UNIVERSIDADE DE SÃO PAULO - FACULDADE DE DIREITO

BARBARA NICOLE LIMA ORIHUELA

IMPLICAÇÕES PENAIS DO *STALKERWARE*: A TECNOLOGIA COMO FACILITADORA DA VIOLÊNCIA DE GÊNERO

São Paulo

2024

UNIVERSIDADE DE SÃO PAULO - FACULDADE DE DIREITO

BARBARA NICOLE LIMA ORIHUELA

IMPLICAÇÕES PENAIS DO *STALKERWARE*: A TECNOLOGIA COMO FACILITADORA DA VIOLÊNCIA DE GÊNERO

Trabalho de Conclusão de Curso ("Tese de Láurea") apresentado à Faculdade de Direito da Universidade de São Paulo como requisito parcial para obtenção do título de bacharel em Direito

Orientadora: Prof. Associada Mariângela Gama de Magalhães Gomes

São Paulo

2024

AGRADECIMENTOS

Nesse encerramento de ciclo, eu não poderia deixar de agradecer à minha família, que sempre me estimulou a buscar uma melhor versão de mim mesma e a nunca parar de sonhar, mesmo que às custas de adiar ou sacrificar os seus próprios sonhos. Aos meus pais Luciana e José Enrique, que sempre acreditaram em mim, sou extremamente grata pela entrega diária e pelo apoio incondicional durante essa jornada, seja com palavras doces, seja com necessários choques de realidade. Ao meu irmão Patrick, muito obrigada por ser uma escuta ativa e oferecer palavras de incentivo ao longo desse processo.

Em segundo lugar, agradeço enormemente pela orientação dada pela Professora Mariângela Gama de Magalhães Gomes, por ter contribuído enormemente à condução da presente Tese de Láurea, com imperiosos *insights* sobre o tema, e por ser um exemplo de professora e pesquisadora.

Da mesma forma, sou extremamente grata à Faculdade de Direito da Universidade de São Paulo, a qual assegurou, não só um ensino gratuito de altíssima qualidade, mas também inúmeras oportunidades de crescimento profissional e acadêmico, como a participação em extensões (GPEIA, DJ e Arcadas), o programa PITES, o intercâmbio acadêmico na Alemanha e as experiências de estágio. Assim, eu me despeço da Sanfran já saudosa, com a esperança de que a Faculdade prossiga com mudanças institucionais em prol da inclusão e da diversidade.

Igualmente, não poderia deixar de agradecer aos amigos que a Faculdade de Direito me proporcionou, em especial a Arthur, Larissa, Nadia, Paulo e Vinicios, com os quais tive a sorte de compartilhar esse sonho maior. Mais do que companhias para estudo e risadas, são pessoas que foram meus pilares de apoio e de conforto no Largo e com quem espero sempre criar novas memórias. Às amigas de escola, obrigada pelo eterno acolhimento e pela preocupação ao longo desse processo.

Por fim, dirijo meus agradecimentos a todos os professores e educadores, tanto da minha trajetória escolar como universitária. Ao longo de todos esses anos, tive a oportunidade de aprender com mestres excelentes, cujos ensinamentos permitiram que eu chegasse até aqui.

RESUMO

Dada a crescente informatização da sociedade e a infiltração diária dos avanços tecnológicos no cotidiano, a concretização da violência de gênero assume inevitavelmente um componente tecnológico. Assim, no âmbito da *technology-facilitated violence*, a presente pesquisa pretende compreender o fenômeno do *stalkerware*, bem como suas implicações penais. Nesse sentido, devido à ausência de jurisprudência consolidada e à intersecção entre os marcos da violência de gênero, da cibercriminalidade e do *stalking*, objetivou-se debater a natureza do bem jurídico a ser tutelado e o regime jurídico-penal aplicável a essa prática no Brasil, assim como os desafios de sua persecução penal. Ao fim, concluiu-se como tipificação que o *stalkerware*, enquanto expressão de *cyberstalking*, representaria perseguição (crime-fim) mediante a invasão de dispositivo informático (crime-meio), razão pela qual é viável a aplicação do princípio da consunção, sob uma perspectiva de direito penal mínimo.

Palavras-chave: *stalkerware*; *technology-facilitated violence; cyberstalking*; invasão de dispositivo informático; princípio da consunção.

ABSTRACT

In light of the increasing digitalization of society and the daily infiltration of technological advances into everyday life, the embodiment of gender-based violence inevitably incorporates a technological component. Thus, in the context of technology-facilitated violence, this research aims to comprehend the phenomenon of stalkerware, as well as its criminal implications. Due to the absence of consolidated case law and the intersection between the frameworks of gender violence, cybercrime and stalking, it was proposed to debate about the legal good to be protected and the criminal arrangements applicable to this practice in Brazil, as well as the challenges of its criminal persecution. Finally it was concluded that stalkerware, as an expression of cyberstalking, represents stalking (an end crime) through the invasion of a computing device (a means crime), and therefore it is viable to apply the principle of absorption, from a minimum criminal law perspective.

Keywords: stalkerware; technology-facilitated violence; cyberstalking; invasion of computing device, criminal implications; principle of absorption.

SUMÁRIO

INTRODUÇÃO

Em vista da informatização crescente da sociedade e da infiltração diária dos avanços digitais no cotidiano, a violência de gênero inevitavelmente incorpora um componente tecnológico. Uma vez que a tecnologia, longe de ser neutra, reproduz e impõe padrões de poder, é inconteste o emprego de ferramentas cibernéticas na perpetuação de desigualdades. Centrando-se precipuamente sobre o reflexo negativo do meio virtual sobre a dinâmica de gênero, o *stalkerware*, como uma das expressões do *cyberstalking*, inova como forma de controle e de vigilância das vítimas mediante a instalação de aplicativos espiões, originalmente com finalidades lícitas, em aparelhos eletrônicos.

Mais do que um dos pontos de intersecção entre violência de gênero e tecnologia, a ameaça do *stalkerware* consiste em um dos reflexos de uma sociedade gradativamente informatizada, que, ao distorcer as funcionalidades originais dos meios cibernéticos e cometer ilícitos, enseja uma especialização do direito penal tradicional, sendo outros meios de controle social, como as restrições pelos desenvolvedores do *software*, aparentemente ineficazes.

Tratando-se de fenômeno que perpassaria, a princípio, pela violência digital de gênero, pela cibercriminalidade e pelo *stalking*, compreender as particularidades do fenômeno do *stalkerware*, bem como seu regime jurídico adequado, exigiria um estudo aprofundado dessas três violências que se relacionam entre si, cujas características potencialmente coincidiriam com as do *stalkerware*. Sob um recorte brasileiro, ante a novidade do uso de aplicativos espiões, subsistem incertezas quanto ao tipo penal que atenderia simultaneamente aos interesses da proteção à violência de gênero e das peculiaridades específicas do *stalkerware*, dada a falta de jurisprudência consolidada e maiores produções no assunto. A partir dessa perspectiva, ante o papel da tecnologia como facilitadora da violência de gênero, consiste em enfoque principal da presente pesquisa debater as implicações penais do *stalkerware*. Ou seja, pretende-se averiguar qual representaria uma resposta criminal adequada com base nos tipos penais existentes e quais seriam os desafios de sua persecução penal.

Essencial, para tanto, delimitar o bem jurídico a ser protegido, tendo em vista o seu papel como parâmetro de proibição e limitador da intervenção penal, uma vez que restringe a criminalização apenas a comportamentos verdadeiramente gravosos a valores sociais fundamentais. A princípio, com base na conduta do *stalkerware*, depreende-se que o bem jurídico tutelado coincidiria com a proteção do tipo incriminador do *stalking*, pois o crime de perseguição, disposto no art. 147-A do Código Penal, contemplaria a finalidade da prática do

stalkerware, ainda que abranja outros meios de execução. Sob um prisma preliminar, por outro lado, o delito da invasão de dispositivo informático, instituído no art. 154-A do Código Penal pela Lei nº 12.737/2012, apresentaria peculiaridades compatíveis com o fenômeno em questão, de modo que representaria um meio para a prática do crime.

Com base em análise preambular da relação entre os dois tipos penais, propõe-se que o *stalkerware* consistiria em um *stalking* mediante a invasão de dispositivo informático, tendo em vista que a perseguição reiterada de alguém "por qualquer meio" abarca o meio da invasão. Em termos técnicos, diante de uma potencial relação de crime-fim e crime-meio, há de se verificar a viabilidade da aplicação do princípio da consunção, a qual, exigindo uma análise *in concreto*, propõe a absorção do crime-meio pelo crime-fim e limita a condenação ao tipo penal mais abrangente. Para tanto, analisa-se se a forma de persecução penal apresentada se adequa aos avanços tecnológicos na esfera criminal e à tutela do bem jurídico atacado pelo *stalkerware*. Em prol desse propósito, é desejável o contato com as respostas jurídicas estrangeiras no âmbito penal, tradicionalmente com doutrina e jurisprudência mais desenvolvidas acerca desse delito cibernético.

A favor de uma proposta de criminalização ao *stalkerware*, é imperioso que a determinação de qualquer resposta criminal se conforme com o princípio do direito penal mínimo, visto que, partindo da proteção do bem jurídico como pressuposto norteador do regime jurídico penal, a atividade legislativa deve ser limitada ante seus drásticos efeitos à liberdade individual. Nesse cenário, somente caberia recorrer em última instância à criação de um tipo penal específico ao *stalkerware*, ou seja, apenas na ausência de normas penais suficientemente eficazes à proteção do bem jurídico ofendido. Assim, em defesa da fragmentariedade do direito penal e de uma visão intersetorial do fenômeno, é certo que a intervenção penal não representa o único meio de enfrentamento ao *stalkerware*, necessitando ser combinada com práticas fora do domínio jurídico, a qual envolveria rede de colaboração entre empresas de segurança digital, centros de pesquisa, desenvolvedoras de aplicativos, atores de serviços sociais, entre outros.

Metodologicamente, a presente pesquisa pauta-se essencialmente em uma revisão bibliográfica na literatura, dotada de bases dogmáticas e empíricas. Para tanto, visa-se dispor tanto da base doutrinária nacional, especialmente acerca da compreensão da violência de gênero, do *cyberstalking* e da cibercriminalidade no ordenamento jurídico brasileiro, como também da doutrina internacional, notavelmente mais aprofundada nos temas de *technology-facilitated violence* e *stalkerware*, inclusive com pesquisas empíricas. Em adição, considerando

a dificuldade de produção de dados estatísticos sobre esse fenômeno no Brasil e no mundo, serve-se de relatórios fornecidos por equipes de pesquisa de empresas de cibersegurança, como a Avast e a Kaspersky.

Preliminarmente, tendo em vista a complexidade da instrumentalização do *stalkerware* para a perpetração da violência de gênero, é de suma relevância definir o fenômeno e delinear o arcabouço teórico que revolve tal temática, isto é, os fundamentos da violência digital de gênero, da cibercriminalidade e do *cyberstalking*, assim como seus regimes jurídicos de proteção correspondentes à luz do direito penal.

Posteriormente, cabe adentrar a resposta criminal ao *stalkerware*, delimitando o bem jurídico atingido e os desafios de sua persecução penal, mas há de se reputar que sua efetividade deve ser combinada com estratégias intersetoriais de prevenção e de combate ao *stalkerware*, executadas tanto pelo Estado como pela iniciativa privada, com apoio ou não de ferramentas tecnológicas. Quanto aos tipos penais que usualmente melhor descrevem a conduta analisada, visa-se um exame da aplicabilidade do princípio da consunção aos tipos penais da invasão de dispositivo informático (art. 154-A, CP) e do *stalking* (art. 147-A, CP), em prol de uma proposta de criminalização atenta aos bens jurídicos lesionados.

1. A ATUAL PROBLEMÁTICA DO *STALKERWARE*

Preliminarmente, tem-se como premissa que a tecnologia se situa em contexto sociocultural específico, de sorte que seu processo de invenção e suas finalidades respondem às normas culturais e sociais vigentes, apresentando, portanto, potencial para reproduzir padrões de poder e de controle (WINNER, 1986).

Nessa instância, a violência de gênero frequentemente associa-se a tentativas de exercício de poder e de controle sobre as ações de outrem, desde o modo de se portar socialmente até os locais que frequenta. À vista disso, o uso de tecnologia possibilita o rastreamento da localização e o monitoramento das vítimas remotamente, principalmente parceiras, alvos de uma sensação de onipresença e onipotência dos perpetradores, os quais se apropriam de interfaces de usuário, *keyloggers*, câmeras ocultas, *softwares* aptos a download, como *spyware*, e rastreadores de GPS para derrubar paredes temporais e espaciais (HARKIN; MERKEL, 2023; FREED *et al*., 2019; LEITÃO, 2021; YARDLEY, 2021). Prova disso é que, nos Estados Unidos, uma pesquisa conduzida pela *National Public Radio* em 72 abrigos de violência doméstica constatou que 85% dos abrigos assistiam vítimas cujos agressores as rastreavam com GPS (SHAHANI, 2014).

Dentre as ferramentas tecnológicas existentes, insere-se especificamente o *stalkerware*, configurando monitoramento viabilizado por *softwares* de *spyware* e por *dual-apps*, ou seja, aplicativos voltados para realização do *cyberstalking* (CHATTERJEE *et al*., 2018). Nessa perspectiva, aplicativos legítimos, originalmente idealizados para rastreio de crianças, animais de estimação e aparelhos perdidos, evoluíram, diante de sentimentos de suspeita de traição ou separação, para a vigilância de pessoas adultas sem seu consentimento, tornando-se um instrumento da violência de gênero no meio digital (SYDOW, 2022).

Em uma escala global, depois da Rússia, o Brasil foi o país mais afetado em 2020 pela atividade *stalkerware*, segundo relatório produzido pela Kaspersky e pela *Coalition Against Stalkerware* (COALITION AGAINST STALKERWARE; KASPERSKY, 2020). De modo complementar, a telemetria da empresa de cibersegurança Avast constatou que, no Brasil, o risco de encontrar *stalkerware* em um dispositivo móvel aumentou 358% entre janeiro de 2020 e dezembro de 2022 (AVAST, 2023).

Além da instrumentalização na violência de gênero, os sistemas de *spyware* são inclusive utilizados por órgãos de defesa de governos democráticos e autoritários, os quais, explorando a deficiência de cada tecnologia, acessam e monitoram dados armazenados em

dispositivos eletrônicos de alvos sob um discurso de combate à criminalidade e de preservação da segurança pública, ensejando discussões sobre a legitimidade dessa tecnologia em face da violação sistemática de direitos fundamentais (WOODHAMS, 2021). Para além da investigação criminal, detecta-se abuso dessa prática de ciberespionagem para perseguição de jornalistas, ativistas de direitos humanos, acadêmicos e adversários políticos (DEIBERT, 2023). Da mesma forma, há de se considerar o emprego do *spyware* para cometimento de outros delitos informáticos por civis, como aqueles de caráter patrimonial:

> Os spywares são, também, programas automáticos de coleta de ações dos usuários, como seus costumes no ciberespaço; todavia, estes programas espiões podem ser programados para encontrar e guardar dados confidenciais do usuário - por exemplo, os logins bancários -, remetendo-os, então, para seu programador, que terá a oportunidade de lhe causar prejuízos diversos, desde estelionatos até "furtos de identidade". (...) Em regra, tanto spywares quanto adwares são programas embutidos em outros programas de distribuição livre e gratuita, não raro sendo legal sua distribuição, uma vez aceita pelo usuário (SYDOW, 2015, p. 124).

Enquanto tema apenas recentemente dirimido pelas instâncias de poder brasileira, foi noticiado que a Procuradoria-Geral da República propôs Ação Direta de Inconstitucionalidade por Omissão, com pedido de medida cautelar, em razão da ausência de regulamentação normativa do Congresso Nacional sobre uso de programas de intrusão virtual remota por órgãos e agentes públicos. Em sede de despacho do Ministro Relator Cristiano Zanin em abril de 2024, a ação foi convertida em Arguição de Descumprimento de Preceito Fundamental nº 1143 e determinou-se a convocação de audiência pública para oitiva de autoridades e especialistas sobre essa matéria constitucional, que, de acordo com o Ministro, envolve "os direitos fundamentais à intimidade e à vida privada e a inviolabilidade do sigilo das comunicações pessoais (art. 5º, X e XII, da Constituição Federal)"[1].

Em face das diferentes vertentes do uso de aplicativos espiões, tem-se como enfoque a utilização do *spyware* por particulares na violência de gênero, ressaltando que o objeto do presente trabalho não se refere ao uso legítimo de tais *softwares*, isto é, nos cenários em que ambas as partes consentem com a instalação das funcionalidades.

Em prol de uma definição que abarque as características do *stalkerware*, a obra de Harkin *et al* (2020) define que, mediante o *software* de *spyware*, (i) os dados são coletados remotamente de um dispositivo alvo que não seriam compartilhados, a menos que um código ou *software* externo fosse introduzido ou tivesse acesso permitido por um operador; (ii) com a

[1] SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade Por Omissão 84 - Distrito Federal. Min. Relator Cristiano Zanin, Data de Publicação: 17 abr. 2024. Disponível em: < https://portal.stf.jus.br/processos/downloadPeca.asp?id=15366173525&ext=.pdf>. Acesso em: 06 jun. 2024.

forte possibilidade de que o usuário deste dispositivo não esteja ciente das informações extraídas, da presença contínua do código ou *software* estrangeiro ou de quaisquer permissões para divulgar informações; (iii) sua implantação visando atingir um indivíduo ou grupo específico de indivíduos para fins de monitoramento, rastreamento e vigilância; (iv) de modo que os dados coletados incluiriam informações pessoais, privadas e íntimas, como dados de localização, correspondência privada, fotos pessoais, senhas, entre outros (HARKIN *et al.*, 2020). Também cumpre destacar que a instalação da maioria dos aplicativos de *spyware* carece de um acesso físico aos aparelhos móveis pelo *stalker*, ao menos temporariamente, ou do conhecimento de senhas para desativar notificações de segurança e conceder todas as permissões necessárias, assegurando o monitoramento remoto (KHOO *et al*., 2019). Por fim, essa instalação sucederia pela contaminação do dispositivo ou pela contratação espontânea de serviço de aplicativo com pagamento mensal ou único (SYDOW, 2022).

Embora não se pretenda esgotar todos os cenários de ocorrência do *stalkerware*, a partir das características reunidas, o *stalkerware* seria concebido mais frequentemente nos seguintes cenários: (i) quando o parceiro, com acesso ao dispositivo da parceira, instala fisicamente o aplicativo sem que o alvo perceba ou (ii) quando a própria parceira realiza a instalação da ferramenta, induzida em erro pelo parceiro sobre a sua natureza e finalidade.

A respeito do perfil vitimológico dessa conduta criminosa, os principais alvos dessa tecnologia coincidem com as usuais vítimas de violência doméstica, abuso e assédio, ou seja, mulheres em um relacionamento íntimo, ex-parceiras ou conhecidas (KHOO *et al*, 2019). Com base nisso, constata-se que o *stalkerware*, inserindo-se no recorte do *cyberstalking*, exprime uma das modalidades de violência digital de gênero, o que afeta não só as vítimas diretamente. Ou seja, cabe pontuar que o alvo da instalação de aplicativos de *stalkerware* pode ultrapassar a atual ou ex-parceira, vigiando indivíduos no entorno da vítima, como os filhos, tipicamente instrumentalizados como forma de exercer controle sobre a ex-parceira e conhecer seu paradeiro, potencializando ainda mais o obstáculo de rompimento do elo no mundo físico e digital (FREED *et al.*, 2017; PARSONS *et al.*, 2019).

De acordo com pesquisa da Kaspersky e da Sapio Research que entrevistou 21.055 pessoas de 21 países em 2021, mais homens (10%), em oposição ao percentual de mulheres (8%), confessaram ter instalado *stalkerware* no telefone de seus parceiros (KASPERSKY, 2021). Essa estatística não causa estranheza diante da divisão dos papéis de gênero, sendo mais usual em relacionamentos heterossexuais que o homem, com maior contato com tecnologia,

configure dispositivos e gerencie as contas familiares, circunstância essa que favorece abusos, de modo que as mulheres, em uma situação de violência, apresentariam maior dificuldade em recuperar o controle dos seus dispositivos ou contas (KÖVER, 2021; O'BRIEN; MARAS, 2024).

Ainda de acordo com essa pesquisa da Kaspersky, havendo consentimento entre as partes, 48% dos entrevistados monitorariam seus parceiros de forma consensual e, dessa parcela, 25% o fariam por razões de "transparência total" em um relacionamento, enquanto mais 24% apenas sob determinadas circunstâncias, como segurança física ou monitoramento mútuo (KASPERSKY, 2021). Contudo, na hipótese de consentimento do operador e do alvo, tratando-se de um relacionamento afetivo, é questionável se esse mútuo acordo é suficiente para aferir a licitude dessa conduta, uma vez que, inserida em um ciclo de violência, a vontade de uma vítima não é livre, podendo consistir, nas palavras de Yardley (2021), em uma prática abusiva de *overt omnipresence*, marcada por graves impactos à liberdade e à privacidade. Essa relação entre abuso e *stalkerware* foi verificada numericamente, sendo constatado que 34% dos entrevistados que sofreram abusos já tiveram parceiro íntimo que exigisse a instalação de um aplicativo de monitoramento (KASPERSKY, 2021).

Nessa linha, a instalação do aplicativo é instrumentalizada como prova de amor ou de confiança ou ainda decorre de uma pressão do parceiro (BAUER; HARTMANN, 2021). A natureza controladora que motiva tal prática também se revela estatisticamente, uma vez que 64% daqueles que consideram aceitável monitorar o parceiro sem sua ciência o fariam por suspeitas de infidelidade (KASPERSKY, 2021). A título de complementação, há de se considerar a hipótese em que a vítima, sem atribuir grande valor à confidencialidade dos dados pessoais, cede essas informações com facilidade ao perpetrador, desconhecendo os inúmeros perigos potenciais à sua privacidade e intimidade (SYDOW, 2015).

Explorando esses perigos, é viabilizado, a partir da instalação de um *spyware* que não exige um conhecimento técnico específico, o exercício de um controle integral da vida digital das atuais ou ex-parceiras, dado que é possível monitorar mensagens, postagens das redes sociais e visitas a websites, assim como ativar sistema de GPS, bloquear ligações telefônicas e até ativar câmeras e microfones de celulares e computadores (PARSONS *et al.*, 2019). Assim, a partir de capturas de tela, é possível rastrear precisamente quais dados são excluídos, renomeados ou alterados em tempo real ou em momento posterior, bem como exportar ou imprimir todas essas capturas de tela em formato de texto ou excel (BAUER; HARTMANN,

2021). Ou seja, há uma amplificação das práticas comuns do *stalking*, comumente ligações e mensagens de textos recorrentes. O Laboratório Citizen Lab da Universidade de Toronto catalogou tais funcionalidades dos principais aplicativos de *spyware*, organizadas na tabela a seguir:

	Gravar/Acessar/Monitorar																	
	Ligações	**SMS**	**Apps de mensagem**	**Acessos ao telefone**	**Redes sociais**	**Mídia armazenada**	**Navegação na web**	**E-mail**	**GPS**	**Contatos**	**Calendário**	**Keystrokes**	**Ativar microfone**	**Tirar fotos**	**Acesso remoto**	**Bloquear chamadas**	**IOS**	**Android**
Cerberus				X					X					X	X			X
FlexiSPY	X	X	X	X	X	X	X	X	X			X	X	X	X		X	X
Highster Mobile		X	X	X	X	X	X		X	X	X			X			X	X
Hoverwatch	X	X	X	X			X		X	X				X				X
Mobistealth	X	X	X		X	X	X	X	X		X	X	X				X	X
mSpy		X	X	X		X	X	X	X	X	X	X				X	X	X
TeenSafe		X	X	X			X		X	X							X	X
TheTruthSpy	X	X	X	X	X	X	X	X	X				X				X	X

Fonte: PARSONS, 2019

Em consideração às diferentes interfaces dos inúmeros aplicativos espiões catalogados, de acordo com Khoo *et al.,* seria possível classificar as tecnologias utilizadas como *stalkerware* em três grupos (KHOO *et al.,* 2019). Desse modo, na primeira categoria, encontram-se os aplicativos intencionalmente designados para a vigilância do aparelho de um parceiro, com fins abertamente maliciosos.

