

VIOLÊNCIA TECNOLÓGICA E CONTROLE COERCITIVO: O USO DE DISPOSITIVOS SMART HOME (INTERNET DAS COISAS) E STALKERWARES COMO NOVAS FERRAMENTAS DE ABUSO PSICOLÓGICO E MONITORIZAÇÃO CONTÍNUA DAS VÍTIMAS

**TECHNOLOGY-FACILITATED VIOLENCE AND COERCIVE CONTROL: THE
USE OF SMART HOME (INTERNET OF THINGS) DEVICES AND
STALKERWARE AS EMERGING TOOLS OF PSYCHOLOGICAL ABUSE AND
CONTINUOUS SURVEILLANCE OF VICTIMS**

Ciências Humanas, Engenharias, Ciências Sociais Aplicadas •

11/10/2026

REGISTRO DOI: [10.70773/revistatopicos/791610526](https://doi.org/10.70773/revistatopicos/791610526)

Aldo Ramos da Silva Junior¹

Anna Paula Rocha Frazão²

Leyrilane de Souza³

Gisele de Almeida Nascimento⁴

Dayanne Ramos Farias⁵

RESUMO

A incorporação de dispositivos conectados ao cotidiano doméstico transformou a casa em um ambiente computacional distribuído, no qual fechaduras, câmeras, termostatos, assistentes de voz, sistemas de iluminação, televisores, rastreadores e contas em nuvem podem ser administrados remotamente. Essa infraestrutura oferece conveniência e acessibilidade, mas também cria assimetrias de poder quando uma pessoa detém privilégios administrativos sobre dispositivos, contas e dados compartilhados. Em relações abusivas, tais assimetrias podem ser incorporadas a padrões de controle coercitivo, vigilância persistente, intimidação e desestabilização psicológica. Paralelamente, stalkerwares e outras formas de vigilância íntima permitem acompanhar localização, comunicações e atividades digitais, ampliando a sensação de onnipresença do agressor e tornando a separação física insuficiente para interromper o abuso. Este artigo analisa criticamente a violência facilitada por tecnologia em relações íntimas, com ênfase na convergência entre dispositivos Smart Home/Internet das Coisas (IoT), stalkerware, acesso indevido a contas e monitorização contínua. Adota-se revisão sistematizada qualitativa com síntese narrativa, fundamentada em estudos empíricos, revisões, pesquisas de segurança computacional e documentos normativos e institucionais. A literatura indica que o problema não depende apenas de invasões tecnicamente sofisticadas: agressores frequentemente exploram acesso legítimo prévio, credenciais compartilhadas, interfaces de administração, recursos nativos de localização e dispositivos comercialmente disponíveis. Os efeitos relatados incluem medo, hipervigilância, isolamento, restrição de autonomia, prejuízo econômico, perturbação do sono, autocensura e dificuldade de reconstrução da vida após a separação. Conclui-se que respostas eficazes exigem abordagem sociotécnica e centrada na segurança da vítima,

articulando saúde, assistência, justiça, segurança digital, preservação de evidências e Safety by Design. A simples remoção de um dispositivo ou aplicativo não deve ser tratada como solução universal, pois mudanças abruptas podem alertar o agressor e aumentar o risco; por isso, avaliação individualizada, planejamento de segurança e apoio especializado são componentes essenciais.

Palavras-chave: violência facilitada por tecnologia; controle coercitivo; violência doméstica; Internet das Coisas; Smart Home; stalkerware; vigilância íntima; segurança digital.

ABSTRACT

The integration of connected devices into everyday domestic life has transformed the home into a distributed computing environment in which locks, cameras, thermostats, voice assistants, lighting systems, televisions, trackers, and cloud accounts can be remotely administered. This infrastructure provides convenience and accessibility, but it may also create power asymmetries when one person holds administrative privileges over shared devices, accounts, and data. In abusive relationships, such asymmetries can become embedded in patterns of coercive control, persistent surveillance, intimidation, and psychological destabilization. At the same time, stalkerware and other forms of intimate partner surveillance can enable the monitoring of location, communications, and digital activity, intensifying the perceived omnipresence of the perpetrator and making physical separation insufficient to stop the abuse. This article critically examines technology-facilitated violence in intimate relationships, focusing on the convergence of Smart Home/Internet of Things (IoT) devices, stalkerware, account misuse, and continuous monitoring. A systematized qualitative review with narrative synthesis was conducted, drawing on empirical studies, reviews, computer-security research, and institutional and legal documents.

The literature indicates that abuse does not necessarily rely on technically sophisticated intrusions: perpetrators often exploit previously legitimate access, shared credentials, administrative interfaces, native location-sharing functions, and commercially available devices. Reported consequences include fear, hypervigilance, isolation, restricted autonomy, financial harm, sleep disturbance, self-censorship, and difficulties rebuilding life after separation. Effective responses therefore require a sociotechnical and survivor-centred approach integrating health care, social services, justice, digital security, evidence preservation, and Safety by Design. Simply removing a device or application should not be treated as a universal solution, because abrupt changes may alert the perpetrator and increase danger; individualized risk assessment, safety planning, and specialized support are therefore essential.

Keywords: technology-facilitated abuse; coercive control; domestic violence; Internet of Things; smart home; stalkerware; intimate partner surveillance; digital safety.

1. INTRODUÇÃO

A digitalização da vida cotidiana alterou as condições materiais em que a violência doméstica, a perseguição e o abuso psicológico podem ocorrer. Telefones inteligentes, serviços de nuvem, câmeras conectadas, assistentes de voz, sistemas de automação residencial e dispositivos vestíveis passaram a registrar localização, rotinas, contatos, imagens, hábitos de sono, padrões de deslocamento e inúmeras outras informações. Em circunstâncias ordinárias, esses recursos são apresentados como ferramentas de conveniência, segurança e personalização. Em relações marcadas por desigualdade, intimidação e controle coercitivo, entretanto, a mesma infraestrutura pode ser apropriada para reforçar vigilância,

dependência e restrição da autonomia. A literatura sobre violência facilitada por tecnologia demonstra que os dispositivos não criam por si mesmos a lógica do abuso; eles ampliam a capacidade de um agressor de sustentar padrões já existentes de controle e de fazê-los operar em maior escala, velocidade e continuidade (Dragiewicz et al., 2018; Harris; Woodlock, 2019; Cuomo; Dolci, 2021).

O conceito de controle coercitivo é especialmente útil porque desloca a análise de incidentes isolados para padrões de dominação que limitam liberdade, autodeterminação e “espaço de ação” da vítima. Stark (2007) descreve o controle coercitivo como um regime de captura da autonomia que combina intimidação, isolamento, micro-regulação da vida cotidiana e estratégias de dependência. Quando mediado por tecnologia, esse padrão pode tornar-se “sem espaço”, na formulação de Harris e Woodlock (2019): a vigilância deixa de depender da proximidade física e pode acompanhar a vítima no trabalho, em deslocamentos, em ambientes de acolhimento ou após o término da relação. O caráter contínuo é psicologicamente relevante porque a vítima não precisa saber exatamente qual sistema está sendo utilizado; a incerteza sobre o que o agressor consegue ver ou controlar pode ser suficiente para gerar autocensura e hipervigilância.

Estudos empíricos mostram que a violência tecnológica assume formas heterogêneas. Woodlock (2017), ao investigar experiências de vítimas e profissionais, descreveu o uso de tecnologia para criar sensação de onnipresença, humilhar, isolar e punir. Douglas, Harris e Dragiewicz (2019), em entrevistas com 55 sobreviventes, demonstraram que smartphones, câmeras, computadores, plataformas e dispositivos conectados podem integrar o repertório de violência doméstica e familiar. Revisões posteriores confirmam

que monitoramento de localização, controle de contas, mensagens abusivas, spyware, vigilância por vídeo, abuso baseado em imagens e restrição de acesso digital aparecem repetidamente na literatura (Afrouz, 2023; Rogers et al., 2023; Kim; Ferraresso, 2023). A diversidade terminológica ainda dificulta a comparação entre estudos, mas há convergência em torno da ideia de que a tecnologia amplifica poder, alcance e persistência do abuso.

Dois desenvolvimentos tecnológicos merecem atenção particular. O primeiro é a expansão da Internet das Coisas doméstica. O lar contemporâneo pode possuir câmeras, campainhas, fechaduras, termostatos, tomadas, televisores, roteadores, eletrodomésticos, alto-falantes e automações vinculados a contas remotas. A revisão sistemática de Buil-Gil et al. (2023) identificou a privacidade como uma das principais categorias de dano associadas a smart homes e observou que esses ambientes podem favorecer cyberstalking e aumentar assimetrias de poder entre moradores. Stephenson et al. (2023), analisando o ecossistema de abuso interpessoal mediado por IoT, mostraram que numerosos tipos de dispositivos podem ser usados para espionagem ou assédio e propuseram um modelo de “vetores de abuso” que inclui uso intencional, reutilização de funcionalidades, acesso não autorizado e vigilância encoberta.

O segundo desenvolvimento é o stalkerware, denominação utilizada para programas de vigilância comercial ou semicomercial instalados ou configurados para acompanhar silenciosamente a atividade de outra pessoa. Chatterjee et al. (2018) demonstraram a existência de um ecossistema de aplicativos potencialmente utilizáveis em vigilância por parceiro íntimo, enquanto Freed et al. (2018) observaram que muitos ataques em contextos de violência não dependem de habilidades técnicas avançadas. O agressor

frequentemente é um “adversário íntimo” que já conhece senhas, possui acesso físico, compartilhou contas, configurou serviços ou exerceu o papel de administrador tecnológico da casa. Essa diferença desafia modelos tradicionais de cibersegurança, geralmente construídos para proteger contra atacantes externos e não contra alguém autenticado, conhecido e socialmente autorizado a tocar os mesmos dispositivos.

