EXPONDO STALKERWARE

desafios legais e recomendações para o enfrentamento do stalkerware no Brasil

Instituto de Pesquisa em Direito & Tecnologia do Recife

UK Government

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

Expondo stalker(ware) [livro eletrônico] : desafios legais e recomendações para o enfrentamento do stalkerware no Brasil / Mariana Canto ... [et al.] ; coordenação Mariana Canto. -- 1. ed. -- Recife, PE : IP.rec, 2025.
PDF

Outros autores: Anicely Santos, Raquel Saraiva, Luana Batista, Carolina Branco, Rhaiana Valois
Bibliografia
ISBN 978-65-982630-5-8

1. Aplicativos - Programas de computador 2. Aplicativos - Software 3. Abuso de poder - Leis e legislação - Brasil 4. Direitos humanos 5. Direito (Teologia) 6. LGBTQIA - Siglas 7. Violência de gênero I. Canto, Mariana. II. Santos, Anicely. III. Saraiva, Raquel. IV. Batista, Luana. V. Branco, Carolina. VI. Valois, Rhaiana. VII. Canto, Mariana. VIII. Título.

25-310231.0 CDD-384.53

Índices para catálogo sistemático:

1. Aplicativos para celulares : Comunicações sem-fio 384.53

Maria Alice Ferreira - Bibliotecária - CRB-8/7964

FICHA TÉCNICA

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
Mariana Canto
Raquel Saraiva
Rhaiana Valois

REVISÃO ESPECIALIZADA (DIREITO PENAL)

Victor Trajano

PROJETO GRÁFICO:

Estúdio PUYA!

APOIO:

Programa de Acesso Digital da Embaixada
do Reino Unido no Brasil

COMO CITAR:

SANTOS, Anicely; BRANCO, Carolina; ARAÚJO, Luana Batista; CANTO, Mariana; SARAIVA, Raquel; VALOIS, Rhaiana. Expondo Stalker(ware): desafios legais e recomendações para o enfrentamento do stalkerware no Brasil [livro eletrônico]. Coord. Mariana Canto. Recife: IP.rec, 2025.

SUMÁRIO

SUMÁRIO EXECUTIVO 5

1. INTRODUÇÃO 8

2. FUNDAMENTAÇÃO TEÓRICA 12

3. ANÁLISE DO PANORAMA REGULATÓRIO BRASILEIRO 17

3.1. TRATADOS E NORMAS INTERNACIONAIS 18

A) CONVENÇÃO SOBRE A ELIMINAÇÃO DE TODAS AS FORMAS DE DISCRIMINAÇÃO CONTRA AS MULHERES (CEDAW) 18

B) CONVENÇÃO INTERAMERICANA DE BELÉM DO PARÁ 19

3.2. LEGISLAÇÃO NACIONAL 20

A) CÓDIGO PENAL E CÓDIGO DE PROCESSO PENAL 20

I) EVOLUÇÃO LEGISLATIVA, CRIME DE STALKING E FEMINICÍDIO 20

II) CONDUTAS CONEXAS E OUTROS CRIMES INFORMÁTICOS 24

III) DESAFIOS PROCESSUAIS E LACUNAS DO CÓDIGO DE PROCESSO PENAL 27

B) CÓDIGO DE DEFESA DO CONSUMIDOR 34

C) MARCO CIVIL DA INTERNET 37

D) LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) 38

E) ESTATUTO DA CRIANÇA E DO ADOLESCENTE (ECA) E LEI Nº 15.211/2025 40

3.3. PROPOSTAS LEGISLATIVAS EM TRAMITAÇÃO 45

A) PROJETO DE LEI Nº 0219/2024 45

B) PROJETO DE LEI Nº 126/2025 46

4. CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES 48

SUMÁRIO

Sumário Executivo

O uso de ***stalkerware*** e **aplicativos de uso duplo** emerge como uma das formas de **violência de gênero** e abuso de poder no ambiente digital, impactando de forma desproporcional mulheres, pessoas LGBTQIA+, jovens, populações racializadas e outros grupos historicamente vulnerabilizados. A fundamentação teórica desta análise demonstra que essas tecnologias operam em um espaço de sobreposição entre relações íntimas, violência doméstica e desigualdades estruturais, sendo muitas vezes justificadas sob o discurso do "amor e cuidado".

O relatório parte do entendimento de que é indispensável construir respostas que vão além da punição tradicional e do encarceramento, já que a violência mediada por tecnologia tem raízes estruturais e não pode ser reduzida a soluções imediatistas. Para sustentar essa análise, recorre-se a contribuições teóricas de pensadoras como **Lélia Gonzalez, Angela Davis e Françoise Vergès**, que abordam a violência a partir de uma perspectiva interseccional e apontam possibilidades de responsabilização alternativas. Nesse sentido, ao examinar a legislação vigente e questionar os limites do modelo penal, o estudo propõe uma abordagem mais abrangente e crítica, que considere a complexidade do fenômeno e a necessidade de estratégias que combinem responsabilização, transformação social e proteção efetiva das pessoas em situação de vulnerabilidade.

No âmbito internacional, instrumentos como a **Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres (CEDAW)** e a **Convenção Interamericana de Belém do Pará** estabelecem obrigações para os Estados signatários de proteger mulheres contra violência e discriminação em todas as suas formas. Tais tratados orientam a interpretação da legislação nacional, impondo a necessidade de políticas públicas e ações normativas que considerem a vulnerabilidade diferenciada de mulheres e grupos marginalizados frente ao problema aqui tratado.

O panorama regulatório brasileiro apresenta avanços, mas também lacunas significativas na prevenção e responsabilização do uso de softwares de vigilância. No **Código Penal e Código de Processo Penal**, a evolução legislativa inclui a tipificação do crime de perseguição (*stalking*) e a criminalização de condutas conexas, como invasão de dispositivos eletrônicos, divulgação de imagens íntimas e feminicídio. Essas normas fornecem base penal para responsabilizar indivíduos,

mas sua efetividade enfrenta desafios práticos, como por exemplo, condição de hipossuficiência ou dependência financeira das vítimas, a fragilidade da cadeia de custódia, dificuldades de produção de provas digitais, a heterogeneidade da capacidade pericial ao redor do país e a padronização excessiva de medidas protetivas que desconsideram particularidades do uso de diferentes tipos de tecnologia para fins de monitoramento e perseguição. Percebe-se ainda que as políticas criminais voltadas à proteção das mulheres tendem a focalizar os momentos mais extremos da violência, deixando em segundo plano ações estruturais de prevenção e de interrupção precoce do ciclo de agressões, antes que estas atinjam sua forma mais grave.

Na área cível, o **Código de Defesa do Consumidor (CDC)** assegura direitos à informação, segurança e reparação de danos, permitindo, em tese, a responsabilização de fornecedores de softwares de uso duplo ou de *stalkerware*. Já o **Marco Civil da Internet (MCI)** estabelece princípios de privacidade, proteção de dados e inviolabilidade da intimidade, enquanto a **Lei Geral de Proteção de Dados (LGPD)** impõe limites ao tratamento de dados pessoais, exigindo consentimento inequívoco e responsabilizando controladores e operadores de dados. Juntas, essas normas possibilitam uma abordagem preventiva e reparatória. Entretanto, a aplicação desses instrumentos enfrenta desafios estruturais significativos. A identificação dos responsáveis é dificultada pela atuação de empresas estrangeiras, cujos aplicativos podem ter servidores localizados em diferentes jurisdições. Além disso, a ausência de regulamentação específica para produtos digitais de uso duplo compromete a responsabilização efetiva de desenvolvedores e distribuidores. Na prática, as vítimas frequentemente encontram barreiras de acesso à Justiça e enfrentam a morosidade processual, enfraquecendo a efetividade da tutela civil e limitando a proteção contra violações de direitos no ambiente digital.

O **Estatuto da Criança e do Adolescente (ECA)** e a **Lei nº 15.211/2025 (“ECA Digital”)** atualizam a proteção integral de crianças e adolescentes para o ambiente digital, abordando dispositivos de supervisão parental e produtos de monitoramento infantil. Apesar das salvaguardas previstas, como relatórios de impacto, padrões de segurança compatíveis com a LGPD e avisos claros sobre rastreamento, persiste o risco de desvio de finalidade, podendo fazer com que essas ferramentas sejam utilizadas para violência doméstica, vigilância autoritária e restrição de autonomia.

Projetos legislativos estaduais e municipais, como o **PL nº 0219/2024 (Santa Catarina)** e o **PL nº 126/2025 (Rio de Janeiro)**, reforçam o caráter educativo e preventivo, criando canais de denúncia e campanhas de conscientização sobre *stalking* e *cyberstalking*. No entanto, ambos carecem de mecanismos

mais específicos no caso da utilização de ferramentas de monitoramento como o *stalkerware,* limitando sua eficácia prática frente à complexidade do fenômeno e à necessidade de proteção diferenciada para mulheres, adolescentes LGBTQIA+ e outros grupos vulneráveis.

Em síntese, o estudo evidencia que o Brasil possui fundamentos normativos consideráveis para enfrentar o uso abusivo de tecnologias de vigilância. Contudo, concentram-se em respostas no âmbito Penal, que ao contrário disso, deveria ser a *ultima ratio*. A efetividade das normas também depende de interpretação judicial evolutiva, articulação entre instrumentos legais e implementação de medidas técnicas e institucionais. A abordagem interseccional deste relatório demonstra que políticas, regulamentações e respostas jurídicas devem considerar o impacto diferenciado sobre mulheres, crianças, adolescentes pessoas racializadas, pessoas LGBTQIA+ e outras populações historicamente marginalizadas, assegurando que a proteção digital não se converta em uma forma de proteção seletiva, mas sim em um instrumento de promoção de direitos fundamentais, dignidade, autonomia, privacidade e segurança.

1

INTRODUÇÃO

As diversas formas de violência de gênero revelam, de maneira recorrente, a busca pela posse e controle em seu cerne. Essa lógica de dominação atravessa contextos sociais e culturais, adaptando-se às circunstâncias de cada época e encontrando novos meios de expressão.

Com o avanço das tecnologias digitais, surgiram novas formas de vigilância e coerção, entre as quais se destaca o *stalkerware*. Tal prática consiste no uso deliberado de softwares espiões ou aplicativos de uso duplo (desenvolvidos com fins legítimos, mas desviados em instrumentos de vigilância e controle), com a finalidade de monitorar e restringir a autonomia da vítima, frequentemente sem o seu conhecimento ou consentimento. Entre os exemplos mais recorrentes de *stalkerware*, destacam-se aplicativos que permitem rastrear a localização geográfica em tempo real, registrar chamadas telefônicas, ler mensagens privadas em aplicativos de mensageria, acessar histórico de navegação e até mesmo ativar remotamente microfones e câmeras dos dispositivos. Essas funcionalidades, embora apresentem usos legítimos em determinados contextos, como a proteção de dados corporativos ou o controle parental com consentimento, tornam-se instrumentos de violência quando empregadas para vigiar e coagir pessoas em relações abusivas.

Nesse cenário, um dos principais problemas é a ausência de mecanismos de proteção e suporte às vítimas dessa tecnologia. Diante disso, emergem duas questões fundamentais:

1)
Qual é o arcabouço jurídico atualmente disponível no Brasil para tratar do *stalkerware*?

2)
Em que medida esse conjunto normativo assegura proteção às vítimas e promove a responsabilização dos agressores?

Este terceiro relatório do projeto "*Expondo stalker(ware)*" tem como objetivo analisar as legislações nacionais existentes, examinando como podem ser aplicadas ao enfrentamento desse tipo de violência, identificando seus alcances, limitações e possíveis lacunas. Ao fazê-lo, busca-se retirar da vítima o peso da responsabilidade pelo enfrentamento do problema e direcionar o olhar para aqueles que devem ser efetivamente responsabilizados: os desenvolvedores e os usuários que se valem dessas tecnologias como instrumentos de violência.

O Brasil ainda não dispõe de uma lei específica sobre *stalkerware*. Em razão disso, a proteção jurídica tem se apoiado em dispositivos correlatos, como a Lei Carolina Dieckmann (12.737/2012), que trata de crimes informáticos, e o artigo 147-A do Código Penal, que versa sobre o crime de perseguição (*stalking*). Embora essas disposições permitam enquadrar a conduta como ilícito penal, permanecem lacunas significativas, sobretudo no que se refere à proteção efetiva das vítimas, à qualificação da escuta institucional e à responsabilização das plataformas e dos agressores.

Outro obstáculo enfrentado pela vítima está no processo de denúncia, marcado pela dificuldade de comprovar a violência. Enquanto a violência física deixa marcas visíveis, as violências psicológicas e digitais, como o *stalkerware*, permanecem menos perceptíveis, embora sejam igualmente prejudiciais. Além disso, a violência facilitada pela tecnologia raramente ocorre de forma isolada: na maioria dos casos, integra um contexto mais amplo de abuso e dependência, sobretudo financeira, o que dificulta a ruptura com o agressor, uma vez que muitas vítimas não vislumbram alternativas de sustento, abrigo e acolhimento fora do ambiente de violência.