O segundo grupo relaciona-se aos aplicativos de *spyware* direcionados para um propósito supostamente legítimo, como rastreamento de crianças e funcionários, sem comercialização explícita à vigilância oculta nos relacionamentos afetivos (KHOO *et al.*, 2019). Assim, por parte da indústria de *spyware*, dissemina-se discurso ao mercado consumidor que atribui legitimidade e licitude a esses aplicativos, comercializados como programas de controle familiar, de antifurto e rastreadores de empregados, ainda que o controle dos dispositivos de crianças e empregados configure violação à privacidade, danoso às relações sociais (HARKIN *et al*., 2020). Segundo Harkin *et al*., há uma ambiguidade moral, posto que, por trás de um discurso pretensamente ético de segurança, desvelam-se estratégias de vigilância marcadas pela desconfiança e pela manipulação (HARKIN *et al*., 2020).

Perseguindo uma aparente legitimidade, a maioria desses aplicativos explicitamente recomenda a utilização do *software* para controle parental, enquanto evita sugerir explicitamente o emprego para relacionamentos íntimos, tanto que muitos programas são

nomeados de forma eufemística (HARKIN *et al*., 2020; BAUER; HARTMANN, 2021). A título exemplificativo, o aplicativo espião mSpy, publicamente comercializado para controle parental das atividades *online* dos filhos, é apropriado pelo *stalker* para monitoramento, de modo que sua instalação demanda apenas alguns minutos, podendo operar de maneira invisível, camuflada como parte integrante do sistema operacional do dispositivo (SHAHANI, 2014). Por fim, o terceiro grupo refere-se à adaptação de tecnologias com uma funcionalidade *spyware*, as quais não foram originalmente criadas para fins de vigilância, embora apresentem *software* de rastreamento de aparelhos móveis, como o caso dos aplicativos Find My iPhone e Find My Friends (KHOO *et al.*, 2019).

A instalação do *spyware* tem ainda potencial de impactar distintas esferas da vida da vítima, gerando não apenas estresse emocional e sentimentos de paranóia, mas também exposição a novas ameaças de *malware* no dispositivo pela exploração de vulnerabilidades, bem como riscos financeiros, posto que a assinatura do aplicativo poderia ser paga com o próprio cartão de crédito da vítima (EYALSALMAN, 2023). Em adição, os impactos prejudiciais do monitoramento digital não se limitam à falta de sensação de segurança, de privacidade e de confiança das vítimas sobre seus aparelhos eletrônicos, visto que se sobrepõem com outras modalidades de violência de gênero, como violência física, verbal e psicológica ou até feminicídio (LEITÃO, 2021; YARDLEY, 2021). Assim, o *stalkerware* aumenta a situação de risco vivida, eis que a progressão para uma violência física poderia vir à tona nas ocasiões em que, por exemplo, a sobrevivente não oferece uma resposta imediata a mensagens e ligações do agressor; a vítima confronta o agressor da instalação do aplicativo; o agente descobre as intenções de separação da parceira pelo aplicativo; ou em que se localiza uma ex-companheira que tenha recorrido a uma casa abrigo para mulheres em situação de violência doméstica (KÖVER, 2021).

Nesse diapasão, também há inúmeras vulnerabilidades de segurança nos sistemas de *stalkerware*, altamente suscetíveis a vazamentos de dados de usuários por ataques de terceiros e, consequentemente, à exposição das vítimas a novas ameaças, visto que seus dados poderiam ser acessados por atores além do agressor originário (MANNAN; YOUSSEF, 2023).

Em decorrência da funcionalidade de camuflagem do *software*, as vítimas inicialmente não estão cientes ou apenas suspeitam da vigilância, mas, havendo confirmação, dificilmente são capazes de produzir provas, posto que isso requer o conhecimento da existência, da identificação e da remoção do *stalkerware* (LEITÃO, 2021). Em muitas ocasiões, apenas o

perpetrador que adquiriu a licença tem autorização para abrir o *software*, ver ou apagar as gravações, efetuar alterações ou desinstalar o software, tanto que certos aplicativos notificam o abusador quando a vítima realiza tentativas de desinstalação do aplicativo (BAUER; HARTMANN, 2021).

Ainda que se recorra a ferramentas antivírus e anti-*spyware*, elas não se mostram eficazes para detectar muitos dos *dual-apps* e *spyware* existentes, em virtude de sua elevada dinamicidade, tornando necessária a constante atualização de programas de segurança, que, por vezes, resulta insuficiente (SYDOW, 2015). E, caso a vítima opte por denunciar a conduta e transportar evidências para um pendrive USB ou imprimir registros para providenciar provas à autoridade policial, determinados spywares registrariam e informariam qual conteúdo foi copiado ou impresso (BAUER; HARTMANN, 2021).

Diante de prática de difícil detecção e de produção probatória, importante sinalizar que não só as vítimas padecem da falta de conhecimento técnico, porém igualmente muitos operadores do direito e atores da rede intersetorial de apoio não detêm habilidades para diagnosticar e responder adequadamente a essa e outras formas de violência facilitadas pela tecnologia (HARKIN; MERKEL, 2023). Nesse cenário, é notável uma falta de formação adequada e de equipamento técnico das próprias autoridades policiais para rastreamento e persecução dos ataques digitais (BAUER; HARTMANN, 2021).

Além das falhas do aparato policial na persecução penal, conclui-se que a prática de *stalkerware* em cenários de violência de gênero não é visualizada de imediato como conduta autônoma, passível de responsabilização criminal, pelos demais operadores do direito. Nesse sentido, em busca de subsídios na jurisprudência brasileira, localizou-se acórdão criminal de 2020 no Tribunal de Justiça de São Paulo com o assunto de violência contra a mulher (Anexo A), com menção explícita ao fenômeno estudado[2]:

> De forma harmônica e segura, a vítima narrou os fatos descritos na inicial. Esclareceu que apesar de, à época dos fatos, morar com André, estavam separados. Esclareceu que o apelante instalou um "aplicativo espião" em seu telefone celular para monitorá-la e que, na data do crime, trocava mensagens com um amigo quando o recorrente entrou no quarto acusando-a de traição. Narrou que André retirou o aparelho de suas mãos e quando tentou recuperar o telefone móvel o apelante a agrediu, apertando com força seus pulsos. Esclareceu, por fim, que o recorrente somente interrompeu a agressão pois o filho do casal "começou a gritar" (fls. 6/7 e mídias digitais). (TJSP; Apelação Criminal 0000534-35.2017.8.26.0070; Relator: Cesar Mecchi Morales; Órgão

[2] Trata-se de acórdão da Apelação Criminal n. 0000534-35.2017.8.26.0070 do Tribunal de Justiça de São Paulo, localizado mediante a procura por julgados com as palavras-chave "aplicativo espião" ou "stalkerware".

Julgador: 3ª Câmara de Direito Criminal; Foro de Batatais - Vara Criminal; Data do Julgamento: 26/06/2020; Data de Registro: 26/06/2020).

Em conformidade com a literatura, o depoimento da sobrevivente ilustra como o monitoramento das suas comunicações por meio do *stalkerware* pode conferir uma nova camada de violência, dado que, após suposta quebra de confiança da vítima, sucedeu uma agressão física perpetrada pelo ex-parceiro. Nesse caso particular, foi negado provimento à apelação interposta pelo autor dos fatos, mantendo-se a condenação por lesão corporal leve. Todavia, importa destacar que somente houve a criminalização da lesão corporal, não havendo qualquer resposta estatal à instalação do aplicativo espião no celular da vítima, o que indica uma possível dificuldade de adequação do *stalkerware* a um tipo penal específico.

Por fim, é essencial considerar a mobilização dos segundo e terceiro setores frente à minimização do *stalkerware*, vinculado não só ao problema socioestrutural da violência de gênero, como também à monetização dos aplicativos que viabilizam esse fenômeno. Em relação ao *stalkerware*, é evidente que a violência de gênero, perpetuada pela lógica neoliberal, revela-se lucrativa ao segundo setor, de modo que o atual sistema econômico, longe de ocupar uma posição neutra, se beneficia de uma violência que contribui a perpetuar. Em vista do papel dos agentes privados na disponibilização desses *softwares* no mercado e da quantidade considerável de *dual-apps* na Google Play Store, embora o sistema de suporte Google Play Protect tenha avançado com medidas para detectar e suprimir tais aplicativos nocivos, o acesso físico ao telefone pelos agressores facilita a desativação dessas proteções (MANNAN; YOUSSEF, 2023).

Quanto à sociedade civil, não obstante a criação de organizações de cunho social em busca de soluções técnicas[3], sugestões estereotipadas de mudança do comportamento da própria vítima, decorrentes de uma visão patriarcal e limitada sobre o ciclo de violência e ainda frequentemente propagadas socialmente, como trocar o aparelho de celular ou interromper o uso da tecnologia, não bastam e limitam potenciais respostas jurídicas (YARDLEY, 2021). Inclusive, essas sugestões, além de excluírem pessoas com deficiência que necessitam da tecnologia para suas atividades e comunicações diárias, podem contribuir para um maior risco de violência física pelo agressor (FRASER *et al.*, 2010).

[3] A título exemplificativo, frente a essa ameaça, foi fundada a organização *Coalition Against Stalkerware* em 2019, que, contando com a expertise dos seus membros com segurança digital e com suporte a sobreviventes de violência doméstica, visa combater as condutas delitivas perpetradas mediante o *stalkerware*.

A partir desse panorama que investigou o perfil vitimológico, as motivações do agente, o *modus operandi* adotado e as dificuldades de persecução penal, vislumbra-se que a nova ameaça do *stalkerware* é caracterizada por elementos já identificados nos âmbitos da violência digital de gênero, da cibercriminalidade e do *stalking*. Por mais que se revele uma forma sofisticada de invasão da privacidade e de controle do corpo feminino, reproduz sintomas de violências já estudados pela literatura.

Em prol de uma resposta criminal ao *stalkerware*, cumpre mencionar a tramitação do Projeto de Lei nº 402/2024, o qual, embora centrado na utilização de aplicativos espiões por órgãos e agentes públicos, propõe a criminalização do monitoramento remoto de terminais de comunicações sem prévia autorização judicial, disposição esta que se aplicaria a civis. Não obstante, trata-se de proposição que não captura as nuances da violência digital de gênero e de *cyberstalking* que permeiam a lógica do *stalkerware*, de sorte que não se vislumbra como necessária a criação de um tipo penal para esse fenômeno em específico.

Com efeito, conclui-se que, transpondo a análise dessa conduta ao direito penal, consistiria, dadas as particularidades do seu *modus operandi*, em uma perseguição reiterada viabilizada pela instalação de um *spyware*, não se vislumbrando como necessária a criação de um tipo penal específico. Assim, há de se aferir se a combinação entre os tipos penais de *stalking* (art. 147-A do Código Penal) e do delito cibernético de invasão de dispositivo informático (art. 154-A do Código Penal) se adequa ao modo de execução do *stalkerware*. Nesse sentido, abrangendo esferas de proteção pautadas em distintos valores jurídico-penais, importa delinear mais profundamente os marcos teóricos da violência digital de gênero, da cibercriminalidade e do *cyberstalking*, em prol da delimitação do bem jurídico aplicável e da resposta criminal adequada às elementares do *stalkerware*.

2. VIOLÊNCIA DIGITAL DE GÊNERO

Na qualidade de uma das formas de criminalidade digital, o fenômeno do *stalkerware*, com base em seu perfil vitimológico, situa-se majoritariamente em contexto de prática de violência de gênero, reproduzindo opressões sociais longamente perpetuadas. A partir dessa premissa, a formulação de estratégias eficientes de combate a esse artifício na esfera criminal exige um estudo tanto das normas penais existentes em face da violência de gênero no Brasil quanto da estrutura de poder que a mantém.

2.1. Violência de gênero: Contextualização teórica e atual regime jurídico de proteção

Em um primeiro momento, cabe definir a nomenclatura referente à violência praticada no âmbito do *stalkerware* a ser adotada ao longo do presente trabalho. Como ponto de partida, tem-se que a noção de gênero é socialmente construída, firmando-se a partir de uma designação desigual dos papéis sociais fundada na determinação biológica dos corpos. Instituem-se, portanto, relações de poder marcadas pela dominação masculina, cuja manutenção demanda o empreendimento de forças manifestadas na violência simbólica e física contra as mulheres (BOURDIEU, 1999).

Nesse diapasão, compete observar como o contexto político-econômico do neoliberalismo robustece o sistema patriarcal, bem como valida as condutas que o mantêm. Por mais que constem avanços às mulheres em termos de independência econômica e inserção no mercado de trabalho, há, na contramão, um maior ímpeto masculino de exercício da posse e de retomada do controle, em face da perda da posição de único provedor financeiro. Assim, caracterizado por um viés individualista, o aludido liberalismo acaba por legitimar práticas fundadas no abuso e na violência, eis que os agressores priorizam os próprios interesses de proteção de sua autoridade em detrimento dos direitos e liberdades da parceira, sob o véu de um suposto discurso de zelo e de devoção (YARDLEY, 2021). Portanto, pensada dentro dessa estrutura socioeconômica e cultural, a violência de gênero cultiva-se em conjuntura de relações conflitivas marcadas pela força e pela hierarquia, legitimadas pelas instituições, as quais mantêm a submissão da classe dominada à ordem vigente e seu acesso desigual a direitos e a espaços de poder (AUGUSTO, 2015; BARSTED, 2012).

De acordo com artigo 1º da Convenção para Prevenir, Punir e Erradicar a Violência contra as Mulheres da Organização dos Estados Americanos (OEA), instrumento internacional assinado pelo Brasil em 1995, a violência contra a mulher consiste em "qualquer ação ou conduta, baseada no gênero, que cause morte, dano físico, sexual ou psicológico à mulher, tanto no âmbito público como no privado"[4]. À vista disso, ainda que mais amplo que o conceito de violência doméstica, o uso da expressão "violência contra a mulher" no presente trabalho frisaria a condição de mulher como fundamento dessa violência, ocupando uma posição vitimista da dominação masculina (SANTOS; PASINATO, 2005), além de ocultar a existência de múltiplas mulheres, o que veicularia a ideia de um grupo feminino homogêneo:

[4] COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS - OEA. **Convenção interamericana para prevenir, punir e erradicar a violência contra a mulher**, "Convenção de Belém do Pará". 1994.

> Gênero não era a categoria empregada nessa definição e a condição feminina tinha seu significado articulado a pressupostos universalizantes, como a idéia de que a opressão é uma situação partilhada pelas mulheres pelas circunstâncias de seu sexo, independentemente do contexto histórico ou cultural observado. (DEBERT; GREGORI, 2008, p. 168)

Afinal, considerando o marco espacial brasileiro, é de especial relevância a análise do marcador da diferença de cor ou raça nos estudos da violência de gênero, exigindo uma visão interseccional tanto na produção legislativa como na aplicação do direito, a fim de evitar um aprofundamento de vulnerabilidades pelo sistema de justiça criminal (FLAUZINA, 2015). Por mais que ainda não se verifiquem estudos de *stalkerware* sobre o perfil vitimológico em termos de raça e gênero, é de se esperar que, na qualidade de violência de gênero, as desigualdades já constatadas reapareçam.

Nessa vertente, é certo que a desigualdade social e econômica no país se expressa em termos de raça e gênero, constatada em estatísticas de montante salarial, de ocupação de espaços de poder ou de violência (VALENTE, 2023). A título de exemplo, em 2022, apenas 39,3% dos cargos gerenciais eram ocupados por mulheres, porém elas dedicaram aos cuidados de pessoas e/ou afazeres domésticos quase o dobro de tempo que os homens (IBGE, 2024). Em termos de composição racial, 43,5% da população declarou-se brancos, enquanto 55,5% identificam-se como negros, o que inclui pardos e pretos (IBGE, 2024). Embora a população negra constitua maioria numérica, esse dado não se verifica em termos de acesso a direitos e à segurança, conforme evidenciado pelas estatísticas de violência de gênero, visto que as mulheres negras, em 2022, mais sofreram violências, com percentual de 6,3%, enquanto a porcentagem de mulheres brancas era de 5,7% (IBGE, 2024).

Assim, a adoção do marco teórico da interseccionalidade, refutando um feminismo hegemônico, pressupõe que "forças econômicas, culturais e sociais silenciosamente moldam o pano de fundo, de forma a colocar as mulheres em uma posição onde acabam sendo afetadas por outros sistemas de subordinação" (CRENSHAW, 2002, p. 176). Ora, uma política adequada de enfrentamento à violência de gênero exige um reconhecimento das pluralidades dentro do grupo de mulheres, atravessadas por diferentes marcadores da diferença, como raça, classe social e identidade de gênero, cujas vulnerabilidades inflam os impactos da violência (BARSTED, 2012).

Aderindo à visão majoritária da literatura, revela-se mais adequado o emprego da expressão "violência de gênero", conceituando gênero como categoria analítica de relações entre homens e mulheres regidas sob ordem patriarcal (BANDEIRA, 2014; SANTOS;

PASINATO, 2005), de maneira a relativizar o binômio dominação-vitimização, uma vez que as mulheres desempenham papel de protagonistas dessa violência na condição de vítimas e não-sujeitos (GREGORI, 1993). Ainda, aberta ao viés interseccional, a acepção de violência de gênero abrangeria a violência doméstica ou intrafamiliar, assim como homens em qualquer etapa da vida na posição de vítimas (SAFFIOTI; ALMEIDA, 1995).

Em grande parte, a complexidade da violência de gênero, especificamente na relação entre parceiros íntimos, decorre da lógica do ciclo de violência, que envolve momentos de tensão e conciliação, dificultando o fim do relacionamento abusivo pela vítima. Nessa instância, cumpre explicitar as principais fases desse ciclo, as quais não necessariamente sucedem nesta ordem, sendo que, ao longo do tempo, a violência tende a intensificar: (i) fase de construção da tensão, quando pairam conflitos não resolvidos e raiva não expressa; (ii) fase de explosão, ou seja, de ocorrência do ato de violência, seja emocional, verbal e/ou físico; (iii) fase de lua de mel, eis que o parceiro busca o perdão da vítima e promete cessar o comportamento abusivo, perdurando até nova tensão (COLEMAN, 1997). Desse modo, não se trata de problema social facilmente solucionado, pois, ainda que a mulher interrompa esse ciclo e encerre o relacionamento, encontra-se mais vulnerável a contatos indesejados e a reações extremas de violência pelo agressor, como *stalking* e feminicídio.

Embora se pressuponha que a violência de gênero somente seria significativamente reduzida por meio de uma superação das condições sociais que mantêm a construção social desigual dos gêneros, a norma jurídica exerce importante papel no alcance da igualdade formal e material entre homens e mulheres, ampliando garantias já reconhecidas e penalizando violações a esses direitos, de modo que representa um dos instrumentos no enfrentamento da violência contra mulheres (SEVERI; CAMPOS, 2019; AUGUSTO, 2015). Nesse cenário, ao longo de sua construção, o direito penal tem atuado de forma dicotômica, ora no combate às desigualdades sociais, ora na reprodução da violência de gênero. Primeiramente, há de se ter em mente que o direito penal difere de outras esferas do direito, uma vez que, dotado de um caráter particularmente sexista, dificulta o alcance da igualdade (SEVERI; CAMPOS, 2019).

Inicialmente, o Código Penal de 1940 encarava a violência sexual como um crime contra os costumes, tanto que previa a extinção da punibilidade ao estuprador que se casasse com a vítima, enquanto a violência doméstica configurava um "quase não crime" (BARSTED, 2012). Apenas nos anos 1960 e 1970, verificaram-se mobilizações do movimento feminista de publicização da opressão feminana, atribuindo-lhe dimensão política (MARTINS *et al.*, 2015).

Posteriormente, em razão das iniciativas da sociedade civil, do contexto de redemocratização e da produção legislativa internacional, adviram importantes marcos jurídicos nacionais na expansão dos direitos às mulheres, como o reconhecimento constitucional da igualdade formal entre homens e mulheres, a aceitação da Convenção de Belém do Pará da OEA como lei interna pelo Decreto Legislativo 107/95, bem como a eliminação de dispositivos penais sexistas pela Lei 9.520/97 e pela Lei nº 11.106/05 (BARSTED, 2012).

Contudo, no período de 1995 até 2006, a competência de apreciação dos crimes de ameaça e lesão corporal leve dolosa recaía sobre os Juizados Especiais Criminais, de modo que, instituídos pela Lei nº 9.099/95, adotavam uma abordagem conciliatória entre as partes, dificultando a compreensão da violência doméstica como uma questão de natureza criminal (DEBERT; OLIVEIRA, 2007). Ou seja, antes da promulgação da Lei 11.430/2006, notadamente conhecida como Lei Maria da Penha, conflitavam dois paradigmas no direito interno: as condutas de violência contra as mulheres eram tratadas como crimes de menor potencial ofensivo pelo Juizado Especial Criminal, enquanto a Convenção de Belém do Pará as classificava como violações de direitos humanos por limitarem o exercício dos demais direitos fundamentais (BARSTED, 2012; PIOVESAN; PIMENTEL, 2011).

Em prol de um tratamento uniforme às vítimas, foi promulgada, sob pressões do movimento feminista, a Lei Maria da Penha em 2006, a qual, modificando as legislações de direito penal material e processual e estabelecendo medidas de assistência e proteção, visava nos termos do seu artigo 1º, "coibir e prevenir a violência doméstica e familiar contra mulher". Nesse âmbito, instaurou-se o paradigma fixado pelo diploma constitucional e pelos tratados internacionais ratificados no país, afastando a incidência da Lei 9.099/95 com a criação de Juizados de Violência Doméstica e Familiar contra a mulher. Nos termos do artigo 5º da Lei 11.340/2006, embora adote a definição de violência contra mulheres prevista na Convenção de Belém do Pará e reconheça que constitui forma de violação dos direitos humanos, ressalta-se que o escopo protetivo da legislação em questão é direcionado à violência especificamente no âmbito da unidade doméstica, da família ou em qualquer relação íntima afetiva, garantindo a preservação da integridade física, moral e patrimonial das mulheres (MARTINS *et al.*, 2015).

Além da atribuição da qualificadora do feminicídio no artigo 121 do Código Penal pela Lei nº 13.104/2015, resultante de pressões internacionais, efetuaram-se *a posteriori*, por meio da Lei nº 14.188, de 28 de julho de 2021, alterações do Código Penal, incluindo a qualificadora

da lesão corporal simples cometida contra a mulher por razões da condição do sexo feminino e criando o tipo penal de violência psicológica contra a mulher.

