, por exemplo, destaca que a aprovação da lei de *stalking* representou um marco significativo para as vítimas de perseguição, ao reconhecer a gravidade da prática e prever medidas protetivas¹²².

Por outro lado, apontando André Carvalho deficiências na norma quanto à efetiva proteção das vítimas, ressalta a importância de uma transformação cultural profunda para enfrentar o problema. Segundo o autor, é fundamental investir na formação de profissionais como agentes de polícia e membros do Judiciário envolvidos na investigação e no julgamento desses casos, assegurando que a segurança da vítima seja sempre prioridade¹²³.

¹¹⁹ Junior et al., *Clínica Criminal a Tutela das Vulnerabilidades*.

¹²⁰ Ibidem.

¹²¹ Francisco José Pinto, Cybelle Linard, e Tereza Doralucia Ponte, orgs., *Saúde da população em tempos complexos: olhares diversos*, 1º ed (Ampilla Editora, 2022), <https://doi.org/10.51859/ampilla.spt853.1122-0>.

¹²² Gonçalves, “Crime de perseguição (stalking) nova Lei nº 14.132, de 31 de março de 2021”.

¹²³ Carvalho, “A Responsabilidade Civil em casos de Stalking e Cyberstalking”.



Esse alerta torna-se ainda mais relevante, pois muitas vítimas, além de enfrentarem a violência no âmbito doméstico e familiar, também são expostas à violência institucional ao buscarem ajuda. Isso ocorre porque delegacias e o próprio sistema de justiça ainda operam dentro de uma estrutura social marcada pelo machismo, pelo patriarcado e por outras formas de opressão, como o racismo e a LGBTfobia. Nesse cenário, é comum que a vítima seja revitimizada ou até mesmo responsabilizada pela violência sofrida, especialmente quando se trata de mulheres. Nesse contexto, a Kaspersky, como uma exceção no setor privado, faz um alerta pertinente, afirmando que além da resposta mais evidente que seria trazida a partir da regulação, é imprescindível investir em capacitação e conscientização sobre a violência de gênero digital de forma ampla e contínua, promovendo a educação sobre o tema desde as etapas iniciais da formação social¹²⁴.

Em 2024, também é possível identificar referências à importância do investimento em políticas públicas integradas e multissetoriais, com estratégias de intervenção eficazes que garantam às vítimas uma rede de apoio e segurança para que possam buscar ajuda¹²⁵. Além do suporte jurídico, foram mapeados autores que ressaltam a necessidade de medidas de acompanhamento psicológico, fundamentais para que as vítimas consigam superar os traumas decorrentes da perseguição e se recuperem emocionalmente¹²⁶.

Já em 2025, destaca-se a criação do projeto “Vaza Stalker!”, voltado ao desenvolvimento de ações e estratégias eficazes no enfrentamento da violência de gênero digital, a partir da produção de materiais educativos e da mobilização conjunta com outras organizações¹²⁷. Por fim, merece destaque o trabalho da atriz Rose Leonel, que, após ter sido vítima de violência de gênero digital, fundou a ONG Marias da Internet, uma associação dedicada a oferecer suporte jurídico, psicológico e técnico a vítimas da disseminação não consensual de material íntimo¹²⁸.

Diante de todo o exposto, é fundamental que o combate à violência de gênero facilitada pelo uso de ferramentas de *stalkerware* não se limite à criminalização individual da conduta ou que se traduza simplesmente em mais solucionismo tecnológico. Ao contrário disso, é importante também que enfrente e

¹²⁴ “El estado del stalkerware en 2022”.

¹²⁵ Rebouças, “A criminalização do stalking”.

¹²⁶ Silva, Silva, e Almeida, “Stalking e cyberstalking contra a mulher”.

¹²⁷ Dutra, Melo, e Gomes, “Vaza, Stalker! Proteção de Mulheres da Vigilância Digital”.

¹²⁸ Rivelli, “A violência digital e seus efeitos nas vítimas”.



responsabilize o setor que produz esse tipo de *software*, além de incluir políticas de formação continuada, campanhas de conscientização em escolas e universidades, bem como a transformação das instituições públicas, com atenção especial às múltiplas camadas de violência e opressão que atravessam a vida dessas vítimas, visando uma mudança estrutural da sociedade.

6. Abordagens interseccionais

Entre os anos de 2020 e 2025, a discussão sobre o uso de *stalkerware* e aplicativos de uso duplo no Brasil passou por uma significativa ampliação conceitual e empírica. Entretanto, mesmo diante da crescente atenção institucional, acadêmica e midiática ao fenômeno, é possível observar que as abordagens voltadas ao enfrentamento dessa violência muitas vezes carecem de uma perspectiva interseccional robusta e aprofundada que vá além da questão da violência contra mulheres cis de uma forma geral. A revisão aqui apresentada tem como objetivo destacar a urgência de incorporar essa complexidade nos estudos e práticas voltadas à contenção da violência de gênero mediada por tecnologias.

Abordagens voltadas ao enfrentamento do uso de *spyware* e aplicativos de uso duplo como facilitadores de violência de gênero devem considerar questões interseccionais. É imperativo que essa discussão não apenas reconheça, mas problematize como opressões estruturais, como por exemplo de gênero, raça, classe e sexualidade, se entrelaçam de maneira complexa e produzem impactos desproporcionais sobre grupos já marginalizados.