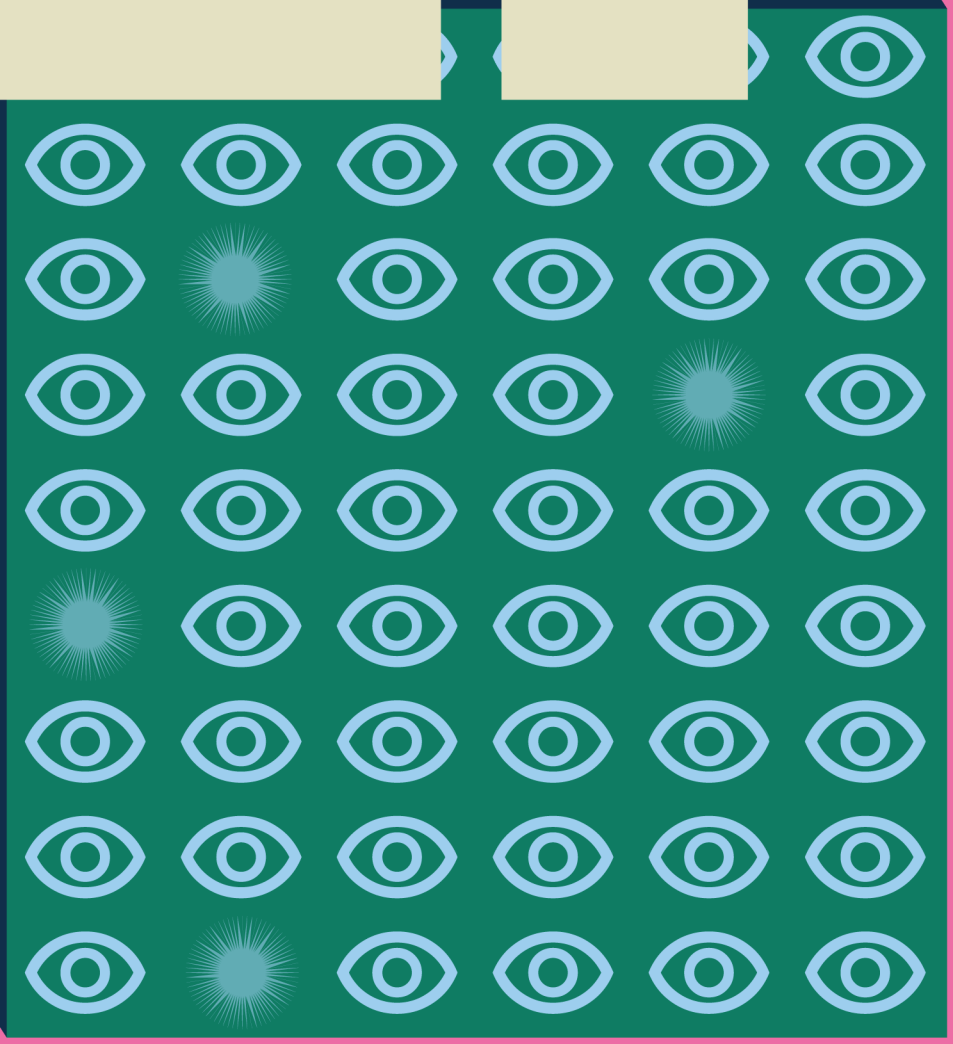
A situação se agrava para grupos historicamente marginalizados. Pessoas LGBTQIA+ e racializadas sofrem violências adicionais decorrentes do preconceito estrutural. A escassez de dados que documentem suas experiências, algo comumente presente para esses grupos, reforça a invisibilidade dessas situações e limita a formulação de respostas eficazes.

No que diz respeito à responsabilização, as empresas que desenvolvem esses aplicativos ainda operam em um ambiente de pouca regulamentação. Frequentemente, tecnologias concebidas para finalidades teoricamente legítimas são deliberadamente promovidas como ferramentas de monitoramento interpessoal, naturalizando a vigilância sob o discurso enganoso de "amor e cuidado". Paralelamente, as plataformas de redes sociais permitem a ampla difusão de propagandas, conteúdos e tutoriais que incentivem o uso abusivo desses recursos, sem nenhum tipo de cuidado com o conteúdo que está sendo veiculado e com as vítimas.

A responsabilização do agressor, por sua vez, constitui outro aspecto central, é preciso entender que o enfrentamento do problema não se esgota na via penal. Pensar em alternativas de responsabilização que ultrapassem a lógica punitivo-carcerária também é uma das abordagens discutidas neste relatório, entendendo que o problema não pode ser tratado de forma superficial. Para compreender o contexto interseccional que envolve a violência facilitada por essa tecnologia, analisamos as legislações nacionais pertinentes e consultamos autoras que tratam da perspectiva da violência interseccional e que abordam outras formas de responsabilização, como Lélia Gonzalez, Angela Davis e Françoise Vergès.

Assim, o presente relatório busca não apenas mapear o arcabouço legal disponível para o enfrentamento do *stalkerware*, mas também propor um olhar mais profundo sobre a questão da responsabilização sobre a violência de gênero facilitada pela tecnologia. Ao integrar análises interseccionais e considerar a vulnerabilidade de grupos específicos, pretendemos oferecer uma visão mais holística do problema e sugerir caminhos para uma responsabilização efetiva dos agressores.

2.



FUNDAMENTAÇÃO TEÓRICA

O *stalkerware* não é um fenômeno criminal emergente, mas sim uma continuidade de práticas de vigilância e monitoramento que sempre foram empregadas para o controle de indivíduos. Desde o século XVI, com a escravização e colonização, consolidaram-se os pilares da modernidade ocidental[1], os quais, ao se entrelaçarem com os avanços tecnológicos, reformulam antigas formas de dominação em novos aparatos de controle. As violências mediadas por tecnologia refletem não apenas atos isolados, mas são também manifestações de estruturas mais amplas, onde o neoliberalismo, o patriarcado e o colonialismo se combinam, perpetuando desigualdades e controles.

Françoise Vergès, ao afirmar que "não podemos lutar pela igualdade das mulheres sem reconhecer que elas, oprimidas como mulheres, também são oprimidas em razão de suas origens raciais e sociais"[2], destaca a interseccionalidade das opressões. Ao tratar o *stalkerware* apenas como um problema individual e genérico, negligenciamos as barreiras adicionais enfrentadas por mulheres racializadas, trans e periféricas. Essas mulheres encontram dificuldades materiais e institucionais significativas para denunciar e se proteger contra tais abusos, ficando ainda mais vulneráveis ao controle tecnológico em relações íntimas.

Pensar esta tecnologia numa perspectiva Amefricanizada[3], utilizando o conceito de Lélia Gonzales, traz a percepção que as tecnologias, inclusive aplicativos de uso duplo, frequentemente refletem e reforçam desigualdades de gênero, raça e classe. A negação inconsciente das raízes afro-indígenas encontra paralelo na maneira como soluções tecnológicas tendem a ser construídas a partir de um olhar eurocêntrico, ignorando contextos históricos e materiais específicos de mulheres diversas. Isso gera políticas e ferramentas que não respondem adequadamente às violências enfrentadas por esses grupos, perpetuando a invisibilização e a vulnerabilidade.

A noção de denegação cultural proposta por González permite compreender como o digital também pode reproduzir estruturas racistas e coloniais se não for analisado criticamente. Isso nos leva a reconhecer que a disseminação e uso desses aplicativos não afetam todas as mulheres da mesma forma, mas incidem com maior peso sobre aquelas cujas condições de vida já estão marcadas por

---

1 VERGÈS, Françoise. Uma teoria feminista da violência. São Paulo: Ubu Editora, 2021, p. 58.

2 VERGÈS, Uma teoria feminista da violência, pag. 20

3 GONZALEZ, Lélia. A categoria político-cultural de amefricanidade. Tempo Brasileiro, Rio de Janeiro, n. 92/93, p. 69-82, jan./jun. 1988.

opressões simultâneas. Nesse sentido, a amefricanidade propõe não apenas uma identidade político-cultural, mas um horizonte de resistência que coloca no centro as experiências de mulheres negras da América Latina, evidenciando a urgência de soluções tecnológicas e políticas que partam dessas realidades e fortaleçam formas alternativas de organização, como historicamente fizeram os quilombos.

A crítica de Vergès aponta que "esses fatos fazem parte da história das políticas estatais de proteção, de sua racialização e de seu sexismo"[4]. Medidas estatais contra mecanismos digitais de perseguição e violência, quando reduzidas a soluções tecnocráticas, tendem a reproduzir a mesma lógica racista e patriarcal que historicamente negou proteção real a mulheres negras, trans, indígenas e periféricas. Políticas que ignoram esse legado não apenas falham em combater a violência, mas também reforçam a exclusão e a vigilância seletiva.

A violência exercida por meio do *stalkerware* pode ser vista como uma extensão do patriarcado institucional, transformando relações afetivas em relações de dominação e inserindo a intimidade no campo da vigilância, como ressalta Vergès, "a violência é, portanto, a consequência lógica de um Estado que estruturalmente oprime as mulheres e as relega a uma posição minoritária"[5]. Esta vigilância não é apenas "doméstica", mas se conecta à mesma lógica extrativista que explora corpos e, no caso das tecnologias digitais, também explora e controla dados, reforçando desigualdades.

As soluções propostas para enfrentar as opressões intermediadas por estas tecnologias frequentemente recaem em medidas de criminalização, sem considerar que o acesso a mecanismos jurídicos e tecnológicos de proteção não é igualmente distribuído. Isso ecoa a crítica de Davis ao punitivismo, e a advertência de Vergès de que "quando a proteção está submetida a critérios raciais, de classe, de gênero e de sexualidade, ela contribui, por sua lógica e sua implementação, para a dominação"[6]. Assim, respostas baseadas apenas em leis e dispositivos de monitoramento podem não apenas falhar em proteger, mas também ampliar o alcance do controle estatal sobre populações vulnerabilizadas.

A crítica de Françoise Vergès ao feminismo carcerário oferece ferramentas para pensar os limites de respostas centradas exclusivamente na punição penal,

---

4 VERGÈS, Uma teoria feminista da violência, pág 67

5 VERGÈS, Uma teoria feminista da violência, pág. 24

6 VERGÈS, Uma teoria feminista da violência. pág. 50

como ela aponta "*o feminismo carcerário busca* "remédios sociais por meio de intervenções da justiça penal, mais do que por intermédio de um Estado social redistributivo, e defende a vida boa das pessoas privilegiadas, mais do que a autonomia das oprimidas'". [7] Confiar apenas no direito penal para enfrentar esta tecnologia pode proteger algumas mulheres, mas tende a aprofundar desigualdades para aquelas mais vulnerabilizadas. Punir apenas o agressor não rompe com a cadeia global de produção e distribuição de softwares de vigilância, que envolve desenvolvedores, distribuidores e grandes plataformas tecnológicas. A responsabilização seletiva, legitima a indústria de vigilância e normaliza a exploração econômica da violência de gênero. A prisão, como lembra Davis, funciona como "local abstrato no qual os indesejáveis são depositados, livrando-nos da responsabilidade de pensar sobre as verdadeiras questões que afligem essas comunidades"[8]. Não responsabilizar toda uma cadeia de facilitação desta vigilância violenta não trata a raiz do problema.

Para Davis, "a punição não é consequência inevitável do crime", mas parte de um projeto político e econômico vinculado ao racismo estrutural e ao lucro corporativo[9], ou seja, a indústria do *stalkerware* não pode ser tratada apenas como campo de delitos individuais, mas como engrenagem de um mercado de vigilância que expande o controle sobre corpos, especialmente corpos femininos e racializados. Por isso, Davis defende alternativas abolicionistas, que não se restrinjam a prisões ou vigilância eletrônica[10], mas que invistam em desmilitarização, educação, saúde mental, reparação e reconciliação.

Esse horizonte abolicionista aponta para soluções estruturais, como a regulação redistributiva das *big techs* e dos desenvolvedores de *spyware*, o fortalecimento de políticas públicas de educação digital feminista, de redes de apoio comunitário e de sistemas de justiça que priorizem reparação e cuidado, em vez de punição seletiva. Articular o enfrentamento não apenas ao uso individual desses aplicativos, mas ao complexo de relações capitalistas, racistas e patriarcais que sustentam sua existência.

Portanto, enfrentar o *stalkerware* exige romper com o paradigma puniti-

---

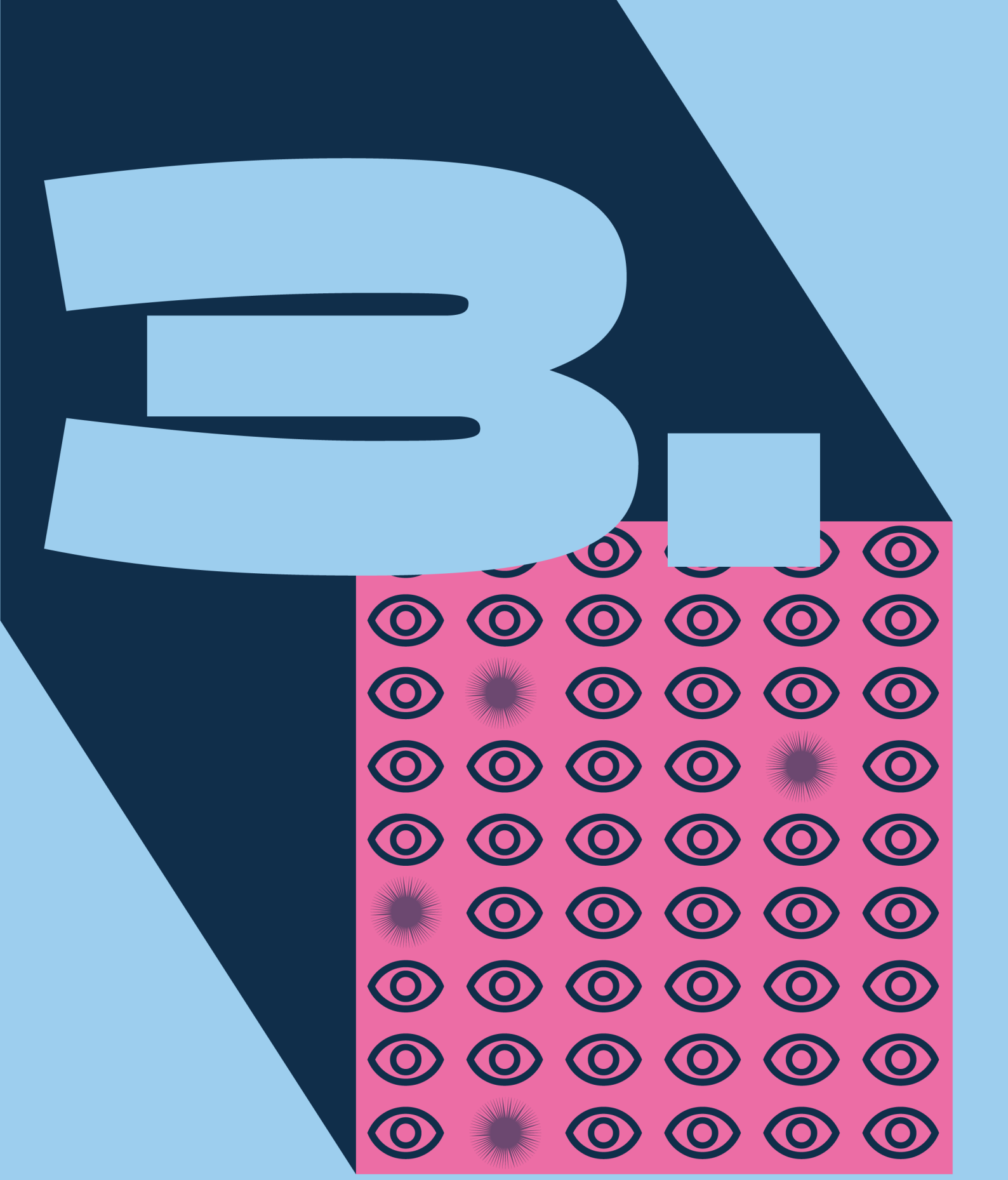
7 VERGÈS, Uma teoria feminista da violência. pag. 90-91

8 DAVIS, Angela. Estão as prisões obsoletas? Rio de Janeiro: Difel, 2018, pág. 14

9 DAVIS, Angela. Estão as prisões obsoletas? pág. 91

10 DAVIS, Angela. Estão as prisões obsoletas? pág. 88

vista e adotar uma abordagem sistêmica, responsabilizando economicamente a cadeia de produção, impondo regulação redistributiva, ampliando o acesso a tecnologias críticas e acessíveis, e investindo em campanhas de prevenção digital feminista. Assim será possível construir políticas que não marginalizem ainda mais populações vulnerabilizadas, mas que reconheçam a tecnologia como mais uma forma de violência estrutural de gênero, raça e classe, e não apenas como crime digital.