Sobre a violência psicológica contra mulher, tipificada no artigo 147-B do Código Penal, verifica-se que foi transportada parte da definição de violência psicológica constante no artigo 7º, inciso II, da Lei Maria da Penha, que cita em seu rol a vigilância constante, a qual se adequaria, em um primeiro olhar, ao *stalkerware*, alcançando precipuamente mulheres em relações íntimas afetivas, de modo compatível ao escopo protetivo da Lei Maria da Penha.

> **Violência psicológica contra a mulher**
> Art. 147-B. Causar dano emocional à mulher que a prejudique e perturbe seu pleno desenvolvimento ou que vise a degradar ou a controlar suas ações, comportamentos, crenças e decisões, mediante ameaça, constrangimento, humilhação, manipulação, isolamento, chantagem, ridicularização, limitação do direito de ir e vir ou qualquer outro meio que cause prejuízo à sua saúde psicológica e autodeterminação:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Tendo a liberdade pessoal como objeto jurídico tutelado, é notável uma redação imprecisa do dispositivo penal pelo legislador, confundindo entre os conceitos de dano emocional e psicológico da mulher, de modo que não é compreensível pelo tipo penal o significado atribuído a dano emocional (BITENCOURT, 2022). Ainda assim, nem sempre a sobrevivente do *stalkerware* sofreu dano emocional ou psicológico com a invasão da privacidade, sendo inconcebível generalizar as reações das vítimas. Logo, apenas havendo efetivo dano emocional ou psicológico à mulher vítima de *stalkerware*, seria possível cogitar a absorção do crime de violência de violência psicológica contra a mulher, dotado de caráter subsidiário, pelo crime de *stalking*.

Assim, por um lado, a norma penal confere maior reprovação à conduta e representa outro mecanismo de fomento à erradicação da violência contra a mulher, conferindo maior visibilidade ao problema social, ainda que não seja o instrumento mais adequado para sua resolução (NUCCI, 2023; SPONCHIADO, 2020). Por outro, é imperativo adotar perspectiva crítica à expansão da intervenção penal no âmbito da violência de gênero, uma vez que a criminalização fortalece igualmente efeitos adversos do sistema penal, particularmente considerando que os principais alvos tendem a ser homens negros de baixa renda, reforçando uma marginalização social (BATISTA, 2008; RIFIOTIS, 2008). Consistindo a violência de gênero em um problema social que demanda transformações estruturais, educacionais e culturais, o direito penal apenas propicia uma aparência de resolução do conflito, desviando a atenção da sociedade a formas de resolução efetivamente eficazes e recaindo, assim, no

fenômeno do simbolismo penal, além de adotar uma postura paternalista que vislumbra a mulher como vítima vulnerável que carece da tutela estatal (SPONCHIADO, 2020). Nesse cenário, também é questionável a eficácia da aplicação isolada da pena privativa de liberdade para ressocialização dos sujeitos (BEIRAS *et al.*, 2012).

Adotando uma perspectiva intersetorial, cabe pontuar que a legislação, mais do que um ato legislativo isolado, não só propicia uma resposta penal aos agressores, como demanda medidas de proteção, de assistência social e de prevenção à violência a serem criados pelos setores públicos, em prol de uma atuação integrada e da articulação em rede das políticas públicas, ante as necessidades de cada vítima (PASINATO, 2015). Nesse sentido, a efetividade dos objetivos normativos exige a capilaridade dos serviços públicos mediante o acompanhamento das políticas públicas pela comunicação entre os entes federativos, bem como por sistemas de informação de geração de dados dessa violência (MARTINS *et al.*, 2015).

Apesar do reconhecimento constitucional da igualdade formal entre homens e mulheres e da promulgação da Lei Maria da Penha, o ordenamento jurídico ainda recentemente autorizava o emprego da tese defensiva de legítima defesa da honra em casos de feminicídio ou de agressão contra mulheres, cuja inconstitucionalidade fora apenas reconhecida pelo Supremo Tribunal Federal no ano de 2023[5]. É evidente, portanto, o caráter dualista do direito penal em relação aos direitos das mulheres, caracterizado por uma conjunção complexa de evoluções e permanências.

A despeito da sensibilização social trazida pela legislação penal no combate à violência de gênero, é crucial cautela para evitar posturas dicotômicas de reprodução da lógica vítima-criminoso, incompatíveis com o grau de complexidade da dinâmica de gênero, de modo a não vincular a figura da vítima à posição de fragilidade (BEIRAS *et al.*, 2012). Nesse contexto sensível, conforme demonstrado no ciclo de violência, há de se reconhecer a dificuldade da vítima de identificar uma conduta como abusiva, a qual se encontra muitas vezes habituada a um relacionamento marcado pela inferioridade e subjugação, até justificando as condutas do agressor, de sorte que o direito penal deve se afastar ao máximo de uma narrativa de culpabilização (CAVALCANTE; LELIS, 2016).

Não obstante o presente trabalho busque apresentar uma forma de persecução penal adequada ao *stalkerware*, observa-se que as respostas jurídicas nem sempre coincidem com as

[5] Supremo Tribunal Federal, ADPF 779.

expectativas das mulheres que recorrem ao Poder Judiciário, uma vez que os conflitos nas relações afetivas não se limitam a meros aspectos processuais penais ou a uma relação de causa e efeito. Nesses termos, explicitada a complexidade da violência de gênero, constata-se que a prática do *stalkerware*, voltada especificamente ao monitoramento das comunicações e das atividades de parceira ou ex-parceira, se revela como mais uma forma de exercício desigual de poder e de controle nas relações de gênero, sendo que as particularidades do recurso tecnológico potencializam ainda mais a assimetria entre vítima e perpetrador.

2.2. Tecnologia como facilitadora da violência de gênero

Perante o papel crucial exercido pelo meio tecnológico na execução do *stalkerware*, cabe tecer considerações a respeito do uso da tecnologia no cometimento de atos de violência de gênero em geral, cujas motivações e percalços aplicar-se-iam ao fenômeno estudado. Torna-se, portanto, inviável conceber o *stalkerware* deslocado do panorama da violência digital de gênero.

Preliminarmente, convém consignar que a tecnologia corresponde a um dos elementos das dinâmicas sociais, revelando-se simplista uma abordagem teórica pautada na separação entre ciberespaço e mundo real, bem como em entusiasmos, seja tecnoutópicos, seja tecnofóbicos (VALENTE; NERIS, 2019). Ou seja, não basta direcionar um olhar analítico a aplicativo, site ou plataforma específicos, mas sim a um uso de mídias digitais articulado frequentemente com formas de interação social fora da *internet* (MISKOLCI, 2011). Mais do que isso, propondo-se um estudo de relações sociais afetadas pelas mídias digitais, não se deve incorrer no perigo de adoção de uma visão dicotômica, isto é, estritamente otimista ou pessimista.

Não sendo possível compreender a tecnologia deslocada do tecido social, cumpre enxergá-la como forma diversa de condução das interações sociais, muitas vezes potencializando e transformando "parcialmente meios anteriores de comunicação, que por sua vez já vinham produzindo seus impactos nos processos sociais e de subjetivação" (VALENTE; NERIS, 2016, p. 15), como ilustra o caso da violência de gênero. Com base nessa premissa, não é concebível o discurso de uma suposta neutralidade dos espaços virtuais, pois, entrelaçados com as dinâmicas de poder, reproduzem as formas de discriminação em voga (SILVA, 2022).

Posto isso, é inegável a complexidade da relação entre tecnologia e violência de gênero, eis que as ferramentas tecnológicas desempenham funções passíveis de estímulo e de repressão

de atos abusivos. Por um lado, entende-se que a tecnologia também possa representar espaço de denúncia do abuso, bem como importante veículo para posicionamento de demandas feministas, de modo a não reduzi-la ao papel de vilã:

> A tecnologia é, portanto, um elemento nessa interação complexa. Com isso, evitam-se armadilhas do determinismo: a pesquisa empírica atenta a essa complexidade é capaz de evidenciar a relação entre possíveis novos usos de tecnologias, vantajosos e emancipatórios para mulheres, com circunstâncias sociais e econômicas mais amplas, inclusive com as diferenças existentes entre mulheres em termos, por exemplo, de classe social e raça (VALENTE; NERIS, 2019, p. 138).

Por mais que se deduza o potencial tecnológico no combate à violência de gênero, tem-se como enfoque o papel da tecnologia como facilitadora da violência de gênero, à vista do ímpeto do presente trabalho de abordagem do fenômeno do *stalkerware*. Nessa linha, a violência digital de gênero não configura um novo fenômeno social, de modo que a tecnologia representaria mais um formato de reprodução das estruturas sociais, dentre elas o modelo patriarcal. Como resultado de uma nova configuração, a amplificação da violência de gênero pelos meios digitais aproveitou-se de características singulares dessa forma de comunicação, como a distância física, o anonimato, a instantaneidade, a automação, a acessibilidade e a propagação (SOTO *et al*., 2023; FASCENDINI; FIALOVÁ, 2011).

Munida dessas peculiaridades, não há dúvidas de que a tecnologia expandiu a capacidade dos perpetradores de monitorar, assediar, ameaçar e stalkear as vítimas, haja vista que, na atual era digital, se torna possível o monitoramento dos contatos, comunicações e redes sociais, tanto pela instalação de aplicativos espiões, como pelo acesso físico aos dispositivos, sem grandes esforços, custos ou nível de expertise (LEITÃO, 2021; YARDLEY, 2021; FASCENDINI; FIALOVÁ, 2011).

Em um espaço amostral de redes sociais, chats de videogrames, fóruns de discussão e relacionamentos afetivos, compete definir o assédio *online* como um contato negativo e indesejado por meios digitais, que pode se resumir a uma ocorrência ou uma série de ataques e ser praticada por conhecidos ou estranhos de outra cidade ou país, abrangendo ofensas, *cyberstalking*, ameaças, humilhações, extorsão, assédio sexual, abuso emocional e psicológico, e assim por diante (LENHART *et al*, 2016; VALENTE, 2023). Nesse âmbito, observam-se manifestações de violência digital tanto em relacionamentos íntimos como em interações *online*, conforme evidenciam o envio de nudes não solicitados e os ataques *online* baseados em discriminação de gênero, raça, orientação sexual, deficiência, entre outros (VALENTE, 2023). A longas distâncias, os perpetradores são capazes de enviar mensagens abusivas incessantemente e publicar imagens reais ou manipuladas com rosto e dados da vítima,

postagens de difícil remoção que são facilmente difundidas e perpetuadas na internet (FASCENDINI; FIALOVÁ, 2011).

A partir desses exemplos, é certo que a invasão de privacidade constitui expressão elementar da violência digital de gênero, ainda que não se resuma a essa manifestação. Sob esse paradigma, tem-se que a invasão de privacidade abrange os danos causados à vítima mediante o acesso não autorizado e a exposição de informações fora do controle do seu titular, incluindo hackeamento, exposição não permitida de imagens ou dados pessoais online, falsificação de identidade, monitoramento ou rastreamento (LENHART *et al*, 2016; VALENTE, 2023).

Na pesquisa *Supporting a Safer Internet*, que coletou dados de violência digital em 18 países, as principais violências mencionadas foram o contato incessante e indesejado de uma pessoa e o recebimento de imagens sexuais indesejadas (VALENTE, 2023). Contudo, há de se discernir que as experiências de violência digital no Sul Global, especificamente no Brasil, apresentam particularidades sociais e culturais distintas das expressões na Europa e na América do Norte. No caso do Brasil, a pesquisa supracitada constatou que 54,2% dos brasileiros entrevistados experienciaram violência *online*, tendo como vítimas 80,4% das pessoas LGBTQIA+, 52.5% de homens e 55,6% das mulheres (VALENTE, 2023).

Nessa linha, em termos de percepção sobre a violência, 31,9% das mulheres e 20,6% das pessoas LGBTQIA+ alegam que o ato decorreu da identidade de gênero, sendo que o perpetrador era um homem para mais da metade das mulheres e pessoas LGBTQIA+ (VALENTE, 2023). À vista da construção social patriarcal no Brasil, é evidente que os efeitos dessa violência são mais sentidos pelas mulheres, de sorte que a pesquisa em análise aferiu que 72% das brasileiras reconhecem a violência digital como um grave problema (VALENTE, 2023). Entretanto, evitando conceder uma centralidade à categoria de gênero que obscureça outros relevantes marcadores de diferenças, é de rigor compreender que mulheres brasileiras negras, indígenas e LGBTQIA+, perpassadas por outros sistemas de subordinação, são afetadas de forma mais gravosa pela violência de gênero digital (PISCITELLI, 2008; VALENTE, 2023).

Em relação à esfera dos relacionamentos íntimos, os dados brasileiros refletem o preocupante panorama de violência doméstica vigente, visto que 38% da amostra relatou ter sofrido violência digital de conhecidos, equivalendo 18,6% a ataques de ex-parceiros contra mulheres (VALENTE, 2023). Notadamente, sob o enfoque de um relacionamento afetivo, mediante o acesso às redes sociais da vítima, possibilita-se o rompimento da rede de apoio da

sobrevivente, bem como interferência em sua vida profissional, na condição de estratégias voltadas ao isolamento da vítima, elemento-chave do ciclo de violência (YARDLEY, 2021).

Por essa razão, entende-se que o abuso cometido é particularmente marcado pela onipresença, pois, rompendo barreiras temporais e espaciais, os abusadores oferecem a sensação de acompanharem todos os passos da vítima, mostrando-se sempre presentes (WOODLOCK, 2017). Objetivando captar comportamentos abusivos a partir da onipresença e ciente do seu caráter multidimensional, Yardley (2021) desenvolveu quatro categorias para compreensão desse fenômeno em vínculos amorosos: *establishing omnipresence*, *overt omnipresence*, *covert omnipresence* and *retributive omnipresence*, dimensões que seriam igualmente aplicáveis à dinâmica do *stalkerware*.

No âmbito do conceito de *establishing omnipresence,* o perpetrador, respaldado pela base patriarcal dos laços familiares, adquire acesso privilegiado a contas e dispositivos da vítima, posto que frequentemente ocupa a posição de titular do plano familiar, detendo autoridade para configuração de senhas (YARDLEY, 2021). Nesse cenário inicial, o autor busca legitimar sua conduta abusiva com base em argumentos de preocupação, de um ciúme "justificado" ou de "prova de amor" e, por essa razão, algumas sobreviventes, ainda vislumbrando os relacionamentos como positivos, compartilham suas senhas com os parceiros, o que facilita, por exemplo, o *cyberstalking* (BAUER; HARTMANN, 2021; YARDLEY, 2021).

Seguidamente ao processo de edificação da onipresença, cabe menção ao *overt omnipresence*, caracterizado pelo exercício do controle e do monitoramento de forma transparente, ou seja, com ciência da vítima. Em paralelo, há um esforço do perpetrador de normalizar tais práticas abusivas e retratá-las como socialmente adequadas, típicas de relacionamentos amorosos (YARDLEY, 2021). A título de exemplo, verifica-se uma explícita onipresença nas hipóteses em que o agente vasculha os aparelhos na frente da parceira, instala câmeras para vigiá-la ou ainda liga e envia mensagens incessantemente, muitas vezes de forma programada (YARDLEY, 2021). Consequentemente, há uma expectativa de que esses chamados sejam respondidos imediatamente pela vítima, a qual por vezes necessita encaminhar registros fotográficos ou realizar videochamadas para comprovar seu paradeiro e, caso descumpra esse regramento, torna-se alvo de humilhações, ameaças e até quebra do dispositivo pelo agente (BAUER; HARTMANN, 2021; DOUGLAS *et al.,* 2019).

No que concerne à quebra do aparelho, cumpre considerar que a tecnologia consiste em importante ferramenta de interação social, de modo que a interrupção do funcionamento do dispositivo objetiva não só punir a parceira, mas também isolá-la ao restringir o contato com sua rede de apoio de familiares e amigos, possível obstáculo à dependência emocional da vítima e ao contínuo controle exercido pelo agressor. Da mesma forma, o bombardeamento de inúmeras mensagens e a falsa denúncia de uma conta por conteúdo problemático ou abusivo também se propõem à limitação do acesso pela sobrevivente às plataformas de comunicação, representando a negação do acesso ao meio virtual uma das modalidades de violência digital de gênero (LENHART *et al*, 2016; BAUER; HARTMANN, 2021).

Como alternativas à explícita vigilância, sobreviventes relatam recorrer à interrupção do uso de aparelhos de fácil acesso pelo agressor, à exclusão de redes necessárias ao crescimento profissional, ao apagamento do seu histórico de atividades ou até ao uso de outro aparelho secretamente (YARDLEY, 2021; LENHART *et al*, 2016). Todavia, há de se ressaltar que tais medidas, se descobertas pelo parceiro, poderiam ameaçar ainda mais a integridade da vítima, revelando-se insustentáveis a longo prazo.

No espectro da *covert omnipresence*, ocorre o acesso às informações pessoais da sobrevivente de forma clandestina pelo agressor, de modo que a vítima apenas apresenta suspeitas de uma vigilância, dificultando a denúncia dessa violência e podendo se prolongar após o fim do relacionamento (YARDLEY, 2021). Por trás dessa prática, Yardley entende haver um desejo do perpetrador de ter suas suspeitas confirmadas acerca de uma falta de lealdade da parceira, isto é, de agir corretamente ao desconfiar da vítima (YARDLEY, 2021).

Em atenção a essa categoria particular, a onipresença oculta se perfaz no fenômeno do *stalkerware*, consistente na instalação de um aplicativo de *spyware* para monitoramento remoto da vítima, geralmente sem sua autorização. Nessa toada, também cabe menção a rastreamento por dispositivos físicos de geolocalização, câmeras escondidas, microfones ou monitoramento do histórico de navegação. Pelas redes sociais, essa vigilância secreta das informações é viabilizado pela violação de senhas, quando os agressores as adivinham ou respondem a questões de segurança para acesso às contas da vítima (FASCENDINI; FIALOVÁ, 2011). E caso essa artimanha se revele inviável, o agente vale-se do *proxy stalking*, ou seja, passa a monitorar o perfil de terceiros, que se encontram no entorno do seu alvo e que acidentalmente podem transmitir dados que comprometam a segurança da vítima (YARDLEY, 2021).

Por fim, no âmbito da *retributive omnipresence*, trata-se de uma onipresença exercida após o fim do relacionamento, quando a sobrevivente decide encerrar a relação abusiva, atitude vislumbrada como extrema pelo perpetrador, que, ante a perda do controle, busca se vingar da ex-parceira (YARDLEY, 2021). Previamente, a autoafirmação do homem, quando desafiado ou rejeitado, era predominantemente viabilizada pela violência física, porém, atualmente, essa violência assume viés simbólico ao expor a vítima publicamente (CAVALCANTE; LELIS, 2016). Assim, em busca dessa punição, o agente intensifica as práticas de abuso facilitado pela tecnologia, como o *proxy stalking*, e adere a novos métodos, dentre eles o compartilhamento público de informações pessoais, a fim de arruinar a reputação pessoal e profissional da sobrevivente, pilar imprescindível para a reconquista de sua autonomia e de seu poder de decisão (YARDLEY, 2021).

Também nessa conjuntura, práticas insistentes, como chamadas e mensagens à sobrevivente, tornam-se paulatinamente mais comuns, cujos conteúdos variam entre declarações de amor e ameaças, assim como o assédio à vítima e sua rede de apoio por meio de perfis falsos, a invasão a contas de redes sociais e a divulgação de imagens íntimas, conhecida como *revenge porn*. Ainda que haja uma exposição da imagem masculina, "os danos à honra sofridos são imperiosamente maiores que aqueles sofridos pelos homens, pois o olhar cultural da sociedade tende a culpar a vítima que compartilha suas imagens, protegendo o agressor e impedindo a sua punição" (CAVALCANTE; LELIS, 2016, p. 65). Aliás, caracteristicamente no meio cibernético, os perpetradores podem muitas vezes contar com uma rede de apoio externo, ou seja, de estranhos que colaboram com as condutas abusivas supracitadas e reforçam a narrativa construída, seja fornecendo sugestões, seja estimulando comportamentos ainda mais violentos, o que foi definido pela doutrina como *peer support* ou *peer influence* (CASTRO; SYDOW, 2021).

Em suma, tais práticas objetivam estabelecer o controle da narrativa pelo perpetrador e arruinar a dignidade da vítima, isolando-a ao máximo de sua rede de apoio (YARDLEY, 2021). Consequentemente, após um incidente de violência digital, a saúde mental é uma das esferas mais impactadas pelo sobrevivente, o que sucedeu com 45% das pessoas entrevistadas, em escala mundial, no estudo *Supporting a Safer Internet* (VALENTE, 2023). Afinal, tem-se que todo o constrangimento infligido causa um sentimento de vergonha e de humilhação à sobrevivente, impedindo sua denúncia às autoridades e gerando uma cifra oculta de vítimas, de sorte que o agente se beneficia dessa angústia e não sofre qualquer repercussão (SILVA, 2022;

YARDLEY, 2021). Apresenta-se igualmente um temor de que o ataque ultrapasse o ambiente online e alcance a segurança das vítimas fisicamente, tanto que 61% das mulheres brasileiras acreditam que a violência digital impacta muito negativamente a integridade física (VALENTE, 2023).

Nos cenários apresentados, tanto vítimas como profissionais não apresentam confiança no próprio conhecimento limitado de privacidade e segurança digital e nas estratégias de combate a essa violência, optando por substituição dos dispositivos para evitar o rastreamento ou pelo bloqueio do agente nas redes sociais, o que poderia refletir em uma reação ainda mais violenta (LEITÃO, 2021). A partir dessa constatação, é justificável que o Brasil, dentre 18 países analisados, seja o país em que as vítimas de violência digital, dotadas de uma percepção pessimista sobre a efetividade do aparato policial, menos recorrem às forças policiais (7%), linhas telefônicas de apoio (3%) ou serviços governamentais (2%) (VALENTE, 2023).

Embora a produção legislativa penal tarde a acompanhar as evoluções sociais, figura mais recentemente certa mobilização do Poder Legislativo a respeito das violências de gênero digitais. Por exemplo, instalou-se Comissão Parlamentar de Inquérito pela Assembleia Legislativa do Estado do Rio de Janeiro destinada ao Combate à Violência Cibernética contra as Mulheres, a fim de apurar causas e formas de prevenção e combate dos casos do Rio de Janeiro, que, em março de 2024, aprovou Relatório Final com 6 propostas de projetos de leis e 60 sugestões de medidas para enfrentamento da violência cibernética[6].

Exploradas as peculiaridades da violência digital de gênero, compete analisar de modo mais amplo o campo da cibercriminalidade que revolve o *stalkerware*, o qual, marcado pela invasão da privacidade telemática, exige uma proteção de novos valores sociais, como a confidencialidade dos dados pessoais, ensejando, para tanto, uma especialização do direito penal.

[6] Relatório de CPI propõe seis projetos de lei para combater a violência cibernética contra a mulher. **O Dia**, Rio de Janeiro, 7 mar. 2024. Disponível em: <https://odia.ig.com.br/rio-de-janeiro/2024/03/6805927-relatorio-de-cpi-propoe-seis-projetos-de-lei-para-o-combate-a-violencia-cibernetica-contra-a-mulher.html>. Acesso em: 06 jun. 2024.