A relevância científica do problema decorre, portanto, de uma interseção entre violência de gênero e familiar, saúde mental, criminologia, direito, design de tecnologia e segurança computacional. Uma resposta exclusivamente técnica corre o risco de atribuir à vítima a responsabilidade de “corrigir configurações” e ignorar o potencial de retaliação; uma resposta exclusivamente psicossocial pode subestimar a persistência de contas, dispositivos e dados que mantêm o agressor informado. A questão norteadora deste estudo é: de que modo smart homes, IoT e stalkerware se incorporam a padrões de controle coercitivo e quais princípios devem orientar identificação, prevenção e resposta sem aumentar o risco para as vítimas? O objetivo é integrar evidências empíricas, mecanismos sociotécnicos, impactos psicológicos, marcos legais e estratégias de Safety by Design, preservando a distinção entre descrição de capacidades tecnológicas e instruções operacionais que poderiam facilitar abuso.

2. METODOLOGIA

O estudo adota uma revisão sistematizada qualitativa com síntese narrativa. Essa denominação é utilizada porque a pesquisa foi estruturada por pergunta, eixos, critérios e busca verificável de literatura, porém não foi executada uma triagem bibliográfica

completa com deduplicação, dupla seleção independente e fluxograma PRISMA auditável. Não são apresentados números artificiais de registros recuperados ou excluídos. A busca foi atualizada em outubro de 2026 e priorizou literatura entre 2016 e 2026, incorporando textos anteriores quando necessários à fundamentação teórica do controle coercitivo. Foram consultados PubMed/PMC, páginas de periódicos e editoras acadêmicas, ACM Digital Library, IEEE/USENIX, ScienceDirect, Oxford Academic, Taylor & Francis e repositórios universitários, além de documentos oficiais e técnicos da ONU Mulheres, eSafety Commissioner, Safety Net Project/NNEDV, Federal Trade Commission, EUR-Lex, legislação brasileira e Diário da República de Portugal.

Os eixos de busca combinaram expressões como “technology-facilitated abuse”, “technology-facilitated coercive control”, “digital coercive control”, “intimate partner surveillance”, “stalkerware”, “spyware intimate partner violence”, “smart home domestic abuse”, “IoT interpersonal abuse”, “Internet of Things coercive control”, “cyberstalking” e equivalentes em português. A seleção privilegiou: estudos empíricos com vítimas, profissionais ou dados do ecossistema tecnológico; revisões sistemáticas ou de escopo; trabalhos de segurança computacional com relevância explícita para violência por parceiro íntimo; e documentos normativos que tratassem de perseguição, violência psicológica, ciberperseguição ou uso abusivo de dispositivos conectados. Foram excluídos textos exclusivamente promocionais, tutoriais de vigilância, materiais que descrevessem exploração técnica sem conexão com abuso interpessoal e fontes cuja origem não pudesse ser verificada.

A extração foi organizada em uma matriz com cinco dimensões: população ou fonte de dados; tecnologia envolvida; mecanismo de

controle; consequência reportada; e implicação para prevenção ou intervenção. Para smart homes, as categorias analíticas foram adaptadas ao modelo de vetores de abuso de Stephenson et al. (2023), distinguindo uso pretendido de uma função que se torna abusiva, reutilização de funções legítimas, acesso não autorizado e vigilância oculta. Para stalkerware e vigilância íntima, a síntese utilizou como referência os trabalhos de Chatterjee et al. (2018), Freed et al. (2018), Havron et al. (2019) e Tseng et al. (2020), que evidenciam a importância de contas compartilhadas, acesso prévio e configurações exploráveis. O conceito de controle coercitivo foi empregado como enquadramento interpretativo, não como instrumento diagnóstico individual.

A análise jurídica é descritiva e comparativa. No Brasil, foram examinadas a Lei Maria da Penha, especialmente sua definição de violência psicológica, e os tipos penais de perseguição e violência psicológica contra a mulher. Em Portugal, foram considerados os artigos 152.º e 154.º-A do Código Penal. No plano da União Europeia, a Diretiva (UE) 2024/1385 foi incluída porque explicita que ciberperseguição pode envolver stalkerware e dispositivos conectados por Internet das Coisas. A discussão não pretende esgotar tipificação penal ou resolver conflitos de jurisdição; seu objetivo é mostrar que monitorização digital e controle remoto podem assumir relevância jurídica quando inseridos em padrões de violência, ameaça, perseguição, violação de privacidade ou dano psicológico.

Uma limitação importante é a concentração geográfica da literatura em países de alta renda, sobretudo Austrália, Estados Unidos e Reino Unido, além da predominância de estudos com mulheres sobreviventes de violência por parceiros homens. Essa assimetria

reflete a produção disponível e não autoriza concluir que pessoas de outros gêneros ou contextos não sofram violência tecnológica. Outra limitação é a rápida mudança do ecossistema de dispositivos e serviços. Recursos de conta, permissões e mecanismos de notificação podem ser alterados por fabricantes, o que torna imprudente transformar achados acadêmicos em instruções técnicas universais. O foco da síntese, portanto, permanece em padrões de risco, impactos e princípios de resposta centrados na segurança.

Quadro 1. Conceitos centrais para a análise da violência tecnológica e do controle coercitivo

Conceito	Definição operacional neste estudo	Exemplos de manifestação	Risco analítico
Violência facilitada por tecnologia	Ações abusivas cometidas, assistidas, ampliadas ou agravadas por tecnologias digitais.	Assédio, ameaças, monitorização, controle de contas, abuso baseado em imagens, restrição de acesso.	Tratar a tecnologia como causa autônoma e ignorar a relação de poder.
Controle coercitivo digital	Padrão repetido de vigilância, intimidação, micro-regulação e isolamento mediado por tecnologia.	Exigência de acesso, rastreamento, administração unilateral da casa conectada, contacto multimodal.	Reduzir o problema a incidentes desconectados.
Vigilância por parceiro íntimo	Monitorização de informações, atividades ou	Localização, contas, histórico digital, câmeras e	Confundir consentimento passado com

	deslocamentos por parceiro/ex-parceiro.	dados de dispositivos.	consentimento permanente.
Stalkerware	Software usado para observar de modo oculto ou não consentido atividades de um dispositivo.	Acompanhamento de localização, comunicações ou uso do aparelho.	Descrever capacidades de forma operacional ou pressupor que todo monitoramento depende de malware.
Abuso por Smart Home/IoT	Uso de dispositivos conectados e privilégios administrativos para vigiar, perturbar ou controlar o ambiente.	Câmeras, fechaduras, termostatos, iluminação, sensores, roteadores, assistentes de voz.	Analisar apenas “hacking” externo e ignorar usuários autenticados.
Safety by Design	Integração de prevenção de abuso e proteção de usuários ao projeto de produtos e serviços.	Logs compreensíveis, gestão granular de acesso, alertas seguros, recuperação de conta, controles compartilhados.	Transferir todo o ônus de segurança para a vítima.

Fonte: elaboração própria a partir da literatura revisada.

3. CONTROLE COERCITIVO E VIOLÊNCIA FACILITADA POR TECNOLOGIA

O valor do conceito de controle coercitivo está em reconhecer que a violência psicológica não se mede apenas pela intensidade de uma

ameaça isolada, mas pela capacidade de uma sequência de atos reduzir a liberdade concreta da vítima. Em ambiente digital, a soma de pequenos comportamentos pode produzir um sistema disciplinar: exigir resposta imediata a mensagens, questionar localização, verificar contatos, interferir em contas, alterar configurações domésticas, vigiar câmeras, controlar meios de pagamento e utilizar crianças ou familiares como fontes involuntárias de dados. Dragiewicz et al. (2018) propõem a expressão *technology-facilitated coercive control* justamente para abranger a dimensão tecnológica e relacional de padrões de abuso. A tecnologia não é um “canal” neutro; suas affordances — persistência, replicabilidade, alcance remoto, automação e agregação de dados — alteram a escala do controle.

Harris e Woodlock (2019) destacam a característica de “spacelessness”. A vítima pode sair da residência, mudar de bairro ou encerrar a convivência e ainda assim permanecer submetida à observação digital. Cuomo e Dolci (2021) descrevem esse fenômeno como extensão do controle no espaço e no tempo: novas ferramentas tornam antigas táticas de intimidação, isolamento e vigilância mais baratas e eficientes. O ponto central é que a separação entre “online” e “offline” se torna artificial. Um alerta em um aplicativo, uma alteração no termostato, a abertura remota de uma câmera ou o conhecimento inexplicável de um deslocamento produzem efeitos físicos e psicológicos na vida cotidiana. A casa, o telefone e a nuvem formam um único ambiente de poder.

A violência tecnológica também favorece a ambiguidade probatória. Uma porta inteligente que muda de estado, uma rotina automatizada ou uma sessão de conta que permanece ativa podem ser explicadas como “falha do sistema”. Em contexto abusivo, essa

incerteza pode ser explorada para desacreditar a percepção da vítima. A literatura de serviços e segurança computacional enfatiza que o aparente caráter “irracional” de certas suspeitas pode desaparecer quando contas, permissões e dispositivos são analisados sistematicamente (Havron et al., 2019; Freed et al., 2019). Ao mesmo tempo, profissionais não devem presumir que toda anomalia tecnológica é evidência de abuso; a avaliação precisa integrar padrão relacional, temporalidade, acesso provável e sinais técnicos verificáveis.