ANÁLISE DO PANORAMA REGULATÓRIO BRASILEIRO

3.1. Tratados e normas internacionais

a) Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres (CEDAW).

Adotada pela Assembleia Geral da ONU em 1979 e ratificada pelo Brasil em 1984, a CEDAW é considerada a Carta Internacional dos Direitos das Mulheres, pois impõe aos Estados signatários o dever de adotar medidas legislativas, administrativas e políticas para eliminar a discriminação contra mulheres em todas as esferas da vida. Sua abordagem é internacional e de direitos humanos, influenciando reformas internas tanto no campo penal quanto no civil, e sendo invocada como parâmetro interpretativo pelo Judiciário brasileiro.

Embora a CEDAW não trate especificamente de tecnologias digitais ou do fenômeno do *cyberstalking*, sua formulação ampla abarca condutas de violência de gênero que comprometem a igualdade material. O Comitê da CEDAW, por meio de recomendações gerais, já interpretou que a violência baseada em gênero é forma de discriminação e que os Estados têm a obrigação de preveni-la, investigá-la e punir os agressores, além de reparar as vítimas[11]. Nessa perspectiva, o *stalkerware* e a perseguição digital podem ser entendidos como novas expressões da violência de gênero, especialmente quando instrumentalizam relações de poder e controle.

No contexto brasileiro, a CEDAW reforça a necessidade de medidas estruturais que vão além do punitivismo. Isso inclui políticas públicas de educação digital, capacitação de agentes estatais para lidar com provas tecnológicas, regulação de plataformas digitais e responsabilização de empresas que se beneficiam da comercialização de ferramentas de espionagem. A Convenção também exige a superação de obstáculos institucionais, como a revitimização, a subnotificação e a naturalização da violência tecnológica.

Assim, a CEDAW funciona como norma de bloqueio e parâmetro interpretativo que amplia o alcance protetivo das leis nacionais, assegurando que violações como o *cyberstalking* sejam tratadas não apenas como delitos individuais, mas como práticas que reforçam desigualdades estruturais de gênero.

---

11 CEDAW. General recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (1992). 26 de julho de 2017. (CEDAW/C/GC/35).

b) Convenção Interamericana de Belém do Pará.

Adotada em 1994 no âmbito da Organização dos Estados Americanos (OEA) e ratificada pelo Brasil em 1995, a Convenção de Belém do Pará é o primeiro tratado internacional vinculante a reconhecer explicitamente a violência contra a mulher como violação dos direitos humanos e das liberdades fundamentais. De natureza regional e protetiva, ela impõe obrigações específicas aos Estados para prevenir, punir e erradicar a violência em seus múltiplos contextos, seja doméstico, comunitário ou perpetrado por agentes do Estado.

A redação do art. 2º da Convenção abrange qualquer "violência contra a mulher" seja a "violência física, sexual e psicológica". Essa definição ampla é plenamente aplicável às práticas de perseguição digital, que comprometem a liberdade, a privacidade e a segurança psicológica das vítimas. Assim, ainda que não mencione o ambiente virtual, o tratado pode ser interpretado para incluir formas contemporâneas de violência, como o *cyberstalking*.

No Brasil, a Convenção de Belém do Pará tem servido de fundamento para decisões judiciais que ampliam a proteção de mulheres em contextos de violência de gênero. Sua força normativa inspira legislações como a Lei Maria da Penha (Lei nº 11.340/2006), que internaliza compromissos internacionais assumidos pelo país. No campo do *cyberstalking*, a Convenção pode ser interpretada de modo a reforçar a obrigação do Estado em adotar medidas protetivas específicas para o ambiente digital, garantindo não apenas resposta punitiva, mas também políticas de prevenção, acolhimento e educação midiática.

Entretanto obstáculos podem ser identificados. Entre as barreiras à plena implementação da Convenção destacam-se: a falta de mecanismos técnicos para monitorar e punir práticas digitais de vigilância e assédio, a morosidade das respostas institucionais diante de denúncias e a persistência da naturalização da violência contra mulheres, inclusive em sua dimensão tecnológica.

Em síntese, a Convenção de Belém do Pará constitui um marco para a regionalização da proteção de gênero, obrigando o Estado brasileiro a adaptar continuamente suas políticas públicas e normas internas para responder a novas formas de violência, incluindo as digitais. Ao lado da CEDAW, funciona como alicerce para a interpretação evolutiva de que o *stalking* e o *cyberstalking* são violações graves de direitos humanos e não apenas delitos isolados.

3.2. Legislação nacional

a) Código Penal e Código de Processo Penal

i) Evolução Legislativa, Crime de Stalking e Feminicídio

Nos últimos anos, o Código Penal Brasileiro incorporou dispositivos que permitem tipificar condutas de perseguição, inclusive em contextos digitais, como o uso de *stalkerware* ou aplicativos de duplo uso. Apesar disso, a legislação apresenta lacunas significativas, especialmente diante da escalabilidade da violência de gênero e do uso de tecnologias para sua reprodução. Medidas punitivistas e individualistas, como já destacado, permanecem insuficientes para enfrentar a complexidade desse problema social.

O marco mais significativo desse processo foi a promulgação da Lei nº 14.132/2021, conhecida como "Lei do *Stalking*", que introduziu o artigo 147-A no Código Penal. O dispositivo passou a tipificar a conduta de perseguir alguém de forma reiterada e por qualquer meio, com o objetivo de ameaçar sua integridade física ou psicológica, restringir sua liberdade de locomoção ou perturbar sua esfera de liberdade e privacidade. Antes da lei, essa conduta era tratada como contravenção penal de "perturbação da tranquilidade" (art. 65 da Lei de Contravenções Penais). Com a nova lei, tornou-se crime a prática reiterada, sujeitando o autor a consequências jurídicas mais severas.

O legislador definiu o stalking como crime formal e o enquadrou como ação penal pública condicionada à representação da vítima[12]. Embora frequentemente associado à violência de gênero, mantém a natureza de crime comum, admitindo como sujeito ativo ou passivo tanto homens quanto mulheres[13]. Nos termos do § 1º desta Lei, a pena desse crime é aumentada em três hipóteses: (I) quando praticado contra criança, adolescente ou idoso; (II) quando praticado contra mulher por razões da condição de sexo feminino; e (III) quando praticado em concurso de duas ou mais pessoas ou com o emprego de arma.

Ressalte-se que, nos termos do § 2º-A do art. 121 do Código Penal (CP),

---

12 CABETTE, Eduardo Luiz Santos. Perseguição, "stalking" ou assédio por intrusão Lei nº 14.132/21. Revista Conceito Jurídico, v. 54, jun. 2021.

13 CABETTE, Eduardo Luiz Santos. Perseguição, "stalking" ou assédio por intrusão Lei nº 14.132/21. Revista Conceito Jurídico, v. 54, jun. 2021.

a expressão “razões da condição de sexo feminino” abrange tanto situações de violência doméstica e familiar quanto aquelas de menosprezo ou discriminação à condição de mulher. Embora a Lei do Feminicídio (Lei nº 13.104/2015) tenha adotado uma definição restritiva e biologizante ao caracterizar o feminicídio como o homicídio cometido “contra a mulher por razões da condição de sexo feminino”, o termo “sexo” é, conforme Normanton e Mazete Lima (2023), equivocado e ambíguo, exigindo interpretação adequada, de modo que, onde se lê “sexo”, deve-se entender “gênero”[14].

De forma mais abrangente, a Lei Maria da Penha, em seu art. 5º, assegura proteção contra a violência doméstica e familiar em contextos domésticos, familiares ou em relações íntimas de afeto, baseada no gênero, sem distinção quanto à orientação sexual ou sexo biológico da vítima. É importante notar que para a incidência do sistema protetivo dessa lei não é necessário a demonstração de uma relação duradoura de afeto, sendo a vulnerabilidade da mulher presumida nesses casos[15]. Assim, mesmo utilizando o vocábulo “sexo”, o Código Penal deve ser interpretado de modo a manter seu caráter de proteção de gênero, pois a condição de “sexo” feminino é, na realidade, uma construção social que reflete papéis historicamente atribuídos às mulheres na sociedade[16].

Nesse sentido, a jurisprudência brasileira vem progressivamente reconhecendo mulheres trans como potenciais vítimas de feminicídio, sobretudo quando presente o componente de ódio de gênero[17]. Tal interpretação encontra respaldo no Protocolo Nacional para Julgamento com Perspectiva de Gênero, utilizado como fundamento pelo Superior Tribunal de Justiça (STJ) em 2022, ao julgar o Re-

---

14 NORMANTON, Anna Catharina Machado; LIMA, Lucas Ferreira Mazete. Da aplicabilidade da Lei Maria da Penha e de normas penais de proteção às mulheres transexuais. *De Jure*, v. 21, n. 38, p. 199-228, jul.-dez. 2023. Pág. 219.

15 BRASIL. Superior Tribunal de Justiça. Sexta Turma.Processo em segredo de Justiça. Relator: Ministro Antonio Saldanha Palheiro. Julgado em: 12 ago. 2024. DJe: 15 ago. 2024. Informativo n. 824. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=0824.cod.&from=feed. Acesso em: 24 set. 2025.

16 NORMANTON, Anna Catharina Machado; LIMA, Lucas Ferreira Mazete. Da aplicabilidade da Lei Maria da Penha e de normas penais de proteção às mulheres transexuais. De Jure, v. 21, n. 38, p. 199-228, jul.-dez. 2023.

17 FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 24 set 2025. Pág. 155.

curso Especial nº 1.977.124-SP, ocasião em que se admitiu a aplicação da Lei Maria da Penha a mulheres trans[18].

Neste ano, o Supremo Tribunal Federal (STF), no Mandado de Injunção nº 7.452, reforçou essa perspectiva ao reconhecer a omissão legislativa que limitava a proteção de grupos historicamente vulneráveis[19]. Na decisão, a Corte decidiu ser possível estender medidas protetivas de urgência a mulheres trans, travestis e a casais homoafetivos masculinos, ainda que, neste último caso, a equiparação plena em ações de natureza penal não tenha sido integralmente admitida.

Ainda cabe destacar que, mesmo sem previsão específica para o *cyberstalking* na Lei de *Stalking*, a redação genérica do tipo penal, ao abranger a perseguição "por qualquer meio", permite ao Judiciário enquadrar condutas digitais. Essa amplitude, contudo, tem sido objeto de críticas. Além disso, a doutrina aponta a ausência de majorante própria para a modalidade virtual, cuja gravidade é intensificada pela facilidade de comunicação à distância, pelo anonimato do agente e pela ampla exposição de dados pessoais na Internet[20]. Isso porque, nessas circunstâncias, são frequentes práticas como a criação de perfis falsos e a difusão de informações difamatórias, capazes de comprometer a vida profissional, acadêmica, social e familiar da vítima, configurando grave afronta à dignidade humana[21].

Outro ponto sensível dessa lei é que, ao responsabilizar apenas a pessoa física que pratica a perseguição, desconsiderou atores centrais do ecossistema digital, como desenvolvedores, fabricantes e plataformas que comercializam ou permitem o uso de tecnologias de monitoramento abusivo. Essa escolha legislativa reforça uma lógica estritamente penal, voltada à tipificação de condutas e à

---

18 LUCAS, Carlos Henrique de; FEITOSA, Leonardo do Nascimento. Mulher trans mulher é! uma análise qualitativa do Recurso Especial n. 1.977.124, decisão que estabelece a aplicação da Lei Maria da Penha para o caso de mulher transexual vítima de violência doméstica e familiar. Revista CNJ, Brasília, v. 8, n. 2, p. 77–94, 2024. Disponível em: https://www.cnj.jus.br/ojs/revista-cnj/article/view/609. Acesso em: 24 set. 2025.

19 BRASIL. Supremo Tribunal Federal. STF amplia proteção da Lei Maria da Penha a casais homoafetivos do sexo masculino, travestis e transexuais. Notícias STF, 12 mar. 2025. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-amplia-protecao-da-lei-maria-da-penha-a-casais-homoafetivos-do-sexo-masculino-travestis-e-transexuais/. Acesso em: 24 set. 2025.

20 LAI, Sauvei. Sucinta análise sobre o novo crime de perseguição do art. 147-A do Código Penal – stalking. Vista do Ministério Público do Estado do Rio de Janeiro, nº 81, jul./set. 2021.

21 LAI, Sauvei. Sucinta análise sobre o novo crime de perseguição do art. 147-A do Código Penal – stalking. Vista do Ministério Público do Estado do Rio de Janeiro, nº 81, jul./set. 2021.

previsão de penas privativas de liberdade, sem propor uma resposta regulatória mais abrangente.

Do mesmo modo, houve pouco avanço quanto à criação de medidas protetivas específicas para o ambiente digital. As ordens tradicionais de afastamento, como as previstas nas alíneas “a”, “b” e “c” do inciso III do art. 22 da Lei Maria da Penha, embora aplicáveis, mostram-se insuficientes diante das formas “invisíveis” e persistentes de vigilância digital, como aquelas perpetradas por softwares espiões.