3. O CAMPO TEÓRICO DA CIBERCRIMINALIDADE E A INVASÃO DE DISPOSITIVO INFORMÁTICO

3.1. Uma introdução à cibercriminalidade

Introduzido o marco teórico da violência de gênero digital, reconhece-se que uma proposta de criminalização do *stalkerware* se sustenta a partir de compreensão mais aprofundada do atual contexto cibernético, cujos avanços e enormes vantagens igualmente propiciaram um espaço livre e inicialmente desregulado para cometimento, não só de delitos antes inimagináveis, intrínsecos ao ciberespaço, como também de delitos clássicos sob nova roupagem.

Evidentemente, esse processo de informatização da sociedade apresentou marcos revolucionários, desde a criação de robôs e computadores até o advento da *Internet of Things*, das redes sociais e da inteligência artificial. Na contemporaneidade, vive-se em uma era de *converged environment*, ou seja, há uma transição quase imperceptível entre o mundo *online* e *offline*, ante a digitalização de atividades das esferas pessoal e profissional da população, representando a computação uma ferramenta facilitadora de tarefas cotidianas (GILLESPIE, 2019; SYDOW, 2015). Nessa nova conjuntura, a internet, qualificada como uma "aldeia global", idealmente representa uma sociedade de iguais e anônimos, não se restringindo a fronteiras estatais e facilitando a ocultação da identidade das pessoas (TOMASEVICIUS FILHO, 2016). Ressalva-se, no entanto, que os domínios técnicos individuais de manipulação de dados e conhecimento da linguagem variam entre si, concedendo poder a uma minoria de usuários antes comuns (SYDOW, 2015).

Cuida-se de uma era de difusão da *Internet of Things*, caracterizada pela interconexão sem fio de dispositivos físicos cotidianos que se comunicam e transmitem dados entre si, mas, sob outro enfoque, é certo que a eclosão do acesso remoto representou nova vulnerabilidade à maioria dos usuários, facilitando ataques maliciosos à privacidade e à confidencialidade dos dados pessoais, os quais, não só afetam a autonomia da vítima, como viabilizam a aquisição de ganho financeiro e de poder pelos perpetradores (CHAI *et al.*, 2021).

Na atualidade, diante da utilização sistemática de dispositivos eletrônicos e do fornecimento de informações em sites e plataformas, os dados informáticos adquirem tamanha importância por representarem extensão e espelho da vida pessoal, por meio dos quais são extraídos aspectos pessoais relativas ao cotidiano do indivíduo, às interações sociais, às escolhas de consumo, aos locais frequentados, entre outros. Diante desse novo perigo à

privacidade internalizado socialmente, Sydow (2015) descreve a sociedade informática como uma sociedade de risco *sui generis*, em que se verifica uma dilatação dos riscos:

> Se por um lado, os objetos e serviços desenvolvidos na sociedade material apresentam riscos, é notório, por outro lado, que boa parte de tais riscos, por serem palpáveis, são mais possivelmente identificáveis, pois que a materialidade implica limites.
>
> No que tange ao crime informático, o risco torna-se dilatado. As prospecções do futuro, o vulto tomado pela tecnologia e os recursos existentes no presente levam-nos à ideia de que o uso da informática é hábil para o cometimento de qualquer conduta que viole bens jurídicos protegidos (SYDOW, 2015, p. 54).

Incapaz de se autorregular e diante da dificuldade de imposição de um instrumento normativo transnacional, propiciou-se a difusão de uma criminalidade virtual, em face da qual o direito penal tradicional se revelou deficitário (SYDOW, 2015; TOMASEVICIUS FILHO, 2016). Na contramão, convém corroborar que a mobilização por soluções jurídicas não acomoda a inauguração de um novo direito penal, e sim o "usual avanço do direito penal em novos espaços de conflitualidade, marcados, *in casu*, por uma muito especial complexidade e por particularidades atinentes ao espaço no qual ele se projeta, a informática" (D'AVILA; SANTOS, 2016, p. 93)

Sob a demanda de adaptação do direito penal a essa realidade, compreende-se que, por um lado, as formas delitivas tradicionais, dotadas de novas formas de realização, passaram a ser concretizadas mediante o computador e outros dispositivos, o que repercutiu, em resposta, na aplicação dos tipos penais usuais, ainda que não tenham sido completamente revisados (D'AVILA; SANTOS, 2016). Por outro lado, partindo da insuficiência dos mecanismos penais preexistentes e de inovadora configuração delitiva, exigiu-se uma nova tipificação voltada aos "*true cybercrimes*", unicamente praticados pela internet (WALL, 2007). Nesse contexto, é inevitável ponderar que potencialidades tecnológicas, dentre elas a inteligência artificial, geraram questionamentos a respeito de categorias e princípios do direito penal até então consolidados, especialmente referente à atribuição de responsabilidade penal (AIRES DE SOUSA, 2020).

Nesse espectro, assimilando a virtualidade como verdadeiro meio ambiente, Sydow (2015) considerou necessária a existência do bem jurídico autônomo da segurança informática, posto que há condutas que, ao comprometer a segurança do ambiente informático, não estariam abrangidas pelos valores jurídico-penais preexistentes. Nesse âmbito, classifica esse novo bem jurídico tanto como de natureza individual como difusa, cuja afetação, em determinado grau, apresenta potencial de causar danos a toda coletividade (SYDOW, 2015). Era de se esperar, portanto, nesse esforço de acompanhamento da tendência tecnológica vigente, a atribuição de

novos conceitos na esfera penal, tais como “crimes informáticos”, “crimes digitais”, “*computer crimes*” ou “crimes cibernéticos”, nomenclaturas que carecem de uma singularização.

Em atenção às elementares do tipo penal, interessa a definição do crime informático ou digital como “toda ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão” (FERREIRA, 2000, p. 207), havendo atos que atentam contra o sistema informático em si ou contra outros bens jurídicos mediante o suporte informático.

De forma semelhante e em sintonia com a doutrina especializada, importa classificar os delitos informáticos em impróprios e próprios, eis que os delitos impróprios podem ser cometidos por outros meios, resumindo o sistema informático a uma das ferramentas possíveis, enquanto os próprios “visam atingir um sistema informático ou seus dados, precisamente violando sua confidencialidade, sua integridade ou sua disponibilidade” (SYDOW, 2015, p. 88). Ou seja, compreende uma divisão baseada na afetação de bens jurídicos, eis que os crimes impróprios atingem interesses fundamentais já tutelados por tipos penais preexistentes, enquanto os próprios atentariam contra um bem jurídico informático, isto é, a inviolabilidade dos dados de um sistema informático. Igualmente, cabe mencionar a classificação dos delitos mistos - caracterizados pela tutela da inviolabilidade dos dados e bem jurídico diverso - e dos delitos informáticos mediatos ou indiretos, quando um delito informático próprio é praticado como crime-meio para a realização de um crime-fim não informático, o que se compatibiliza perfeitamente ao *stalkerware* (VIANNA; MACHADO, 2013). De acordo com essa acepção, ainda que conste lesão ao bem jurídico da inviolabilidade dos dados informáticos, essa ofensa não seria punida autonomamente, em virtude da aplicação do princípio da consunção.

A respeito dos crimes cibernéticos, tem-se como ponto de partida que a cibercriminalidade corresponde a uma das variantes dos crimes digitais ou informáticos, eis que demanda o recurso específico do ciberespaço, explorando suas vulnerabilidades. Nessa toada, em prol da compreensão do conceito de crime cibernético, importa observar que o ciberespaço é o espaço de interconexão de computadores, tendo como principal exemplo de rede a internet, a qual abrange um sistema global de computadores, de forma que as partes dessa rede são navegadas e conectadas por meio da *Web*, viabilizando a disponibilização e o compartilhamento de informações (GILLESPIE, 2019).

Ainda, cumpre introduzir a definição de internet nos termos do artigo 5º, inciso I, da Lei 12.965/2014 (Marco Civil da Internet), segundo o qual a internet consiste em “sistema

constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes". Adotando essa concepção, não se trata tecnicamente de um crime cibernético quando o agente acessa fisicamente o computador da vítima e baixa informações confidenciais em um pendrive para vender a um concorrente, já que o crime ocorreu mediante métodos *offline*, sem envolver o ciberespaço (GILLESPIE, 2019).

Ante a complexidade do campo da cibercriminalidade, Sandywell (2010) diferencia tais crimes em três categorias: crimes tradicionais que são expandidos ou intensificados pela internet, como a fraude de cartão de crédito; crimes generalizados e radicalizados pela internet, por exemplo, o *bullying*; e crimes criados pela internet, exemplificados pelo hackeamento (GILLESPIE, 2019; SANDYWELL, 2010). Entretanto, consciente de definições e classificações não-unânimes de crimes cibernéticos, é razoável apresentar outras categorizações de relevo da cibercriminalidade, como a categorização pelos comportamentos do ofensor e da vítima. Nessa toada, Gillespie divide os crimes cibernéticos em: crimes contra computador, os quais passaram a existir com a internet e o computador é o alvo do crime; crimes contra propriedade, os quais objetivam subtrair propriedade financeira ou intelectual de outrem; crimes envolvendo conteúdo ilícito, relativos à publicação, armazenamento ou acesso a conteúdo questionável; e crimes contra a pessoa, em que a tecnologia é utilizada como arma contra o indivíduo, causando danos a outrem (GILLESPIE, 2019).

Sob uma perspectiva vitimológica, Button *et al.* propõem uma distinção dos crimes computacionais a partir dos impactos sobre a vítima, os quais seriam comparáveis aos efeitos psicológicos decorrentes de crimes tradicionais, categorizando-os em incidente de menor transtorno, crime de transtorno e crime grave de violação pessoal ou de significativa perda financeira (BUTTON *et al.*, 2021). Os incidentes de menor transtorno, esperados no cotidiano moderno, raramente são vislumbrados como crimes e não costumam ser denunciados às autoridades, apresentando nenhum ou pequeno prejuízo financeiro; os crimes de transtorno consistem em incidentes criminosos com uma prioridade média para notificação policial, um dano patrimonial que é recuperado ou não, interrompendo a rotina e gerando possíveis impactos psicológicos; por fim, a última categoria englobaria crimes graves, que geram sentimentos de violação da identidade digital e reflitam em significativo risco ou efeito prejuízo financeiro, sendo prioritariamente denunciados ao poder estatal, de modo que causaram uma interrupção

mais longa do dia a dia e repercutiram mais profundamente na integridade psicológica da vítima (BUTTON *et al.*, 2021).

Ao elencar as distintas possibilidades de assimilação dos crimes cibernéticos, objetiva-se inserir adequadamente o fenômeno do *stalkerware* nesse movimento de especialização do direito penal, cuja preocupação se volta a um novo bem jurídico, ou ao menos, a uma reformulação do tradicional arranjo protetivo, bem como decifrar as singularidades do ambiente virtual, capazes de afetar a eficácia das normativas penais.

Nessa esteira, importa examinar que, de fato, o ciberespaço ostenta determinadas particularidades aptas a expor novos desafios ao direito penal, fomentando a perda da importância das fronteiras espaciais e temporais. Destacam-se o anonimato, auxiliando na ocultação de sua identidade e dificultando a persecução penal, assim como a automação, propiciando potencial delituoso de alcance de centenas ou até milhares de vítimas por meio de sistemas automatizados, sem exigir o cometimento de um crime pessoalmente pelo perpetrador (BRENNER, 2006). Nesse cenário, assenta-se que tanto vítima quanto perpetrador são atingidos por uma sensação de segurança característica do ciberespaço, eis que o agente acredita que suas condutas delituosas são resguardadas pelo anonimato, enquanto o usuário padrão, sem visualizar os riscos informáticos com clareza, tampouco compreende o valor dos seus dados nos meios informáticos (SYDOW, 2015). Há, portanto, uma relativização dos padrões éticos, já que quaisquer condutas, inclusive criminosas, são vistas como toleráveis no ciberespaço por influência de uma percepção social de distância entre realidade e mundo virtual, assim como consta uma pseudoinvisibilidade do dano causado à vítima, uma vez que é difícil identificar tanto a origem como a extensão dos danos materiais e psicossociais, cujos efeitos podem ser intensificados pela difusão nas mídias (CASTRO; SYDOW, 2021).

Dentre as especificidades desse campo, também compete salientar a habilidade de cometer crimes remotamente, o que subverte a lógica face a face dos crimes tradicionais, uma vez que a proximidade física com a vítima equivale a uma reiterada elementar típica dos delitos clássicos e, sendo possível atentar contra vítimas de outros países, não se descartam possíveis conflitos de jurisdição (BRENNER, 2006). Assim, em face da transnacionalidade e da instantaneidade do cometimento de delitos, há evidentemente um redimensionamento das noções de tempo e espaço no âmbito virtual, de sorte que uma persecução penal adequada nem sempre é alcançada mediante uma política estritamente local, exigindo uma cooperação internacional (D'AVILA; SANTOS, 2016). Como resultado, paira uma singular impunidade no

ciberespaço, em razão de precários mecanismos de proteção da vítima e de responsabilização dos autores (CASTRO; SYDOW, 2021).

A título de contraponto, é mais do que viável a ocorrência de crimes cibernéticos em território nacional, dentro dos limites jurisdicionais de um país soberano, de modo que, nessa hipótese, tanto perpetrador como vítima se situam fisicamente no mesmo território soberano (BRENNER, 2006). Exemplificando, Brenner concebe o *cyberstalking* como exemplo de crime cibernético local, pois, embora o ciberespaço compreenda a transmissão de sinais para dentro e fora do território soberano, frequentemente o agente e a vítima residem na mesma comunidade e já se encontraram no mundo físico, de modo que o agente persegue a vítima *online* para ocultar sua identidade, localizando-se ambos no mesmo território (BRENNER, 2006).

À vista da interconexão global entre as redes e do caráter frequentemente transnacional dos crimes cibernéticos, impende estabelecer que a Convenção sobre o Crime Cibernético, firmada pelo Brasil em Budapeste em novembro de 2001 e promulgada em 2023 pelo Decreto nº 11.491, consiste em importante instrumento internacional sobre cibercriminalidade, visando instituir política criminal comum e global em prol da proteção social contra o crime cibernético, de modo a harmonizar procedimentos legais e políticas dos estados signatários, bem como facilitar a cooperação internacional na resposta penal desses crimes (FAUBERT *et al.*, 2021).

Nesse sentido, buscando inspirar a criação de tipos penais incriminadores nos ordenamentos jurídicos internos - influência que se verificou nos tipos penais do ordenamento brasileiro, em especial ao comparar a redação do artigo 2º da Convenção à do artigo 154-A do Código Penal -, esse instrumento postulou a necessária intervenção penal quanto à tutela dos dados pessoais no ambiente informático, contribuindo para a construção de um bem jurídico-penal sob o prisma da "confidencialidade, integridade e disponibilidade dos sistemas informáticos, redes e dados de computador", conforme disposto em seu preâmbulo (FERREIRA, 2023). Ainda assim, há de se analisar que as discussões dominantes no âmbito da cibercriminalidade priorizam dimensões do patrimônio, da propriedade intelectual e da segurança em detrimento de violências interpessoais facilitadas pela tecnologia, de modo que a adoção de uma postura neutra e até insensível quanto aos marcadores da diferença contribui para a atual escassez de estratégias de prevenção e resposta à violência de gênero digital (O'BRIEN; MARAS, 2024).

Nessa linha, repisa-se ser essencial que uma possível proposta de incriminação do *stalkerware* esteja familiarizada com a produção legislativa do ordenamento pátrio direcionada

à cibercriminalidade, possibilitando desde já a identificação do seu fundamento protetivo e de eventuais indeterminações do texto legal. No Brasil, o interesse em uma legislação própria aos crimes informáticos alavancou por influência de clamor social em 2012, após o furto de imagens íntimas da atriz Carolina Dieckmann mediante invasão do seu computador, a qual foi extorquida pelos perpetradores em troca da não divulgação pública das imagens (GRANATO, 2015). Ainda que os autores tenham sido posteriormente identificados e indiciados pelos delitos de furto, extorsão qualificada e difamação, o ordenamento jurídico ainda não apresentava proteção penal contra a invasão de computadores em si. Em razão dessa lacuna jurídica, a repercussão midiática do caso acelerou a tramitação do preexistente Projeto de Lei nº 2.793 e foi sancionada a Lei Federal 12.737/2012, a qual propôs a inclusão de tipos penais voltados ao combate da criminalidade informática.

De acordo com o PL 2.793/2011, criado em substituição ao PL 84/99 e optando por um número diminuto de tipos penais, reconheceu-se que ainda seria possível a persecução de certas condutas praticadas por meios eletrônicos com base no ordenamento jurídico em voga, evitando incorrer na falácia de que a proliferação de tipos penais conduziria à maior repressão (BRASIL, 2011). Assim, contrário a uma expansão desnecessária da tutela penal, propôs a criação de tipos penais com maior grau de determinação "aplicáveis à condutas praticadas na Internet mas apenas aquelas estritamente necessárias à repressão daquelas atividades socialmente reconhecidas como ilegítimas e graves" (BRASIL, 2011, p. 4). Nesse contexto, de modo complementar, foi sancionada a Lei nº 12.735, de 2012, a qual determinou como medida de maior relevo a instalação de delegacias especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado, conforme previsto em seu artigo 4º, eis que se revela urgente a formação de um aparato policial técnico para a persecução penal dos crimes cibernéticos.

3.2. A invasão de dispositivo informático

Dentre os tipos penais criados pela Lei Carolina Dieckmann, em atenção ao recorte temático do *stalkerware*, enfatiza-se a análise do delito de invasão de dispositivo informático, previsto no atual artigo 154-A do Código Penal. Na redação original do projeto de lei, buscando representar um acesso indevido, o elemento nuclear consistia no verbo "devassar", posteriormente substituído pelo verbo "invadir" na Lei nº 12.737, de 2012. Quanto à intenção específica do agente, observa-se que foi mantida a versão do projeto legislativo, uma vez que o

legislador, evitando punir atividades possivelmente legítimas da internet, delimitou o combate apenas às condutas vinculadas a um resultado danoso ou a finalidades efetivamente censuráveis, sob uma perspectiva de direito penal mínimo:

> Art. 154-A. **Devassar** dispositivo informático **alheio**, conectado ou não a rede de computadores, **mediante violação indevida de mecanismo de segurança** e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, instalar vulnerabilidades ou obter vantagem ilícita:
> **Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa** (grifos nossos)

Inserido na seção de crimes contra a inviolabilidade dos segredos, interpreta-se que o bem jurídico a ser protegido não configura o dispositivo informático ou a segurança informática em si, mas a intimidade e a privacidade, componentes da liberdade individual e presentes no artigo 5º, X, do dispositivo constitucional, em prol da inviolabilidade dos dados e informações pessoais em dispositivo informático (COSTA, 2020; RAMOS JÚNIOR, 2012; VIANNA; MACHADO, 2013).

No mesmo sentido, Bitencourt defende que a proteção penal volta-se à privacidade individual, pessoal ou profissional da vítima (BITENCOURT, 2022), eis que, nas palavras de Sydow (2015, p. 87), "a proteção de dados e dispositivos informáticos e, especialmente, dos conteúdos que armazenam é uma exigência fundamental da atual vida social informatizada, que deve ser respeitada como princípio da ordem pública". Em consonância a essas perspectivas, Nucci (2023, p. 1.166) classifica o objeto jurídico como múltiplo, "envolvendo a inviolabilidade dos segredos, cuja proteção se volta à intimidade, à vida privada, à honra, à inviolabilidade de comunicação e correspondência e à livre manifestação do pensamento, sem qualquer intromissão de terceiros" assim como o patrimônio da vítima. Distinguindo-se em parte, conforme já mencionado, Sydow defende que, além da proteção da confidencialidade dos arquivos contidos em dispositivos informáticos, da integridade e da disponibilidade desses dados, cuida-se de tutela do novo bem jurídico a segurança telemática (SYDOW, 2015).

Em exame da compatibilidade dessa conduta ao *stalkerware*, há de se resgatar que esse fenômeno delitivo é constatado não só quando o parceiro instala o aplicativo em um momento de ausência da companheira, mas também quando a própria vítima, induzida em erro, instala o aplicativo. Com base nessas condutas delitivas, depreende-se o crime-meio de invasão de dispositivo informático, ocorrendo o acesso indevido a um dispositivo informático, com o fulcro de instalar vulnerabilidades sem autorização expressa ou tácita da usuária, neste caso um aplicativo *spyware*. Usualmente, têm-se como consequência a obtenção de conteúdo de

comunicações eletrônicas privadas, o que adentraria a forma qualificada do §3º do delito disposto abaixo:

> Invasão de dispositivo informático
>
> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
>
> § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Após a promulgação da Lei em questão, criticou-se a ausência de uma conceituação legal de termos previstos no dispositivo penal, como as expressões “dispositivo informático”, “invasão” e “vulnerabilidades”, conceitos que passaram a serem desenvolvidos pela doutrina e pela jurisprudência (RAMOS JÚNIOR, 2012; SYDOW, 2015).

Em relação à “invasão”, consiste na ação de “violar ou ingressar, clandestinamente, isto é, sem autorização de quem de direito” (CRESPO, 2011, p. 63), interpretada aqui como acesso indevido a um dispositivo, independentemente de haver utilização de senha concedida pelo alvo ou não. A partir desse conceito, importa destacar que igualmente haveria a violação do dispositivo quando o próprio alvo, induzido em erro pelo agente, instala o aplicativo de *spyware* e faculta o acesso ao dispositivo, uma vez que, desconhecendo a real finalidade do *software*, o consentimento da vítima se encontra viciado (FERREIRA, 2023). Dessa forma, não se descarta como sujeito ativo o cônjuge que acessa dados de dispositivo do parceiro sem autorização prévia, posto que o “casamento não concede qualquer tipo de autorização tácita para que se vasculhe a vida privada e íntima do cônjuge [...], razão pela qual não há falar em ‘exercício

regular de direito' de bisbilhotar os dados no computador ou no celular do cônjuge sem a sua autorização" (VIANNA; MACHADO, 2013, p. 95).

Ainda no cerne das relações afetivas, há de se problematizar as hipóteses em que, embora o uso do dispositivo pelo parceiro para determinadas atividades seja autorizado pela usuária, ele pode se aproveitar para instalar vulnerabilidades não autorizadas, como o aplicativo de *spyware*, em prol do controle das comunicações. A partir dessa situação hipotética, tendo em vista que o ingresso ao dispositivo chegou a ser permitido, alguns argumentariam não haver propriamente uma invasão nos termos do tipo penal, ensejando dúvidas a respeito da tipicidade da conduta descrita. Nesse âmbito, observa-se que o legislador falhou ao não refletir sobre os distintos graus de acesso a dados informáticos, eis que se vislumbram os cenários de proibição ou permissão de acesso total ou parcial a um dispositivo, evidenciando que um ato de anuência do titular do dispositivo afeta significativamente o nível de lesividade da conduta (SYDOW, 2015). Portanto, a respeito do consentimento de acesso pela vítima, há de se concordar com Sydow:

> Qualquer que seja a maneira pela qual o meio de acesso ao sistema informático de um usuário é obtido, o ingresso em bem jurídico (propriedade) alheio exige anuência e permissão, sob pena de ser considerado abusivo. [...] A violência da conduta está no fato de que o acesso e tudo o que está relacionado com ele são individuais, exclusivos e somente podem ter seu caráter íntimo e pessoal publicado por quem detém o direito de divulgação e permissão (SYDOW, 2015, p. 116).