Um desafio adicional é a normalização social da partilha de senhas e localização em relações íntimas. Recursos desenvolvidos para conveniência familiar podem ser apresentados como símbolos de confiança e, gradualmente, convertidos em obrigações. O consentimento, porém, é contextual e revogável. Ter autorizado acesso a uma conta durante a convivência não transforma monitorização pós-separação em prática legítima. Estudos de vigilância íntima mostram que a fronteira entre “cuidado”, ciúme e controle pode ser obscurecida por discursos de proteção, especialmente em relações jovens (Atiénzar-Prieto; Baker; Meyer, 2025). A avaliação do comportamento deve considerar coerção, medo, assimetria, possibilidade real de recusa e consequências do não consentimento.

Do ponto de vista psicológico, a percepção de que o agressor “sempre sabe” pode funcionar como mecanismo de disciplina mesmo quando o acesso técnico não é contínuo. Woodlock (2017) descreveu a sensação de onnipresença como efeito central. Rogers et al. (2023) encontraram impactos sociais, financeiros e de saúde mental, além da onnipresença, nas pesquisas incluídas em sua revisão de escopo. Esse resultado ajuda a compreender por que o

dano não pode ser avaliado apenas pela quantidade de dados efetivamente coletados. A crença plausível de estar sendo observada pode levar a vítima a mudar trajetos, evitar contatos, abandonar contas, reduzir uso de serviços digitais, dormir mal e limitar iniciativas de saída da relação.

4. SMART HOME E INTERNET DAS COISAS COMO INFRAESTRUTURA DE ABUSO

4.1. Assimetria Administrativa, Acesso Remoto e Controle Ambiental

Smart homes reúnem dispositivos que medem o ambiente, registram eventos e executam ações a partir de comandos locais, aplicativos ou serviços em nuvem. A segurança tradicional tende a imaginar um invasor externo tentando quebrar autenticação; em violência doméstica, o risco pode residir em quem instalou o sistema, criou a conta principal ou conserva privilégios administrativos. Safety Net Project e eSafety Commissioner chamam atenção para o uso indevido de campainhas, câmeras, termostatos, fechaduras, iluminação e alto-falantes conectados para monitorar ou controlar moradores. Não é necessário “hackear” o produto quando a arquitetura pressupõe uma conta proprietária central e essa conta pertence ao agressor.

Buil-Gil et al. (2023), em revisão sistemática de 63 estudos sobre danos digitais em smart homes, identificaram problemas de confidencialidade, autenticação e acesso não autorizado, além do potencial de cyberstalking e aprofundamento de assimetrias entre moradores. Stephenson et al. (2023) ampliam essa compreensão ao mostrar que o abuso pode decorrer tanto de acesso clandestino

quanto do uso pretendido de funcionalidades legítimas. Uma câmera projetada para segurança, por exemplo, já possui capacidade de transmitir imagens; uma fechadura conectada já permite gestão de acesso; um termostato já altera condições térmicas. O risco interpessoal surge quando essas funções são exercidas unilateralmente para vigiar, punir, intimidar ou demonstrar domínio.

A assimetria de administração também tem dimensão econômica e informacional. Quem controla o roteador, a conta da residência ou os pagamentos vinculados ao ecossistema pode restringir conectividade, interromper serviços ou dificultar que a vítima compreenda quais dispositivos existem e como se relacionam. O problema cresce quando equipamentos de diferentes marcas compartilham uma identidade digital única, automações cruzadas ou contas familiares. Uma única credencial comprometida pode representar acesso a múltiplos componentes da casa. Em termos de controle coercitivo, essa centralização converte conveniência em concentração de poder: o administrador tecnológico pode decidir quem vê logs, quem recebe alertas e quem tem capacidade de alterar rotinas.

A literatura de proteção a vítimas adverte, entretanto, contra respostas simplistas. Desconectar uma câmera, mudar uma senha ou excluir um usuário pode gerar notificações, interromper evidências ou informar ao agressor que seu acesso foi descoberto. O Safety Net Project recomenda planejamento estratégico porque alguns agressores podem escalar comportamento quando percebem perda de controle. A Federal Trade Commission oferece orientação semelhante no contexto de stalkerware: antes de alterações, deve-se considerar segurança física, preservação de

evidências e uso de dispositivo confiável para buscar ajuda. Em um artigo acadêmico, essa cautela é fundamental para que recomendações de cibersegurança não produzam risco inadvertido.

4.2. Vigilância Doméstica, Manipulação Ambiental e Desestabilização Epistêmica

A casa conectada produz uma forma particular de abuso porque combina vigilância e capacidade de agir sobre o espaço físico. Câmeras e sensores podem revelar presença, horários e visitantes; sistemas de climatização e iluminação podem ser usados para produzir desconforto; fechaduras e alarmes podem interferir na sensação de segurança; assistentes de voz podem registrar ou exibir informações vinculadas à conta. O efeito não depende de uma função “maliciosa” do dispositivo, mas da relação entre funcionalidade, privilégios e intenção. Em vez de considerar cada equipamento isoladamente, a análise deve perguntar quem controla a conta, quem recebe notificações, quem pode revogar acessos, como o histórico é apresentado e se há mecanismos seguros para contestar autoridade administrativa.

Essa combinação de informação e intervenção favorece a desestabilização epistêmica: a vítima percebe alterações ou demonstrações de conhecimento, mas pode não conseguir provar sua origem. O agressor pode negar envolvimento, atribuir eventos a bugs ou sugerir que a vítima está confundida. Essa dinâmica se aproxima do gaslighting, embora nem toda falha tecnológica corresponda a manipulação intencional. O aspecto clínico e pericialmente relevante é o padrão: eventos recorrentes, assimétricos, temporalmente associados a conflitos ou separação e acompanhados por outras formas de intimidação merecem

investigação sociotécnica. Profissionais devem validar o relato sem afirmar causalidade técnica antes da verificação.

Os danos podem atingir crianças e outras pessoas do agregado familiar. Dispositivos infantis, tablets, relógios e contas de família podem revelar localização ou servir de canal indireto de acesso. Após a separação, rotinas parentais compartilhadas podem manter vínculos tecnológicos entre vítima e agressor. A literatura de violência facilitada por tecnologia mostra que crianças podem ser incorporadas a estratégias de controle, seja como fontes involuntárias de informação, seja como justificativa para exigir acesso permanente a contas e localização (Rogers et al., 2023). Respostas devem equilibrar responsabilidades parentais legítimas com o direito à privacidade e à segurança, evitando configurar sistemas de coparentalidade como infraestrutura de vigilância.

A questão do design é, portanto, inseparável da segurança. Produtos domésticos são frequentemente projetados para ameaças externas e para um modelo de “família confiável”. Em ambientes abusivos, a confiança é precisamente o recurso explorado. Safety by Design requer que fabricantes considerem adversários íntimos: diferentes níveis de privilégio, revogação segura, histórico de acessos compreensível, transparência sobre sensores ativos, canais alternativos de recuperação e alertas que não coloquem a vítima em perigo. A meta não é eliminar toda capacidade de compartilhamento, mas reduzir o potencial de que uma relação de conveniência se converta em dependência tecnológica irreversível.

Quadro 2. Dispositivos Smart Home/IoT e mecanismos de controle coercitivo

Categoria	Função legítima	Possível uso abusivo em alto nível	Efeito sobre a vítima	Princípio preventivo
Câmeras/campainhas	Segurança e registro de eventos.	Observação persistente de entradas, saídas e visitantes.	Sensação de onnipresença, autocensura e isolamento.	Acesso granular, logs compreensíveis e gestão compartilhada.
Fechaduras/alarmes	Controle de acesso e proteção patrimonial.	Uso unilateral de privilégios para criar medo ou restringir previsibilidade e do acesso.	Perda de segurança e autonomia no próprio lar.	Revogação segura, múltiplos administradores e trilhas de auditoria.
Termostatos/iluminação	Conforto, eficiência energética e automação.	Alterações remotas repetidas usadas como intimidação ou perturbação.	Ansiedade, privação de sono e desestabilização.	Controles locais preservados e histórico de mudanças.
Assistentes de voz/TV	Comandos, entretenimento e integração doméstica.	Exposição de rotinas, conteúdo de conta ou uso de funções de comunicação.	Invasão de privacidade e insegurança.	Indicadores claros de sensores e permissões por usuário.
Roteadores/hubs	Conectividade e integração do	Administração unilateral da rede e dos dispositivos conectados.	Dependência digital e dificuldade de identificar o	Separação de privilégios, recuperação independent

	ecossistema .		alcance do acesso.	e e inventário visível.
Wearables/ rastreadores	Saúde, atividade e localização voluntária.	Monitorização de deslocamentos ou dados pessoais sem consentimento atual.	Vigilância contínua e restrição de liberdade.	Consentimento revogável e alertas de compartilhamento.

Fonte: elaboração própria a partir da literatura revisada.