Em 2024, verificou-se um crescimento expressivo do crime de perseguição. De acordo com o Anuário Brasileiro de Segurança Pública de 2025, foram 95.026 mulheres vítimas, o que corresponde a uma média de 10 vítimas por hora no Brasil, representando um crescimento de 18,2% em relação a 2023[22]. Os dados, contudo, não detalham quais casos de *stalking* foram facilitados pelo uso de tecnologias, como *stalkerware*. O levantamento também mostra que o crime de *stalking* é marcado pela subnotificação, pois depende do reconhecimento da conduta pela vítima e sua denúncia. Em 2023, o stalking já era reconhecido como fator de risco que pode levar a prática de feminicídios, uma vez que permite, ao agressor, acumular informações sobre os hábitos da vítima, facilitando, assim, a escalada da violência[23]. Com a expansão das redes sociais, o risco é maior, de modo que práticas de *cyberstalking* podem intensificar ainda mais a possibilidade de vigilância e perseguição, ampliando os riscos para as vítimas.

Nesse cenário, ainda é fundamental observar que no país, a maioria das vítimas de feminicídio são mulheres negras (63,6%), entre 18 e 44 anos (70,5%), assassinadas dentro de casa (64,3%) por companheiros ou ex-companheiros (79,8%)[24]. Em 2024, a Lei nº 14.994/2024 transformou o feminicídio em crime

---

22 FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 24 set 2025.

23 BUENO, Samira; MARTINS, Juliana; LAGRECA, Amanda; SOBRAL, Isabela; BARROS, Betina; BRANDÃO, Juliana. O crescimento de todas as formas de violência contra a mulher em 2022. In: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 17º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, p. 136-145, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Acesso em: 24 set 2025.Pág.138.

24 FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://

autônomo, aumentando sua pena-base. Embora represente avanço em termos estatísticos para análise da evolução desse crime, a lei concentra-se no endurecimento punitivo, sem abordar medidas estruturais de prevenção nem considerar a sequência de agressões e perseguições que antecedem o crime como vetor de risco relevante no ciclo de violência[25].

ii) Condutas Conexas e Outros Crimes Informáticos

Antes da Lei de *Stalking* entrar em vigor, a Lei nº 13.772/2018, conhecida como "Lei Rose Leonel", tinha promovido alterações significativas também nesse contexto. O art. 7º, II, da Lei Maria da Penha já previa a violência psicológica como qualquer conduta capaz de causar dano emocional, reduzir a autoestima, comprometer o desenvolvimento da mulher ou restringir sua autonomia, por meio de práticas como ameaça, constrangimento, humilhação, manipulação, isolamento, vigilância constante, perseguição contumaz, insulto, chantagem, ridicularização, exploração e limitação do direito de ir e vir, entre outras formas que afetem a saúde psicológica e a autodeterminação.

Essa lei, além de criminalizar o registro não autorizado de conteúdo íntimo de nudez ou ato sexual (Art. 216-B do CP), passou a reconhecer a violação da intimidade da mulher como forma de violência psicológica e, portanto, como espécie de violência doméstica e familiar, nos termos já expostos. Assim, além de condutas como "vigilância constante", "perseguição contumaz" e, a partir dessa nova lei, a "violação da intimidade", passaram a compor um arcabouço jurídico mais robusto para enfrentar práticas de controle abusivo.

Ademais, a divulgação não autorizada de cenas de sexo, nudez ou pornografia (art. 216-B, CP), ainda que nem sempre ligada ao uso de aplicativos espiões, pode ocorrer por acessos ilícitos, sendo este crime de ação penal pública condicionada à representação. Outras condutas comumente associadas ao *cyberstalking* e à violência de gênero incluem: ameaça (art. 147, CP) e constrangimento ilegal (art. 146, CP), também condicionadas à representação; uso de falsa identidade (art. 307, CP), de ação penal pública incondicionada; e crimes contra a honra

publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 24 set 2025.

25 FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 24 set 2025.

(arts. 138 a 140, CP), de ação penal privada. Essas condutas podem evoluir ainda para práticas mais graves, com estupro (art. 213, CP), lesões corporais (art. 129, §9º, CP) ou feminicídio (art. 121, §2º, CP), todos de ação pública incondicionada[26].

Essa diferenciação entre ações penais implica que a forma de acesso à Justiça e o início do processo variam, uma vez que crimes de ação pública incondicionada são processados independentemente da vontade da vítima. Já os condicionados à representação dependem do seu requerimento e os de ação privada, por seu turno, exigem que a vítima atue diretamente para que haja persecução penal.

Contudo, importa notar que o *stalking* é um tipo penal subsidiário, de modo que não se aplica se for parte de outro crime mais grave. Dessa forma, quando a perseguição é meio para outro delito, não há crime autônomo e a conduta pode ser considerada elemento de crimes como constrangimento ilegal, homicídio, roubo, extorsão, estupro[27]. Eventualmente, essas práticas podem ser avaliadas cumulativamente ou em relação a tipos penais mais específicos, respeitando-se as regras de concurso formal e material previstas nos arts. 69 a 71 do Código Penal[28].

Outra lei relevante nesse contexto é a chamada "Lei Carolina Dieckmann" (Lei nº 12.737/2012), que introduziu no Código Penal o crime de invasão de dispositivo informático (art. 154-A). A redação atual do dispositivo, com as alterações promovidas pela Lei nº 14.155/2021, prevê pena de 1 a 4 anos de reclusão e multa. Com isso, a infração deixou de ser considerada de menor potencial ofensivo, afastando a competência dos Juizados Especiais Criminais e, por consequência, a possibilidade de suspensão condicional do processo. Ressalte-se, entretanto, que, com base no art. 41 da Lei Maria da Penha, mesmo antes dessa alteração legislativa, quando o crime era praticado no contexto de violência doméstica e familiar contra a mulher, não se aplicava a Lei nº 9.099/1995, independentemente da pena prevista. É importante observar ainda que a exigência de rompimento de mecanismos de segurança (senhas, *firewalls*, antivírus etc.) prevista no tipo penal para

---

26 CABETTE, Eduardo Luiz Santos. Perseguição, "stalking" ou assédio por intrusão Lei nº 14.132/21. Revista Conceito Jurídico, v. 54, jun. 2021.

27 MOREIRA, Rômulo de Andrade. Crime de stalking: três anos de vigência do tipo penal. Consultor Jurídico (ConJur), 5 abr. 2024. Disponível em: https://www.conjur.com.br/2024-abr-05/crime-de-stalking-tres-anos-de-vigencia-do-tipo-penal/#_ftn2. Acesso em: 24 set 2025.

28 CABETTE, Eduardo Luiz Santos. Perseguição, "stalking" ou assédio por intrusão Lei nº 14.132/21. Revista Conceito Jurídico, v. 54, jun. 2021.

configurar o crime pode tornar atípicas invasões sem barreiras técnicas, situação comum no cotidiano, já que o agressor pode ter as senhas e acesso aos dispositivos da vítima[29].

Outro ponto importante é que, apesar de não fazer menção expressa a *spywares* ou aplicativos similares, a lei alcança tanto quem invade dispositivo alheio, mediante violação de mecanismo de segurança, quanto quem comercializa ou distribui programas destinados a viabilizar a prática. Assim, em tese, não apenas usuários, mas também fabricantes e fornecedores de *stalkerware* poderiam ser responsabilizados penalmente. Dessa forma, a lei tem o mérito de romper com a responsabilização meramente individual e alcançar também os responsáveis pela cadeia de distribuição desses softwares.

Cabe salientar ainda a Lei do Sinal Vermelho (Lei nº 14.188/2021), que criou um tipo penal específico para a violência psicológica contra a mulher (art. 147-B do CP). Antes desta lei, embora a Lei Maria da Penha trouxesse a definição de violência psicológica, incrementada, conforme mencionado, pela Lei Rose Leonel, o Código Penal não dispunha de um tipo específico para enquadrar condutas que causasse dano psicológico às mulheres, muitas das quais configuravam apenas ilícitos civis[30]. Para evitar sobreposição de dispositivos legais, mesmo estando contida na definição do art. 7º, II, da Lei Maria da Penha, expressões como "vigilância constante", "perseguição contumaz" e "violação de intimidade" não foram incorporadas à tipificação da violência psicológica, pois já estão previstas no art. 147-A do CP, que trata do crime de *stalking*.

A Lei nº 15.123/2025 alterou o dispositivo em questão, aumentando a pena quando o crime for cometido usando inteligência artificial ou outro recurso tecnológico que modifique a imagem ou a voz da vítima. Vale destacar que a violência psicológica contra mulher, ao contrário do *stalking*, não exige reiteração das condutas, aplicando-se sempre que a ação não configure crime mais grave, podendo ser absorvida por este quando presente.

---

29 JUSTIÇA DE SAIA. Núcleo de Suporte à Investigação de Delitos Cibernéticos do Ministério Público de SP disponibiliza cartilha sobre a Lei Carolina Dieckmann. *Justiça de Saia*, 7 jun. 2017. Disponível em: https://www.justicadesaia.com.br/nucleo-de-suporte-a-investigacao-de-delitos-ciberneticos-disponibiliza-cartilha-sobre-a-lei-carolina-dieckmann/. Acesso em: 24 set 2025.

30 SILVA, Wagner Luís da Fonseca e. Conflitos interpretativos entre o crime de descumprimento das medidas protetivas de urgência, crime de stalking e crime de violência psicológica. Migalhas de Peso, 30 nov. 2022. Disponível em: https://www.migalhas.com.br/depeso/377863/crime-de-stalking-e-crime-de-violencia-psicologica. Acesso em: 24 set 2025.

O crime de *stalking* possui pena de 6 meses a 2 anos, aumentada pela metade quando praticado contra mulher, tornando-se mais gravoso que a violência psicológica, que de acordo com o tipo legal só é aplicável quando a vítima é uma mulher[31]. Dessa forma, em casos de atos reiterados, prevalece a tipificação pelo *stalking*, absorvendo a configuração da violência psicológica[32].

Por fim, a Lei nº 14.188/2021 também instituiu o programa "Sinal Vermelho contra a Violência Doméstica", concebido para oferecer apoio e segurança às vítimas, permitindo que o pedido de ajuda seja feito por meio de um código em forma de "X", preferencialmente desenhado na mão com tinta vermelha. Além disso, modificou o art. 12-C da Lei Maria da Penha, ampliando as hipóteses de concessão de medida protetiva de urgência. Assim, além do risco à integridade física, passou a ser contemplado igualmente o risco atual ou iminente à integridade psicológica da vítima.

iii) Desafios Processuais e Lacunas do Código de Processo Penal

No plano das medidas cautelares, o Código de Processo Penal (CPP) prevê uma caixa de ferramentas relativamente ampla (art. 319) e o magistrado tem margem para inovar. Não obstante, a aplicação prática em casos de violência digital segue uma sequência padronizada de ordens de afastamento, proibição de contato e medidas clássicas concebidas para relações físicas. Isso evidencia um problema institucional de padronização excessiva e a ausência de avaliação de risco que incorpore fatores tecnológicos. Acontece que os formulários e rotinas de avaliação não mencionam a frequência com que o agressor usa contas falsas, a criação de perfis duplicados, a utilização de terceiros para burlar bloqueios ou a presença de softwares de monitoramento ocultos.

Diante disso, ordens judiciais que proíbem "contato por qualquer meio" são teoricamente corretas, porém ineficazes quando o agressor opera por nomes fic-

---

31 SILVA, Wagner Luís da Fonseca e. Conflitos interpretativos entre o crime de descumprimento das medidas protetivas de urgência, crime de stalking e crime de violência psicológica. Migalhas de Peso, 30 nov. 2022. Disponível em: https://www.migalhas.com.br/depeso/377863/crime-de-stalking-e-crime-de-violencia-psicologica. Acesso em: 24 set 2025.

32 SILVA, Wagner Luís da Fonseca e. Conflitos interpretativos entre o crime de descumprimento das medidas protetivas de urgência, crime de stalking e crime de violência psicológica. Migalhas de Peso, 30 nov. 2022. Disponível em: https://www.migalhas.com.br/depeso/377863/crime-de-stalking-e-crime-de-violencia-psicologica. Acesso em: 24 set 2025.

tícios, perfis anônimos e aplicativos que operam por canais técnicos. A lacuna entre o que o CPP permite e o que o Judiciário efetivamente desenha materializa-se numa proteção formal que não se traduz em proteção real. Essas insuficiências também tornam inócua a sanção por descumprimento, uma vez que detectar, provar e imputar o descumprimento exige capacidade técnica e tempo que o sistema raramente dispõe.

A inclusão do art. 400-A pela Lei Mariana Ferrer (que impõe deveres de zelo à integridade física e psicológica da vítima em audiência e prevê responsabilização por atos atentatórios) é um avanço processual importante no plano simbólico e prático do trato com vítimas em juízo. No entanto, sua aplicação em casos de perseguição digital ilustra a natureza parcial dessa proteção. O Art. 400-A atua sobre o modo como o processo trata a vítima em audiências, mas não repara os problemas anteriores e paralelos: a obtenção, a preservação e a avaliação técnica das provas digitais, a formulação de medidas protetivas tecnicamente eficazes e a mitigação da sobrecarga probatória imposta à vítima. Ou seja, o art. 400-A corrige um andar do edifício processual (a audiência), mas não conserta as fundações técnicas e institucionais que permitem que o *stalkerware* prospere e que a vítima seja revitimizada antes mesmo de chegar ao palco judicial. O alcance prático do dispositivo depende, portanto, de políticas e práticas complementares que o CPP não disciplina de forma suficiente.

A Lei Maria da Penha (arts. 22 a 24), por sua vez, prevê um conjunto de medidas protetivas de urgência (MPU) para casos de violência doméstica e familiar, como a suspensão do porte de armas do agressor, o afastamento do lar, a proibição de aproximação física ou de contato por qualquer meio (inclusive redes sociais e aplicativos de mensagens), a restrição de visitas a dependentes e até a submissão a monitoramento eletrônico. Além disso, assegura instrumentos de proteção direta à vítima, como auxílio-aluguel, transferência de matrícula de filhos, restituição de bens e preservação de direitos patrimoniais.