O aspecto de gênero é particularmente crítico nesse contexto. Em 2021, o estudo de Gisella Ferreira¹²⁹ mostra que os rígidos estereótipos de masculinidade e feminilidade continuam sendo reproduzidos como norma cultural: o controle exercido por homens é frequentemente justificado como uma expressão aceitável, ou até mesmo “natural”, de ciúmes, enquanto a submissão das mulheres é romantizada. De acordo com a autora, esses padrões arcaicos não apenas sustentam o controle coercitivo digital (CCD), mas são amplificados por uma mídia que reforça essas dinâmicas, retratando comportamentos abusivos como demonstrações de afeto ou zelo amoroso¹³⁰. Trata-se de um ciclo de normalização

¹²⁹ Ferreira, “Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence”.

¹³⁰ Ibidem.



que mina qualquer tentativa de responsabilização e obscurece os limites entre o cuidado e o abuso.

A vigilância digital, nesse contexto, emerge como uma extensão moderna do poder patriarcal: silenciosa, eficiente e socialmente tolerada. O dado alarmante divulgado pela Kaspersky em 2021¹³¹, de que aproximadamente 80% das vítimas de espionagem digital são mulheres, não pode ser lido como mera estatística: trata-se de um sintoma de um sistema que continua a instrumentalizar a tecnologia como ferramenta de opressão de gênero. Essa desproporcionalidade escancara a seletividade da violência digital e denuncia a cumplicidade de uma cultura que naturaliza o acesso não consentido à vida íntima de mulheres como se fosse direito legítimo dos homens. O problema, portanto, não está apenas na tecnologia, mas em como ela é mobilizada dentro de uma lógica de gênero desigual e violenta, amplamente tolerada tanto no discurso midiático quanto na negligência institucional.

A relação entre o uso de ferramentas de monitoramento e a racialização da violência de gênero revela camadas profundas de desigualdade que não podem ser ignoradas em análises sérias sobre o tema. Conforme apontado por participantes no estudo de Ferreira¹³², fatores como classe social e nível educacional limitam o acesso a estratégias de proteção digital, criando barreiras adicionais para mulheres negras e periféricas. Entretanto, as desigualdades raciais intensificam ainda mais essa vulnerabilidade. O racismo estrutural expõe mulheres negras e indígenas a múltiplas formas de violência, frequentemente invisibilizadas pelas instituições e pelas políticas públicas.

O acesso precário a informações sobre segurança digital, a menor familiaridade com os recursos técnicos de proteção e a histórica negligência estatal diante da violência contra mulheres negras e indígenas resultam em uma desigualdade de risco. No Brasil mulheres negras enfrentam não apenas o controle de parceiros, mas também o silenciamento institucional que normaliza a vigilância como parte de uma estrutura colonial de dominação. Portanto, discutir a violência facilitada por tecnologias sem uma perspectiva crítica de raça e colonialismo é perpetuar a falsa ideia de que as tecnologias operam de forma neutra, quando, na verdade, reproduzem e aprofundam desigualdades históricas.

¹³¹ Glazova, “Stalkerware ainda é um problema em 2020”.

¹³² Ferreira, “Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence”.



Embora o Brasil ocupe a segunda posição no ranking global de uso de *spyware*, essa realidade não afeta todas as mulheres da mesma maneira. As vítimas desse tipo de violência enfrentam ameaças qualitativamente diferentes e ignorar essas nuances é perpetuar a invisibilização de parcelas da população já historicamente negligenciadas. Como destaca Mirela Silva¹³³, mulheres em situação de vulnerabilidade socioeconômica frequentemente hesitam em recorrer às autoridades em casos de violência doméstica. Essa hesitação, longe de ser irracional, é fruto de uma desconfiança estrutural em relação a instituições estatais que muitas vezes se mostram inoperantes, coniventes ou mesmo cúmplices em contextos dominados por redes de narcotráfico, frequentemente entrelaçadas com casos de violência por parceiro íntimo (VPI) de acordo com a autora.

No que tange à dimensão etária, a situação é igualmente alarmante. A juventude, especialmente no Sul Global, é negligenciada nas pesquisas sobre o uso de tecnologias como ferramentas de controle coercitivo digital (CCD)¹³⁴. Embora essa etapa da vida seja marcada pelas primeiras experiências em relacionamentos íntimos, experiências que moldam expectativas e padrões afetivos futuros, o debate sobre CCD entre jovens ainda é incipiente. Ainda em 2021, Ferreira evidencia essa lacuna ao apontar que a produção acadêmica no Brasil tem se limitado a mapear a prevalência da VPI entre jovens, sem explorar com profundidade as formas tecnológicas de coerção e vigilância que marcam esses relacionamentos¹³⁵. Esse apagamento é sintomático de uma visão reducionista que desconsidera abordagens interseccionais.