5. STALKERWARE E VIGILÂNCIA POR PARCEIRO ÍNTIMO

5.1. Ecossistema de Vigilância e o “Adversário Íntimo”

O stalkerware ocupa posição emblemática na violência tecnológica porque transforma um dispositivo pessoal em sensor do agressor. Chatterjee et al. (2018) realizaram um dos primeiros estudos sistemáticos do ecossistema de spyware usado em vigilância por parceiro íntimo e demonstraram que aplicações comercialmente disponíveis poderiam ser encontradas e empregadas para monitorização de alto impacto. O problema não se limita à existência de software explicitamente vendido para “espionagem”; funcionalidades de controle parental, gestão de dispositivos ou administração remota podem ser desviadas de finalidade quando utilizadas sem consentimento. Por isso, a classificação deve considerar contexto, transparência, legitimidade de acesso e capacidade da pessoa monitorada de recusar ou encerrar o acompanhamento.

Freed et al. (2018), em estudo qualitativo com 89 participantes, observaram que muitos ataques em relações abusivas são

tecnicamente simples para padrões de segurança computacional. O agressor pode ser um usuário autenticado, ter acesso físico anterior ao aparelho, conhecer perguntas de recuperação ou administrar uma conta compartilhada. Essa figura do “UI-bound adversary” é central: mecanismos que funcionam contra um desconhecido remoto podem falhar contra alguém que viveu com a vítima e participou da configuração dos dispositivos. O erro de segurança não está necessariamente em uma vulnerabilidade de código, mas na suposição de que usuário autenticado e usuário legítimo são sempre a mesma pessoa.

Tseng et al. (2020), ao analisar fóruns relacionados à vigilância íntima, documentaram a combinação de spyware, comprometimento de contas e engenharia social em estratégias de monitorização. A literatura, portanto, recomenda olhar além do “aplicativo espião” e investigar o ecossistema de acesso: contas de e-mail, serviços em nuvem, compartilhamento familiar, histórico de sessão, cópias de segurança, localização, contas de operadora e credenciais reutilizadas. Essa abordagem é relevante para serviços de apoio porque a remoção de um único programa pode não interromper a vigilância se o agressor mantém outros caminhos de acesso.

Havron et al. (2019) propuseram a ideia de “segurança computacional clínica”: atendimento em que profissionais treinados analisam, com a vítima, o conjunto de dispositivos, contas e ameaças, em vez de oferecer listas genéricas de correções. Em estudo de campo, essa abordagem identificou comprometimentos de conta, configurações exploráveis e suspeitas de spyware. Freed et al. (2019) reforçaram que intervenções precisam considerar a narrativa da vítima e o contexto de violência para evitar falsos

negativos técnicos e recomendações perigosas. O modelo aproxima cibersegurança de práticas clínicas: diagnóstico diferencial, avaliação de risco, intervenção proporcional e acompanhamento.

5.2. Limites da Detecção e Riscos de Intervenções Precipitadas

A pergunta “meu telefone está sendo monitorado?” raramente possui resposta simples. Consumo de bateria, aquecimento ou uso de dados são sinais inespecíficos e podem ter múltiplas causas. Ao mesmo tempo, ausência de um aplicativo desconhecido não exclui vigilância, porque o agressor pode explorar contas sincronizadas ou funções nativas. A prática responsável evita tanto alarmismo quanto minimização. Em vez de instruir a vítima a realizar ações técnicas de alto risco, recomenda-se uso de dispositivo confiável para procurar apoio, documentação de ocorrências e avaliação das consequências de qualquer mudança. A FTC e organizações especializadas alertam que remover stalkerware ou alterar acessos pode avisar o agressor e provocar escalada.

A preservação de evidências cria tensão adicional. Uma redefinição de fábrica pode reduzir risco digital, mas também apagar registros úteis. A desconexão imediata de contas pode interromper monitorização, porém informar ao agressor que seu acesso foi descoberto. Não existe estratégia universal: em alguns casos, a prioridade será sair rapidamente de um ambiente perigoso; em outros, será possível preservar evidência antes de alterar configurações. Essa decisão deve ser orientada pelo risco físico e pelo plano de segurança, não pela lógica abstrata de “higiene digital”.

O ecossistema de stalkerware também envolve responsabilidade empresarial. A FTC, em ações contra fornecedores de software de vigilância, destacou riscos associados à coleta oculta de localização, uso do telefone e atividades online. Políticas de lojas de aplicativos, detecção antimalware, requisitos de notificação e regras de publicidade podem reduzir oferta e normalização de ferramentas abusivas, embora não eliminem a vigilância por funcionalidades legítimas. A governança tecnológica precisa lidar simultaneamente com softwares explicitamente voltados à espionagem e com usos abusivos de produtos convencionais.

Do ponto de vista de pesquisa, é importante evitar uma hierarquia simplista entre “stalkerware sofisticado” e “abuso comum”. Estudos de Freed et al. (2018) e Matthews et al. (2017) mostram que o dano decorre menos da sofisticação técnica do que da combinação entre conhecimento íntimo, acesso, persistência e medo. Uma mensagem enviada no momento em que a vítima chega a determinado local pode ter efeito intimidatório comparável ao de malware complexo. A análise deve, portanto, perguntar como a tecnologia sustenta o controle, e não apenas qual ferramenta foi usada.

Quadro 3. Diferenciação entre rotas de monitorização em relações abusivas

Rota	Característica	Dependência de malware	Risco principal	Abordagem de avaliação
Stalkerware/spyware	Software usado para observar atividade do dispositivo.	Pode existir, mas não é a única possibilidade.	Coleta persistente e opaca de informações.	Análise especializada, contexto de acesso e plano de segurança.

Conta compromete	Acesso indevido a e-mail, nuvem, redes ou serviços.	Não.	Visibilidade de mensagens, cópias, localização e recuperação de senhas.	Revisão de sessões e privilégios em dispositivo seguro.
Compartilhamento nativo	Recursos legítimos de família, localização ou sincronização.	Não.	Consentimento antigo transformado em vigilância contínua.	Reavaliar consentimento e governança de compartilhamento.
IoT/Smart Home	Privilegio administrativo sobre dispositivos conectados.	Não.	Vigilância doméstica e controle do ambiente físico.	Inventário de dispositivos, contas e administradores.
Rastreador dedicado	Dispositivo físico usado para localização.	Não.	Acompanhamento de deslocamentos.	Avaliação segura e apoio especializado antes de remoção.
Engenharia social	Obtenção de informação por terceiros, crianças ou recuperação de conta.	Não.	Contorno de barreiras técnicas pela relação social.	Mapear fontes de informação e reduzir exposição sem isolar a vítima.

Fonte: elaboração própria a partir da literatura revisada.

6. IMPACTOS PSICOLÓGICOS, SOCIAIS E FUNCIONAIS DA MONITORIZAÇÃO CONTÍNUA

A monitorização contínua produz dano psicológico por mecanismos que ultrapassam a violação de privacidade. A primeira dimensão é a imprevisibilidade: a vítima não sabe quando está sendo observada, quais dados estão disponíveis ou que comportamento poderá desencadear retaliação. Essa incerteza favorece hipervigilância e comportamentos de verificação repetida. A segunda dimensão é a onnipresença: o agressor parece capaz de atravessar fronteiras físicas e permanecer presente após a separação. Woodlock (2017) identificou esse fenômeno nas narrativas de vítimas; Rogers et al. (2023) o reconheceram como categoria recorrente de impacto. O resultado pode ser uma mudança da própria conduta da vítima, que deixa de fazer algo não porque recebeu ordem explícita, mas porque antecipa que será observada.

A terceira dimensão é a erosão da confiança epistêmica. Se objetos domésticos mudam de comportamento, se informações privadas chegam ao agressor ou se contas parecem “se abrir sozinhas”, a vítima pode começar a duvidar de suas percepções. Em relações nas quais já existe manipulação psicológica, a tecnologia oferece matéria-prima para gaslighting. Esse processo pode ser agravado quando profissionais minimizam o relato por não encontrarem malware na primeira inspeção. A segurança computacional clínica propõe justamente evitar essa dicotomia: um resultado técnico negativo não prova que não exista abuso, porque a fonte pode estar em outra conta ou dispositivo; mas também não autoriza concluir que toda anomalia é causada pelo agressor.

A quarta dimensão é a restrição social. Sobreviventes podem reduzir o uso de redes, deixar de procurar serviços, trocar rotas e afastar-se de pessoas para não “entregar informação”. Woodlock et al. (2020) destacam o dilema dos profissionais: recomendar afastamento da

tecnologia pode reduzir exposição imediata, mas também retirar da vítima acesso a trabalho, apoio, educação, serviços financeiros e vínculos sociais. A meta deve ser tecnologia segura, não exclusão digital. Isso é especialmente relevante para pessoas com deficiência, migrantes, residentes em áreas rurais ou economicamente dependentes, para quem o acesso digital pode ser uma das poucas vias de assistência.

A quinta dimensão é econômica. Dispositivos conectados e contas digitais podem ser usados para controlar despesas, interromper serviços, criar custos ou restringir acesso a recursos. O abuso financeiro mediado por tecnologia integra o mesmo padrão de coerção: reduzir capacidade de escolha e aumentar dependência. Quando contas familiares, assinaturas e meios de pagamento estão tecnicamente sob controle do agressor, a saída da relação pode exigir reconstrução de identidade digital e financeira. Esses custos raramente aparecem nas métricas tradicionais de violência, mas influenciam a capacidade de permanecer separada e segura.