O rol legal, também não taxativo, permite ao juiz criar ou adaptar medidas às especificidades do caso concreto e desde 2019, tais medidas podem inclusive ser concedidas pela autoridade policial (Lei nº 13.827/2019), buscando dar maior celeridade à proteção. Conforme dispõe o Informativo 836 do STJ, as MPUs têm caráter inibitório, de modo que não dependem da existência de boletim de ocorrência, inquérito policial, processo cível e criminal[33]. Apesar de serem provi-

---

33 BRASIL. Superior Tribunal de Justiça. 3ª Seção. Recursos Especiais n. 2.070.717/MG, 2.070.857/MG, 2.070.863/MG e 2.071.109/MG. Relator: Ministro Joel Ilan Paciornik. Relator

sórias, não possuem prazo de vigência e podem vigorar até o término da situação de violência. Na prática, conforme mencionado, obstáculos institucionais como a sobrecarga do sistema de Justiça, a falta de preparo de agentes, padronização das medidas de proteção, limitadas ao que prevê a lei, e a demora na efetivação das ordens revelem que o tempo de resposta muitas vezes não é suficiente para evitar desfechos fatais[34].

Em julho de 2025, o Tribunal de Justiça de Pernambuco (TJPE) lançou uma ferramenta, chamada "Medida Protetiva Eletrônica", permitindo que mulheres vítimas de violência doméstica solicitem medidas protetivas de urgência (MPUs) diretamente pela Internet, sem necessidade de comparecer pessoalmente a delegacias ou ao Judiciário[35]. A plataforma oferece um formulário, no qual é possível relatar o ocorrido e anexar evidências, sem a necessidade de ir a uma delegacia. Após o envio, o processo é automaticamente instaurado e, dependendo da gravidade, a medida protetiva pode ser deferida imediatamente.

A Lei nº 13.641/2018, por sua vez, criminalizou o descumprimento das medidas (art. 24-A), reconhecendo sua gravidade. No entanto, dados sugerem que, o afastamento do agressor tem caráter apenas momentâneo, sem alterar as condições sociais e econômicas que sustentam a violência[36]. A análise das medidas concedidas também tem evidenciado uma atuação do Judiciário limitada a soluções uniformes e baseadas no distanciamento entre autor e vítima[37]. O reconheci-

---

para acórdão: Ministro Rogerio Schietti Cruz. Julgado em: 13 nov. 2024. Recurso Repetitivo – Tema 1249. Informativo n. 836. Disponível em: http://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=0836.cod.&from=feed. Acesso em: 24 set 2025.

34 FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 24 set 2025.

35 TRIBUNAL DE JUSTIÇA DE PERNAMBUCO. TJPE lança ferramenta que agiliza proteção à mulher vítima de violência doméstica. Portal TJPE, 21 jul. 2025. Disponível em: https://portal.tjpe.jus.br/-/tjpe-lan%C3%A7a-ferramenta-que-agiliza-prote%C3%A7%C3%A3o-%C3%A0-mulher-v%C3%ADtima-de-viol%C3%AAncia-dom%C3%A9stica%C2%A0. Acesso em: 25 set. 2025.

36 FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 24 set 2025.

37 FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 24 set 2025.

mento efetivo do direito à proteção também costuma depender da capacidade da vítima de denunciar, algo que também pode ser limitado ou até inviável diante de barreiras de acesso à Justiça[38].

Há, ademais, um efeito perverso de institucionalização da resposta punitiva no rito. A tendência a escalonar medidas punitivas como resposta principal. Quando o ordenamento dispõe da prisão preventiva (art. 312) ou de sanções penais para descumprimento de medida protetiva, a aplicação imediata da lógica punitiva parece oferecer uma solução objetiva. Contudo, no espaço digital essa lógica colide com limitações de detectabilidade e com o caráter fluido da prova. A consequência acaba sendo o processo penal se colocando como mecanismo de resposta predominante, sem, no entanto, oferecer instrumentos processuais de prevenção e monitoramento que reduzam a reincidência.

Nesse sentido, a centralização da responsabilização individual é estruturalmente ineficaz para oferecer a proteção material que as vítimas perseguem e pode agravar seu sofrimento ao obrigá-las a múltiplos relatos e exposições. Essa crítica ao motor punitivo do processo não se trata de negar a utilidade da responsabilização, mas de reconhecer que o processo penal, se não acompanhado de instrumentos processuais técnicos, de políticas administrativas e de medidas protetivas tecnológicas, opera como paliativo ineficiente.

Além disso, as informações do relatório revelam limites críticos da efetividade dessas medidas. Somente em 2024 foram registrados 101.656 descumprimentos de MPU (alta de 10,8% em relação a 2023), além de ao menos 121 mulheres assassinadas entre 2023 e 2024 enquanto estavam sob medida protetiva ativa[39]. Esse cenário reforça o diagnóstico de Lagarde (2024), citado no relatório, que interpreta o feminicídio também como uma forma de violência estatal por omissão e negligência, já que o aparato institucional não assegura a proteção prometida[40]

---

38 FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 24 set 2025.

39 FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 24 set 2025.

40 LAGARDE, Marcela y de los Ríos. Del femicidio al feminicidio. Desde el jardín de Freud. Bogotá, 2006 apud *In*: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 24 set 2025.

e que, nesse contexto, também pode ser ampliado para abarcar os vários tipos de violências facilitadas pelo uso de tecnologias.

Outro ponto sensível em relação ao crime de perseguição diz respeito à produção de provas. A demonstração da conduta reiterada por meio de *stalkerware* exige perícias técnicas, análise de registros digitais, coleta de dados sensíveis e observância da cadeia de custódia, com procedimentos caros, complexos e muitas vezes inacessíveis às vítimas. O cenário se agrava diante da postura de certas empresas desenvolvedoras, que podem impor barreiras técnicas ou jurídicas à disponibilização de informações essenciais à investigação, além de um ônus probatório desproporcional a quem sofre a violência. A delimitação da conduta típica também permanece problemática, já que o uso esporádico de ferramentas de vigilância pode ser considerado atípico, a depender da interpretação judicial, o que fragiliza ainda mais a proteção conferida às vítimas[41].

O CPP foi desenhado num tempo em que a prova era majoritariamente material, localizada e relativamente estável, o dispositivo que comanda a ação imediata da polícia, o art. 6º, continua a sublinhar esse imaginário: "logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá atuar para apreender objetos e colher as provas úteis ao esclarecimento do fato". Em teoria, essa cláusula confere ao aparelho estatal o dever de proteção probatória desde o primeiro contato com a vítima. Na prática, quando a violência se dá por meio de softwares de vigilância instalados em dispositivos e espalhados por nuvens e infraestruturas transnacionais, a execução desse dever encontra obstáculos técnicos, institucionais e normativos que transformam a formalidade do dever em inefetividade real. Apesar do dever expresso no art. 6º, o aparato público frequentemente não dispõe de protocolos operacionais, kits técnicos nem rotinas administrativas para impedir que provas digitais sejam alteradas ou perdidas desde o primeiro momento do contato com a vítima. Isso força a vítima a agir (capturas de tela, backups, encaminhamento de logs) e, assim, a assumir um papel investigativo que deveria caber ao estado, aumentando seu risco e sua exposição.

A centralidade do exame pericial no CPP (arts. 158 e seguintes) também reforça outro ponto crítico que é o paradigma do corpo de delito como "vestígio" privilegiado não se traduz com facilidade para as características voláteis de um

---

41 JUSTIÇA DE SAIA. Núcleo de Suporte à Investigação de Delitos Cibernéticos do Ministério Público de SP disponibiliza cartilha sobre a Lei Carolina Dieckmann. Justiça de Saia, 7 jun. 2017. Disponível em: https://www.justicadesaia.com.br/nucleo-de-suporte-a-investigacao-de-delitos-ciberneticos-disponibiliza-cartilha-sobre-a-lei-carolina-dieckmann/. Acesso em: 24 set 2025.

sistema digital. O art. 158 reafirma a indispensabilidade do exame quando há vestígios. Contudo, o que constitui "vestígio" em um ambiente de *stalkerware* é um problema técnico profundo. Logs, artefatos em memória, backups na nuvem, metadados de serviços e evidências de comunicação são extremamente perecíveis e exigem técnicas especializadas e de aquisição forense de imagem *bit* a *bit* para garantir integridade e auditabilidade.

Os regramentos periciais do CPP não explicitam procedimentos mínimos de preservação, nem disciplinam formalmente a priorização de medidas voltadas à prova digital emergente. Em um cenário ideal, o procedimento previsto no CPP deveria remeter a protocolos técnicos padronizados (imagem forense, sumarização de hashes, fluxo auditável de custódia), mas hoje tais procedimentos dependem, em larga medida, da existência de laboratórios periciais bem estruturados e de agentes com formação específica. Esses recursos são escassos nas delegacias e regiões mais vulneráveis do país, resultando em uma heterogeneidade dessa capacidade pericial pelo Brasil e a ausência de protocolos nacionais uniformes, o que amplifica o risco de invalidação probatória ou impugnação técnico-jurídica.

A busca e apreensão, regulada pelo art. 240 do CPP, consagra modalidades clássicas (domiciliar, pessoal) e enumera objetos dignos de apreensão. No entanto, a materialidade do "objeto" é hoje frequentemente intangível: credenciais, backups em servidores estrangeiros, sessões autenticadas e logs distribuídos por provedores. O ordinário mandado de busca dirigido a um endereço físico não é, por si só, suficiente para capturar a totalidade da prova técnica, e a jurisprudência ainda oscila sobre limites e requisitos para ordens que atinjam provedores de nuvem e serviços transnacionais.

Essa lacuna operacional tem consequências práticas imediatas: ordens tardias ou mal direcionadas significam perda de dados voláteis, destruição de vestígios durante tentativas precipitadas de remoção do *stalkerware* pela própria vítima, e a necessária cooperação de fornecedores que, muitas vezes, têm sede fora do Brasil ou políticas internas pouco transparentes. O Marco Civil da Internet e a LGPD estabelecem princípios e limites para o tratamento de dados e para as responsabilidades de provedores, mas não substituem a necessidade de instrumentos processuais céleres e técnicos de preservação e entrega de provas. Consequentemente, existe um hiato entre o alcance jurisdicional do magistrado e a arquitetura técnica que abriga a prova.

Nesse contexto, a fragilidade da cadeia de custódia merece ainda atenção detalhada. Em provas digitais, cadeia de custódia não é apenas um expediente formal, e sim um conjunto de operações técnicas que garantem a identicidade e

integridade do vestígio. Na ausência de uma regulação processual que imponha protocolos mínimos e formas de registro padronizado aceitas por tribunais, torna-se fácil que provas cruciais sejam questionadas por questões técnicas, contaminando a prova e revitimizando a pessoa que já sofreu a invasão. O resultado prático é trágico: vítimas que deixam de denunciar por temer o ônus probatório, processos que não prosperam por fragilidades técnicas, e uma sensação generalizada de impotência institucional.

A dependência de cooperação internacional e de empresas privadas é outro traço que o CPP não enfraquece, porque não o trata. Quando evidências estão armazenadas fora do território nacional, o acesso passa por canais de cooperação jurídica internacional, instrumentos morosos que raramente atendem à urgência de preservação de prova volátil. Ademais, provedores privados podem oferecer retenção temporária mediante ordens de preservação, mas as rotinas de atendimento variam e nem sempre há canais claros e acessíveis para delegacias. O resultado prático é que o Estado depende de terceiros sem um arcabouço processual eficaz para impor prazos, selar material, exigir produção técnica com cadeia de custódia e obter logs completos. O Marco Civil e a LGPD desenham princípios e deveres de tratamento, mas, na prática investigativa, faltam mecanismos de emergência processual que integrem a ordem judicial e a resposta técnica do provedor de maneira padronizada e auditável.

No Protocolo para Julgamento com Perspectiva de Gênero mencionado, mesmo não tratando expressamente do *cyberstalking*, são oferecidas orientações relevantes ao abordar essa questão, como a valorização da palavra da vítima. O documento também enfatiza que os atos persecutórios devem ser analisados em sua natureza reiterada e contextualizada, pois condutas isoladas podem parecer inofensivas, mas, inseridas em um histórico de violência, revelam perseguição[42]. O Protocolo também valoriza a dimensão simbólica e psicológica da violência, reconhecendo que, mesmo sem ameaças explícitas, a vigilância constante gera forte impacto emocional[43].

---

42 BRASIL. Protocolo para julgamento com perspectiva de gênero. Brasília: Conselho Nacional de Justiça (CNJ); Escola Nacional de Formação e Aperfeiçoamento de Magistrados (Enfam), 2021. Disponível em: https://www.cnj.jus.br/programas-e-acoes/protocolo-para-julgamento-com-perspectiva-de-genero/. Acesso em: 24 set 2025.

43 BRASIL. Protocolo para julgamento com perspectiva de gênero. Brasília: Conselho Nacional de Justiça (CNJ); Escola Nacional de Formação e Aperfeiçoamento de Magistrados (Enfam), 2021. Disponível em: https://www.cnj.jus.br/programas-e-acoes/protocolo-para-julgamento-com-

No caso do *stalkerware*, tais parâmetros são especialmente úteis. Já que indica que Judiciário deve considerar as dificuldades probatórias, valorizando o relato da vítima, e alertando para o risco de revitimização em situações de perseguição intermitente, nas quais o agressor alterna períodos de afastamento e retomada[44]. Instrumentos como o Formulário Nacional de Avaliação de Risco, mencionado no documento, poderiam igualmente auxiliar na identificação do caráter sistemático da perseguição digital.

Portanto, o que se verifica, nessa análise, é que, ainda que existam iniciativas importantes, as políticas criminais de proteção às mulheres parecem estar concentradas no ápice da violência, relegando a segundo plano medidas estruturais de prevenção e mitigação que atuem sobre o ciclo contínuo de agressões antes que alcance seu estágio mais grave.

b) Código de Defesa do Consumidor

O Código de Defesa do Consumidor (Lei nº 8.078/1990) é o principal marco normativo da proteção dos consumidores no Brasil. Estruturado em torno de uma abordagem civilista e protetiva, ele assegura direitos fundamentais nas relações de consumo, impondo deveres de informação, segurança e reparação de danos por parte de fornecedores de bens e serviços. Embora concebido em um contexto pré-digital, sua redação ampla permite sua aplicação a produtos e serviços virtuais, incluindo aplicativos e *softwares*.

O CDC reconhece, no art. 6º, III e VI, como direitos básicos do consumidor a informação adequada e clara sobre os produtos e serviços e a efetiva prevenção e reparação de danos patrimoniais e morais. Esses dispositivos se conectam diretamente com a problemática do monitoramento abusivo, uma vez que a omissão de alertas sobre riscos potenciais, ou a comercialização de aplicativos que possibilitam espionagem sem transparência suficiente, pode configurar violação do dever de informação.