Em seu estudo de 2021, Ferreira revela que jovens no Brasil tendem a normalizar práticas invasivas como o monitoramento, rastreamento e perseguição por meio de dispositivos móveis¹³⁶. O acesso não autorizado aos dispositivos e contas de parceiros, por meio de ferramentas como WhatsApp Web e “aplicativos ocultos de espionagem”, que parece ser a nomenclatura utilizada pela autora para a denominação de *stalkerware*, é tratado como algo corriqueiro. Essa banalização da vigilância íntima evidencia não apenas um déficit educacional sobre privacidade e consentimento, mas também um reflexo direto de dinâmicas de poder

¹³³ Silva e Oliveira, “Brazilian Favela Women: How Your Standard Solutions for Technology Abuse Might Actually Harm Them”.

¹³⁴ Ferreira, “Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence”.

¹³⁵ Ibidem.

¹³⁶ Ibidem.



profundamente enraizadas nas relações de gênero e afetivas da sociedade brasileira.

A correlação entre gênero e práticas de vigilância em relacionamentos abusivos não é apenas retomada, mas duramente criticada por Almir Junior et al.¹³⁷ e, mais recentemente, por Evelin da Silva, Gabrielle Silva e Andreia Almeida¹³⁸ e pelo estudo do Instituto de Referência em Internet e Sociedade (IRIS)¹³⁹. Esses estudos evidenciam que tais dinâmicas de controle não são desvios comportamentais isolados, mas estão profundamente enraizadas em estruturas culturais e sociais de dominação, como o machismo e o patriarcado. A persistência desses sistemas garante que, mesmo em contextos de crescente digitalização da vida cotidiana, o controle sobre os corpos e a intimidade das mulheres se reinvente e perpetue por meio de tecnologias.

Apesar de não desenvolver esse importante argumento de forma mais aprofundada, Ferreira também chama atenção para a tendência de se tratar a violência por parceiro íntimo (VPI) como um fenômeno exclusivamente heterossexual¹⁴⁰. A homogeneização das experiências de violência de gênero contribui para um apagamento sistemático das formas diversas que o controle e a violência podem assumir. Mulheres lésbicas, bissexuais e *queer* também lidam com formas específicas de violência que escapam à lógica heteronormativa e, por isso, muitas vezes não são reconhecidas nem adequadamente tratadas pelas políticas públicas desenvolvidas.

Graves lacunas também foram identificadas em relação a produções científicas que adentrem a violência facilitada por tecnologias no Brasil no caso de mulheres trans. A interseção entre transfobia estrutural, marginalização social e precariedade econômica impõe a essas mulheres uma série de barreiras adicionais que não apenas agravam sua exposição à violência, mas também limitam significativamente seu acesso a mecanismos de proteção e justiça. Essa realidade se torna ainda mais preocupante diante da ausência de estudos brasileiros que abordem o uso de tecnologias específicas — como *spyware* ou aplicativos de uso duplo — nos contextos de relacionamentos abusivos envolvendo mulheres trans. A escassez de pesquisas locais contrasta com a literatura internacional, que já

¹³⁷ Junior et al., *Clínica Criminal a Tutela das Vulnerabilidades*.

¹³⁸ Silva, Silva, e Almeida, “Stalking e cyberstalking contra a mulher”.

¹³⁹ Dutra, Melo, e Gomes, “Vaza, Stalker! Proteção de Mulheres da Vigilância Digital”.

¹⁴⁰ Ferreira, “Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence”.



reconhece o impacto desproporcional da VPI nesse grupo. Trabalhos conduzidos principalmente na América do Norte e Europa demonstram que mulheres trans frequentemente enfrentam múltiplas formas de controle e vigilância por parte de parceiros, incluindo a manipulação de tecnologias digitais como forma de impor isolamento, medo e dependência.¹⁴¹

O resultado são lacunas de proteção e invisibilidade institucional. Como forma de endereçar essas questões de forma contundente, uma abordagem interseccional se faz essencial. Isso significa incluir, além do gênero, marcadores como idade, classe, raça, etnia e os legados coloniais que ainda estruturam as relações sociais e institucionais. Essa perspectiva é indispensável para desmascarar a falsa universalidade das experiências de violência e evidenciar como determinadas populações são sistematicamente mais expostas e menos protegidas.

Em relação a questões territoriais, não foi possível identificar estudos voltados ao uso de *stalkerware* em zonas rurais e regiões remotas brasileiras. Entretanto, Ferreira¹⁴² observa que a eficácia de aplicativos que conectam usuários a serviços policiais, por exemplo, é severamente limitada pela infraestrutura desigual de acesso à internet e à telefonia móvel no Brasil. Essa limitação se acentua em regiões remotas e rurais, onde a exclusão digital é uma realidade persistente. Tal constatação evidencia a fragilidade de soluções tecnológicas - e legais - que desconsideram as disparidades territoriais e socioeconômicas do país, reproduzindo uma lógica de exclusão que privilegia contextos urbanos e conectados, ao mesmo tempo em que marginaliza populações rurais já vulnerabilizadas. A dependência de tecnologias digitais sem a devida atenção à infraestrutura básica revela uma abordagem tecnocrática e elitista, que ignora os princípios de equidade e acessibilidade necessários para o enfrentamento efetivo da violência de gênero facilitada por tecnologias.

¹⁴¹ Suzie Dunn, Tracy Vaillancourt e Heather Brittain, “Special Report: Supporting Safer Digital Spaces” (Centre for International Governance Innovation, 2023).