A sexta dimensão envolve saúde e funcionamento. Medo constante, interrupção do sono, atenção direcionada à ameaça, vergonha e perda de confiança podem afetar desempenho profissional, cuidado parental e saúde mental. Não é adequado inferir diagnósticos psiquiátricos a partir da presença de violência tecnológica; contudo, a literatura de violência por parceiro íntimo sustenta que exposição continuada a ameaça e controle está associada a sofrimento psicológico. O que a tecnologia acrescenta é a percepção de que não existe “tempo fora” do abuso. Por isso, a avaliação clínica deve perguntar sobre monitorização digital, controle de contas e dispositivos de forma integrada à anamnese de violência, quando isso for pertinente e seguro.

A resistência das vítimas também merece destaque. Sobreviventes desenvolvem estratégias de uso seletivo, criam contas alternativas, recorrem a profissionais, documentam ocorrências e aprendem a reconhecer padrões de acesso. Rogers et al. (2023) observam, porém, que estudos relatam menos as formas de resistência do que as táticas do agressor. Uma abordagem centrada na vítima deve evitar representá-la como passiva ou tecnicamente incapaz. O objetivo do suporte é ampliar autonomia e opções, não impor uma sequência padronizada de ações.

7. MAPA DAS EVIDÊNCIAS EMPÍRICAS

A literatura empírica combina entrevistas com sobreviventes e profissionais, estudos de segurança computacional, análises de ecossistemas de software e revisões. O quadro a seguir sintetiza trabalhos particularmente relevantes sem tratá-los como equivalentes em desenho ou força de inferência.

Quadro 4. Estudos selecionados e contribuição para compreender violência tecnológica

Estudo	Fonte/amostra	Objeto tecnológico	Achado central	Limitação/alcance
Woodlock (2017)	152 profissionais e 46 vítimas.	Telefones, computadores, redes e monitorização.	Tecnologia foi associada a onnipresença, isolamento, punição e humilhação.	Contexto australiano; autorrelato.

Freed et al. (2018)	Estudo qualitativo com 89 participantes.	Dispositivos, contas e apps de vigilância.	Muitos ataques são tecnicamente simples e exploram acesso íntimo/prévio.	Não estima prevalência populacional.
Chatterjee et al. (2018)	Medição de ecossistema de apps e recursos online.	Spyware/stalkerware.	Identificou disponibilidade de software utilizável para vigilância por parceiro íntimo.	Ecossistema de apps muda rapidamente.
Douglas; Harris; Dragiewicz (2019)	Entrevistas com 55 sobreviventes.	Smartphones, câmeras, contas, dispositivos conectados.	A tecnologia integra e amplia violência doméstica e familiar.	Amostra qualitativa localizada.
Havron et al. (2019)	Serviço de segurança computacional com 44 sobreviventes.	Contas, configurações e potencial spyware.	Abordagem clínica identificou múltiplos vetores de insegurança.	Modelo especializado, difícil de escalar sem formação.
Woodlock et al. (2020)	Survey com 546 profissionais.	Diversos meios digitais.	Profissionais relataram impacto amplo e dilema entre segurança e inclusão digital.	Percepções profissionais, não incidência populacional.
Tseng et al. (2020)	Análise de fóruns de	Spyware, contas,	Vigilância íntima combina	Dados de fórum não equivalem a

	vigilância íntima.	engenharia social.	ferramentas técnicas e estratégias relacionais.	casos confirmados .
Stephenso n et al. (2023)	Análise em larga escala de fontes sobre IoT e abuso.	32 categorias/dispositivos IoT identificados.	Propõe vetores: uso pretendido, reutilização, acesso não autorizado e vigilância encoberta.	Baseada em material online sobre casos e cenários.
Buil-Gil et al. (2023)	Revisão sistemática de 63 estudos.	Smart home.	Privacidade, acesso e assimetrias domésticas são riscos relevantes; IoT pode facilitar cyberstalking.	Foco amplo em danos digitais, não apenas violência doméstica.
Rogers et al. (2023)	Revisão de escopo com 22 estudos.	Tecnologias diversas.	Impactos incluem saúde mental, social, financeiro e sensação de onnipresença.	Heterogeneidade de conceitos e medidas.

Kim; Ferraresso (2023)	Revisão sistemática com 31 estudos empíricos.	TFIPV em geral.	Terminologia e instrumentos são heterogêneos ; muitos estudos usam jovens/adulto s jovens.	Pouca padronizaçã o limita comparabili dade.
------------------------------	---	--------------------	---	--

Fonte: elaboração própria a partir da literatura revisada.

8. MARCOS JURÍDICOS E PROTEÇÃO DE DIREITOS

8.1. Brasil

No Brasil, a Lei Maria da Penha define violência psicológica de forma compatível com muitos elementos do controle coercitivo, incluindo condutas que visem degradar ou controlar ações, comportamentos, crenças e decisões, bem como vigilância constante, perseguição contumaz e violação da intimidade. O texto não depende de uma tecnologia específica, o que permite compreender comportamentos digitais dentro do padrão mais amplo de violência quando presentes os requisitos legais. Essa abertura é importante porque o ecossistema tecnológico muda mais rápido que listas legislativas de dispositivos.

A Lei nº 14.132/2021 inseriu no Código Penal o crime de perseguição, definido como perseguir alguém reiteradamente e por qualquer meio, ameaçando integridade, restringindo locomoção ou invadindo/perturbando liberdade ou privacidade. A expressão “por qualquer meio” é relevante para cyberstalking e monitorização digital, embora a qualificação de cada caso dependa de seus

elementos concretos. A Lei nº 14.188/2021 criou o tipo de violência psicológica contra a mulher, abrangendo dano emocional ou condutas voltadas a degradar ou controlar ações, comportamentos, crenças e decisões. A análise acadêmica deve evitar transformar qualquer incidente tecnológico em crime automaticamente; a tecnologia é meio, e a tipificação depende de conduta, contexto, dolo, reiteração quando exigida e demais elementos jurídicos.

A resposta jurídica também depende de preservação de evidências. Logs, capturas de tela, registros de conta, fotografias de dispositivos e relatos cronológicos podem adquirir relevância, mas sua coleta deve ser compatível com a segurança da vítima e com regras de integridade probatória. Recomendações técnicas de “apagar tudo” podem destruir evidências; recomendações de “não mexer em nada” podem prolongar risco. O plano deve ser individualizado e, quando necessário, envolver polícia, advocacia, perícia e serviço especializado em violência doméstica.

8.2. Portugal e União Europeia

Em Portugal, o artigo 152.º do Código Penal tipifica violência doméstica incluindo maus-tratos físicos ou psíquicos e outras formas de abuso em relações abrangidas pelo dispositivo. O artigo 154.º-A prevê o crime de perseguição quando alguém, de modo reiterado, persegue ou assedia outra pessoa por qualquer meio, direta ou indiretamente, de forma adequada a provocar medo, inquietação ou prejuízo à liberdade de determinação. A redação tecnologicamente neutra permite que meios digitais sejam considerados conforme os fatos do caso.

No plano europeu, a Diretiva (UE) 2024/1385 representa marco especialmente explícito. Ao tratar da ciberperseguição, a norma descreve vigilância repetida ou contínua por tecnologias da informação e comunicação e menciona, entre os meios possíveis, aplicações de geolocalização, incluindo stalkerware, e monitorização por dispositivos conectados à Internet das Coisas, como aparelhos smart home. Essa formulação reconhece normativamente que a casa conectada e o software de vigilância podem integrar violência contra mulheres e violência doméstica, deslocando o debate de “mau uso privado” para problema de direitos, proteção e responsabilização.

A diretiva também é relevante por articular criminalização mínima de determinadas formas de ciberviolência com direitos das vítimas, prevenção e intervenção. Para o design tecnológico, isso significa que compliance não deve ser interpretado apenas como proteção de dados em sentido abstrato. Produtos que possibilitam monitorização persistente, controle remoto ou administração assimétrica devem ser avaliados também sob a perspectiva de abuso por usuários conhecidos. Privacy by Design e Safety by Design se tornam complementares: privacidade protege contra coleta e acesso indevidos; segurança contra abuso considera a forma como funções legítimas podem ser instrumentalizadas em relações coercitivas.

Quadro 5. Enquadramentos jurídicos selecionados e sua relação com violência tecnológica

Jurisdição/norma	Elemento relevante	Relação com o tema	Observação
------------------	--------------------	--------------------	------------

Brasil – Lei 11.340/2006	Violência psicológica, vigilância constante, perseguição e violação de intimidade.	Permite compreender monitorização digital dentro de padrões de violência doméstica.	Aplicação depende do contexto e dos requisitos legais do caso.
Brasil – Lei 14.132/2021 / art. 147-A	Perseguição reiterada “por qualquer meio” com invasão/perturbação de liberdade ou privacidade.	Pode alcançar perseguição mediada por tecnologia.	Não transforma automaticamente e todo rastreamento em crime; é necessária análise jurídica.
Brasil – Lei 14.188/2021 / art. 147-B	Dano emocional e controle de ações, comportamentos, crenças e decisões.	Dialoga com efeitos psicológicos do controle coercitivo digital.	Tipo voltado à violência psicológica contra a mulher.
Portugal – Código Penal, art. 152.º	Maus-tratos físicos ou psíquicos em relações abrangidas.	Tecnologia pode ser meio de violência doméstica.	Avaliação concreta segundo direito português.
Portugal – Código Penal, art. 154.º-A	Perseguição ou assédio reiterado por qualquer meio.	Abrange potencialmente cyberstalking e monitorização digital.	Exige adequação a provocar medo/inquietação ou prejudicar liberdade de determinação.
União Europeia – Diretiva 2024/1385	Ciberperseguição, stalkerware e monitorização via IoT mencionados expressamente.	Reconhece a relevância de smart home e stalkerware na ciberviolência.	Estabelece regras mínimas e direitos de vítimas, com transposição pelos Estados-Membros.