---

perspectiva-de-genero/. Acesso em: 24 set 2025.

44 BRASIL. Protocolo para julgamento com perspectiva de gênero. Brasília: Conselho Nacional de Justiça (CNJ); Escola Nacional de Formação e Aperfeiçoamento de Magistrados (Enfam), 2021. Disponível em: https://www.cnj.jus.br/programas-e-acoes/protocolo-para-julgamento-com-perspectiva-de-genero/. Acesso em: 24 set 2025.

Do mesmo modo, os arts. 8º a 10 estabelecem a responsabilidade do fornecedor quanto à segurança dos produtos e serviços. Produtos não podem ser colocados no mercado se acarretarem riscos à saúde ou segurança além dos "normais e previsíveis" em decorrência de sua natureza. Para tecnologias digitais, esse dispositivo exige interpretação adaptada: aplicativos que possam ser convertidos em ferramentas de vigilância não podem ser disponibilizados sem a devida advertência quanto à sua periculosidade. Se o fornecedor tem ciência, ou deveria ter, da possibilidade de uso abusivo, é obrigado a informar os consumidores e adotar medidas preventivas, sob pena de responsabilização.

A lógica do CDC é a da responsabilidade objetiva do fornecedor, prevista no art. 12, segundo a qual fabricantes, importadores e desenvolvedores respondem independentemente de culpa por danos causados por defeitos de projeto, fabricação, apresentação ou por informações insuficientes ou inadequadas sobre o uso e os riscos do produto. Isso implica que empresas que distribuem ou comercializam *stalkerware* podem ser responsabilizadas, mesmo que não tenham participado ativamente do ato persecutório praticado por terceiros.

Outro aspecto relevante é a disciplina contratual. O art. 51 declara nulas cláusulas que busquem exonerar ou atenuar a responsabilidade do fornecedor por vícios ou defeitos, o que invalida, por exemplo, termos de uso que tentem excluir a responsabilidade de empresas por falhas de segurança ou por usos abusivos previsíveis de seus produtos. O art. 54, por sua vez, exige que contratos de adesão sejam redigidos de forma clara e legível, reforçando o dever de transparência e evitando que riscos tecnológicos sejam mascarados em cláusulas obscuras.

Apesar dessas previsões, a aplicação do CDC em casos de vigilância digital enfrenta obstáculos estruturais. Um dos principais desafios está na identificação dos responsáveis, já que muitos aplicativos de *stalkerware* estão sediados fora do Brasil e utilizam servidores em múltiplas jurisdições. O nosso segundo relatório do projeto *Expondo Stalkerware*[45] aponta que empresas desse setor frequentemente escolhem países como o Chipre para estabelecer suas sedes, justamente por apresentarem legislações mais flexíveis e suscetíveis a brechas regulatórias. Em 2023, por exemplo, verificou-se que a aplicação dos controles de exportação da União Europeia pelo Chipre revelou evidências de má administração, conforme observado pelo Comitê de Inquérito do Parlamento Europeu sobre o uso do Pega-

45 SANTOS, Anicely; BRANCO, Carolina; ARAÚJO, Luana Batista; CANTO, Mariana; SARAIVA, Raquel; VALOIS, Rhaiana. Expondo stalker(ware): uma análise discursiva e técnica do ecossistema de stalkerware no Brasil [livro eletrônico]. Coord. Mariana Canto. Recife: IP.rec, 2025.

sus e de *spyware* equivalente[46]. Esse cenário torna certos países particularmente atrativos para a instalação de empresas de tecnologias de vigilância e serviços correlatos, já que normas menos rígidas sobre exportação acabam fragilizando a proteção de direitos humanos, sobretudo no caso de softwares classificados como de uso "dual", como é o caso do spyware.

Em segundo lugar, a caracterização do dolo ou da negligência em omissões informativas nem sempre é simples, sobretudo quando o fornecedor alega que seu produto tem "uso legítimo" e que eventuais abusos são responsabilidade exclusiva do usuário. As lacunas regulatórias específicas para produtos digitais de uso duplo ainda dificultam a responsabilização efetiva, já que a legislação foi concebida em um contexto que não previa riscos digitais complexos. Na prática, isso significa que consumidores lesados por tecnologias de espionagem muitas vezes enfrentam barreiras de acesso à Justiça e morosidade processual, o que enfraquece a efetividade da tutela civil. Além disso, a regulação de softwares e aplicativos é dependente de iniciativas complementares do Judiciário ou de órgãos administrativos, como o Procon e a Senacon.

Ainda assim, a redação ampla do CDC permite interpretações evolutivas. O princípio da vulnerabilidade do consumidor, reconhecido pelo art. 4º, assegura que eventuais dúvidas interpretativas sejam solucionadas em favor da parte mais frágil na relação de consumo. Isso abre espaço para que o Judiciário responsabilize desenvolvedores e plataformas de forma solidária, considerando que, em casos de *stalkerware*, a falha na prevenção de riscos não é apenas um vício técnico, mas também uma violação grave da dignidade, privacidade e segurança dos consumidores.

Em síntese, embora o Código de Defesa do Consumidor não trate diretamente de perseguição ou espionagem digital, sua aplicação analógica e principiológica representa um caminho relevante para enfrentar o problema. Ao deslocar a responsabilidade também para fornecedores e intermediários do ecossistema tecnológico, o CDC contribui para romper com a lógica estritamente penal e individualista, apontando para uma regulação mais abrangente que reconhece a centralidade das empresas na prevenção de danos em contextos digitais.

---

46 UNIÃO EUROPEIA. Parlamento Europeu**.** *Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware.* Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware. Rapporteur: Sophie in 't Veld. Bruxelas: Parlamento Europeu, 22 de maio de 2023. (2022/2077(INI)). Disponível em https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html Acesso em 02 de outubro de 2025.

c) Marco Civil da Internet

O Marco Civil da Internet (Lei nº 12.965/2014) consolidou-se como a "Constituição da Internet" no Brasil, ao estabelecer princípios, direitos e deveres para o uso da rede. Sua abordagem é civilista, mas com desdobramentos relevantes também nas esferas administrativa e penal, sobretudo na proteção da privacidade, neutralidade de rede e tratamento de dados pessoais. Embora não trate de maneira direta do fenômeno do *stalkerware*, a redação aberta de seus dispositivos permite enquadrar práticas de monitoramento abusivo como violações a direitos fundamentais dos usuários, criando hipóteses de responsabilização civil e administrativa para desenvolvedores, fornecedores e até mesmo usuários dessas tecnologias.

O art. 3º do MCI define como princípios do uso da Internet a proteção da privacidade (inciso II) e a proteção dos dados pessoais (inciso III), fundamentos que são diretamente comprometidos pelo uso de *stalkerwares* e aplicativos de duplo uso. Já o art. 7º reconhece o acesso à Internet como essencial ao exercício da cidadania e garante ao usuário a inviolabilidade da intimidade e da vida privada, a proteção contra fornecimento indevido de seus dados pessoais e o sigilo das comunicações digitais. Assim, quando um software é utilizado para rastrear ou espionar atividades digitais sem consentimento, ocorre violação direta desses direitos, passível de indenização por danos materiais e morais.

O art. 10 reforça essa proteção ao condicionar a guarda e disponibilização de registros digitais à preservação da intimidade e da vida privada, enquanto o art. 11 estabelece a obrigatoriedade de observância da legislação brasileira em qualquer operação de coleta ou armazenamento de dados pessoais realizada em território nacional, ainda que por provedores estrangeiros. Isso significa que empresas estrangeiras que comercializam ou disponibilizam aplicativos de espionagem a usuários no Brasil estão, em tese, submetidas ao MCI e podem ser responsabilizadas judicialmente.

No entanto, a efetividade dessa proteção enfrenta obstáculos práticos significativos. Entre eles, destacam-se: (i) a ausência de regulamentação específica para aplicativos de uso duplo, que dificulta distinguir funções tidas como legítimas de monitoramento parental ou corporativo de práticas abusivas de espionagem íntima; (ii) a limitação da jurisdição brasileira diante de empresas sediadas no exterior, com servidores em países que não cooperam judicialmente; e (iii) a falta de fiscalização técnica sobre funcionalidades ocultas de aplicativos, que permanecem disponíveis em lojas virtuais mesmo quando violam direitos fundamentais.

Em situações de *stalkerware*, as vítimas dependem não apenas da respon-

sabilização dos indivíduos que praticam a perseguição, mas também da imputação de deveres mais claros a desenvolvedores e distribuidores de aplicativos. O MCI, ao lado da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), poderia servir de base para ampliar esse alcance, já que ambos tratam da privacidade e do tratamento adequado de dados pessoais como direitos fundamentais. Contudo, sem mecanismos normativos mais rígidos essa realidade ainda parece estar longe de ser alcançada.

Em síntese, embora o Marco Civil da Internet não tipifique crimes nem estabeleça sanções penais para o uso de tecnologias de espionagem, ele se consolida como instrumento fundamental para afirmar o direito à privacidade e ao sigilo das comunicações na era digital. Sua articulação com outros diplomas legais, como o CDC e a LGPD, possibilita construir uma tutela civil e administrativa mais robusta contra o *cyberstalking*, deslocando parte da responsabilidade para os agentes econômicos que estruturam o ecossistema tecnológico e permitindo respostas jurídicas mais adequadas às novas formas de violência digital.

d) Lei Geral de Proteção de Dados (LGPD)

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), estabeleceu no Brasil um regime normativo específico para o tratamento de dados pessoais, aplicável a pessoas físicas ou jurídicas, públicas ou privadas. Inspirada em legislações internacionais, como o Regulamento Europeu de Proteção de Dados (GDPR), a LGPD possui caráter essencialmente civilista e preventivo, mas também prevê sanções administrativas relevantes, com impactos diretos sobre a atividade de empresas que coletam, processam ou armazenam informações pessoais.

A lógica central da LGPD é garantir que o tratamento de dados respeite a privacidade, liberdade e segurança dos titulares, impondo aos agentes de tratamento o dever de observar princípios como finalidade, necessidade, adequação, transparência, segurança e prevenção (art. 6º). Nesse contexto, o uso de *stalkerware* ou outros aplicativos de vigilância se insere como prática claramente irregular ou ilícita, pois envolve coleta e monitoramento de dados pessoais sem consentimento válido, violando a finalidade original do tratamento e expondo os titulares a riscos desproporcionais.

O art. 7º da LGPD condiciona o tratamento de dados à presença de hipóteses legais, sendo a principal delas o consentimento livre, informado e inequívoco do titular. Aplicativos espiões, no entanto, funcionam muitas vezes em modo ocul-

to, impossibilitando a manifestação de vontade do usuário, o que os torna incompatíveis com a legislação. Ademais, o art. 8º reforça que consentimento obtido mediante vício (coação, erro, ocultação) é inválido, tornando irregular a coleta silenciosa típica desses softwares.

A responsabilização civil é prevista nos arts. 42 a 44. Dessa forma, o controlador ou operador que, no exercício de suas atividades, causar dano patrimonial, moral, individual ou coletivo, responde pela reparação, independentemente de culpa, sempre que o tratamento for irregular ou não oferecer a segurança que o titular razoavelmente espera. Isso permite imputar responsabilidade não apenas aos usuários que instalam o *stalkerware*, mas também aos desenvolvedores e distribuidores, quando deixam de adotar salvaguardas técnicas e jurídicas para impedir usos abusivos.

Apesar dessa base normativa robusta, a aplicação da LGPD enfrenta desafios práticos importantes: (i) a dificuldade de comprovar a inexistência de consentimento em contextos de aplicativos ocultos, o que transfere à vítima um ônus probatório desproporcional; (ii) a presença de empresas estrangeiras, que frequentemente escapam da jurisdição brasileira, ainda que seus serviços sejam ofertados a cidadãos nacionais; e (iii) a ausência de mecanismos claros de responsabilização solidária entre desenvolvedores e distribuidores, o que fragiliza a proteção do usuário diante da fragmentação da cadeia de fornecimento.

Esses obstáculos revelam a necessidade de aprimoramento regulatório pela Autoridade Nacional de Proteção de Dados (ANPD). Entre as recomendações apontadas por esse relatório, destacam-se: (i) regulamentar expressamente o tratamento de dados por aplicativos de vigilância e rastreamento, exigindo transparência técnica e jurídica; (ii) proibir o funcionamento de *softwares* que operem sem consentimento explícito e verificável do titular; (iii) exigir Relatórios de Impacto à Proteção de Dados (RIPD) para aplicativos de controle parental, monitoramento e geolocalização; (iv) definir, por resolução, regras de consentimento destacado para dados sensíveis ou de crianças; e (v) prever sanções específicas para aplicativos de uso duplo que sejam utilizados para fins de espionagem ou abuso.

Em conclusão, a LGPD representa um instrumento jurídico fundamental para enfrentar as práticas de *cyberstalking* e o uso de *stalkerware*, não apenas como questão de privacidade, mas também como violação de direitos fundamentais à dignidade, liberdade e segurança pessoal. Ao lado do CDC e do Marco Civil da Internet, a LGPD desloca parte da responsabilidade para os agentes econômicos que estruturam o ecossistema digital, permitindo uma resposta mais preventiva e abrangente frente às novas formas de violência tecnológica.

e) Estatuto da Criança e do Adolescente (ECA) e Lei nº 15.211/2025

O Estatuto da Criança e do Adolescente (ECA), promulgado em 1990, consolidou uma mudança paradigmática no ordenamento jurídico brasileiro. Inspirado nos princípios constitucionais da proteção integral e da prioridade absoluta, o Estatuto rompeu com a tradição tutelar que tratava crianças e adolescentes como objetos de intervenção estatal e inaugurou um regime de reconhecimento desses sujeitos como indivíduos dotados de direitos fundamentais próprios. Essa transformação histórica reposicionou a infância e a adolescência no centro da agenda normativa: não mais como categorias subordinadas, mas como pessoas em desenvolvimento, merecedoras de tutela jurídica específica, que articula garantias de autonomia progressiva e de proteção contra abusos.