A respeito do especial fim de agir da instalação de vulnerabilidades para obtenção de vantagem ilícita, a vulnerabilidade compreenderia uma "entrada escondida" de acesso livre e desimpedido instalada a partir de um programa, raramente percebida pela vítima da violação da privacidade (SYDOW, 2015). Para fins exemplificativos, a doutrina cita o upload de *malwares*, "*softwares* utilizados para causar danos ou permitir o acesso indevido a informações em dispositivos informáticos" (COSTA, 2020, p. 616), os quais podem depender da interação do alvo para instalação, como cavalo de Troia, *rootkis* e o *spyware*, surgindo com a aparência de um s*oftware* legítimo ou introduzido como um anexo de e-mail, download ou execução de arquivo de determinado website (PASCOLATI JUNIOR, 2022).

Nesse cerne, no ordenamento jurídico brasileiro, somente se verifica a responsabilização criminal da inserção do *malware* no contexto da invasão de dispositivo informático quando aliada à obtenção de vantagem indevida, nos termos do artigo 154-A do Código Penal. Opondo-se à classificação da instalação de vulnerabilidade como especial fim de agir, Nucci entende que "invadir" e "instalar vulnerabilidades" seriam dois núcleos da conduta, na qualidade de tipo misto alternativo, ou seja, caso o mesmo agente instale a

vulnerabilidade e, em seguida, invada, comete um único delito; se ele instalar e outro se aproveitar da vulnerabilidade invadindo, cada um teria cometido um delito (NUCCI, 2023).

Importa ademais registrar a problemática utilização do plural "vulnerabilidades", pois uma leitura restritiva do texto normativo admitiria somente a instalação de mais de um mecanismo de vulnerabilidade para a configuração do tipo, ainda que já efetivados danos ao ofendido com um só (SYDOW, 2015). Trata-se de falha do legislador, pois, em termos práticos, caso somente ocorresse a instalação de um único aplicativo *spyware* que viabilizasse o acesso às comunicações do alvo, essa conduta resultaria atípica. Na sequência, o legislador optou por não especificar a natureza da vantagem ilícita, o que poderia abranger vantagens de teor patrimonial, sexual, competitiva, entre outros (SYDOW, 2015).

Sendo a forma qualificada do §3º do artigo 154-A de especial relevância ao estudo do *stalkerware*, cumpre mais uma vez sinalizar que foi delegado à doutrina o papel de conceituar o "conteúdo de comunicações eletrônicas privadas", gerando a dúvida de abranger apenas questões íntimas e de relevo sigilo ou também de mero caráter pessoal (REALE JÚNIOR, 2023). Nesse escopo, interpreta-se que esse conteúdo alcançaria "dados utilizados via VoIP (telefonia por meio da internet), arquivos de log de comunicadores instantâneos, registros e arquivos de backup de mensagens trocadas por redes sociais, fax enviados por meio de programas específicos" (SYDOW, 2015, p. 313), respaldados constitucionalmente pelo art. 5º, XII, da Constituição Federal.

Com o propósito de evidenciar as falhas da redação antiga do artigo 154-A quando aplicadas ao *stalkerware*, considera-se a decisão monocrática do Agravo em Recurso Especial n. 1.721.099 pelo Superior Tribunal de Justiça (Anexo B), publicada em 13 de agosto de 2020. No caso concreto, de acordo com perícia e acórdão da segunda instância, o ex-namorado instalou três *softwares* espiões no notebook da vítima, por meio dos quais monitorava suas conversas e atividades, a fim de "averiguar se 'valeria a pena investir' no relacionamento, o que, indubitavelmente, pode ser caracterizado como ganho pessoal". Nesse típico exemplo de *stalkerware*, é importante observar que o Tribunal de origem entendeu pela incriminação de duas condutas de invasão de dispositivo informático, mantendo a condenação pela forma qualificada do delito de dispositivo informático: "Pois bem, a instalação do referido programa 'espião' pelo recorrente, conduta que, por si só, já configura a figura típica prevista no artigo 154-A do Código Penal, viabilizou a prática da segunda conduta prevista no referido dispositivo, qual seja, a da invasão em si". Portanto, nesse caso concreto, interpretou-se

configurar tipo misto alternativo, vislumbrando a ocorrência de duas condutas: a invasão de dispositivo informático e a instalação de vulnerabilidade.

Ainda que a condenação tenha sido mantida e o agravo, não conhecido sob o fundamento da Súmula 7 do STJ, a argumentação aventada pelo recorrente possibilita a problematização das elementares do tipo penal do artigo 154-A, eis que se demonstram a restrição da interpretação do dispositivo mediante a exigência da violação a mecanismo de segurança e o impasse dos graus de autorização concedidos pela vítima, assim como nem sempre é automática a aferição da obtenção de uma vantagem ilícita:

> No decorrer do processo (defesa e apelação), o Recorrente demonstrou que não é qualquer dispositivo informático invadido que conta com a proteção legal e que, para que seja configurado o crime, **é necessário que ele conte com "mecanismo de segurança", como antivírus, firewall, senhas, etc. e que, no caso, o computador não possuía qualquer - a perícia realizada também não apontou a existência ou violação dos citados dispositivos de segurança.** (fl. 429 - g.n.). Sucedeu-se a interposição de apelo pela ora Recorrente, que arguiu que a sentença mereceria reforma em virtude da conduta ser atípica, pois os requisitos caracterizadores do delito previsto no artigo 154-A do Código Penal não se fazem presentes: (fl. 430). [...] **porque não houve violação a mecanismos de segurança;** (fl. 430 - g.n.). [...] porque havia autorização tácita da Ofendida para que o Recorrente utilizasse seu computador; e (fl. 430 - g.n.). [...] **porque não houve qualquer "obtenção de vantagem ilícita"; (fl. 430).** Demonstrou, ainda, a ausência de animus nocendi do Recorrente, não restando configurado o tipo subjetivo (dolo) [...] (fl. 430 - g.n.).
>
> Não há nos autos demonstração das elementares do tipo penal do crime de invasão a dispositivo informático. Muito embora a sentença recorrida tenha, exaustivamente, analisado o conceito do objeto da conduta dispositivo informático - nada foi analisado quanto às demais elementares do tipo. (fl. 435). (AREsp n. 1.721.099, Ministro Presidente do STJ, DJe de 13/08/2020, grifos nossos)

Evidentes as indeterminações do dispositivo normativo original, alterou-se, mediante a Lei nº 14.155, de 2021, a redação referente à caracterização de dispositivo informático como "alheio" para "de uso alheio", uma vez que o usuário principal nem sempre é o titular do dispositivo informático. Ou seja, é possível que o dispositivo invadido pertença à empresa ou a outrem, desde que o alvo da intrusão seja aquele destinado a utilizá-lo. Ademais, foi acertadamente excluído o meio "violação indevida de mecanismo de segurança", que antes conferia uma aplicação restrita do tipo penal, posto que a tutela penal não alcançava aqueles aparelhos sem mecanismos de segurança. Sob essa leitura, a configuração do tipo penal antes exigia o meio específico de violação de senhas, travas de segurança ou *softwares* de antivírus, de modo que usuários, que não escolheram acionar esses meios assecuratórios por desnecessidade ou falta de conhecimento técnico, encontravam-se fora do âmbito de proteção penal (COSTA, 2020; DE BARROS, 2015). Mediante essa supressão do requisito da violação de mecanismo de segurança, o conceito de invasão, interpretado como acesso não autorizado,

passaria a abarcar condutas antes não abrangidas pelo tipo penal, como o *stalkerware* (SYDOW, 2022).

Em adição, aumentou-se a pena-base originalmente prevista de 3 meses a 1 ano e multa, equivalente à pena do delito de violação de sigilo profissional (art. 154, CP), para a pena de 1 a 4 anos e multa, assim como as penas das qualificadoras igualmente foram agravadas. Nessa medida, cumpre antecipar uma das decorrências da exasperação da pena para a tipificação da prática do *stalkerware*, dentre elas, a impossibilidade de absorção do crime-meio, consistente na invasão de dispositivo informático, pelo crime-fim de *stalking*, disposto no artigo 147-A do Código Penal, preocupação esta que será analisada em capítulo posterior.

No ordenamento penal brasileiro, inicialmente não causaria estranheza vincular a prática do *stalkerware* ao crime de interceptação legal, tipificada no artigo 10 da Lei nº 9.296/1996, o qual abrange a interceptação telemática ou informática. Todavia, conquanto constitua crime informático que viola o sigilo das comunicações, não constitui obtenção de informações de dispositivo informático da vítima a qualquer momento, somente sucedendo uma interceptação com a captura de dados transferidos de um dispositivo para outro, isto é, em trânsito (VIANNA; MACHADO, 2013). De modo complementar, usualmente o sujeito ativo do crime de interceptação configura empresa prestadora de serviço, ou seja, pessoa jurídica, e não a pessoa efetivamente interessada nas comunicações interceptadas (SYDOW, 2022). À vista dessas críticas, o meio de prática do *stalkerware* ainda é melhor descrito pela atual redação do crime de invasão de dispositivo informático do artigo 154-A do Código Penal.

Em suma, por mais que se conclua pela necessidade de um dispositivo penal que inserisse em sua esfera normativa a violação da privacidade em dispositivos informáticos, contudo, não se ignora a problemática técnica legislativa da Lei de Crimes Cibernéticos, tampouco a afronta ao princípio da proporcionalidade, em vista da gravidade das penas a serem cominadas (REALE JÚNIOR, 2023). Nessa perspectiva, há de se sopesar que, a despeito das inúmeras críticas e de necessárias modificações para melhor aplicabilidade da política legislativa penal vigente, a presente legislação penal cibernética configura importante medida de delimitação do injusto informático, garantindo proteção maior à vítima. Ao mesmo tempo, tratando-se de uma demanda com elevada mobilização social, há de se atentar ao risco de produção de uma legislação penal simbólica, cuja criação, resultante de uma pressão popular, é instrumentalizada pelo legislador para garantir apenas ganhar políticos e enganar a população

sobre uma suposta capacidade de resolução de problemas sociais, revelando-se, assim, ineficaz para a tutela do bem jurídico (HASSEMER, 2001).

Diante da tutela de um bem jurídico no espaço virtual, a aplicabilidade de uma produção legislativa penal cibernética, em conformidade ao princípio da *ultima ratio,* exige, inicialmente, contornos mínimos legais referentes à virtualidade, sendo evidente que uma maior regulamentação global cibernética por outras searas auxiliaria igualmente na prevenção do cometimento desses delitos (FERREIRA, 2023; SYDOW, 2015). Nesse sentido, ainda que posterior, a Lei nº 12.965, de 2014, largamente conhecida como Marco Civil da Internet, objetivou estabelecer "princípios, garantias, direitos e deveres para o uso da Internet no Brasil", conforme prevê no seu artigo 1º.

Em atenção à base principiológica desse dispositivo, é introduzida a preocupação com a autodeterminação informativa, isto é, o direito à proteção dos dados pessoais, inclusive nos meios digitais, consagrado pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) e alçado a nível constitucional em 2022 pela Emenda Constitucional nº 115 (FERREIRA, 2023). Reconhecendo a assimetria de poder informacional entre o usuário e outras figuras da realidade digital, essa difusão de valores vinculados à confidencialidade dos dados, privacidade e neutralidade da rede pelo texto legal cível confere maior legitimidade à tutela do bem jurídico penal (SYDOW, 2015).

Em razão do exposto, ainda que não se trate de um novo direito penal, mostrou-se primordial, em prol da proteção de bens jurídicos vinculados à liberdade e à privacidade em dispositivo informático, a criação de tipos penais que propiciem o combate aos crimes cibernéticos, cujas particularidades impõem novos temores à vítima e dificultam sua persecução penal, a qual exige um aparato policial especializado e, por vezes, uma cooperação internacional. Porém, não há de se denotar dessa inferência a imprescindibilidade de uma contínua expansão do direito penal, a qual somente deve ocorrer quando o conjunto normativo vigente não restar suficiente para a proteção de determinados valores jurídico-penais sob ataque. Optando por um equilíbrio entre as noções de direito penal mínimo e o surgimento de condutas que atentem contra o bem-estar social, essa perspectiva revela-se verdadeiramente proveitosa para a delimitação do bem jurídico a ser protegido no combate ao *stalkerware*, cuja tutela não demanda a invenção de uma norma penal incriminadora própria.

Consciente disso, cabe compreender que, no caso do *stalkerware*, e consequentemente do *cyberstalking*, a intrusão informática não constitui o crime-fim dos perpetradores,

consistindo, na realidade, em um dos meios de configuração de outro delito. Em conformidade a essa premissa, retoma-se que o *stalkerware* ocorre quando o perpetrador persegue alguém reiteradamente, geralmente companheiras ou ex-companheiras, por meio da invasão de dispositivo informático, invadindo sua esfera de liberdade ou privacidade. Nesse viés, tendo delineado o fundamento penal de combate à cibercriminalidade, é imperioso discorrer a respeito do marco teórico do *cyberstalking*, precipuamente sob o viés da violência de gênero, a fim de assegurar uma criminalização adequada do *stalkerware.*

4. CONTORNOS JURÍDICO-PENAIS DO *CYBERSTALKING*

Em tópico anterior, evidenciou-se que uma resposta ao *stalkerware* demanda uma compreensão do regime jurídico dos crimes cibernéticos estabelecido pelo ordenamento pátrio e da delimitação do bem-jurídico do crime-meio. Entretanto, é de rigor frisar que esse fenômeno apresenta como núcleo de sua conduta a prática de perseguição da vítima pelo monitoramento remoto de suas comunicações e rastreamento da localização, possibilitados, por sua vez, pela instalação do *spyware* em dispositivos. Logo, embora seja de suma relevância apresentar resposta estatal a comportamentos cibernéticos danosos a bens jurídicos, uma intervenção penal legítima em face do *stalkerware* centrar-se-ia sobre a criminalização de condutas atentatórias à liberdade e à privacidade da vítima, as quais coincidem com os bens jurídicos resguardados pelo tipo penal do *stalking*, previsto no artigo 147-A do Código Penal.

4.1. Atual intervenção penal em face do *stalking*

Nessa linha, situando-se próximo a condutas de assédio moral e *bullying*, o *stalking* consistiria em "forma específica de assédio, ligada à perseguição e limitação da liberdade da vítima pelo stalker, seja essa liberdade física ou virtual, no mundo digital" (CARVALHO; HENRIQUES, 2021, p. 130), cujo comportamento hostil e indesejado é caracterizado pelo critério objetivo da habitualidade. Ou seja, embora a conduta do *stalker* isoladamente possa soar insignificante, o estilo comportamental, marcado pela reiteração de atos dotados de relevância, afeta gravemente a vítima, não bastando igualmente um único ato intenso (CARVALHO; HENRIQUES, 2021; SOUZA 2022). Assim, por mais que o legislador não tenha delimitado um número mínimo de atos para qualificação como *stalking*, delegando essa análise à apreciação judicial do caso concreto, postulou-se na literatura ao menos dois atos de perseguição (SOUZA, 2022; WILSON *et al.*, 2022).

Trata-se de conduta que recebeu maior notoriedade nos anos 1990, em especial nos países anglo-saxônicos, de forma que o assassinato da atriz norte-americana Rebecca Schaefer por um fã obcecado, em 1989, impulsionou o desenvolvimento de uma legislação antistalking (FLORES, 2014; VANDER, 2006). Inicialmente, os meios de comunicação midiáticos associavam o *stalking* unicamente às perseguições infundadas de celebridades, mas passou-se a relacioná-lo com a violência doméstica e de gênero, ante episódios de perseguição após términos de relacionamentos (FLORES, 2014). Portanto, em análise do perfil vitimológico do *stalking*, nota-se que a prática de perseguição ininterrupta e intrusiva de um sujeito se vincula ao propósito de iniciar, restabelecer ou manter uma relação, apesar da recusa da vítima, o que atinge precipuamente mulheres.

Em sua maioria ex-parceiros íntimos, os perpetradores não só estão mental e emocionalmente obcecados pela sua vítima, como também distorcem a realidade ao responsabilizar a vítima pelo seu comportamento, justificando que ela os teria provocado, que não sabe que ambos estariam predestinados um ao outro ou que o havia tratado mal a ponto de merecer uma vingança sob a forma de terror psicológico (HOFFMANN; WONDRACK, 2005). No mais, em um contexto de relacionamento íntimo, os perpetradores, ainda quando desinteressados em mantê-lo, nutrem sentimento de posse sobre o corpo feminino e tampouco aceitam que a ex-companheira constitua novo vínculo afetivo, passando a perseguir seus passos, o que demonstra a influência direta do *stalking* pelas expectativas sociais de gênero (CASTRO; SYDOW, 2021).

Desse modo, afirma-se que a perseguição, ocorrendo frequentemente após a ruptura de relacionamentos, se apresenta como extensão da violência já presente na relação entre agente e vítima, de modo que essa postura controladora se associa à necessidade de afirmação de poder exercido em níveis físico, social, psicológico e financeiro sobre a sobrevivente, vindo à tona quando a autoridade de uma das partes se vê ameaçada, o que explicaria o aumento da violência após uma separação (COELHO; GONÇALVES, 2007).

Contribuindo para a impunidade, precipuamente na conjuntura de relações afetivas abusivas, a literatura menciona a auto-culpabilização da sobrevivente pela violência sofrida, sentimento esse aproveitado pelo *stalker*, haja vista que a vítima inicialmente enxerga as práticas de perseguição como inocentes e se sente culpada por reagir exageradamente ou demonstrar desconforto, muitas vezes relevando o comportamento criminoso por dependência emocional ou cobrança social (CASTRO; SYDOW, 2021; CARVALHO; HENRIQUES,

2021). Assim como nos casos de violência doméstica, é de se esperar uma subnotificação do *stalking* em relações íntimas, em virtude da relação de proximidade entre agente e vítima (WINTERER, 2005).

Com o aprofundamento da perseguição, além dos efeitos sobre a saúde, auto-estima e credibilidade da vítima, resultam usuais prejuízos financeiros, em razão de abandono laboral, gastos com aumento da segurança, mudança de residência e até terapia, e sobretudo a sua reificação, a qual, incapaz de resistir ao poder do assediador, passa a se vislumbrar como mero objeto de controle, de sorte que quaisquer tentativas de autodeterminação agravariam a postura implacável do perpetrador, alcançando eventualmente amigos e outros membros de sua família (COELHO; GONÇALVES, 2007; GUDÍN RODRÍGUEZ-MAGARIÑOS, 2014; WILSON *et al.*, 2022). Temendo esse escalonamento da agressão após o *stalking*, previamente capitulado como contravenção penal de perturbação da tranquilidade alheia, a criação de um tipo penal autônomo partiu especialmente das demandas de movimentos feministas, tanto que a preocupação com a vinculação entre perseguição e violência de gênero foi veiculada durante a tramitação do PL 1369/2019, projeto que originou a Lei nº 14.132/2021, pois uma intervenção penal em face do *stalking*, ainda em escala inaugural, procuraria evitar a progressão a crimes mais violentos, como feminicídio (SOUZA, 2022).

Por conseguinte, tendo em vista o limitado âmbito de incidência do direito penal como *ultima ratio*, nem toda conduta intrusiva deve ser qualificada como perseguição, de forma que o *ius puniendi* deve recair sobre condutas verdadeiramente hostis e indesejadas que perturbem gravemente a esfera de liberdade e de intimidade do indivíduo, embora sem número predeterminado, conforme disposto no artigo 147-A do Código Penal, incluído pela Lei nº 14.132, de 2021:

> Perseguição
>
> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.
>
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.
>
> § 1º A pena é aumentada de metade se o crime é cometido:
>
> I – contra criança, adolescente ou idoso;
>
> II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código;
>
> III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.
>
> § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência.
>
> § 3º Somente se procede mediante representação.

Destrinchando o tipo penal, há de se reforçar que a perseguição reiterada não se limita à conotação clássica de seguir no encalço de alguém, devendo ser apta a causar: (i) ameaça à integridade física ou psicológica de alguém, (ii) restrição à capacidade de locomoção da vítima ou (iii) invasão ou perturbação de sua esfera de liberdade ou privacidade (BIANCHINI *et al.*, 2023). A respeito da tipicidade subjetiva, não consta elemento subjetivo especial do tipo, de modo que as razões da perseguição variam entre paixão, motivos profissionais, idolatria da vítima, entre outros (SOUZA, 2022).

Em referência aos critérios objetivos, Souza realça que, em prol da configuração do *stalking*, a restrição ao direito de ir e vir da vítima não provém de medo baseado em meras presunções de caráter do agente, e sim em seu comportamento concreto reiterado (SOUZA, 2022). Nesse sentido, convém mencionar que, embora a percepção da vítima quanto ao evento e sua relação com o agente sejam fatores relevantes para a configuração do *stalking*, nem sempre o alvo, afetado negativamente pela conduta indesejada, reage com medo, critério extremamente subjetivo. Caso considerássemos o medo como elemento da perseguição, seria possível inferir que o efeito emocional sentido interfere mais do que a própria intensidade do ato intrusivo, descartando legítimas condutas de *stalking* lesivas à privacidade e à liberdade (STRAWHUN *et al*., 2013; WILSON *et al*, 2022). Em termos de objeto jurídico de proteção, tem-se como consenso que o bem jurídico tutelado é a liberdade individual, cuja afetação se desdobra nos âmbitos da (i) "liberdade psíquica, em face do temor infundido pela ameaça à integridade física ou psíquica, (ii) o direito de ir e vir, diante da restrição à capacidade de locomoção ou (iii) autonomia individual ou a privacidade, por conta da sua invasão ou perturbação" (SOUZA, 2022, p. 401).

Assim, não restam dúvidas do potencial ofensivo do *stalking* ou do *cyberstalking* de limitação das atividades das vítimas e interferência não autorizada em sua vida privada, violando a intimidade e a privacidade, reconhecidas como invioláveis, encontrando-se alçadas a nível constitucional nos termos do artigo 5º, inciso X, da Constituição Federal, eis que necessárias ao desenvolvimento humano (MACHADO; MOMBACH, 2016). Embora similares, tem-se que "a vida privada diz respeito aos elementos que formam a vida de uma pessoa e que não são de conhecimento público", dentro da qual se situa a intimidade (MACHADO; MOMBACH, 2016, p. 211). Igualmente, como extensão do direito fundamental à intimidade, nos termos do artigo 5º, inciso XII, da Constituição da República, atribuiu-se

tutela constitucional à inviolabilidade do sigilo das comunicações telegráficas, de dados e das comunicações telefônicas.

Embora reconheçam o cerceamento da liberdade e autonomia da vítima de *stalking*, Carvalho e Henriques consideram o principal bem jurídico lesionado a integridade moral, a qual abarcaria a autonomia individual e não se confundiria com a integridade psíquica ou física, equiparando o *stalking* a um tratamento degradante e humilhante. Em termos probatório, esse entendimento repercutiria na desnecessidade de comprovação médica de um sofrimento psíquico para a configuração do tipo, pois "isso não seria justo para com aqueles indivíduos que possuem uma elevada resistência psíquica a ponto de não apresentar qualquer alteração psicológica, apesar das agressões sofridas, embora sua dignidade resultaria incontestavelmente lesionada" (CARVALHO; HENRIQUES, 2021, p. 143). Nessa toada, julga-se como problemática a exigência de prova do prejuízo causado pelo *stalking*, dotado de difícil capacidade probatória frente aos danos comumente psicológicos (COELHO; GONÇALVES, 2007).