Fonte: elaboração própria a partir da literatura revisada.

9. RESPOSTA INTERDISCIPLINAR E PLANEJAMENTO DE SEGURANÇA

9.1. Princípios para Serviços de Saúde, Assistência e Justiça

A primeira regra de atendimento é não pressupor que a vítima “deveria simplesmente trocar a senha” ou abandonar a tecnologia. Essa resposta transfere responsabilidade, pode gerar isolamento e ignora a possibilidade de escalada. O profissional deve perguntar de forma não julgadora o que a pessoa observa, quem teve acesso aos dispositivos, quando os eventos começaram, se existem ameaças associadas e quais mudanças poderiam ser percebidas pelo agressor. A investigação deve priorizar segurança física e emocional antes da correção técnica. Em situação de risco iminente, procedimentos de emergência e redes locais de proteção prevalecem sobre qualquer auditoria digital.

A segunda regra é separar descoberta de intervenção. Identificar uma possível via de monitorização não significa removê-la imediatamente. A FTC e o Safety Net Project alertam que a interrupção pode informar ao agressor que perdeu acesso. A vítima deve participar da decisão sobre quando alterar contas, dispositivos ou serviços. Quando possível, comunicações sensíveis e busca de ajuda devem ocorrer por meio considerado mais seguro. Essa orientação não é um convite a realizar perícias improvisadas; ao contrário, reconhece que avaliação especializada pode ser necessária.

A terceira regra é documentar com proporcionalidade. Uma linha do tempo com datas, mensagens, comportamentos, alterações em

dispositivos e testemunhas pode ajudar a demonstrar padrão. Evidências digitais, entretanto, podem conter informações íntimas e expor terceiros. Serviços devem possuir protocolos de armazenamento seguro, minimização de dados e consentimento. O objetivo é apoiar a vítima, não criar novo repositório vulnerável de sua vida privada.

A quarta regra é reconhecer que segurança digital e segurança relacional se influenciam. Um novo dispositivo pode ser tecnicamente seguro, mas tornar-se comprometido se a conta de recuperação continua vinculada ao agressor. Uma conta pode estar segura, mas a localização ser revelada por um carro conectado ou wearable. A avaliação precisa mapear o ecossistema, não apenas o telefone. Havron et al. (2019) mostram a utilidade de procedimentos estruturados para descobrir comprometimentos multimodais; esse princípio pode ser adaptado a serviços sem transformar profissionais de saúde ou assistência em peritos forenses.

A quinta regra é preservar agência. Sobreviventes podem optar por manter temporariamente um canal monitorado para evitar suspeita, buscar evidência ou organizar saída. Profissionais devem explicar riscos e alternativas sem impor decisões. Essa postura é coerente com o próprio problema: controle coercitivo retira autonomia; uma intervenção protetiva não deve reproduzir a mesma lógica ao substituir as escolhas da vítima por decisões técnicas externas.

9.2. Safety By Design e Responsabilidade dos Fabricantes

A prevenção estrutural exige reduzir a “abusabilidade” dos produtos. Sistemas smart home podem adotar múltiplos administradores independentes, níveis de permissão, histórico de acessos, alertas

contextualizados, indicadores claros de sensores, confirmação segura de mudanças críticas e procedimentos de recuperação que não dependam exclusivamente da conta controlada pelo agressor. O desafio é evitar que mecanismos de proteção alertem inadvertidamente o próprio abusador. Por isso, Safety by Design deve ser desenvolvido com participação de sobreviventes, organizações especializadas e pesquisadores de segurança.

A arquitetura de contas familiares merece atenção especial. Muitos sistemas são construídos em torno de um “proprietário” que controla todos os demais membros. Esse modelo pode ser eficiente para uma residência estável, mas perigoso em separações e relações abusivas. A possibilidade de exportar dados pessoais, separar perfis, transferir titularidade e encerrar compartilhamentos sem perda desnecessária de funcionalidade pode reduzir dependência. Do mesmo modo, fabricantes devem permitir que usuários entendam quais dados são coletados e quem os acessou, sem exigir conhecimento técnico avançado.

No campo de aplicativos móveis, lojas, sistemas operacionais e antivírus possuem papel de governança. Políticas contra software de vigilância oculta, transparência de permissões e notificações de acesso podem reduzir stalkerware. Entretanto, uma política focada apenas em “malware” não resolve funções legítimas usadas abusivamente. O problema é sociotécnico: a mesma API ou recurso de localização pode ter usos benéficos e abusivos. Avaliações de risco devem considerar contexto de relacionamento e oferecer controles reversíveis, consentimento contínuo e caminhos de ajuda.

Por fim, responsabilidade empresarial inclui resposta a denúncias. Uma vítima que relata controle abusivo de um dispositivo não

deveria ser obrigada a provar invasão criminal antes de receber orientação básica sobre contas, logs e recuperação. Equipes de suporte podem ser treinadas para reconhecer cenários de abuso, evitar instruções que aumentem risco e encaminhar para serviços especializados. Essa capacidade transforma suporte técnico em componente de prevenção de violência sem exigir que empresas decidam a culpabilidade de indivíduos.

Quadro 6. Matriz integrada de resposta à violência tecnológica (MIR-VT)

Dimensão	Pergunta-chave	Risco de resposta inadequada	Resposta centrada na segurança
Relação e padrão	Há histórico de intimidação, controle, perseguição ou violência?	Tratar incidente digital como problema técnico isolado.	Mapear contexto e risco relacional antes da intervenção.
Dispositivos e contas	Quem administra, compartilha ou recupera os acessos?	Focar apenas no telefone e ignorar nuvem/IoT.	Inventariar ecossistema e privilégios em dispositivo seguro.
Evidência	O que pode ser preservado sem ampliar perigo?	Apagar dados ou gerar exposição adicional.	Documentação proporcional e armazenamento protegido.
Intervenção	Uma mudança será percebida pelo agressor?	Escalada após perda de acesso.	Planejar momento, canal e suporte antes de mudanças críticas.

Saúde mental	Como o monitoramento afeta sono, medo, funcionamento e autonomia?	Patologizar a vítima ou minimizar relato por falta de prova técnica.	Validar impacto e investigar sem afirmar causalidade prematura.
Justiça/protensão	Há elementos de ameaça, perseguição, violação de privacidade ou violência doméstica?	Fragmentar fatos e perder o padrão de coerção.	Organizar cronologia e buscar avaliação jurídica especializada.
Design/indústria	O produto permite revogação, logs e administração equitativa?	Transferir todo o ônus de segurança ao usuário vulnerável.	Safety by Design, privilégios granulares e suporte sensível ao abuso.

Fonte: elaboração própria a partir da literatura revisada.

10. DISCUSSÃO

A síntese evidencia que a violência tecnológica é melhor compreendida como transformação do meio do controle, e não como categoria completamente separada da violência doméstica. A contribuição das tecnologias conectadas está em reduzir custo e esforço necessários para manter vigilância, aumentar persistência e tornar a fronteira entre presença e ausência menos relevante. Cuomo e Dolci (2021) descrevem “novas ferramentas, antigo abuso”; essa formulação evita determinismo tecnológico, mas também impede minimizar o que mudou. Uma câmera acessível remotamente, um serviço de localização ou uma automação residencial tornam possível exercer controle à distância com

velocidade e frequência antes inviáveis. O abuso permanece relacional, porém suas affordances se ampliam.

A literatura também mostra que smart home e stalkerware não devem ser analisados em silos. Em casos concretos, um agressor pode combinar acesso a contas, localização nativa, câmera doméstica, rastreador físico e mensagens intimidatórias. O conceito de ataque multimodal é mais fiel à experiência da vítima do que a busca por um “aplicativo culpado”. Esse achado tem consequências metodológicas: pesquisas que perguntam apenas por cyberstalking em redes sociais podem subestimar abuso por IoT; estudos que procuram apenas malware podem perder vigilância baseada em conta; pesquisas que contabilizam incidentes isolados podem não captar o padrão coercitivo.

O caráter íntimo do atacante altera pressupostos clássicos de cibersegurança. Muitos produtos assumem que a pessoa que possui credencial principal é a autoridade legítima. Em relações abusivas, a posse técnica da conta pode coexistir com exercício ilegítimo de poder. Essa tensão é difícil de resolver apenas com autenticação forte, porque o agressor pode ter sido legitimamente administrador no passado. Soluções precisam contemplar transições relacionais: separação de contas, remoção segura de usuários, transferência de dispositivos, recuperação independente e registro de alterações. Em outras palavras, a segurança deve lidar não apenas com “quem é você?”, mas com “que autoridade você deveria ter agora?”.

A noção de “desestabilização epistêmica” emerge como eixo promissor de pesquisa. Smart homes produzem eventos que podem ser automatizados, registrados parcialmente ou controlados remotamente. Em um contexto coercitivo, a incerteza sobre autoria

pode ser usada para causar medo e descrédito. Estudos futuros poderiam investigar como interfaces, logs e notificações influenciam a capacidade de uma vítima explicar o que ocorreu a profissionais, polícia ou tribunais. Produtos que mostram apenas estados atuais, sem histórico inteligível de ações administrativas, podem dificultar reconstrução do padrão de abuso.