Passadas mais de três décadas desde sua promulgação, o ECA enfrenta um cenário social e tecnológico radicalmente distinto daquele em que foi concebido. Se nos anos 1990 a preocupação regulatória estava centrada em formas tradicionais de violência, negligência e exploração, hoje emergem novas modalidades de risco associadas à cultura digital: exposição massiva em redes sociais, processos de adultização mediados pela internet, circulação de imagens íntimas e, de maneira crescente, vigilância tecnológica sobre a vida cotidiana de crianças e adolescentes. Esses fenômenos tensionam os dispositivos do Estatuto, colocando à prova sua capacidade de assegurar a proteção integral no ambiente digital.

É nesse contexto que se insere a discussão sobre o *stalkerware*, sendo necessário avaliar como o Estatuto, em sua estrutura normativa, responde - ou falha em responder - às formas de controle e monitoramento que marcam a contemporaneidade. Um dos achados centrais da pesquisa foi justamente a recorrência do "controle parental" como justificativa para a existência e a comercialização de softwares de monitoramento. Sob o discurso da proteção, esses aplicativos oferecem vigilância em tempo real sobre a vida digital de crianças e adolescentes, muitas vezes de forma oculta e intrusiva. Essa ambiguidade entre cuidado e violação desafia diretamente a finalidade do ECA, que busca equilibrar proteção e autonomia progressiva, sempre a partir da compreensão da criança como sujeito de direitos.

Os dispositivos do Estatuto permitem uma leitura crítica desse fenômeno. O art. 5º estabelece a proibição de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punindo toda ação ou omissão que viole direitos fundamentais. O art. 17 garante a inviolabilidade da integridade física, psíquica e moral, incluindo a preservação da imagem, da identidade, da autonomia e dos espaços pessoais, dimensões gravemente atingidas quando o monitoramento digital se converte em vigilância abusiva. O art. 18 reforça o dever

coletivo de velar pela dignidade, afastando tratamentos desumanos, vexatórios ou constrangedores, categoria na qual práticas de controle invisível por *stalkerware* podem ser enquadradas.

Outros dispositivos também oferecem pontos de apoio. O art. 70 atribui a todos o dever de prevenir ameaças ou violações de direitos, enquanto o art. 71 assegura que produtos e serviços destinados a crianças respeitem sua condição peculiar de desenvolvimento. Esse último artigo é particularmente relevante diante de aplicativos de "controle parental" que, ao serem desenhados sem salvaguardas contra abusos, podem contribuir para a adultização precoce e a supressão da privacidade infantojuvenil. Do ponto de vista penal, o art. 232 tipifica como crime submeter criança ou adolescente a vexame ou constrangimento, o que pode ser aplicado a situações em que o monitoramento se torna forma de intimidação ou violência psicológica. Já o art. 241-A responsabiliza indivíduos e prestadores de serviço envolvidos na circulação ou armazenamento de material pornográfico infantil, o que convida à reflexão sobre o dever de empresas digitais de impedir que seus produtos sejam instrumentalizados em práticas ilícitas contra menores, a exemplo do acesso irrestrito e não notificado da câmera do celular que é fornecido por essas ferramentas.

A análise regulatória evidencia, portanto, que o ECA dispõe de fundamentos principiológicos robustos para coibir práticas de vigilância abusiva, mas carece de previsões específicas que o tornem efetivo diante da sofisticação tecnológica atual. A ausência de normas expressas sobre softwares de monitoramento deixa a aplicação dependente de interpretações judiciais e da atuação de conselhos tutelares e Ministério Público, sem instrumentos técnicos para identificar *stalkerware*, preservar provas digitais ou responsabilizar empresas de tecnologia.

O que está em questão, portanto, não é apenas a ausência de menção expressa a tecnologias como o *stalkerware*, mas o risco de que a finalidade histórica do Estatuto seja esvaziada se não for reinterpretada e atualizada para enfrentar o ambiente digital. O eixo do ECA sempre foi garantir que a proteção não se converta em opressão, que o cuidado não se traduza em vigilância e que a criança não seja tratada como objeto, mas como sujeito de direitos. Quando práticas de monitoramento excessivo ou abusivo são normalizadas, mesmo sob o discurso de proteção, a coerência normativa do Estatuto é colocada em xeque.

Assim, a análise regulatória do ECA à luz dos desafios contemporâneos demonstra tanto sua potência quanto suas limitações. Potência, porque dispõe de princípios robustos (dignidade, autonomia, respeito à imagem e à integridade) capazes de fundamentar respostas jurídicas contra formas de vigilância abusiva.

Limitações, porque não oferece instrumentos técnicos nem previsões específicas para enfrentar os riscos digitais. A consequência é uma dependência de interpretações judiciais e de esforços institucionais fragmentados, que muitas vezes não conseguem acompanhar a sofisticação tecnológica das práticas abusivas.

Diante dos riscos e problemas apresentados, foi sancionado neste ano o PL 2628/2022, resultando na Lei nº 15.211/2025, apelidada de "ECA Digital". A nova lei estabelece um marco regulatório para a proteção de crianças e adolescentes no ambiente digital, articulando direitos fundamentais como acesso à informação, melhor interesse, autonomia progressiva e segurança. Também impõe deveres às empresas fornecedoras de produtos e serviços digitais, atribui responsabilidades aos pais e responsáveis e prevê medidas voltadas à transparência, à prevenção de abusos e à promoção da educação digital.

Entre as inovações normativas, destacam-se duas categorias diretamente relacionadas ao uso de *stalkerware* e aplicativos de uso duplo: (i) os "mecanismos de supervisão parental" (art. 2º, parágrafo único, VIII), definidos como salvaguardas embutidas nos próprios serviços digitais para controle de conteúdo, tempo de uso e tratamento de dados; e (ii) os "produtos ou serviços de monitoramento infantil" (art. 2º, parágrafo único, II), destinados ao registro e transmissão de informações sobre a atividade da criança ou adolescente. Enquanto os primeiros estão sujeitos a regras mais amplas, incluindo relatórios de impacto, padrões de segurança compatíveis com a LGPD e medidas de transparência, os segundos concentram-se em requisitos mínimos, como a inviolabilidade das informações e a observância ao princípio do melhor interesse da criança.

Apesar dos avanços, é necessário reconhecer os riscos associados ao desvio de finalidade desses mecanismos mencionados na lei. Em primeiro lugar, porque ferramentas de supervisão parental e aplicativos de monitoramento infantil podem ser apropriados para a vigilância entre parceiros e ex-parceiros, perpetuando ciclos de violência doméstica e de gênero. Ainda que de forma não intencional, a lei prevê salvaguardas importantes nesse sentido.

O inciso III do caput do art. 17, por exemplo, estabelece o dever dos fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e a adolescentes ou de acesso provável de exibir aviso claro e visível quando as ferramentas de supervisão parental estiverem em vigor e quais configurações ou controles foram aplicadas. O § 4º, VI, por sua vez, prevê que os mecanismos de supervisão parental devem conter configurações padrão com o mais alto nível de proteção, incluindo restrições ao compartilhamento de geolocalização e avisos claros sobre rastreamento.

Já em relação aos produtos de monitoramento infantil, o art. 19, §1º determina que as crianças e adolescentes sejam informadas, em linguagem adequada, acerca da realização do monitoramento. Essas disposições ao evitar a vigilância oculta sobre os jovens, que poderia prejudicar a relação de confiança e diálogo entre pais e filhos, também é importante para coibir o uso indevido desses recursos para a perseguição de parceiros íntimos por meio dessas ferramentas.

Embora tais dispositivos tenham relevância, é necessário avançar, como defendem Angelika Strohmayer, Rosanna Bellin e Julia Slupska, na incorporação de análises que considerem os impactos físicos, emocionais e sociais das tecnologias, sobretudo sobre mulheres, pessoas negras, LGBTQIA+, imigrantes e pessoas com deficiência[47]. Softwares desenvolvidos com finalidades legítimas podem ser facilmente apropriados para práticas de vigilância, exploração e abuso, em especial no âmbito de relações íntimas. Nesse sentido, como já ressaltado no relatório anterior[48], a avaliação da abusabilidade das ferramentas é fundamental, tanto para antecipar quanto para mitigar riscos de uso indevido, promovendo uma abordagem mais ética e responsável.

Apesar da lei prever o respeito aos direitos fundamentais desses indivíduos, o respeito ao seu melhor interesse e ao desenvolvimento progressivo, é preciso ressaltar ainda que esses aplicativos podem reforçar práticas parentais disfuncionais, sobretudo em contextos autoritários contra meninas e indivíduos LGBTQIA+. Isso pode resultar em vigilância excessiva, restrição da autonomia e até mesmo a inclusão de barreiras para a busca de ajuda por jovens que sofrem algum tipo de violência, especialmente diante do fato de que grande parte das violências sofridas por crianças e adolescentes ocorre no próprio espaço doméstico[49].

---

47 STROHMAYER, Angelika; BELLINI, Rosanna; SLUPSKA, Julia. Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm From Security to Safety. 2022. Disponível em: https://www.rosiebellini.com/wp-content/uploads/2022/09/safety.pdf. Acesso em: 24 set. 2025.

48 SANTOS, Anicely; BRANCO, Carolina; ARAÚJO, Luana Batista; CANTO, Mariana; SARAIVA, Raquel; VALOIS, Rhaiana. Expondo stalker(ware): uma análise discursiva e técnica do ecossistema de stalkerware no Brasil [livro eletrônico]. Coord. Mariana Canto. Recife: IP.rec, 2025.

49 TEMER, Luciana. Violência sexual infantil: aumentaram os casos ou as denúncias. In: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 17º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, p. 204-213, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/08/anuario-2023-texto-10-violencia-sexual-infantil-aumentaram-os-casos-ou-as-denuncias.pdf. Acesso em: 24 set. 2025.

Além disso, diante da realidade dos aplicativos já disponíveis nas principais lojas de aplicativos no Brasil, destacada no relatório anterior[50], chama atenção a ausência de referência expressa à LGPD e de garantias técnicas mais robustas na seção destinada aos serviços de monitoramento infantil, ainda que uma interpretação sistemática da lei e do ordenamento jurídico brasileiro, garanta o uso do mais alto nível de proteção e de medidas de proteção inclusive para esses aplicativos.

A lei, em seu art. 40, também determina que os fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e adolescentes no País, ou de provável acesso por eles, mantenham representante legal no Brasil, com poderes para receber comunicações oficiais e responder perante órgãos do Executivo, do Judiciário e do Ministério Público. Trata-se de uma importante exigência, pois assegura que empresas estrangeiras que ofereçam produtos ao público infantil brasileiro, estejam igualmente sujeitas às normas nacionais e possam ser responsabilizadas por eventuais violações.

Por fim, cabe destacar que, por tratar de tema urgente, foi vetado o dispositivo que previa *vacatio legis* de doze meses. O governo anunciou, portanto, que editará Medida Provisória para reduzir o prazo das obrigações operacionais e procedimentais para seis meses, antecipando assim o tempo para que as empresas se adequem às novas exigências estabelecidas pela lei[51].

---

50 SANTOS, Anicely; BRANCO, Carolina; ARAÚJO, Luana Batista; CANTO, Mariana; SARAIVA, Raquel; VALOIS, Rhaiana. Expondo stalker(ware): uma análise discursiva e técnica do ecossistema de stalkerware no Brasil [livro eletrônico]. Coord. Mariana Canto. Recife: IP.rec, 2025.

51 BRASIL. Lula sanciona lei que protege crianças na internet e anuncia medidas para ampliar concorrência e infraestrutura digital. Agência Planalto, 17 set. 2025. Disponível em: https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2025/09/lula-sanciona-lei-que-protege-criancas-na-internet-e-anuncia-medidas-para-ampliar-concorrencia-e-infraestrutura-digital. Acesso em: 29 set. 2025.

3.3. Propostas legislativas em tramitação

A pesquisa legislativa sobre *stalkerware* revelou apenas dois projetos de lei com alguma relação ao tema, ambos de caráter indireto. Essa constatação, por si só, já constitui um achado importante: a ausência de proposições normativas específicas evidencia a pouca atenção do legislador ao fenômeno do uso de softwares de vigilância em contextos de violência digital e doméstica. Embora o *stalkerware* seja um problema crescente, no Brasil as respostas regulatórias permanecem incipientes e, quando existem, concentram-se em medidas educativas de sensibilização.

Ambos os projetos concentram-se em medidas de natureza civilista e administrativa, voltadas à conscientização, prevenção e acolhimento de vítimas, sem introduzir mecanismos regulatórios capazes de enfrentar o uso de softwares de vigilância. Essa opção legislativa revela, por um lado, a importância atribuída ao caráter pedagógico das campanhas públicas, fundamentais para difundir conhecimento, estimular denúncias e legitimar a percepção do *stalking* e do *cyberstalking*, por exemplo, como formas de violência. Por outro lado, evidencia também as limitações de iniciativas desse tipo, que não abordam as dimensões técnicas, jurídicas e de responsabilização necessárias para lidar adequadamente com a problemática do *stalkerware*.

O resultado é um quadro normativo fragmentado e insuficiente: há reconhecimento do problema, mas não há medidas concretas voltadas à definição legal de softwares de vigilância, à responsabilização de desenvolvedores, distribuidores e usuários, nem à criação de protocolos de cooperação entre entes públicos e empresas de tecnologia. Além disso, tanto no nível estadual quanto no municipal, a implementação das medidas previstas depende de estruturas de segurança pública que já enfrentam sobrecarga e restrições de competência, o que pode dificultar a efetividade prática das iniciativas.

a) Projeto de Lei nº 0219/2024

O Projeto de Lei nº 0219/2024 institui, em âmbito estadual de Santa Catarina, o Programa de Combate ao Crime de Perseguição (“SOS *Stalking*”), bem como a Semana Estadual de Conscientização e Combate ao Crime de Perseguição. O texto prevê ações de prevenção, conscientização, criação de canais de denúncia e fortalecimento da Polícia Civil Virtual, além de medidas gerais de proteção às vítimas. A proposta, de natureza civilista e administrativa, enquadra o crime de

perseguição nos termos do art. 147-A do Código Penal, referindo-se a perseguição "por qualquer meio", o que pode abranger condutas praticadas com o auxílio de aplicativos de monitoramento, embora não haja menção expressa a *stalkerware* ou a softwares de vigilância.

Um dos pontos centrais do PL é a criação de canais digitais de denúncia, sob responsabilidade da Secretaria de Estado da Segurança Pública, que deverá disponibilizar portal e atendimento virtual. Contudo, o texto não detalha recursos tecnológicos, protocolos de capacitação específica ou mecanismos técnicos para a identificação e contenção de *stalkerware*. Na prática, a proposição amplia as possibilidades formais de denúncia, mas não enfrenta as dificuldades operacionais que costumam marcar a investigação desse tipo de crime, como a coleta e a preservação de provas digitais ou a articulação com provedores de serviços online.