Em contrapartida, admite-se que o *stalking* nem sempre gera sentimentos de humilhação e desmoralização, típicos do assédio moral, e mais age sobre a sensação de segurança da vítima e, por assim dizer, seu equilíbrio emocional, tornando possível inferir que a perseguição se aproximaria da classificação de assédio psicológico - e não tanto do assédio moral (FLORES, 2014; GUDÍN RODRÍGUEZ-MAGARIÑOS, 2014). Nessa ótica, não se restringindo aos âmbitos privados e íntimos, é possível inferir que o *stalking* conduziria ao escalonamento para lesões a outros bens jurídicos da vítima, como integridade psicológica, patrimônio e ainda integridade física (CASTRO; SYDOW, 2021).

Em atenção às causas de aumento do crime de perseguição, é possível observar que o legislador se preocupou em agravar a pena e expressar a maior reprovabilidade da conduta nos casos em que o *stalking* é praticado contra mulher em decorrência da condição do sexo feminino, a qual representa um alvo frequente nas relações afetivas, geralmente após o fim de um relacionamento (CARVALHO; HENRIQUES, 2021). Originalmente, o PL 1369/2019 somente estabelecia a forma qualificada à hipótese genérica em que o agente fosse íntimo da vítima. Assim, buscou-se reproduzir a mesma lógica do feminicídio, incluída como qualificadora do homicídio (§ 2º-A do art. 121 do Código Penal), de sorte que, em ambos os tipos penais, as razões de condição do sexo feminino envolveriam a violência doméstica e familiar, o menosprezo ou à discriminação à condição de mulher. Nesse viés, mais condizente

aos casos de *stalkerware*, aplicar-se-ia a causa de aumento quando a vítima de uma perseguição, baseada no gênero, se encontra em situação de violência doméstica e familiar, abarcando, nos termos da definição do artigo 5º da Lei Maria da Penha, os âmbitos da unidade doméstica, da família e da relação íntima de afeto, independentemente de coabitação.

Ora, à vista do vínculo estreito entre *stalking* e violência doméstica e de gênero, impende assinalar que o *stalking* não somente seria atravessado por um marcador de gênero, mas também pelo marcador de diferença racial, um catalisador dessa violência ante a hipersexualização dos corpos negros, tornando a perseguição reiterada uma postura socialmente aceita (DE SOUSA, 2021). Ainda, sob um viés do marcador de renda, nem sempre a compra de um novo aparelho, a mudança de residência ou de emprego são soluções viáveis financeiramente para todas as vítimas. Nesse paradigma, enquanto manifestação da violência de gênero, tanto a compreensão do fenômeno delitivo da perseguição como a eleição de soluções exigem um olhar interseccional do operador do direito, a fim de não generalizar os alvos dessa perseguição. Analisado o atual leque de proteção normativa contra a perseguição, fundado no interesse de combate à violência de gênero, cumpre delinear seu *modus operandi* pelo meio informático, compreendido na acepção de *cyberstalking.*

4.2. *Cyberstalking:* A perseguição por meio informático

Sabendo que a perseguição é consumada além do viés presencial, cabe tecer considerações a respeito da diferença entre *cyberstalking* e *stalking*, eis que o cometimento do primeiro exige necessariamente o meio informático, assim como a repetição do comportamento e reflexos na liberdade e na intimidade da vítima (ALMEIDA; ZAGANELLI, 2021). Diante dessa definição, cabe traçar críticas quanto à nomenclatura *cyberstalking*, uma vez que o termo "*cyber*" se refere especificamente à Internet, não abrangendo completamente outras ferramentas informáticas utilizadas maliciosamente pelo *stalker* (FRASER *et al*, 2010).

Embora haja corrente doutrinária abrangente que compreenda o *cyberstalking* como uma soma de atos de *cyberharassment*, opta-se aqui pela sua definição como conduta de perturbação que implica dano recorrente e repetitivo através do meio telemático e das possibilidades intrusivas que outorga a rede (GUDÍN RODRÍGUEZ-MAGARIÑOS, 2014). Em virtude de seu inerente elemento informático, a doutrina classifica o *cyberstalking*, dentre a categorização de delitos informáticos próprios e impróprios, enquanto crime informático

impróprio, pois a prática da perseguição adquire novo contorno ao ser praticada pelo computador, um de seus meios de consumação delitiva (SOUZA, 2022; DE SOUSA, 2021).

Haja vista que o ciberespaço representa nova área de intrusão de privacidade sem conhecimento ou consentimento da vítima, aferiu-se empiricamente que condutas de *cyberstalking* são comumente precedidas por práticas passadas de *stalking* tradicional, de forma que apego prévio, ciúmes e atos de agressão durante e após o relacionamento são antecedentes significativos de *cyberstalking*, ainda que também seja praticado por completos estranhos (STRAWHUN *et al.*, 2013; WILSON *et al.*, 2022). Não por acaso, a literatura sugere que aqueles com experiências prévias de vitimização, *online* ou *offline*, apresentam mais chances de sofrer *cyberstalking*, indicando que o assédio online é reflexo de violências que ocorram presencialmente, inclusive possivelmente perpetradas pela mesma pessoa (WILSON *et al.*, 2023). Entretanto, ciente de que uma separação estrita entre atos *offline* e *online* possa soar artificial em uma era de *converged environment*, em que se espera uma prática combinada, o *stalking* e o *cyberstalking* constituem atos independentes entre si, ou seja, nada impede que um *cyberstalker* inicie a perseguir a vítima presencialmente e participe da sua vida ou jamais ultrapasse as telas por falta de coragem ou por pura impossibilidade (CASTRO; SYDOW, 2021; WILSON *et al.*, 2023).

Também é perceptível a diferença entre essas duas práticas com base nos temores da vítima e na localização do *stalker*, pois, enquanto o alvo de *stalking* perde a liberdade de ir e vir e teme a progressão da violência para um confronto físico com o agente, o qual costuma estar nas proximidades, aquela vitimada pelo *cyberstalking*, por sua vez, tem medo dos contatos virtuais, dos potenciais danos à sua reputação e à violação de segmento informático que invada ainda mais sua privacidade pelo agressor, situado em qualquer local do mundo (CASTRO; SYDOW, 2021). Ainda, enquanto o *stalking* abarca atos personalíssimos, o *cyberstalking* admite a prática por terceiros, como na modalidade *cyberstalking-by-proxy*, quando o c*yberstalker* difunde um discurso controverso como se fosse a vítima, a qual, por sua vez, passa a receber uma enxurrada de pessoas que não se conformam com o conteúdo enviado (CASTRO; SYDOW, 2021). Por fim, além de ser capaz de manipular seus rastros virtuais e ser beneficiado por uma maior impunidade na qualidade de crime cibernético, é cediço que o agente do *cyberstalking* não investe tanto tempo, dinheiro ou energia na sua perseguição, recorrendo frequentemente à automação dos seus atos, aptos a atingir uma pluralidade de alvos (CASTRO; SYDOW, 2021).

Em um primeiro momento, verifica-se que o *cyberstalking* não apresenta um tipo penal próprio, de modo que a incriminação dessa conduta estaria abarcada pelo tipo penal aberto da perseguição, cometida por "qualquer meio", nos termos do artigo 147-A do Código Penal. A partir disso, é possível depreender que o legislador idealizou uma legislação tecnoneutra, a qual se revela mais flexível a abranger meios tecnológicos futuros; por outro prisma, há de se questionar se a imprecisão e a vagueza do meio de cometimento dificultam a sua aplicação às novas formas de *cyberstalking* (ROYER; VANLEEUW, 2023).

Nesse sentido, confirma-se que os bens jurídicos violados pelo *cyberstalking*, relativos à privacidade e vida íntima da vítima, coincidem com aqueles lesionados pela perseguição, não demandando a criação de tipo penal específico. Sob outro enfoque, importa contemplar as particularidades de persecução penal do meio cibernético, circunstâncias que ensejariam, de acordo com a doutrina especializada, a atribuição de causa de aumento de pena à perseguição ou ainda a figuração como uma das agravantes gerais previstas no artigo 61 no Código Penal (BRITO, 2013; CARVALHO; HENRIQUES, 2021). Indubitavelmente, ante a difícil persecução penal e manifesta impunidade no meio cibernético, amplia-se a capacidade dos perpetradores de monitoramento e de contato com as vítimas por vias digitais, de sorte que o reiterado contato *online* conduz a um sentimento de insegurança e medo da vítima (LENHART *et al*, 2016).

Para consecução do *cyberstalking*, há de se considerar que nem toda obtenção de dados da vítima pelo *stalker* necessariamente apresenta caráter ilícito, o qual pode adquirir informações a partir da internet, das redes sociais ou voluntariamente da própria vítima (GUDÍN RODRÍGUEZ-MAGARIÑOS, 2014). Cumpre, desse modo, apresentar os exemplos mais recorrentes dessa prática:

> São exemplos de stalking e cyberstalking, do ponto de vista do modus operandi do autor do assédio, as seguintes condutas: coleta de informações sobre o alvo, seja por meio da internet, de amigos, da escola, do emprego; repetidos contatos não ameaçadores, sejam cibernéticos, por telefone ou pessoais; persistentes tentativas de aproximação e/ou convites para encontros; notas, objetos ou flores deixados no veículo; vigilância para aparecimento "acidental" no local onde a vítima se encontra ou trabalha; espera em frente à casa, trabalho da vítima ou junto a seu carro em estacionamento; comunicação falsa de crime; dano à reputação, ameaças, sexting e crimes contra a honra. Em casos mais raros, a perseguição pode escalar para danos ao patrimônio, lesões corporais e até mesmo homicídio (CARVALHO; HENRIQUES, 2021, p. 137).

Tendo em vista as diversas esferas de ocorrência do *cyberstalking*, que abarcaria emprego de e-mails, chamadas eletrônicas e redes sociais, práticas de assédio sexual, contato inadequado ou ainda perturbação da liberdade da vítima, tampouco seria incomum no

cyberstalking a "utilização de brechas nos sistemas de segurança para que ocorra invasão de dispositivos eletrônicos da vítima, para aplicativos do tipo espião" (BIANCHINI *et al.*, 2023, p. 116). Em razão disso, em 2021, o Ministério Público do Distrito Federal e Territórios definiu diretivas sobre o crime de *stalking*, exemplificando inclusive a instalação de dispositivo eletrônico que prolonga no tempo a conduta de vigilância:

> 11) Na hipótese de instalação de dispositivo de vigilância em aparelho celular, no veículo da vítima ou outros dispositivos de internet das coisas, um único episódio de instalação com monitoramento que se prolonga no tempo já é uma conduta de perseguição reiterada, apta a configurar o crime de perseguição (CP, art. 147-A), sem prejuízo de eventual incidência do crime do art. 154-A do CP, se for o caso. (MPDFT, 2021)

Nessa toada, Castro e Sydow compreendem o assédio não só pela comunicação direta e por uso da internet, como também pela intrusão informática, categoria esta que se comunica diretamente com o tema do *stalkerware*. Na visão dos autores, o assédio por intrusão informática não deve ser confundido com a intrusão com a finalidade de obter, adulterar ou destruir dados, correspondendo ao "uso da intrusão informática como método de importunação e geração de danos de natureza psicológica ou financeiras" (CASTRO; SYDOW, 2021, p. 262), o qual se apropria de brecha de segurança, infecção por *malware* ou emprego de ardil para acesso ao dispositivo informático da vítima, razão pela qual demandaria repressão mais grave.

Na qualidade de *malware*, o *spyware* seria meio de intrusão telemática utilizado pelo perpetrador para supervisão de todas as atividades no computador ou celular da vítima, tendo acesso a grande volume de informações pessoais e senhas, por meio das quais deteria a capacidade de postar e enviar mensagens como a vítima, usurpando sua identidade (GUDÍN RODRÍGUEZ-MAGARIÑOS, 2014). Nessa linha, embora o bem jurídico informático seja atingido, ao perseguir objetivo final diverso à violação do sistema informático, eventual acesso indevido integraria o feito delitivo como meio necessário para a execução desse ulterior delito, exigindo, na percepção de Gudín Rodríguez-Magariños, a punição pelas normas gerais de concurso de delitos (GUDÍN RODRÍGUEZ-MAGARIÑOS, 2014). Em outra linha, Vianna e Machado argumentam pelo cabimento do princípio da consunção e, consequentemente, pela não incidência da pena de invasão do dispositivo informático enquanto crime-meio (VIANNA; MACHADO, 2013). Assim, antecipa-se debate acerca da regra do concurso de delitos ou da aplicabilidade do princípio da consunção no âmbito do *cyberstalking*, a ser explorado em capítulo próprio.

Por fim, conclui-se que o *stalkerware,* enquanto uma manifestação do *cyberstalking*, se diferencia pela intrusão de dispositivo informático, pelo elevado poder do *cyberstalker* sobre

dados pessoais e pelo usual desconhecimento da vítima sobre a violação de sua privacidade. Embora Castro e Sydow argumentem acertadamente que não se deve confundir o *cyberstalking* com o delito de invasão de dispositivo informático previsto no artigo 154-A do Código Penal (CASTRO; SYDOW, 2021), não há como se descartar a qualificação desse delito como crime-meio do *stalkerware*, o qual reclama a intrusão informática para a invasão da esfera de privacidade. Dessarte, recapitulando os pontos centrais que compõem o *stalkerware*, cabe propor a delimitação dos interesses jurídico-fundamentais afetados e, a partir disso, apresentar os desafios de sua persecução penal.

5. IMPLICAÇÕES PENAIS DO *STALKERWARE*

5.1. Bem jurídico e desafios da persecução penal do *stalkerware*

Em vista dos efeitos drásticos aos direitos fundamentais pelo direito penal, a oferta de qualquer resposta criminal no atual Estado Democrático de Direito está ancorada na observância aos princípios da subsidiariedade e do direito penal mínimo. Ou seja, na qualidade de *ultima ratio*, uma intervenção penal legítima incidirá sobre valores sociais previamente elencados como dignos de um tratamento mais gravoso do Estado, somente quando outros meios de proteção não se revelarem suficientes (ROXIN, 2004).

Nessa premissa, adota-se como concepção que o bem jurídico compreende interesse humano fundamental que demanda uma proteção penal (HASSEMER; MUÑOZ CONDE, 1989). Tendo como substrato valores tidos como relevantes pelo crivo social, o bem jurídico não retrata uma categoria imutável, eis que se sujeita e responde às mudanças inerentes à evolução da comunidade, valorando interesses sociais preexistentes. Contudo, não se supõe que recaia a criminalização à qualquer lesão ao bem jurídico, de sorte que o paradigma de proteção ao bem jurídico busca limitar o direito penal, eliminando da sua abrangência condutas que não atinjam ou ameacem gravemente bens jurídicos (HASSEMER, 2005). Afinal, por mais que seja parâmetro imprescindível à proibição, não basta a satisfação do requisito do bem jurídico, exigindo-se que a proteção penal exercida seja também, entre outros fatores, subsidiária, ou seja, incapaz de ser evitada por meios de controle social menos gravosos, como outras searas do direito e medidas extrajurídicas (ROXIN, 2004).

A partir desse pressuposto teórico, reconhece-se que a proteção penal é apenas uma das searas de combate ao *stalkerware*, fenômeno esse que, dada sua complexidade, exige uma atuação multidisciplinar e intersetorial. Todavia, considera-se impossível discutir uma

criminalização do *stalkerware* sem delimitar o grau de ofensividade dessa prática a valores basilares do bem-estar social. Em prol dessa finalidade, ao longo do presente trabalho, pretendeu-se identificar as distintas dimensões do *stalkerware* merecedoras de tutela específica do direito penal, revelando o caráter pluriofensivo dessa prática.

Antes de delimitar o grupo social ao qual a criminalização desse comportamento destinar-se-ia, cumpre analisar as condutas compreendidas pelo *stalkerware*, as quais perpassam pelos campos do *stalking* e da cibercriminalidade, cujas sanções constituem demanda da atual sociedade de risco. Nesse sentido, ante o descompasso entre o desenvolvimento de inovações científicas e tecnológicas e o conhecimento dos seus efeitos sobre a vida em sociedade, vive-se em estado de risco caracterizado por efeito bumerangue, que afeta todas as classes sociais, as quais, sob forte sentimento de insegurança, reivindicam o gerenciamento desses novos riscos, papel este assumido pelo direito penal contemporâneo (BOTTINI, 2007). Diante disso, o fenômeno do *stalkerware*, permeado pelo uso de aplicativo espião, constitui um dos novos riscos gerados pela deturpação dos meios tecnológicos, cujo potencial ofensivo à inviolabilidade e à integridade dos dados estende-se às esferas de privacidade e intimidade, atingindo o livre desenvolvimento da personalidade individual.

Em sua essência, o *stalkerware* visa à perseguição reiterada e indesejada de atuais ou ex-parceiras pela intrusão informática, invadindo sua esfera de liberdade ou privacidade. Nessas condições, impende registrar que, no *stalkerware*, se cuida da aplicação da forma qualificada da invasão de dispositivo informático, eis que resulta na obtenção de conteúdo de comunicações eletrônicas privadas e, por certo, geralmente há incidência da causa de aumento do *stalking*, pois cometido contra mulher por razões de violência doméstica e familiar, menosprezo ou discriminação à condição de mulher.

Contemplando as condutas de perseguição e de invasão de dispositivo informático, infere-se que o *stalkerware* tem como bem jurídico geral a liberdade individual, a qual se desdobra em intimidade ou privacidade, mas também na inviolabilidade dos dados informáticos. Evidentemente, na atual sociedade informática, a tecnologia criou novos espaços privados, como as contas de redes sociais, a caixa de mensagens, as fotos, o histórico de navegação, de modo que "seu monitoramento ou violação certamente violenta os direitos do usuário e configura nova forma de intrusão ou violação da privacidade" (CASTRO; SYDOW, 2021, p. 273-274). Nessa instância, o *stalkerware* consolida-se como violência digital de gênero

pautada na vigilância e no monitoramento da vítima, invadindo completamente sua vida privada, refletida no âmbito virtual.

Dada a participação do elemento informático nessa prática, classifica-se o *stalkerware* como delito informático mediato ou indireto, posto que, embora haja a violação concomitante dos seus bens jurídicos correlatos, observa-se o cometimento de crime-meio informático para consumação de um delito-fim. Traduzindo, constata-se que o delito de intrusão informática é praticado como meio para consecução do *cyberstalking*, e, incidindo o princípio da consunção, não se verificaria tutela imediata ao bem jurídico ligado ao crime-meio.

Em oposição a essa concepção, Sydow considera cabível a aplicação do delito de invasão de dispositivo informático à lógica do *stalkerware*, porém interpreta que esse fenômeno não compreenderia o *cyberstalking*, em razão da afetação de bens jurídicos diversos e dos distintos *modus operandi* (SYDOW, 2022). De acordo com o autor, o *stalkerware* consistiria em monitoramento espião que, ao contrário do *cyberstalking*, não tolheria a liberdade informática da vítima, a qual não perceberia em seu cotidiano um crescente cerceamento pelo agente. Em sua visão, apenas quando a vítima descobre essa prática ilegal, configura-se a violência, que, por sua vez, não corresponderia ao cerceamento da liberdade informática, mas à "violação da intimidade, da confidencialidade dos dados e interceptação não autorizada de dados, conversas, localização e até registro não autorizado de imagens" (SYDOW, 2022, p. 605).

Todavia, por mais que se considere importante a percepção da vítima quanto à perseguição, não se trata de requisito objetivo para a configuração do *stalking*, o qual poderia ocorrer com ou sem ciência da vítima, desde que haja sua perseguição reiterada com invasão de sua esfera de liberdade individual. Nesses termos, mais do que mera limitação de ir e vir, admite-se conceito amplo de liberdade individual, a qual engloba a privacidade e a intimidade como componentes. No mais, há de se argumentar pela presença de uma violação da liberdade informática em sentido estrito, posto que a vítima, já com suspeitas ou com ciência do aplicativo espião, adotaria medidas de autolimitação, evitando realizar determinadas comunicações pelo dispositivo, interromperia o uso de redes sociais ou ainda compraria um novo dispositivo para se libertar da violência.

Feitas essas considerações, conclui-se que uma tipificação penal adequada consistiria na prática do crime de *stalking*, mediante a invasão de dispositivo informático[7], não vislumbrando como necessária a criação de norma incriminadora informática específica. Ora, à luz do princípio da subsidiariedade, somente é imprescindível a produção de nova norma incriminadora quando os tipos penais existentes não descreverem suficientemente a conduta analisada, ou seja, quando não há correspondência entre as elementares mínimas do tipo, incapaz de oferecer resposta criminal adequada. Nessa perspectiva, por um lado, é inconcebível ignorar a tendência de expansionismo penal à cibercriminalidade, ante a conformação de realidade informática acompanhada de novos riscos e de consequências delitivas, em que mais pessoas se identificam como vítimas (SILVA SÁNCHEZ, 2006). Por conseguinte, em defesa de um direito penal mínimo, eventual produção penal legiferante deve ser planejada com parcimônia, não cabendo se alinhar a um irrazoável movimento de expansionismo do direito penal, voltado à oferta de respostas estatais simbólicas e à aparição de novos bens jurídicos injustificadamente.

Nessa alçada, julga-se pertinente depreender a relevância social dos bens jurídicos a partir da identificação das principais vítimas do ataque a esses interesses fundamentais e do contexto de ocorrência dessa violação sistemática. Particularmente no âmbito do *stalkerware*, embora esses aplicativos sejam comercializados publicamente como *software* de rastreamento dos filhos, destinados a pais preocupados com o conteúdo acessado pelo filho, ou de ferramenta anti-furto, trata-se de estratégia apta a mascarar uma espionagem sem ciência ou consentimento dos alvos, utilizada sobretudo por homens que adquirem as funcionalidades do aplicativo para espionar atuais ou ex-parceiras (KÖVER, 2021).

Evidentemente, é irrealista uma proibição desses aplicativos deturpados para o *stalkerware*, de sorte que as empresas de tecnologia, cientes do potencial ofensivo, devem se atentar a aspectos éticos e limitar ao máximo o uso criminoso dessas ferramentas tecnológicas (ROYER, VANLEEUW, 2023). Contudo, isentando-se de qualquer responsabilização, os aplicativos consideram que o usuário controlador dos dados coletados no *stalkerware* é a parte contratante do *software*, à qual delega a responsabilidade de obter consentimento da parte

[7] Não obstante se proponha intervenção penal do *stalkerware* à luz dos tipos penais supracitados, há de se repisar a ausência de jurisprudência pátria consolidada, de sorte que o eventual reconhecimento de sua (in)efetividade será melhor aferido nas fases de inquérito policial e de ação penal, com atuação da autoridade policial, do Ministério Público e do órgão julgador em face do caso *in concreto*.

monitorada, ignorando que as informações coletadas pertencem ao alvo da vigilância e não lhe oferecendo meios de suporte (PARSONS *et al.*, 2019).