Outro problema é a carga de segurança colocada sobre a vítima. Recomendações populares frequentemente sugerem abandonar redes, desligar recursos ou excluir contas. Harris e Woodlock (2019) criticam essa transferência de “safety work” porque a vítima paga o preço da violência com exclusão digital. Uma política adequada deve preservar participação social e acesso a serviços. Isso exige que designers, plataformas, provedores de nuvem, operadores de telecomunicações e serviços de apoio assumam responsabilidades proporcionais, em vez de considerar o ambiente tecnológico neutro e o usuário vulnerável como único agente de correção.

Os marcos legais recentes sinalizam mudança importante. A Diretiva (UE) 2024/1385 menciona explicitamente stalkerware e IoT na ciberperseguição, enquanto legislações brasileira e portuguesa empregam conceitos tecnologicamente neutros de perseguição, violência psicológica e violência doméstica. Essa combinação é vantajosa: leis gerais evitam obsolescência rápida, ao passo que referências explícitas ajudam operadores a reconhecer novas formas de violência. Ainda assim, criminalização não substitui prevenção, suporte e design responsável. Muitas vítimas procuram ajuda antes de haver prova suficiente para processo penal, e respostas precoces podem ser decisivas para segurança.

Do ponto de vista clínico e psicossocial, a contribuição central é reconhecer a monitorização contínua como potencial componente de trauma relacional e restrição de autonomia. Profissionais não precisam dominar engenharia reversa para perguntar sobre controle de senhas, localização, dispositivos conectados e acesso a contas. O papel clínico é identificar impacto, risco e necessidade de encaminhamento. A investigação técnica aprofundada deve ser feita por pessoal qualificado, sobretudo quando há possibilidade de destruição de evidência, exposição de dados íntimos ou escalada de violência.

O avanço das tecnologias de IA, wearables, veículos conectados e automação tende a aumentar a complexidade. Sistemas podem inferir hábitos a partir de dados distribuídos, e dispositivos podem interagir sem ação manual a cada evento. A prevenção precisa antecipar esse cenário. Segurança por design voltada apenas a hackers externos continuará insuficiente. Testes de abuso, threat modeling com “adversário íntimo”, revisão de permissões familiares e canais de suporte a vítimas deveriam integrar o ciclo de desenvolvimento de produtos conectados.

A proposta da Matriz Integrada de Resposta à Violência Tecnológica (MIR-VT) busca sintetizar essas implicações em sete dimensões — relação, ecossistema tecnológico, evidência, intervenção, saúde mental, justiça e design. A matriz não é instrumento diagnóstico validado; sua função é conceitual e organizacional. Ela enfatiza que qualquer intervenção muda o sistema: trocar uma senha altera o conhecimento do agressor; desconectar um dispositivo pode interromper prova; manter um canal pode preservar evidência, mas prolongar exposição. Decisões devem ser tomadas com avaliação de risco e consentimento da vítima.

Por fim, o campo precisa de maior padronização de medidas. Kim e Ferraresso (2023) demonstram heterogeneidade terminológica e ausência frequente de instrumentos validados; Rogers et al. (2023) observam que impactos e resistências nem sempre são relatados de forma sistemática. Pesquisas futuras devem distinguir tecnologia usada, relação entre agressor e vítima, consentimento, fase da relação, coexistência de violência offline, impacto funcional e estratégias de resistência. Estudos longitudinais e comparativos em países de renda média e baixa são particularmente necessários para evitar que respostas globais sejam construídas apenas a partir de ecossistemas tecnológicos e jurídicos do Norte Global.

11. CONSIDERAÇÕES FINAIS

A análise realizada demonstra que Smart Home, Internet das Coisas e stalkerware não devem ser entendidos apenas como novos “instrumentos” acrescentados a uma lista de formas de violência. Eles modificam a arquitetura do controle ao permitir que vigilância e intervenção acompanhem a vítima para além da presença física do agressor. A casa conectada pode funcionar simultaneamente como ambiente, sensor e interface de administração; o telefone pode concentrar identidade, localização, comunicações e recuperação de contas; a nuvem pode manter persistência mesmo após troca de aparelho. Essa interconexão explica por que respostas limitadas a um dispositivo frequentemente falham e por que o mapeamento do ecossistema tecnológico é mais adequado que a busca por um único ponto de comprometimento.

A literatura é consistente em mostrar que grande parte do abuso não exige alta sofisticação técnica. O fator decisivo é a intimidade: conhecimento de hábitos, acesso físico, senhas compartilhadas,

contas familiares e autoridade administrativa acumulada durante a relação. Esse “adversário íntimo” desafia os modelos convencionais de cibersegurança e exige produtos capazes de lidar com mudanças de confiança ao longo do tempo. Recursos de compartilhamento devem ser acompanhados por consentimento revogável, visibilidade sobre privilégios, separação de perfis e caminhos de recuperação que não dependam exclusivamente do administrador original.

Os efeitos psicológicos não podem ser reduzidos à quantidade de dados capturados. Sensação de onnipresença, incerteza, medo, hipervigilância, autocensura e perda de confiança nas próprias percepções podem emergir mesmo quando a vítima não consegue identificar exatamente o mecanismo de monitorização. Por isso, ausência imediata de prova técnica não deve ser convertida em desqualificação do relato. Ao mesmo tempo, investigação responsável evita afirmar causalidade sem evidência. A posição profissional adequada combina validação do sofrimento, análise contextual e verificação técnica quando necessária.

A resposta prática precisa ser centrada na segurança e na autonomia. Medidas tecnicamente corretas — redefinir aparelho, excluir conta, remover rastreador — podem ser perigosas se alertarem o agressor ou destruírem evidências. Planejamento de segurança, apoio especializado, uso de canais confiáveis e decisão compartilhada com a vítima devem anteceder mudanças críticas. Essa abordagem também evita reproduzir a lógica do controle coercitivo: o objetivo não é substituir a autoridade do agressor pela autoridade do especialista, mas devolver opções e capacidade de decisão à pessoa afetada.

No plano jurídico, a evolução normativa oferece bases importantes. A legislação brasileira contempla violência psicológica, perseguição e vigilância constante em marcos relevantes; o direito português criminaliza violência doméstica e perseguição por qualquer meio; e a Diretiva europeia 2024/1385 reconhece explicitamente stalkerware e dispositivos IoT como possíveis meios de ciberperseguição. Esses avanços ampliam a inteligibilidade do fenômeno, mas a eficácia depende de capacitação de profissionais, preservação probatória, cooperação com plataformas e disponibilidade de suporte técnico especializado.

A prevenção de longo prazo exige Safety by Design. Fabricantes de produtos conectados precisam testar não apenas ataques externos, mas cenários de abuso por usuários autenticados e parceiros íntimos. Controles granulares, logs acessíveis, indicadores transparentes, revogação segura, múltiplos administradores e suporte sensível ao abuso podem reduzir a concentração de poder tecnológico. Plataformas e lojas de aplicativos, por sua vez, devem restringir softwares de vigilância oculta e desenvolver mecanismos que identifiquem usos incompatíveis com consentimento e segurança.

Finalmente, o campo científico deve avançar na padronização de conceitos, instrumentos e indicadores de impacto. A rápida evolução tecnológica torna impossível depender de listas fixas de dispositivos. Modelos baseados em mecanismos — vigilância, controle ambiental, acesso assimétrico, isolamento, intimidação e exploração de dados — são mais duráveis. A investigação futura deve incluir diversidade de gênero, orientação sexual, deficiência, idade, ruralidade, migração e desigualdade econômica, além de contextos do Sul Global, onde acesso a suporte técnico e jurídico pode ser menor. A violência

tecnológica é um problema sociotécnico: enfrentá-la exige que tecnologia, serviços e instituições sejam projetados para preservar autonomia, dignidade e liberdade, sobretudo quando a ameaça vem de alguém que já esteve dentro do círculo de confiança da vítima.

REFERÊNCIAS BIBLIOGRÁFICAS

AFROUZ, Rojan. The nature, patterns and consequences of technology-facilitated domestic abuse: a scoping review. *Trauma, Violence, & Abuse*, v. 24, n. 2, p. 913-927, 2023. DOI: 10.1177/15248380211046752.

ATIÉNZAR-PRIETO, María; BAKER, Steven; MEYER, Silke. Young people's attitudes and perceptions of technology-facilitated coercive control: a scoping review. *Aggression and Violent Behavior*, v. 82, art. 102054, 2025. DOI: 10.1016/j.avb.2025.102054.

BRASIL. Lei nº 11.340, de 7 de agosto de 2006. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher. Brasília, DF: Presidência da República, 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm. Acesso em: 3 out. 2026.

BRASIL. Lei nº 14.132, de 31 de março de 2021. Acrescenta o art. 147-A ao Código Penal para prever o crime de perseguição. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm. Acesso em: 3 out. 2026.

BRASIL. Lei nº 14.188, de 28 de julho de 2021. Cria o tipo penal de violência psicológica contra a mulher. Brasília, DF: Presidência da República, 2021. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14188.htm. Acesso em: 3 out. 2026.

BUIL-GIL, David; KEMP, Steven; KUENZEL, Stefanie; COVENTRY, Lynne; ZAKHARY, Sameh; TILLEY, Daniel; NICHOLSON, James. The digital harms of smart home devices: a systematic literature review. *Computers in Human Behavior*, v. 145, art. 107770, 2023. DOI: 10.1016/j.chb.2023.107770.