¹⁴² Ferreira, “Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence”.



Conclusão

Os resultados da pesquisa evidenciam que, embora o debate sobre o uso de *stalkerware* e tecnologias de uso duplo como facilitadores de violência de gênero tenha ganhado relevância no Brasil nos últimos anos, ainda há importantes lacunas na produção científica e na formulação de respostas institucionais. A violência de gênero mediada por tecnologias continua sendo subestimada, tanto em sua complexidade técnica quanto em suas implicações sociais e interseccionais.

A partir da análise realizada, torna-se claro que a compreensão e o enfrentamento dessa forma de violência exigem uma abordagem multidisciplinar, que articule saberes jurídicos, tecnológicos, sociais e de gênero. Também se destaca a necessidade urgente de incorporar uma perspectiva interseccional mais robusta às pesquisas e às políticas públicas, reconhecendo as especificidades de grupos como mulheres trans, lésbicas, bissexuais, negras, indígenas e outras populações sistematicamente marginalizadas, cujas vivências seguem invisibilizadas nas análises predominantes.

O projeto *Expondo stalker(ware)* contribui significativamente para esse avanço ao mapear os caminhos já percorridos pela produção científica brasileira e ao apontar direções estratégicas para futuras investigações e ações. Ao promover uma compreensão mais aprofundada sobre a violência de gênero facilitada por tecnologias, a iniciativa fortalece os esforços para a construção de ambientes digitais mais seguros, igualitários e atentos à diversidade das experiências de violência.



Apêndice I

Google Acadêmico							
Foco Temático	Termo de Pesquisa Abreviado	2020	2021	2022	2023	2024	2025
Violência de gênero com spywares	Spyware	3	6	11	11	9	3
	Software Espião	0	1	3	0	2	1
	Aplicativo Espião	0	3	1	1	1	3
Stalkerware no Brasil	Stalkerware	0	3	6	3	2	0
	Spouseware	0	0	1	0	0	0
Cyberstalking e Spywares no Brasil	Cyberstalking + Spyware	3	6	9	7	4	1
	Perseguição Online + Spyware	0	1	1	0	0	1
	Perseguição Digital + Spyware	0	1	0	0	1	1
	Perseguição Cibernética + Spyware	0	1	1	1	0	0
Cyberstalking e Violência de Gênero no Brasil	Cyberstalking + Violência Gênero	32	46	65	82	69	12
	Perseguição Online + Violência Gênero	3	5	6	6	7	2
	Perseguição Digital + Violência Gênero	1	1	2	1	3	3
	Perseguição Cibernética + Violência Gênero	0	3	2	3	3	0
Violência de Gênero com Aplicativos de Uso Duplo	Aplicativos de Uso Duplo	0	0	0	0	0	0
	Aplicações de Uso Dual	0	0	0	0	0	0
	Aplicativos de Monitoramento	0	0	6	1	6	5
TOTAL		42	77	114	116	107	32

Google Web							
Foco Temático	Termo de Pesquisa Abreviado	2020	2021	2022	2023	2024	2025
Violência de gênero com spywares	Spyware	23	49	54	67	111	90
	Software Espião	7	7	12	15	18	18
	Aplicativo Espião	8	9	14	17	23	16
Stalkerware no Brasil	Stalkerware	51	78	74	69	72	100
	Spouseware	4	6	9	6	5	7
Cyberstalking e Spywares no Brasil	Cyberstalking + Spyware	10	20	28	20	31	23
	Perseguição Online + Spyware	2	3	1	3	9	3
	Perseguição Digital + Spyware	1	3	3	0	2	2
	Perseguição Cibernética + Spyware	0	0	1	3	2	20



Google Web							
Foco Temático	Termo de Pesquisa Abreviado	2020	2021	2022	2023	2024	2025
Cyberstalking e Violência de Gênero no Brasil	Cyberstalking + Violência Gênero	26	81	76	70	138	111
	Perseguição Online + Violência Gênero	10	16	10	20	24	39
	Perseguição Digital + Violência Gênero	6	15	7	6	20	61
	Perseguição Cibernética + Violência Gênero	1	4	0	3	3	6
Violência de Gênero com Aplicativos de Uso Duplo	Aplicativos de Uso Duplo	0	0	0	0	0	5
	Aplicações de Uso Dual	0	0	0	0	0	0
	Aplicativos de Monitoramento	0	6	8	9	14	22
TOTAL		149	297	297	308	472	523