Ou seja, embora a indústria tecnológica apresente uma série de termos de serviços, diretrizes da comunidade, políticas de uso e até mecanismos de detecção e filtro de práticas proibidas, as empresas desenvolvedoras não evidenciam com clareza às vítimas de *stalkerware* como elas podem ter seus dados apagados sem seu consentimento expresso, falham em justificar a possibilidade de captura das informações de identificação pessoal durante o funcionamento do *software* apesar das políticas de privacidade, bem como fracassam na adoção de medidas de notificação dos alvos de *stalkerware* e até dos indivíduos contratantes desse serviço em eventual violação de dados do sistema (PARSONS *et al.*, 2019). Nesse viés, as ações de contenção pela empresa são, por si só, insuficientes para o combate das violências digitais de gênero, já que a execução dessas políticas pelo segundo setor é lenta e não uniforme, desperdiçando-se uma oportunidade de promoção da equidade de gênero e de prevenção do abuso em estágios iniciais (O'BRIEN; MARAS, 2024). Assim, por mais que o *spyware* propicie inúmeras ilicitudes, a presente produção limitou-se ao estudo da instrumentalização dessa ferramenta tecnológica, instalada nos dispositivos de atuais ou ex-parceiras dos perpetradores, para cometimento da violência de gênero, visando o monitoramento remoto de suas comunicações e a constante vigilância do seu paradeiro.

Como já ensina a literatura especializada, em razão de um contexto sociocultural caracterizado pela imposição das normas do patriarcado e pelo controle do corpo feminino, não se deve perder de vista que essa e outras violências afetam majoritariamente mulheres, e claro, mais gravosamente aquelas atravessadas por outros marcadores da diferença, como raça, classe, orientação sexual e deficiência. Nesse cenário, há de se atentar que, por um lado, a criminalização da violência de gênero estimula que essa problemática seja reconhecida como uma questão de interesse público, evidenciando à população a seriedade dessa violência (YARDLEY, 2021). Por outro lado, embora teoricamente encarregado de uma das vertentes da defesa social, o direito penal igualmente tem potencial de reproduzir violências contra o mesmo grupo que busca proteger, pois, ao adotar uma postura neutra quanto ao marcador de gênero, revitimiza as sobreviventes no sistema de justiça criminal, rotulando-as ou culpabilizando-as pelas agressões (BECHARA, 2014; YARDLEY, 2021).

Nessa esteira, em substituição a tipos penais neutros, uma criminalização gênero-específica proporia uma punição de acordo com a gravidade do fato, buscando romper a

invisibilidade da violência de gênero em cenário sociocultural que favorece sua impunidade (BIANCHINI, 2016). Entretanto, não basta uma intervenção penal que se atente à complexidade e à sensibilidade da violência afligida: primeiro, a criminalização, regida pelo modelo tradicional de responsabilidade pessoal, centra-se em uma resposta a incidentes individuais de violência, sem endereçar sua natureza estrutural que se encontra naturalizada *online* e *offline*; segundo, os atores do sistema que executam essas normas, sem formação técnica adequada e pouco familiarizados com os novos meios tecnológicos de cometimento, ainda prosseguiriam reproduzindo estereótipos machistas (O'BRIEN; MARAS, 2024).

Portanto, sem uma mudança estrutural da mentalidade sobre a violência de gênero tanto *online* como *offline*, ainda regida pela lógica patriarcal, dificulta-se a efetividade dos avanços jurídicos-penais, uma vez que são sugeridas soluções improdutivas e estereotipadas que, fundadas na responsabilidade individual típica do neoliberalismo, atribuem à vítima a responsabilidade de encerrar a violência, como o fim de um relacionamento abusivo, a mudança do número de telefone ou ainda a interrupção do uso de redes sociais (YARDLEY, 2021). Assim sendo, tem-se que a mera atuação do direito penal, contrastante com as expectativas das vítimas, não resulta suficiente para repressão da violência de gênero, a qual tampouco deve ser concebida como uma questão privada ou familiar a ser solucionada entre as partes envolvidas.

Envolvendo frequentemente não só questões penais, como litígios cíveis de divórcio e guarda de filhos, torna-se imperativa uma abordagem intersetorial, prezando-se pela colaboração em rede entre as instâncias de justiça e equipe técnica multidisciplinar, a qual facilita o acesso a abrigos, atendimento médico, apoio psicológico, entre outros (ALMEIDA, 2014). Nesse aspecto, é essencial a criação de um projeto assistencial comum e integral à sobrevivente da violência de gênero, com base nas necessidades de cada caso, de modo a articular profissionais de diferentes setores, devendo ser capacitados para a abordagem da violência contra a mulher sob uma perspectiva de gênero (AGUIAR *et al.*, 2020). Particularmente no âmbito da violência de natureza digital, em que há uma trivialização do controle tecnológico, é necessário um treinamento dos atores do sistema acerca das novas formas de mau uso dessa tecnologia e de suas repercussões às vítimas, equivocadamente encaradas como menos lesivas que as das violências *offline* (O'BRIEN; MARAS, 2024). Ora, assim como os *stalkers* adaptaram suas práticas delitivas ao desenvolvimento tecnológico, as estratégias dos operadores do sistema de justiça também devem se modernizar (FRASER *et al.*, 2010).

A respeito da produção probatória, diante de uma incompreensão da dinâmica da violência de gênero e das técnicas de anonimização do agente, presume-se equivocadamente sobre uma elevada capacidade de reconhecimento e armazenamento de evidências digitais pela vítima, muitas vezes inacessíveis ou ocultas, cuja maior dificuldade é convencer as autoridades sobre existência de um crime (O'BRIEN; MARAS, 2024). Especialmente, tratando-se de crime de meio informático, geralmente sua existência somente é percebida após seu cometimento, possibilitando que o agente oculte ou delete seus rastros, o que evidencia a volatilidade dos elementos de prova (SYDOW, 2015). E ainda, importa considerar que nem sempre é seguro que ela retenha evidências consigo, à vista do monitoramento de seus aparelhos ou das suas comunicações digitais pelos perpetradores (O'BRIEN; MARAS, 2024). Nesse cenário, enquanto ainda não há elementos suficientes para um indiciamento, recomenda-se que as autoridades policiais não culpabilizem a sobrevivente e demonstrem encarar com seriedade o *stalking*, colaborando com a vítima na identificação de evidências e envolvendo-a no processo de decisão em prol de seu empoderamento (FRASER *et al.*, 2010).

Ainda pouco reportado nacionalmente, com o fulcro de elencar desde já possíveis desafios de persecução penal do *stalkerware*, buscou-se respaldo na doutrina estrangeira, ressalvando, porém, que não se pretende uma transposição acrítica ao Brasil, em reconhecimento às distinções entre os contextos culturais e jurídicos dos países.

Na Europa em geral, as legislações *anti-stalking* em voga dividem-se em dois grupos: por um lado, há dispositivos normativos que realizam lista exaustiva de táticas possíveis de perseguição, o que limita a tipificação das novas formas de *stalking* facilitadas por tecnologia; por outro, as normas penais mais genéricas exigem que a vítima tenha experienciado aflição ou perturbação de sua vida cotidiana e, por mais flexíveis que sejam, há dificuldade em sustentar uma perturbação da paz de espírito da vítima em cenários que a própria não percebe a perseguição digital (ROYER; VANLEEUW, 2023). Vislumbrando como insuficientes as legislações mais genéricas para endereçar os casos de *cyberstalking*, dentre eles, o *stalkerware*, a Comissão Europeia apresentou, em 2022, proposta de nova diretiva no combate à violência contra mulher e doméstica, a qual exigiria que os Estados-Membros explicitamente criminalizassem variadas formas de *cyberstalking* em seus ordenamentos, o que incluiria o uso de tecnologias para monitorar atividades e movimentos da vítima sem seu consentimento (ROYER; VANLEEUW, 2023).

Já especificamente na Alemanha, por mais que se verifique quadro de proteção penal em face de violação da privacidade mais consolidado, são raras as denúncias pela prática do *stalkerware*, uma vez que as pessoas afetadas dificilmente descobrem a vigilância e, caso suspeitem de um monitoramento, tem dificuldades em provar a existência do *spyware* (KÖVER, 2021). As forças policiais tampouco se encontram aptas ou compreensivas a dispor dos meios para efetuar uma análise forense do aparelho e, ainda que comprovada a instalação do aplicativo no aparelho, nem sempre é possível estabelecer o liame entre o agente e conduta, o qual eventualmente exigiria uma fatura de compra do aplicativo, testemunhas ou uma confissão do próprio autor (KÖVER, 2021).

No Canadá, a depender do caso concreto, o uso dos aplicativos do *stalkerware* qualifica-se como criminoso por si só ou apenas um dos componentes de uma conduta criminosa, separando os delitos em: invasões sérias de privacidade, medo e dano psicológico associado a assédio e ameaças e violação da integridade sexual do indivíduo (KHOO *et al.*, 2019). Dentre as invasões de privacidade, destacam-se os delitos de interceptação de comunicação privada em momento real sem o consentimento de uma das partes da comunicação (seção 184(1) do Código Criminal canadense), de uso não autorizado de computador (seção 342.1), diante da obtenção de acesso não autorizada a dispositivo, e de violação relacionada a dados computacionais, quando o agente bloqueia certas comunicações ou manipula os dados do alvo (seção 430 (1.1)) (KHOO *et al.*, 2019).

Já no âmbito do medo e dano psicológico, além da extorsão, impõe-se a possível tipificação por *criminal harassment*, disposta na seção 264 do Código Criminal, a qual abrangeria atos de perseguição, controle e ameaça em que o alvo sabe ou tem conhecimento posterior do abuso tecnológico e das intrusões de privacidade, temendo pela segurança (KHOO *et al.*, 2019). Assim, observa-se que a configuração da conduta no Canadá atribui como requisito o medo da vítima pela sua segurança ou de outrem, elencando uma série de condutas proibidas, enquanto no Brasil, o tipo penal de perseguição abarca mais a ameaça à integridade física ou psicológica, a restrição à capacidade de locomoção e a invasão à esfera de liberdade ou privacidade.

Nesse âmbito, com base nas experiências mencionadas, importa estabelecer que não basta uma resposta penal à problemática do *stalkerware* no Brasil e no mundo, e sim uma intervenção intersetorial com participação de diversos atores sociais, marcada por políticas de conscientização sobre a importância da confidencialidade dos dados e os potenciais delitos

informáticos, pelo aperfeiçoamento dos canais de denúncia, pela restrição à disponibilização de aplicativos facilitadores da violência de gênero, pelo maior sistema do apoio dos aplicativos às vítimas, pelo estímulo ao desenvolvimento de programas de detecção do *spyware* por empresas de cibersegurança, pela formação técnica dos atores do sistema de justiça a respeito de produção de provas e de um atendimento especializado em violência de gênero, entre outras. Por fim, diante da atual utilização dos *spywares* em diferentes vertentes, seja como instrumento de violência de gênero, seja como meio de obtenção de prova na persecução penal, consideram-se urgentes a contínua produção de pesquisas relativas ao seu funcionamento e o debate público no que tange a sua regulamentação.

Estabelecida a presença dos tipos penais da invasão de dispositivo informático e do *stalking* na prática do *stalkerware*, há de se analisar a necessidade de uma resposta penal a cada ação, sob uma incidência de concurso material de crimes, ou o cabimento de uma única sanção para capturar o injusto de ambas as condutas, em aplicação ao princípio da consunção.

5.2. *Stalkerware*: Um caso de incidência do princípio da consunção?

Conforme elucidado, entende-se que uma resposta criminal ao *stalkerware* deve comportar os tipos penais de invasão de dispositivo informático e de perseguição, uma vez que sua consecução compreenderia as duas ações expressas pelos núcleos “invadir” e “perseguir”. No entanto, persistem questões a respeito do modo de persecução penal dessa conduta pelos operadores do direito no que tange à incidência de um concurso material de crimes ou do princípio da consunção, essencial para fins de imputação penal. Em face da dissonância doutrinária quanto à aplicação desses dois institutos, importa definir a natureza da relação entre os tipos incriminadores da invasão de dispositivo informático e da perseguição em prol da prática do *stalkerware*.

Em oposição à relação de consunção, inserida como uma das soluções do conflito aparente de normas incriminadoras, o concurso de delitos é caracterizado pela pluralidade real de resultados típicos, presente na hipótese de unidade de conduta, isto é, quando uma ação ou omissão resulta em mais de um delito, ou de pluralidade de ações, cenário em que diferentes condutas produzem distintos delitos (FARIAS; PIEGEL, 2013; CARVALHO, 2020). Nesse ponto, destacam-se dois critérios de determinação da pena: de acordo com o critério de cúmulo material, somam-se as penas de cada delito; já o critério de exasperação, válido ao concurso formal e ao crime continuado, impõe majorante nos termos do artigo 71 do Código Penal

(CARVALHO, 2020; GRECO; LEITE, 2022). Particularmente na alçada do *stalkerware*, identifica-se o cometimento de mais de uma ação, o que já descartaria eventual concurso formal, restando analisar mais profundamente a imposição do concurso material ou do princípio da consunção, uma espécie do concurso aparente de normas.

Quando há concurso material de crimes, a cumulação das penas decorre da realização de mais de um desvalor autônomo pelos fatos praticados, suficientemente independentes um do outro, a ponto de justificar uma nova pena (GRECO; LEITE, 2022). Logo, constando dois ou mais sentidos de ilicitude sem que nenhum deles seja dominante, mostra-se admissível o concurso de crimes diante do comportamento global do autor, pois são preenchidos determinados tipos penais que não excluem a aplicação de outros tipos, carregando sentidos autônomos entre si (VINAGRE, 2011). Nessa hipótese, impende estabelecer que não haveria violação do *ne bis in idem*, reconhecendo aqui a necessidade de resposta penal autônoma a cada parte ilícita dos atos que compõem a conduta, não guardando relação de fim e meio entre si:

> Nessa conformidade, se do comportamento global do agente se retiram dois ou mais sentidos de ilicitude resultantes da conduta praticada, mesmo que um deles seja preponderante, não estaremos a violar a proibição *ne bis in idem* ao condenarmos o agente por concurso de crimes, porque o crime dominado foi efetivamente praticado e a proibição da sua prática não foi suficiente para demover o agente (VINAGRE, 2011, p. 81).

Quanto ao conflito aparente de normas incriminadoras, cabe introduzir que as regras da especialidade, subsidiariedade e consunção buscam descrever essas relações de concurso aparente de normas, em que não existe desvalor novo que exija uma exasperação do fato, bastando o marco penal de único delito (GRECO; LEITE, 2022). É um concurso aparente, pois há uma pluralidade de normas aparentemente aplicáveis ao caso concreto, preenchendo os requisitos mínimos essenciais dos mandamentos penais (COSTA, 2012). Assim, dentre essas relações, realça-se que o princípio da consunção, aferido a partir do caso concreto, se verifica quando determinado crime é fase de realização ou meio de realização de outro crime, geralmente mais grave que aquele, ocorrendo a absorção do conteúdo do injusto do tipo penal secundário pelo tipo penal mais amplo (FARIAS; PIEGEL, 2013; GOMES, 2014).

Sob um viés axiológico, por mais que haja conexão material objetiva e subjetivamente entre os delitos, o fato criminoso é interpretado como insignificante valorativamente frente ao fato principal, não sendo razoável responsabilizar o indivíduo com base nesse tipo penal secundário (COSTA, 2012). Igualmente, cumpre instar que esse crime-meio não é sempre ato necessário ou indispensável, representando apenas meio regular de execução do crime

consuntivo, o qual, por sua vez, é passível de ser cometido de outras maneiras (GOMES, 2014; CIRINO DOS SANTOS, 2020).

A princípio, presume-se que a punição do fato mais grave não só supriria a responsabilização penal pela conduta menos gravosa, como englobaria o desvalor de todo o comportamento e o juízo de censura dirigido ao agente, ou seja, nenhuma parte do injusto restaria sem resposta penal (FARIAS; PIEGEL, 2013; GOMES, 2014; VINAGRE, 2011). De modo complementar, ainda que os tipos legais tutelem bens jurídicos distintos, devem guardar proximidade objetiva entre si, situando-se na mesma linha de progressão de ataque a um mesmo bem jurídico (FARIAS; PIEGEL, 2013). Contudo, há quem defenda o concurso efetivo de normas quando envolvidos bem jurídicos eminentemente pessoais, a fim de que nenhuma norma seja excluída, ante a impossibilidade de esgotamento do desvalor comportamental dessas condutas por um outro tipo legal (VINAGRE, 2011).

Em oposição a essa crítica, adotando a concepção de Figueiredo Dias, Vinagre esclarece haver concurso aparente, desde que haja um único sentido de desvalor jurídico-social, pertencente à norma penal que absorve a proteção das demais, de forma que a aplicação dessa norma prevalecente se legitima pelo *ne bis in idem* (VINAGRE, 2011). Tendo em vista a proibição da dupla valoração de uma mesma conduta, é cabível a aplicação de apenas um dos tipos incriminadores enquanto imperativo de justiça material, em defesa de uma restrição justa e proporcional de direitos fundamentais pelo direito penal, haja vista que a outra alternativa, muito mais gravosa ao réu, seria o concurso de crimes (COSTA, 2012; GOMES, 2014).

Nessa toada, a tipicidade subjetiva igualmente compreende elemento de relevo, posto que quando o autor apresenta finalidade de cometer um único delito, empregando crime-meio para tanto, há de se considerar a intenção última do agente de lesão ao bem jurídico, prevalecendo o crime-fim (GOMES, 2014). A título de exemplo, no viés dos crimes informáticos, geralmente ocupando posição secundária para cometimento de outro crime, a intenção do agente direcionada ao crime principal é sublinhada por Vianna e Machado:

> Quando a invasão a dispositivos informáticos for crime-meio para a prática de outro delito, não será punido, aplicando-se ao caso o princípio da consunção e o delito-fim será denominado de crime informático mediato ou indireto. Esse é o caso, por exemplo, do agente que invade o dispositivo informático da vítima e nele instala uma vulnerabilidade (um malware, por exemplo) no intuito de obter sua senha da conta bancária para, então, subtrair valores da respectiva conta. Nesse caso, embora tenha ocorrido um crime informático anterior (art. 154-a do CPB), a finalidade do agente, desde o início, era a prática de um crime contra o patrimônio, sendo, in casu, um furto qualificado pela fraude (art. 155, §4º, II, do CPB). Logo, o agente responderá pelo furto,

> o qual absorverá a invasão de dispositivo informático (VIANNA; MACHADO, 2013, p. 99).

Além disso, importante ressaltar que a identidade entre os bens jurídicos tutelados não corresponde a um dos requisitos da aplicação da consunção, porém inegável que sua delimitação contribui para validação da conexão material e subjetiva entre os delitos e, sobretudo, do potencial ofensivo do delito secundário. Diante dessas considerações, com o fulcro de avaliar a aplicação do princípio da absorção ou do concurso material no *stalkerware*, importa fixar os bens jurídicos tutelados.

Por um lado, buscando avaliar a relação entre os tipos penais no *cyberstalking*, Cabette defende que a solução correta seria o concurso de crimes, pois o crime de invasão de dispositivo informático não representaria meio necessário para o crime de perseguição, além de tutelarem bens jurídicos diversos: liberdade individual e segurança de sistemas informáticos (CABETTE, 2021). Entretanto, discorda-se dessa posição, sob a premissa de que os bens jurídicos dos dois crimes se enquadram no leque da liberdade individual e de que a perseguição consiste em conduta dominante, configurando a invasão informática um meio regular para a consecução desse delito.

Contemplando os dois fatos criminosos que compõem o *stalkerware*, trata-se de perseguição reiterada de alguém pela invasão informática, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Ainda que sob distintos âmbitos, há de se evidenciar que ambos os tipos penais contemplados se propõem à tutela da liberdade individual, um mais voltado ao âmbito da privacidade e da intimidade, enquanto outro vinculado à inviolabilidade dos dados em dispositivo informático.

Nessa linha, ao se afirmar que essa inviolabilidade dos dados pessoais se encontra subsumida ao conceito de privacidade e intimidade protegido pelo tipo penal da perseguição, configuraria *bis in idem* responsabilizar penalmente duas vezes o autor pelo atentado à liberdade individual somente em virtude da localização desses dados. Isso posto, avalia-se como excessiva a imposição do concurso de delitos em decorrência do meio de ocorrência da perseguição; afinal, caso o legislador veja como necessária a exasperação da pena nos casos que envolvam meio cibernético, seria possível a criação de agravante específica ou de causa de aumento, não cabendo recorrer a outra forma de interpretação da relação entre as normas.

Logo, vale-se da delimitação dos bens jurídicos atingidos pelo *stalkerware* para, ciente do potencial ofensivo de cada conduta, evitar uma dupla valoração. Sob essa perspectiva, à vista

da divergência doutrinária sobre o artigo 154-A do Código Penal, caso o bem jurídico eleito fosse a segurança telemática, absolutamente distinto da liberdade individual, seria plausível pressupor um concurso de delitos, já que o injusto penal do *stalking* não abarcaria o desvalor de conduta que violasse a segurança do dispositivo em si. Evidente, portanto, que a interpretação sobre o interesse jurídico-penal relevante atentado pela conduta disposta no artigo 154-A influencia diretamente a configuração de um concurso efetivo de delitos ou de um concurso aparente de normas, ancorado na relação da consunção, como leciona Cabette no âmbito específico da perseguição por intrusão informática:

> Anote-se, porém, que para quem não aponte a "segurança dos sistemas informáticos" como bem jurídico tutelado afora a liberdade individual, intimidade e vida privada, tornar-se-á mais difícil sustentar a tese do concurso, prevalecendo, nesse caso, a absorção do art. 154-A como crime-meio. Não obstante, razão parece assistir ao entendimento que advoga o concurso (CABETTE, 2021, p. 48).

No entanto, cabe rememorar que, para fins de aplicação do princípio da consunção, o potencial ofensivo dessas outras condutas não poderia se concretizar, uma vez que o sentido protetivo da norma consuntiva não seria capaz de abranger o desvalor total da norma absorvida, restringindo-se tal captura do risco ou do dano punível aos limites da norma mais abrangente (HORTA, 2007). Transpondo essa premissa à prática do *stalkerware*, a aplicação desse princípio somente se admitiria quando o potencial lesivo da invasão de dispositivo informático se exaure no crime de perseguição. Isto é, não cabe aqui defender uma aplicação unânime do princípio da consunção a todos os casos de *stalkerware*, cujo exame se restringe ao caso concreto, uma vez que esse princípio não incide, caso o invasor se valha da instalação do *spyware* para cometer outros delitos, como aqueles ligados ao patrimônio da vítima.

Dirimida a questão dos bens jurídicos do *stalkerware*, pontua-se como problemática a desproporção entre as penas dos delitos de invasão de dispositivo informático e de perseguição, o que poderia ensejar um discurso favorável ao concurso de crimes. Aplicando o princípio da consunção ao caso particular do *stalkerware,* registra-se que o crime de perseguição, possível crime absorvente, apresenta pena de reclusão de seis meses a dois anos e multa, enquanto a forma qualificada de invasão de dispositivo informático com obtenção de conteúdo de comunicações eletrônicas privadas possuiria pena de reclusão de dois a cinco anos, e multa. Trata-se de situação em que "o tipo penal consumido apresenta margem penal abstrata maior do que a relativa ao tipo que o consome" (GOMES, 2014, p. 257), de forma que o desvalor da conduta absorvida, traduzido em uma pena maior, desapareceria com a consunção.