CHATTERJEE, Rahul; DOERFLER, Periwinkle; ORGAD, Hadas; HAVRON, Sam; PALMER, Jackeline; FREED, Diana; LEVY, Karen; DELL, Nicola; MCCOY, Damon; RISTENPART, Thomas. The spyware used in intimate partner violence. In: *IEEE SYMPOSIUM ON SECURITY AND PRIVACY*, 2018. Proceedings [...]. Los Alamitos: IEEE, 2018. p. 441-458. DOI: 10.1109/SP.2018.00061.

CUOMO, Dana; DOLCI, Natalie. New tools, old abuse: technology-enabled coercive control (TECC). *Geoforum*, v. 126, p. 224-232, 2021. DOI: 10.1016/j.geoforum.2021.08.002.

DOUGLAS, Heather; HARRIS, Bridget A.; DRAGIEWICZ, Molly. Technology-facilitated domestic and family violence: women's experiences. *The British Journal of Criminology*, v. 59, n. 3, p. 551-570, 2019. DOI: 10.1093/bjc/azy068.

DRAGIEWICZ, Molly; BURGESS, Jean; MATAMOROS-FERNÁNDEZ, Ariadna; SALTER, Michael; SUZOR, Nicolas P.; WOODLOCK, Delanie; HARRIS, Bridget. Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, v. 18, n. 4, p. 609-625, 2018. DOI: 10.1080/14680777.2018.1447341.

ESAFETY COMMISSIONER. Coercive control: what does it mean? Canberra: Australian Government, 2026. Disponível em: <https://www.esafety.gov.au/key-topics/domestic-family-violence/coercive-control>. Acesso em: 3 out. 2026.

ESAFETY COMMISSIONER. Internet of Things (IoT) and coercive control. Canberra: Australian Government, 2026. Disponível em: <https://www.esafety.gov.au/industry/tech-trends-and-challenges/convergence-series/internet-of-things-iot-and-coercive-control>. Acesso em: 3 out. 2026.

EUROPEAN UNION. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. Official Journal of the European Union, 2024. Disponível em: <https://eur-lex.europa.eu/eli/dir/2024/1385/oj>. Acesso em: 3 out. 2026.

FEDERAL TRADE COMMISSION. FTC bans SpyFone and CEO from surveillance business and orders company to delete all secretly stolen data. Washington, DC: FTC, 2021. Disponível em: <https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data>. Acesso em: 3 out. 2026.

FEDERAL TRADE COMMISSION. Stalkerware: what to know. Washington, DC: FTC, 2026. Disponível em: <https://consumer.ftc.gov/articles/stalkerware-what-know>. Acesso em: 3 out. 2026.

FREED, Diana; HAVRON, Sam; TSENG, Emily; GALLARDO, Andrea; CHUGH, Rahul; RISTENPART, Thomas; DELL, Nicola. "Is my phone hacked?" Analyzing clinical computer security interventions with

survivors of intimate partner violence. Proceedings of the ACM on Human-Computer Interaction, v. 3, CSCW, art. 202, p. 1-24, 2019. DOI: 10.1145/3359304.

FREED, Diana; PALMER, Jackeline; MINCHALA, Diana; LEVY, Karen; RISTENPART, Thomas; DELL, Nicola. "A Stalker's Paradise": how intimate partner abusers exploit technology. In: CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 2018. Proceedings [...]. New York: ACM, 2018. art. 667, p. 1-13. DOI: 10.1145/3173574.3174241.

HARRIS, Bridget A.; WOODLOCK, Delanie. Digital coercive control: insights from two landmark domestic violence studies. The British Journal of Criminology, v. 59, n. 3, p. 530-550, 2019. DOI: 10.1093/bjc/azy052.

HAVRON, Sam; FREED, Diana; CHATTERJEE, Rahul; MCCOY, Damon; DELL, Nicola; RISTENPART, Thomas. Clinical computer security for victims of intimate partner violence. In: USENIX SECURITY SYMPOSIUM, 28., 2019. Proceedings [...]. Berkeley: USENIX Association, 2019. p. 105-122.

KIM, Chunrye; FERRARESSO, Riccardo. Examining technology-facilitated intimate partner violence: a systematic review of journal articles. Trauma, Violence, & Abuse, v. 24, n. 3, p. 1325-1343, 2023. DOI: 10.1177/15248380211061402.

LEVY, Karen E. C. Intimate surveillance. Idaho Law Review, v. 51, n. 3, p. 679-693, 2015.

MATTHEWS, Tara; O'LEARY, Kathleen; TURNER, Anna; SLEEPER, Manya; WOELFER, Jill Palzkill; SHELTON, Martin; MANTHORNE, Cori; CHURCHILL, Elizabeth F.; CONSOLVO, Sunny. Stories from survivors:

privacy & security practices when coping with intimate partner abuse. In: CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 2017. Proceedings [...]. New York: ACM, 2017. p. 2189-2201. DOI: 10.1145/3025453.3025875.

ONU MULHERES. Technology-facilitated violence against women: towards a common conceptual definition. New York: UN Women, 2025. Disponível em: <https://knowledge.unwomen.org/>. Acesso em: 3 out. 2026.

PORTUGAL. Código Penal: artigo 152.º – Violência doméstica. Diário da República, versão consolidada em vigor. Lisboa, 2026. Disponível em: <https://diariodarepublica.pt/>. Acesso em: 3 out. 2026.

PORTUGAL. Código Penal: artigo 154.º-A – Perseguição. Diário da República, versão consolidada em vigor. Lisboa, 2026. Disponível em: <https://diariodarepublica.pt/>. Acesso em: 3 out. 2026.

ROGERS, Michaela M.; FISHER, Colleen; ALI, Parveen; ALLMARK, Peter; FONTES, Lisa. Technology-facilitated abuse in intimate relationships: a scoping review. Trauma, Violence, & Abuse, v. 24, n. 4, p. 2210-2226, 2023. DOI: 10.1177/15248380221090218.

SAFETY NET PROJECT. Smart home devices: survivor privacy and safety for the “smart” home (Internet of Things). Washington, DC: National Network to End Domestic Violence, 2026. Disponível em: <https://www.techsafety.org/smart-home>. Acesso em: 3 out. 2026.

SAFETY NET PROJECT. Technology safety plan. Washington, DC: National Network to End Domestic Violence, 2026. Disponível em: <https://www.techsafety.org/resources-survivors/technology-safety-plan>. Acesso em: 3 out. 2026.

STARK, Evan. Coercive control: how men entrap women in personal life. New York: Oxford University Press, 2007.

STEPHENSON, Sophie; ALMANSOORI, Majed; EMAMI-NAEINI, Pardis; HUANG, Danny Yuxing; CHATTERJEE, Rahul. Abuse vectors: a framework for conceptualizing IoT-enabled interpersonal abuse. In: USENIX SECURITY SYMPOSIUM, 32., 2023. Proceedings [...]. Berkeley: USENIX Association, 2023. p. 69-86.

TSENG, Emily; BELLINI, Rosanna; MCDONALD, Nora; DANOS, Matan; GREENSTADT, Rachel; MCCOY, Damon; DELL, Nicola; RISTENPART, Thomas. The tools and tactics used in intimate partner surveillance: an analysis of online infidelity forums. In: USENIX SECURITY SYMPOSIUM, 29., 2020. Proceedings [...]. Berkeley: USENIX Association, 2020.

WOODLOCK, Delanie; MCKENZIE, Mandy; WESTERN, Deborah; HARRIS, Bridget. Technology as a weapon in domestic violence: responding to digital coercive control. Australian Social Work, v. 73, n. 3, p. 368-380, 2020. DOI: 10.1080/0312407X.2019.1607510.

WOODLOCK, Delanie. The abuse of technology in domestic violence and stalking. Violence Against Women, v. 23, n. 5, p. 584-602, 2017. DOI: 10.1177/1077801216646277.

¹ Universidade do Estado do Amazonas (UEA). Manaus, Amazonas, Brasil. Mestrando. ORCID: <https://orcid.org/0009-0000-7570-553X>. Lattes: <http://lattes.cnpq.br/7119459369582263>. E-mail: [acesse o artigo original para visualizar o e-mail](#).

² Universidade do Estado do Amazonas (UEA). Manaus, Amazonas, Brasil. Mestranda. ORCID: <https://orcid.org/0009-0002-4567-2719>. Lattes: <http://lattes.cnpq.br/8273109846633134>. E-mail: [acesse o artigo original para visualizar o e-mail](#).

³ Universidade do Estado do Amazonas (UEA). Manaus, Amazonas, Brasil. Mestranda. ORCID: <https://orcid.org/0009-0003-0438-1381>. Lattes: <http://lattes.cnpq.br/8596584203898728>. E-mail: [acesse o artigo original para visualizar o e-mail](#).

⁴ Universidade do Estado do Amazonas (UEA). Manaus, Amazonas, Brasil. Mestranda. ORCID: <https://orcid.org/0009-0006-9380-8384>. Lattes: <http://lattes.cnpq.br/6718522744209371>. E-mail: [acesse o artigo original para visualizar o e-mail](#).

⁵ UEA. Manaus, Amazonas, Brasil. Especialista. ORCID: <https://orcid.org/0009-0004-0088-8000>. Lattes: <http://lattes.cnpq.br/2968031807911939>. E-mail: [acesse o artigo original para visualizar o e-mail](#).