O PL nº 0219/2024 representa um avanço simbólico, pois reconhece a importância de canais acessíveis e da sensibilização social, entretanto, permanece limitado por não propor instrumentos para capacitação de agentes públicos em perícia digital, por exemplo. O fortalecimento da Polícia Civil Virtual, mencionado no texto, depende de detalhamento normativo e de investimento financeiro, sob pena de se restringir a uma diretriz programática sem eficácia prática. Em última instância, trata-se de um projeto com potencial de ampliar a visibilidade do problema, mas que não atinge a complexidade do uso de softwares de vigilância como ferramenta de perseguição.

b) Projeto de Lei nº 126/2025

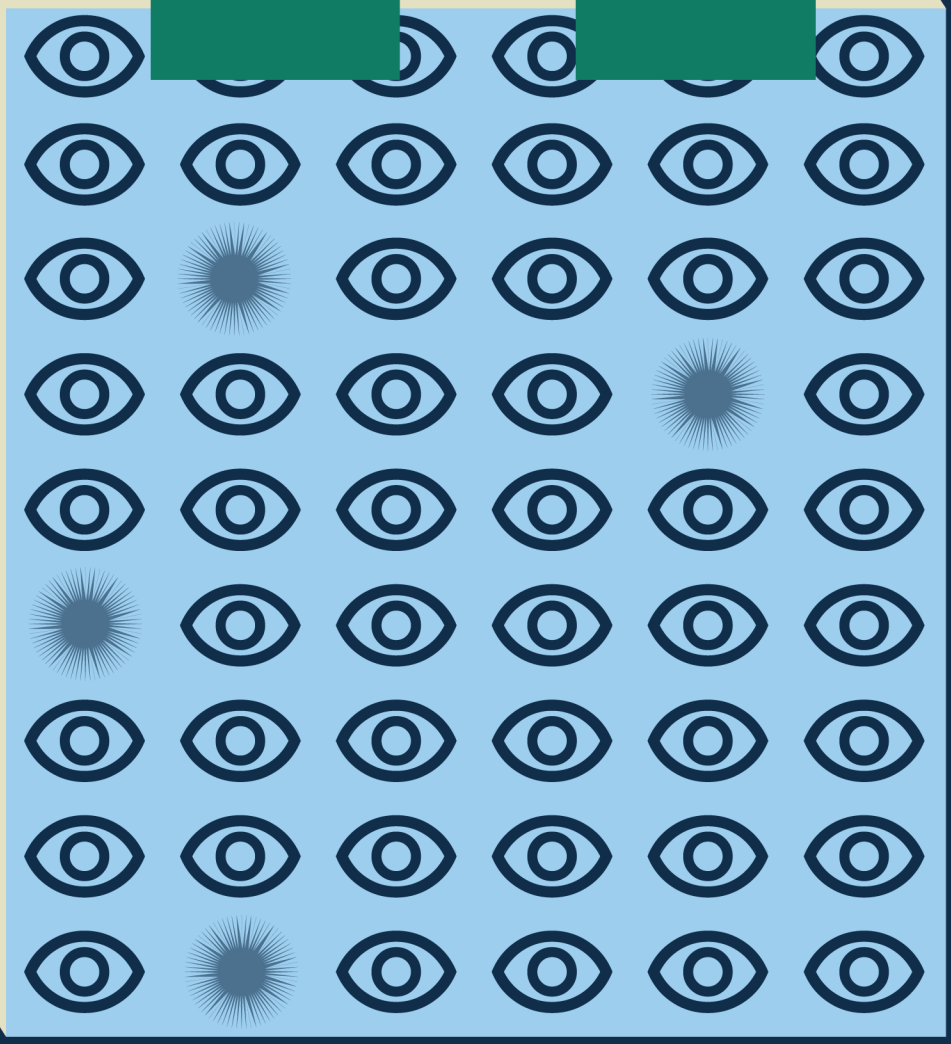
O Projeto de Lei nº 126/2025, da câmara municipal do Rio de Janeiro, institui a Campanha de Mobilização, Conscientização e Prevenção aos Crimes de Perseguição (*stalking* e *cyberstalking*) contra mulheres, também com enfoque civilista e administrativo. A iniciativa busca promover ações de caráter educativo e mobilizador, dirigidas especificamente à violência de gênero, com ênfase no reconhecimento da perseguição virtual como forma de violação de direitos.

Embora mencione o *cyberstalking*, o projeto não apresenta definições jurídicas ou técnicas sobre *stalkerware*, nem prevê instrumentos para identificar ou lidar com softwares de uso malicioso. Diferentemente do PL do tópico anterior, tampouco cria canais digitais de denúncia, restringindo-se a campanhas de mobilização e conscientização. A execução é atribuída genericamente ao Poder Público municipal, sem detalhamento de órgãos responsáveis, instrumentos de fiscalização ou previsão orçamentária.

O mérito do projeto está em reconhecer explicitamente a dimensão de gênero do problema, destacando as mulheres como principais vítimas. Campanhas desse tipo têm potencial de ampliar a percepção social sobre a gravidade do *cyberstalking* e incentivar denúncias. Contudo, o alcance prático da proposta é reduzido. Sem articulação com as instâncias de investigação criminal, que competem, em regra, à esfera estadual e federal, e sem previsão de medidas de proteção imediata, a campanha corre o risco de permanecer no plano simbólico. Além disso, a ausência de protocolos técnicos e de previsão de recursos compromete sua sustentabilidade e eficácia.

Assim, o PL nº 126/2025 reforça a importância da abordagem educativa, mas deixa em aberto a necessidade de iniciativas legislativas mais robustas, que contemplem tanto o fortalecimento institucional quanto a responsabilização de agentes envolvidos no desenvolvimento e uso de softwares de vigilância.

4.



CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

O uso de *stalkerware* e aplicativos de uso duplo evidencia uma forma de violência de gênero que se sobrepõe a relações íntimas, estruturas sociais e desigualdades históricas. Apesar dos avanços legislativos no Brasil, incluindo tipificação penal do *stalking*, proteção civil pelo CDC, princípios do Marco Civil da Internet e normas da LGPD, bem como dispositivos do ECA, e agora também o chamado "ECA Digital", a efetividade das respostas jurídicas ainda enfrenta desafios significativos. Entre eles, destacam-se a fragilidade da cadeia de custódia em provas digitais, a dificuldade de responsabilização de desenvolvedores e fornecedores dessas ferramentas e a tendência das políticas criminais de focar nos momentos mais extremos da violência, deixando lacunas na prevenção e na interrupção precoce do ciclo de agressões.

A análise interseccional deste relatório demonstra que mulheres, adolescentes, pessoas LGBTQIA+ e grupos racializados são desproporcionalmente afetados, exigindo que a proteção digital seja orientada pela dignidade, autonomia, privacidade e segurança de todas as pessoas, sem discriminação ou seletividade. Diante desse panorama, recomenda-se a implementação de políticas públicas e medidas institucionais mais robustas e integradas. Nesse contexto, destacam-se:

(i) **Regulamentar expressamente aplicativos de monitoramento**, responsabilizando desenvolvedores e distribuidores, com a proibição da criação, comercialização, aquisição e utilização de programas e dispositivos que viabilizem o monitoramento não autorizado de pessoas, incluindo *stalkerware* e outras tecnologias capazes de invadir a privacidade, monitorar atividades online e offline, comunicações e localização geográfica;

(ii) **Exigir Relatórios de Impacto à Proteção de Dados (RIPD)** para aplicativos de monitoramento e ferramentas de supervisão infantil , de modo a avaliar caso a caso o uso dessas ferramentas, assegurando a vedação daquelas que sejam utilizadas com o desvio de sua finalidade. Os relatórios devem ainda verificar a aplicação das salvaguardas previstas na legislação, incluindo a exibição de avisos claros, visíveis e periódicos sobre o monitoramento em vigor;

(iii) **Estabelecer obrigação legal para que lojas de aplicativos e intermediários online** fiscalizem, removam e impeçam a circulação de *stalkerware*, incluindo a realização de varreduras periódicas, a notificação de usuários que tenham instalado aplicativos proibidos e a adoção de mecanismos de *recall* público com vistas à proteção de potenciais vítimas;

(iv) **Tornar obrigatório o dever de cuidado** de desenvolvedores, produtores e fornecedores de tecnologia, prevendo sanções financeiras em caso de descumprimento e a criação de incentivos para estimular o cumprimento adequado. A avaliação da potencial abusabilidade das ferramentas deve ser realizada de forma contínua, permitindo a identificação precoce e a mitigação de riscos de uso indevido;

(v) **Fortalecer canais de denúncia** acessíveis, linhas de ajuda emergencial, e plataformas de denúncia seguras e confidenciais e **capacitação de autoridades** policiais, judiciais e periciais em práticas de *cyberstalking.* Recomenda-se também a **criação de protocolos processuais** padronizados e auditáveis para preservação de provas digitais, garantindo cadeia de custódia segura e evitando revitimização;

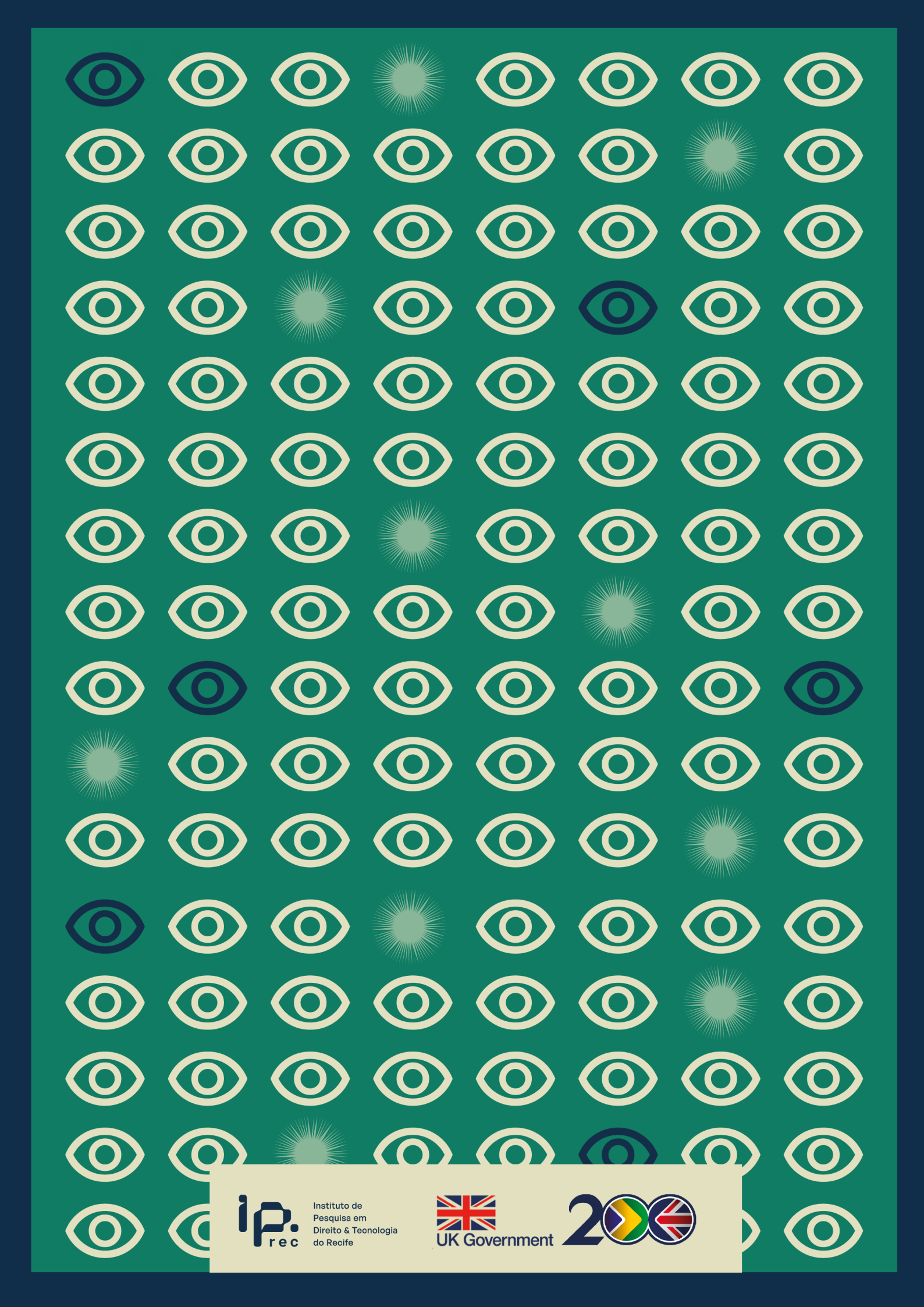
(vi) **Estabelecer mecanismos de apoio direto às vítimas,** incluindo atendimento psicológico especializado, orientação jurídica gratuita, serviços de mediação e acompanhamento durante todo o processo investigativo e judicial;

(vii) **Incorporar perspectivas interseccionais em todas as políticas e protocolos,** reconhecendo a vulnerabilidade diferenciada de mulheres, adolescentes, pessoas racializadas, pessoas LGBTQIA+ e outros grupos historicamente marginalizados;

(viii) **Priorizar medidas preventivas e educativas,** promovendo campanhas de conscientização sobre riscos digitais e estratégias de proteção pessoal, de modo a interromper precocemente o ciclo de violência antes que alcance seu estágio mais grave.

(ix) **Oferecer subsídios** a centros de pesquisa independentes e instituições acadêmicas de modo a fomentar estudos que investiguem o impacto de tecnologias de vigilância e monitoramento no Brasil, com atenção especial a mulheres, crianças, adolescentes, pessoas racializadas, pessoas LGBTQIA+ e outros grupos historicamente marginalizados.

A implementação coordenada dessas recomendações pode consolidar uma abordagem preventiva e efetiva, garantindo que instrumentos legais não apenas coíbam abusos, mas se tornem ferramentas concretas de proteção no ambiente digital, com atenção especial à diversidade e à vulnerabilidade diferenciada de grupos específicos.



Instituto de Pesquisa em Direito & Tecnologia do Recife

UK Government