Termo Abreviado	Expressão Completa Utilizada
Spyware	("spyware" OR "spywares") AND ("violência contra mulheres" OR "violência contra a mulher" OR "violência de gênero" OR "violência doméstica" OR "violência por parceiro íntimo" OR "relacionamento abusivo" OR "controle coercitivo" OR "abuso digital" OR "abuso psicológico") AND "Brasil"
Software Espião	"software espião" AND ("violência contra mulheres" OR "violência contra a mulher" OR "violência de gênero" OR "violência doméstica" OR "violência por parceiro íntimo" OR "relacionamento abusivo" OR "controle coercitivo" OR "abuso digital" OR "abuso psicológico") AND "Brasil"
Aplicativo Espião	("aplicativo espião" OR "aplicativos espiões") AND ("violência contra mulheres" OR "violência contra a mulher" OR "violência de gênero" OR "violência doméstica" OR "violência por parceiro íntimo" OR "relacionamento abusivo" OR "controle coercitivo" OR "abuso digital" OR "abuso psicológico") AND "Brasil"
Stalkerware	"stalkerware" AND "Brasil"
Spouseware	"spouseware" AND "Brasil"
Cyberstalking + Spyware	("cyberstalking" OR "ciberstalking") AND ("spyware" OR "spywares" OR "software espião" OR "aplicativo espião" OR "aplicativos espiões") AND "Brasil"
Perseguição Online + Spyware	"perseguição online" AND ("spyware" OR "spywares" OR "software espião" OR "aplicativo espião" OR "aplicativos espiões") AND "Brasil"
Perseguição Digital + Spyware	"perseguição digital" AND ("spyware" OR "spywares" OR "software espião" OR "aplicativo espião" OR "aplicativos espiões") AND "Brasil"
Perseguição Cibernética + Spyware	"perseguição cibernética" AND ("spyware" OR "spywares" OR "software espião" OR "aplicativo espião" OR "aplicativos espiões") AND "Brasil"



Termo Abreviado	Expressão Completa Utilizada
Cyberstalking + Violência Gênero	("cyberstalking" OR "ciberstalking") AND ("violência contra mulheres" OR "violência contra a mulher" OR "violência de gênero" OR "violência doméstica" OR "violência por parceiro íntimo" OR "relacionamento abusivo" OR "controle coercitivo" OR "abuso digital" OR "abuso psicológico") AND "Brasil"
Perseguição Online + Violência Gênero	"perseguição online" AND ("violência contra mulheres" OR "violência contra a mulher" OR "violência de gênero" OR "violência doméstica" OR "violência por parceiro íntimo" OR "relacionamento abusivo" OR "controle coercitivo" OR "abuso digital" OR "abuso psicológico") AND "Brasil"
Perseguição Digital + Violência Gênero	"perseguição digital" AND ("violência contra mulheres" OR "violência contra a mulher" OR "violência de gênero" OR "violência doméstica" OR "violência por parceiro íntimo" OR "relacionamento abusivo" OR "controle coercitivo" OR "abuso digital" OR "abuso psicológico") AND "Brasil"
Perseguição Cibernética + Violência Gênero	"perseguição cibernética" AND ("violência contra mulheres" OR "violência contra a mulher" OR "violência de gênero" OR "violência doméstica" OR "violência por parceiro íntimo" OR "relacionamento abusivo" OR "controle coercitivo" OR "abuso digital" OR "abuso psicológico") AND "Brasil"
Aplicativos de Uso Duplo	"aplicativos de uso duplo" AND ("violência contra mulheres" OR "violência contra a mulher" OR "violência de gênero" OR "violência doméstica" OR "violência por parceiro íntimo" OR "relacionamento abusivo" OR "controle coercitivo" OR "abuso digital" OR "abuso psicológico") AND "Brasil"
Aplicações de Uso Dual	"aplicações de uso dual" AND ("violência contra mulheres" OR "violência contra a mulher" OR "violência de gênero" OR "violência doméstica" OR "violência por parceiro íntimo" OR "relacionamento abusivo" OR "controle coercitivo" OR "abuso digital" OR "abuso psicológico") AND "Brasil"
Aplicativos de Monitoramento	"aplicativos de monitoramento" AND ("violência contra mulheres" OR "violência contra a mulher" OR "violência de gênero" OR "violência doméstica" OR "violência por parceiro íntimo" OR "relacionamento abusivo" OR "controle coercitivo" OR "abuso digital" OR "abuso psicológico") AND "Brasil"



Apêndice II

2020

Título	Autoria	Setor	Tipo	Disciplinas
CYBERSTALKING: A necessidade de tipificação no Direito Penal Brasileiro	Carlos Henrique de Espindola Mota	Academia	Trabalho de conclusão	Direito
A conduta do stalking sob o paradigma do ordenamento jurídico brasileiro	Amanda Vasconcelos Arruda e Prof. Ms. Ilton Vieira Leão	Academia	Artigo científico	Direito
STALKING E VIOLÊNCIA CONTRA A MULHER: a necessidade de mecanismos jurídicos de proteção frente a um contexto de impunidade	Adrielly Pinto dos Reis, Bruna Velloso Parente e Margareth Vetis Zaganelli	Academia	Artigo científico	Direito
A mulher, a violência e a internet	Joana Paula Lima de Castro	Academia	Trabalho de conclusão	Direito
Como evitar que agressores tenham acesso ao seu celular	MariaLab	Terceiro Setor	Tutorial	Segurança da informação
Relatório da Avast	Avast	Setor empresarial	Relatório	Segurança da informação
Mapa do acolhimento #Quarentena sem violência	Mapa do acolhimento, Maria Lab e FrontLine Defenders	Terceiro Setor	Cartilha	Segurança da informação
O estado do Stalkerware em 2020	Kaspersky	Setor empresarial	Relatório	Segurança da informação
Referências técnicas	Governo do Estado	Governament	Nota Técnica	Serviço



para atuação profissional nos Centros de Referência de Atendimento às Mulheres em Situação de Violência Caderno 1 - Organização cotidiana do trabalho	de Minas Gerais, por meio da Secretaria de Estado de Desenvolvimento Social	al		Social
--	---	----	--	--------

2021

Título	Autoria	Setor	Tipo	Disciplinas
Brazilian Favela Women: How Your Standard Solutions for Technology Abuse Might Actually Harm Them	Mirela Silva, Daniela Oliveira	Academia	Artigo científico	Sociologia
Inovações digitais no combate à violência contra a mulher: iniciativas durante a pandemia da Covid-19 no Brasil	Roberta Salomone de Paiva	Academia	Trabalho de conclusão	Relações Internacionais
O DIREITO A PRIVACIDADE DA MULHER NO MUNDO DIGITAL, E A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) COMO INSTRUMENTO DE ENFRENTAMENTO À VIOLÊNCIA DE GÊNERO NO PAÍS	JOSÉ LUIZ MAFRA JÚNIOR	Academia	Trabalho de conclusão	Direito
CYBERSTALKING:	EDILAYNE SILVA DE	Academia	Trabalho	Direito



UMA ANÁLISE DO CRIME DE PERSEGUIÇÃO CONTRA MULHERES NA INTERNET, SOB O OLHAR DO ART. 147 – A, CP INSERIDO PELA NOVA LEI 14.132/2021	BRITO		de conclusão	
STALKING OU ASSÉDIO POR INTRUSÃO: Tipificação penal como forma de prevenção à violência de gênero	Ester Santos Silveira	Academia	Trabalho de conclusão	Direito
Violência contra a mulher por parceiro íntimo: contextos online e offline	Pâmela Fardin Pedruzzi e Agnaldo Garcia	Academia	Artigo científico	Psicologia
Technology as Both a Facilitator of and Response to Youth Intimate Partner Violence: Perspectives from Advocates in the Global-South	Gisella Lopes Gomes Pinto Ferreira	Academia	Artigo científico	Direito
Stalkerware ainda é um problema em 2020	Kaspersky - Julia Glazova	Setor empresarial	Relatório	Segurança da informação
SEGURANÇA DIGITAL: uma análise de gestão de risco em empresas brasileiras	NIC.br	Sociedade Civil	Relatório	Governança
Violência cibernética contra as mulheres	Poder Judiciário do Estado do Rio de Janeiro - TJRJ	Governamental	Relatório	Direito



2022

Título	Autoria	Setor	Tipo	Disciplinas
CLÍNICA CRIMINAL A TUTELA DAS VULNERABILIDADES VOL. 3	Almir Junior, Ana Carolina Hass, Ana Julia Tamiozo, Heloísa Meneguette Silveira, Luciana Caetano da Silva, Manuel Arnança, Maria Carolina de Liberali de França, Vitoria Gualberto Vagetti, Vitória Luiza Rossi	Academia	Livro	Direto
A CRIMINALIDADE NA SOCIEDADE DA ERA DIGITAL: uma reflexão acerca das presenças digitais e o cyberstalking	Líliam dos Santos Vasconcelos	Academia	Trabalho de conclusão	Direto
Digitalización de las mujeres en América Latina y el Caribe: Acción urgente para una recuperación transformadora y con igualdad	Iliana Vaca Trigo, María Elena Valenzuela	Academia	Relatório	Ciências Sociais
CIBERVIOLENCIA Y CIBERACOSO contra las mujeres y niñas en el marco de la Convención Belém Do Pará	Iniciativa Spotlight	Academia	Relatório	Ciências Sociais
Criminalização do stalking no Brasil: análise do artigo 147-A do código penal em	Daniel Lopes do Nascimento	Academia	Trabalho de conclusão	Direito



face do direito à privacidade				
Predizendo o abuso digital nas relações amorosas à luz da dependência emocional e aceitação da violência	Thereza Christina Garcia Bezerra	Academia	Dissertação de Mestrado	Psicologia
Crimes cibernéticos: evolução e perseguição contra privacidade feminina e infantil	Luana Rodrigues de Carvalho	Academia	Trabalho de conclusão	Direito
CYBERSTALKING: PERSEGUIÇÃO, PRIVACIDADE E SUAS CONSEQUÊNCIAS NO AMBIENTE DE REDE	Mateus de Oliveira Fornasier, Tiago Protti Spinato, Fernanda Lencina Ribeiro	Academia	Artigo Científico	Direito
VIOÊNCIA NOS RELACIONAMENTOS ÍNTIMOS ENTRE JOVENS: UM ESTUDO TEÓRICO	Dayanne dos Santos Benicio	Academia	Trabalho de conclusão	Psicologia
Stalking e cyberstalking: percepções incipientes acerca da criminalização da prática no Brasil	Marjorie Gomes Andrade	Academia	Artigo Científico	Direito
STALKING: UMA NOVA FORMA DO CRIME DE PERSEGUIÇÃO HABITUAL E IMPLACÁVEL SOFRIDO PELAS	Márcio Magliano Barbosa, Romulo Rhemo Palitot Braga	Academia	Artigo Científico	Direito



MULHERES NO BRASIL				
SAÚDE DA POPULAÇÃO EM TEMPOS COMPLEXOS (Capítulo XXI)	Francisco José Maia Pinto, Cybelle Façanha Barreto Medeiros Linard, Tereza Doralucia Rodrigues Ponte	Academia	Livro	Saúde pública
Tecnopolítica #148 - Stalkerware e a violência dos apps que espionam as mulheres	Sergio Amadeu e Raquel Marques	Academia	Podcast	Saúde pública

2023

Título	Autoria	Setor	Tipo	Disciplinas
Misoginia na internet: uma década de disputa por direitos	Mariana Valente	Academia	Livro	Direito
Crime de Perseguição (Stalking): Nova lei nº 14.132, de 31 de março de 2021	Ana Carlyne Matos Gonçalves	Academia	Trabalho de conclusão	Direito
Stalking e Cyberstalking: uma violação à privacidade e à intimidade	Jair Ilídio da Silva	Academia	Capítulo de livro	Direito
Repercussões Emocionais, Sociais e na Rotina em Mulheres Vítimas de Stalking	Bianca Zambelli Alves, Clarissa De Antoni	Academia	Artigo científico	Psicologia
Cyberstalking scale: development and relations with gender, FOMO and social media engagement	Isabel Leandra Silva Santos, Carlos Eduardo Pimentel e Tailson Evangelista Mariano	Academia	Artigo científico	Psicologia
A responsabilidade civil	André Furegate de	Academia	Trabalho de	Direito



em casos de stalking e cyberstalking: um estudo comparado entre os ordenamentos jurídicos do Brasil e do Estados Unidos da América	Carvalho		conclusão	
Mapeando o abuso digital no namoro no Brasil e na Austrália: uma revisão das experiências de vitimização do Sul Global	Gisella Lopes Gomes Pinto Ferreira	Academia	Artigo científico	Direito
Crime de Stalking: Uma análise sobre a subjetividade do tipo penal	Mateus Leite Marques, Vanessa Érica da Silva Santos	Academia	Livro	Direito
Juventudes e direitos humanos: redes, violências e representações na era digital	Aline Moerbeck da Costa	Academia	Trabalho de conclusão	Direito
Impactos psicossociais das redes sociais (e como lidar com eles)	Isabella Leandra Silva Santos, Débora Cristina Nascimento de Lima, Tailson Evangelista Mariano, Carlos Eduardo Pimentel.	Academia	Capítulo de livro	Psicologia
Crime de perseguição (stalking) nova Lei nº 14.132, de 31 de março de 2021	Ana Carolyne Matos Gonçalves	Academia	Trabalho de conclusão	Direito
Repensando os Tipos Penais do Crime Permanente, Crime Instantâneo de Efeito Permanente e do Crime Continuado no Âmbito da Rede Mundial de	Mozart Gustavo Faria de Oliveira	Academia	Trabalho de conclusão	Direito



Computadores e Redes Sociais. Qual a melhor forma de qualificação do Stalking agora previsto no Art. 147 A do Código Penal Brasileiro?				
Diálogos entre Direito Penal e Direito Processual Penal: Volume 2	Rafhael Lima Ribeiro	Academia	Livro	Direito
A nova lei de stalking: o cyberstalking, a vitimização das mulheres e os meios de investigação	Nicole Soldi Goncalves	Academia	Trabalho de conclusão	Direito
Referências técnicas para atuação profissional os Centros de Referência de Atendimento às Mulheres em Situação de Violência	Secretaria de Estado de Desenvolvimento Social do Governo de Minas Gerais	Governamental	Cartilha	Direito, Psicologia, Serviço Social
Nos últimos três anos, stalkerware cresce 358% no Brasil	Avast	Setor empresarial	Relatório	Segurança da informação
Crescem casos de stalkerware no Brasil; saiba como identificá-los e removê-los	Perallis Security	Setor empresarial	Relatório	Segurança da informação
Como detectar e remover spyware em um celular Android	Kaspersky	Setor empresarial	Tutorial	Segurança da informação
El estado del stalkerware en 2022	Kaspersky	Setor empresarial	Relatório	Segurança da informação



2024

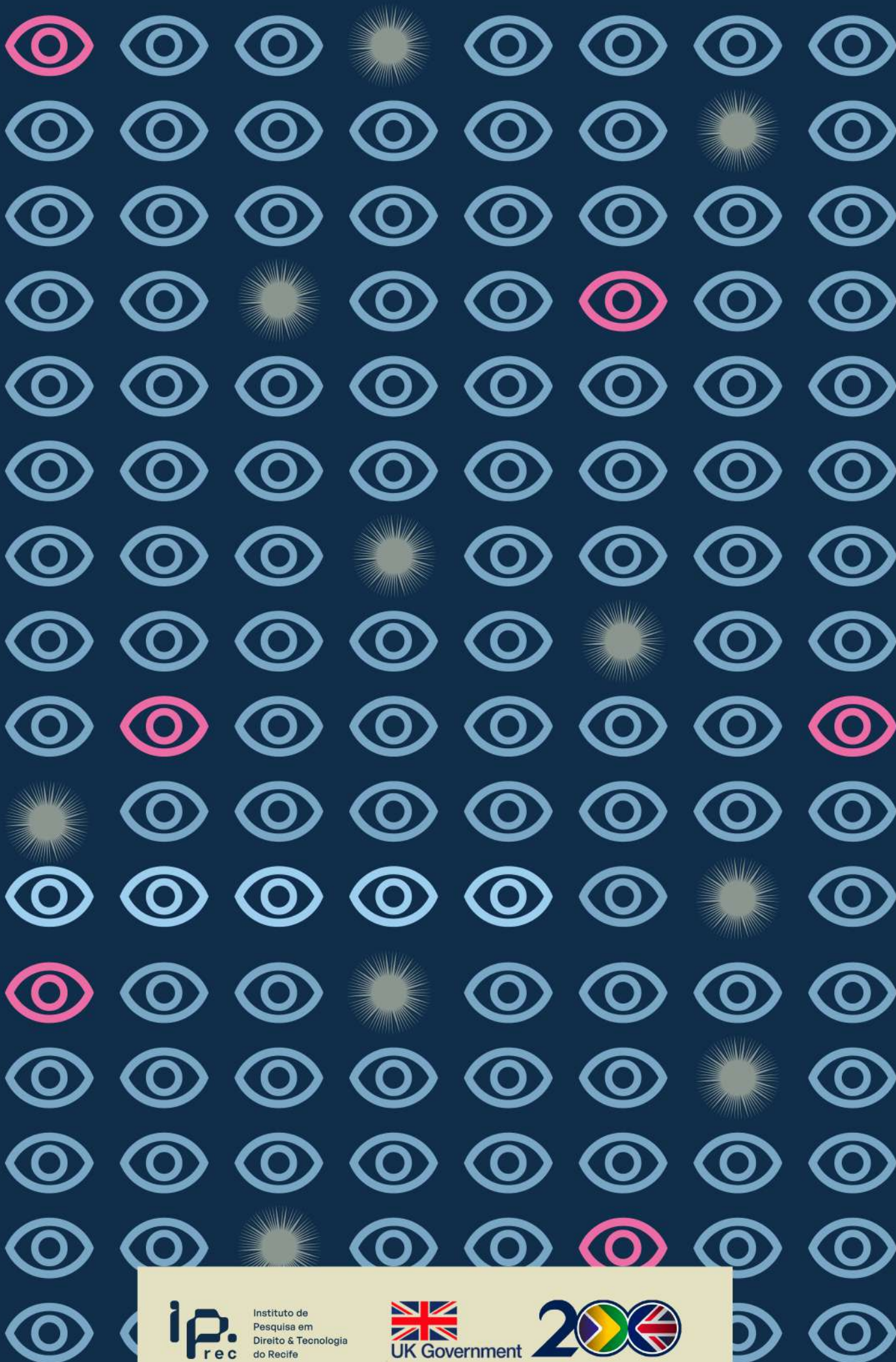
Título	Autoria	Setor	Tipo	Disciplinas
Efetividade da criminalização do cyberstalking (lei 14.132/2021)	Leticia Sampaio Gonçalves	Academia	Trabalho de conclusão	Direito
A CRIMINALIZAÇÃO DO STALKING: ABORDAGENS LEGAIS PARA PREVENIR O FEMINICÍDIO E COMBATER A VIOLÊNCIA DE GÊNERO	Jessica Gomes Rebouças	Academia	Trabalho de conclusão	Direito
STALKING: as implicações da incorporação do tipo penal de perseguição no ordenamento jurídico brasileiro	PPP Danille	Academia	Trabalho de conclusão	Direito
Manual de Segurança Digital - Fascículo Violência Cibernética Contra as Mulheres	Gabinete de Segurança Institucional da Presidência da República	Setor governamental	Relatório	Segurança da informação
O que é Stalkerware? Como encontrar e remover stalkerware	Kaspersky	Setor privado	Tutorial	Segurança da informação
Stalkerware: Guia completo para se proteger	Kaspersky	Setor privado	Guia	Segurança da informação
STALKING E CYBERSTALKING CONTRA A	Evelin de Lima Belfort da Silva; Gabrielle Duarte	Academia	Artigo científico	Direito



MULHER	Silva; Andreia Alves de Almeida			
--------	---------------------------------------	--	--	--

2025

Título	Autoria	Setor	Tipo	Disciplinas
A violência digital e seus efeitos nas vítimas: desafios contemporâneos e perspectiva do ser humano digital	Fabio Rivelli	Academia	Artigo científico	Direto
Jungian clinical approach with women in abusive relationships and post-divorce abuse: challenges and coping	Fabiana Teixeira Pithon	Academia	Artigo científico	Psicologia
Crime de Stalking: teoria e prática	Fabricio Realzi Zia	Academia	Livro	Direito
Lei n.º 11.340 de 07 de agosto de 2006: Patrulha Maria da Penha-guardiões da vida	Bruno Aurélio de Carvalho, Ana Maria Dinardi Barbosa Barros, Roberta Aline Oliveira Guimarães	Academia	Artigo científico	Direito
Projeto Vaza Stalker	IRIS	Terceiro Setor	Relatório	Direitos digitais
Cartilha Não é Paranoia	IP.rec	Terceiro Setor	Cartilha	Direitos digitais



Instituto de
Pesquisa em
Direito & Tecnologia
do Recife



UK Government