Nessa instância, paira a dúvida a respeito de qual crime será absorvido e de qual pena será finalmente aplicada, posto que a gravidade atribuída pelo legislador em forma de pena desvaneceria com a absorção do crime de maior pena. Por um lado, avalia-se que esse vício de desproporção de pena entre as normas decorreria da falibilidade do processo legislativo, eis que idealmente o legislador, no plano teórico, determinaria a pena mais grave ao tipo penal com base na prática de outras infrações mais leves (GOMES, 2014; HORTA, 2007). Por outro lado, seria impossível inferir que sucede a absorção da totalidade do conteúdo do injusto da norma consumida, consistente em fundamento material da pena atribuída pelo legislador, de modo que "a norma consuntiva só absorve o desvalor de uma parcela do universo de fatos puníveis segundo a norma consumida, correspondente aos que normalmente acompanham ou decorrem da realização dos pressupostos da primeira" (HORTA, 2007, p. 152), ou seja, a norma consumida pode prever outras condutas lesivas além daquela que viabilizou o crime-fim, o que justificaria a maior gravidade de sua pena. Diante dessa desproporção entre as penas, Gomes propõe três soluções possíveis de aplicação da sanção:

> Diante dessa matéria, podemos encontrar três formas diferentes de solucionar a questão. De um lado, há quem argumente que deve ser aplicada a pena maior, ainda que esta esteja relacionada ao crime absorvido; de outro lado, encontramos o argumento segundo o qual deve ser aplicada a norma de comportamento previsto no crime mais leve e a sanção correspondente ao delito mais grave; por fim, sustenta-se que a pena aplicada deve ser a do crime absorvente, ainda que menor (GOMES, 2014, p. 258).

As duas primeiras correntes defendem a imposição de punição mais gravosa do crime absorvido, a fim de impedir a oferta de melhor tratamento penal ao autor responsável pelo cometimento de dois atos ilícitos (COSTA, 2012). Buscando uma solução intermediária entre o rigor do concurso efetivo de crimes e a "excessiva suavidade da consunção", a doutrina alemã sustenta a aplicação do efeito de bloqueio ou da cláusula impeditiva da norma afastada ao concurso aparente de normas penais incriminadoras, surtindo efeitos na determinação da pena pelo Juízo, o qual fixaria a maior entre as penas mínimas e a pena máxima da norma prevalente (COSTA, 2012).

No entanto, essas propostas ignoram o próprio fundamento do princípio da consunção, o qual pressupõe o afastamento da incidência do tipo penal secundário como um todo, tanto que Costa aponta como contraditória a imposição do efeito de bloqueio de uma norma excluída (COSTA, 2012). Compete notabilizar que, não obstante seja desconsiderada a sanção do tipo penal secundário, não se deve depreender que o cometimento de segundo crime seja irrelevante para o ordenamento penal, mas sim que o "marco penal da infração mais grave já oferece margem suficiente para dar conta de qualquer incremento de desvalor" (GRECO; LEITE, 2022,

p. 142), uma vez que as circunstâncias do crime consumido poderiam, para parcela da doutrina, apresentar efeitos sobre a dosimetria da pena (COSTA, 2012).

Diante dessa discrepância entre as penas, o Ministério Público do Distrito Federal e Territórios, em suas diretivas sobre o crime de *stalking*, excluiu de imediato a possibilidade de consunção pela perseguição e postula que "na hipótese de conduta única de invasão de dispositivo informático da vítima, a configuração do crime do art. 154-A do CP tem preferência sobre o crime de perseguição (CP, art. 147-A), diante da maior reprovabilidade da conduta, sem prejuízo de eventual concurso de crimes na hipótese de diversas condutas de perseguição" (MPDFT, 2021, p. 3).

Discordando desse parecer, repisa-se que a consunção não se justifica pela maior intensidade da ofensa punida pelo tipo penal mais abrangente, mas é fundada na tradução mais abrangente por esse tipo dos aspectos lesivos do fato, independentemente da identidade ou diversidade dos bens jurídicos tutelados (HORTA, 2007). Dessarte, em respeito ao princípio da legalidade penal e à opção mais favorável ao acusado, Gomes defende a aplicação da pena pertencente ao crime absorvente, julgando-a a única opção correta em termos de dogmática penal (GOMES, 2014). Essa posição não é repudiada na jurisprudência, eis que fixada, na Súmula 17 do Superior Tribunal de Justiça, a possibilidade de absorção dos crimes de falsidade pelo delito de estelionato, ainda que a pena de determinados crimes de falsidade ultrapasse a pena do estelionato.

Nesses termos, na alçada do *stalkerware*, por mais que a forma qualificada do delito de invasão de dispositivo informático apresente uma sanção mais grave, interpreta-se a favor da aplicação tanto da norma de comportamento como da sanção do crime absorvente da perseguição, em conformidade ao princípio da consunção, excluindo o tipo legal consumido, o qual não contribuiria para o injusto típico, tampouco para a determinação dos limites da sanção (VINAGRE, 2011). Desse modo, vê-se como lógica a aplicação integral do tipo penal absorvente, não se produzindo um malabarismo de política criminal apenas para punir mais intensamente o agente ou para reparar uma falha de formulação normativa do próprio legislador.

Portanto, superadas as divergências a respeito dos bens jurídicos tutelados e da desproporção entre as sanções, defende-se, em geral, a possibilidade de aplicação do princípio da consunção ao *stalkerware*, ainda que se demande uma análise de cada caso concreto. Nesses termos, é viável a absorção da forma qualificada do crime de invasão de dispositivo informático

(art. 154-A) pelo crime de perseguição (art. 147-A), desde que o potencial ofensivo do crime de invasão de dispositivo informático não se desvie a outras práticas delitivas.

CONCLUSÃO

Face ao emprego de ferramentas cibernéticas tanto para o combate, como para a execução de crimes em nova interface, os meios de controle perpatrados pelo agressor, inerentes à violência de gênero, assumem inevitavelmente um componente tecnológico. Enquanto manifestação da violência digital de gênero, insere-se o *stalkerware*, consistente em monitoramento e rastreamento remoto viabilizado por sistemas de *spyware* e *dual-apps*, cujas funcionalidades são deturpadas para o cometimento do *cyberstalking*, atentando gravemente contra a confidencialidade dos dados pessoais e, consequentemente, contra privacidade e intimidade.

Perante diferentes vertentes de instalação de aplicativos espiões, a presente Tese de Láurea centrou-se na sua operacionalização para cometimento da violência de gênero, de modo que o perpetrador usualmente instala o aplicativo no dispositivo da atual ou ex-parceira sem seu consentimento, por meio do qual se possibilita a coleta de dados pessoais, comunicações privadas, histórico de navegação, senhas, localização, o bloqueio de chamadas e eventualmente a ativação de microfones e câmeras. Além de potencialmente causar danos à saúde mental e patrimoniais, o *stalkerware* configura fator de risco para atos mais extremos de violência e, ainda que haja autorização da companheira, muitas vezes a instalação do aplicativo decorre de uma pressão do agente, justificando-a como prova de amor ou de confiança.

Desse modo, verificou-se que o *stalkerware*, na condição de meio sofisticado de invasão da privacidade e de controle integral da vida digital de suas vítimas, compreende ato de violência complexo, que reúne peculiaridades já identificadas na violência digital de gênero, na cibercriminalidade e no *stalking*, ofendendo o bem jurídico da liberdade individual em diferentes âmbitos. Nesses termos, considerando a suficiência do atual leque normativo em termos de tutela penal e a ausência de jurisprudência consolidada sobre a temática, propôs-se, como resposta criminal, a capitulação desse fenômeno como prática de perseguição (art. 147-A) mediante o delito de invasão de dispositivo informático (art. 154-A). No entanto, tratando-se de problemática multidisciplinar que envolve valores jurídicos distintos, não basta a mera intervenção penal para minimização dessa violência, eis que a formulação de estratégias

eficientes de combate a esse mau uso exige uma análise da produção legislativa brasileira em face da violência de gênero, dos crimes cibernéticos e do *stalking*.

Representando o *stalkerware* uma modalidade da violência de gênero, fundada em relações de poder desiguais entre homens e mulheres, importa refutar, sob uma lente interseccional, a noção de um grupo homogêneo de vítimas, as quais são perpassadas por diferentes marcadores da diferença, impactando nas experiências de violência de cada uma, sejam digitais ou não. No que tange à violência de gênero, historicamente, o direito penal atuou de forma dicotômica, ora como frente de combate, ora na reprodução dessa violência, uma vez que, embora confira maior reprovação e visibilidade à conduta, tem risco de desviar a atenção da sociedade a outras formas de resolução social e de adotar uma postura paternalista para com a vítima. Além disso, é relevante considerar que as respostas jurídicas nem sempre coincidem com as expectativas das mulheres que recorrem ao Poder Judiciário, uma vez que os conflitos nas relações afetivas não se limitam a meros aspectos processuais penais ou a uma relação de causa e efeito.

Quando inserida como componente dessa violência, cumpre reconhecer a tecnologia como elemento de dinâmicas sociais articulado com formas de interação *offline*, ou seja, de *converged environment*, sem recair em uma separação simplista entre ciberespaço e mundo real. Portanto, ainda que a tecnologia sirva de estratégia de erradicação da violência de gênero, reconhece-se, no presente trabalho, seu papel como sua facilitadora, diante de particularidades do meio informático que tanto amplificam a capacidade de monitoramento e ameaça de vítimas como dificultam sua persecução penal, como o anonimato, a instantaneidade, a capacidade de propagação, a sensação de segurança, a relativização dos padrões éticos, entre outros. Mediante o rompimento de barreiras temporais e espaciais, o abuso, especialmente em relacionamentos afetivos, é marcado pela onipresença do agressor, verificando-se quando o perpetrador adquire inicialmente acesso a contas e dispositivos como supostas demonstrações de amor, quando vigia a parceira de forma transparente ou oculta e, ainda, quando se vale da ferramenta informática para se vingar da sobrevivente pelo fim do relacionamento e arruinar sua reputação. Nessa instância, o *stalkerware* consolida-se como violência digital de gênero pautada na vigilância e no monitoramento da vítima, invadindo completamente sua vida privada, refletida no âmbito virtual.

Aprofundando sobre os crimes cometidos nesse meio e seu regime jurídico de proteção, estabelece-se viver em uma sociedade de risco informática, em que se difundiu uma

criminalidade virtual com ataques remotos e facilmente ocultados à privacidade e à confidencialidade dos dados, em face da qual o direito penal tradicional se revelou deficitário. Por essa razão, repercutiram a criação de categorias voltadas aos delitos contra ou pela utilização do meio informático, bem como a existência de bem jurídico autônomo de segurança informática. Nesse cenário, objetivando inserir o fenômeno do *stalkerware* nesse movimento de especialização do direito penal, analisou-se o delito de invasão de dispositivo informático como crime-meio dessa prática, já que a consecução do *stalkerware* pressupõe um acesso indevido a um dispositivo informático, com o objetivo de instalar o *spyware* sem autorização expressa ou tácita da usuária, usualmente resultando na obtenção de conteúdo de comunicações privadas, o que ofenderia os bens jurídicos da intimidade e da privacidade, compreendidos no direito à inviolabilidade dos dados em dispositivo informático.

Apesar das modificações do tipo penal examinado, como a exclusão do requisito da violação do mecanismo de segurança, entende-se que a atual redação da norma ainda é problemática no que concerne à ausência de definição dos termos técnicos e de consideração sobre os distintos graus de acesso a dados informáticos de outrem. Todavia, o dispositivo em questão ainda é extremamente relevante, por inserir, em sua esfera normativa, a violação da privacidade em dispositivos informáticos, conferindo maior proteção à vítima. Mais uma vez, para a prevenção do cometimento desses delitos, não se infere a imprescindibilidade de uma contínua expansão do direito penal, e sim uma demanda de maior regulamentação global cibernética por outras searas.

Ato contínuo, tendo em mente que o *stalkerware* configura manifestação do *cyberstalking,* é de rigor associar a perseguição à violência de gênero, posto que sua prática, amparada por sentimento de posse sobre o corpo feminino, frequentemente ocorre após a ruptura de relacionamentos, possivelmente antecipando atos mais extremos de violência, como o feminicídio, o que justifica sua causa de aumento quando praticada contra mulher pelas mesmas razões do feminicídio. Há de se pontuar, entretanto, que o direito penal incide sobre prática de perseguição verdadeiramente hostil, reiterada e indesejada que perturbe gravemente a esfera de liberdade e de intimidade do indivíduo, restrinja sua capacidade de locomoção ou ameace sua integridade física ou psicológica. Por mais que o sofrimento psíquico da vítima contribua para prova da configuração delitiva, essa conduta é aferida objetivamente, sendo possível que as vítimas tenham sua privacidade invadida, mas não reajam com medo ou com desequilíbrio emocional.

Sem tipo penal próprio, o *cyberstalking* é qualificado como prática de perseguição cometida por meio informático, beneficiando-se das características dos crimes informáticos, como a possibilidade de manipulação dos rastros virtuais, além de violar os bens jurídicos de privacidade e vida íntima da vítima, coincidindo com aqueles violados pelo *stalking*. Inserido como espécie de *cyberstalking*, o *stalkerware* corresponderia à prática de *stalking* mediante intrusão informática, diferenciando-se pela forma sofisticada e pelo elevado poder sobre dados sensíveis.

Delineados os marcos dignos de tutela penal que compreendem o *stalkerware*, compete ofertar uma resposta criminal a essa prática como uma das frentes de combate, sob o paradigma de um direito penal mínimo. Delimitando o grau de ofensividade dessa prática pelo parâmetro do bem jurídico, entende-se que o bem jurídico geral consiste na liberdade individual em sentido amplo, a qual se desdobra em intimidade e privacidade, mas também na inviolabilidade dos dados informáticos. Conclui-se, então, que uma tipificação penal adequada consistiria na prática do crime de *stalking* mediante a invasão de dispositivo informático, não se vislumbrando como imprescindível uma criminalização primária.

Entretanto, não resulta suficiente uma mera intervenção penal, naturalmente voltada a incidentes individuais de violência, eis que o presente fenômeno, enquanto novo risco gerado pela deturpação dos meios tecnológicos e instrumentalizado pela violência de gênero, exige, pela sua natureza estrutural, atuação multidisciplinar e intersetorial. Na contramão, observam-se ainda grandes percalços para sua efetivação. Primeiramente, as empresas desenvolvedoras dos aplicativos apresentam formalmente uma série de termos de serviços e condições de uso, porém ineficazes para a contenção da violência praticada, e raramente oferecem suporte à vítima de violação de dados, delegando a responsabilidade de obtenção de consentimento ao contratante do serviço de monitoramento. Ainda, em face de obstáculos de persecução penal dos crimes informáticos, como difíceis detecção do s*talkerware*, produção probatória e formulação de plano de segurança à sobrevivente, os agentes públicos que implementam a norma penal subestimam o potencial lesivo dos novos meios tecnológicos de cometimento e não detêm formação técnica adequada de enfrentamento, reproduzindo soluções estereotipadas passíveis de aumentar a situação de risco vivida pela sobrevivente.

A partir das experiências internacionais com o *stalkerware*, verificam-se igualmente as dificuldades de persecução intrínsecas às violências digitais de gênero, bem como distintas percepções a respeito da tipificação penal dessa conduta, exemplificando a incidência de

normas incriminadoras de *stalking*, interceptação de comunicação de privada, uso não autorizado de computador, variando a partir das circunstâncias do caso concreto. Diante disso, em prol de um enfrentamento mais técnico do *stalkerware* e de um atendimento sensibilizado no Brasil, defendem-se políticas de conscientização sobre a importância da confidencialidade dos dados e os potenciais delitos informáticos, aperfeiçoamento dos canais de denúncia, restrição à disponibilização de aplicativos facilitadores da violência de gênero, maior sistema do apoio dos aplicativos às vítimas, estímulo ao desenvolvimento de programas de detecção do *spyware* por empresas de segurança digital, formação técnica dos atores do sistema de justiça a respeito de produção de provas, assistência social em rede perante a violência de gênero, entre outras medidas.

Por fim, explorando a relação entre os tipos penais no *stalkerware*, concluiu-se que, embora o bem jurídico informático seja atingido, o acesso indevido integra o feito delitivo como meio necessário para cometimento do monitoramento e da vigilância da vítima, na qualidade de crime informático mediato ou indireto. Apesar da desproporção entre as sanções e das variações atinentes ao episódio examinado, julga-se possível a incidência do princípio da consunção no *stalkerware*, ocorrendo a absorção da conduta qualificada de invasão de dispositivo informático pela perseguição, tipo penal a ser aplicado integralmente por melhor abranger os aspectos lesivos do fato criminoso.

Logo, depreende-se que o *stalkerware*, relativamente novo no Brasil, consiste em fenômeno delitivo complexo e ainda pouco estudado que atinge bens jurídicos inerentes à personalidade e ostenta particularidades já identificadas na violência digital de gênero, do *stalking* e da cibercriminalidade, às quais qualquer proposta de criminalização deve se atentar. Contudo, mais do que uma tutela penal, a erradicação dessa espécie de *cyberstalking* que se apropria de aplicativos espiões, demanda ações intersetoriais de conscientização e de atendimento especializado às sobreviventes, além de contínuas pesquisas sobre sua abordagem e um maior debate público a respeito de seu enfrentamento.

BIBLIOGRAFIA

AGUIAR, Janaina Marques de; D'OLIVEIRA, Ana Flavia Pires Lucas; SCHRAIBER, Lilia Blima. Mudanças históricas na rede intersetorial de serviços voltados à violência contra a mulher – São Paulo, Brasil. **Interface**, v. 24, 2020.

AIRES DE SOUSA, Susana. Um direito penal desafiado pelo desenvolvimento tecnológico: alguns exemplos a partir das neurociências e da inteligência artificial. **Revista da Defensoria Pública da União**, n. 14, p. 21-37, 18 dez. 2020.

ALMEIDA, Angélica de Maria Mello de. Aspectos processuais e penais: Lei Maria da Penha. **Cadernos Jurídicos**, São Paulo, v. 15, n. 38, p. 105-111, jan./abr. 2014.

ALMEIDA, Karen Rosa de; ZAGANELLI, Margareth Vertis. Cyberstalking: Do enquadramento atual à necessidade de tutela específica – Uma análise à luz do ordenamento jurídico brasileiro e do direito comparado. **Revista do Programa de Pós Graduação em Direito da UFBA**, v. 31, n. 1, p. 167-187, Jan-Jun 2021.

AUGUSTO, Cristiane Brandão. **Violência contra a mulher e as práticas institucionais**. Série Pensando o Direito, vol. 52, Brasília: Ipea/Ministério da Justiça, 2015.

AVAST. Nos últimos três anos, stalkerware cresce 358% no Brasil. São Paulo, 14 mar. 2023. Disponível em: <https://press.avast.com/pt-br/press-release-final-nos-ultimos-tres-anos-stalkerware-cresce-358-no-brasil>. Acesso em: 03 jun. 2024.

BADA, Maria; CHUA, Yi Ting; COLLIER, Ben; PETE, Ildikó. Exploring masculinities and perceptions of gender in online cybercrime subcultures. *In:* WEULEN KRANENBARG, M.; LEUKFELDT, R. (coords.). **Cybercrime in Context**, 2021, p. 237–257.

BANDEIRA, Lourdes Maria. Violência de gênero: a construção de um campo teórico e de investigação. **Sociedade e Estado**, Brasília, v. 29, n. 2, p. 449-469, ago. 2014.

BARROS, Juliana Motta de. **Lei nº 12.737:** a nova tipificação criminal de delitos informáticos. Artigo Científico (Pós-Graduação). Escola de Magistratura do Estado do Rio de Janeiro, 2015.

BARSTED, Leila Linhares. O avanço legislativo contra a violência de gênero: a Lei Maria da Penha. **Revista EMERJ** (Escola da Magistratura do Estado do Rio de Janeiro), Rio de Janeiro, v. 15, n. 57 (Edição Especial), jan.-mar. 2012. pp. 90-110.

BATISTA, Nilo. Só Carolina não viu - Violência doméstica e políticas criminais no Brasil. Só Carolina não viu – Violência doméstica e políticas criminais no Brasil. **Jornal do Conselho Regional de Psicologia**, ano 5, Rio de Janeiro, mar/2008.

BAUER, Jenny-Kerstin; HARTMANN, Ans. Formen digitaler geschlechtsspezifischer Gewalt. *In*: PRASAD, Nivedita (Ed.). **Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung:** Formen und Interventionsstrategien. Bielefeld: transcript Verlag, 2021, p. 63-100.

BECHARA, Ana Elisa Liberatore Silva. **O bem jurídico-penal**. São Paulo: Quartier Latin, 2014.

BEIRAS, Adriano; MORAES, Maristela; ALENCAR-RODRIGUES, Roberta de; CANTERA, Leonor M.. Políticas e leis sobre violência de gênero - reflexões críticas. **Psicologia & Sociedade**, v. 24, n. 1, p. 36-45, 2012.

BIANCHINI, Alice. A Qualificadora do Feminicídio é de Natureza Objetiva ou Subjetiva?. **Revista EMERJ**, Rio de Janeiro, v. 19, n. 72, p. 203 - 219, jan.-mar. 2016.

BIANCHINI, Alice; BAZZO, Mariana Seifert; CHAKIAN, Silvia. **Crimes contra mulheres:** Lei Maria da Penha, crimes sexuais, feminicídio. 5. ed. rev., ampl. e atual. São Paulo: JusPodivm, 2023.

BITENCOURT, Cezar Roberto. **Tratado de direito penal:** parte especial. 22. ed., v. 2. São Paulo: Saraiva, 2022.

BOURDIEU, Pierre. **A dominação masculina**. Tradução de Maria Helena Kühner. Rio de Janeiro: Bertrand Brasil, 1999.

BOTTINI, Pierpaolo Cruz. **Crimes de perigo abstrato e princípio da precaução na sociedade de risco**. São Paulo: Editora Revista dos Tribunais, 2007.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.793, de 29 de novembro de 2011**. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Brasília: Câmara dos Deputados, 2011. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=944218&filename=PL%202793/2011>. Acesso em: 07 jun. 2024.

BRENNER, Susan W.. Cybercrime jurisdiction. **Crime, Law and Social Change**, v. 46, p. 189–206, 2006.

BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2013.

BUTTON, M.; BLACKBOURN, D.; SUGIURA, L.; SHEPERD, D.; KAPEND, R.; WANG, V.. Victims of Cybercrime: Understanding the Impact Through Accounts. *In:* WEULEN KRANENBARG, M.; LEUKFELDT, R. (coords.). **Cybercrime in Context**. Crime and Justice in Digital Society. Cham: Springer, v. 1, 2021.

CABETTE, Eduardo Luiz Santos. Perseguição, "stalking" ou assédio por intrusão Lei nº 14.132/21. p. 22-58. **Conceito Jurídico**, n. 54, jun. 2021.

CARVALHO, Salo de. **Penas e medidas de segurança no direito penal brasileiro**: fundamentos e aplicação judicial. São Paulo: Saraiva, 2020.

CARVALHO, Gisele Mendes de; HENRIQUES, Hamilton Belloto. A criminalização do "stalking" e do assédio moral no Brasil: uma lacuna (quase) colmatada. **Revista Brasileira de Ciências Criminais**, vol. 183, ano 29. p. 125-170, 2021.

CASTRO, Ana Lara Camargo de; SYDOW, Spencer Toth. **Stalking e Cyberstalking**. Salvador: Juspodivm, 1 ed., 2021.

CAVALCANTE, Vivianne Albuquerque Pereira; LELIS, Acácia Gardenia Santos. Violência de gênero contemporâneo: Uma nova modalidade através da pornografia da vingança. **Interfaces Científicas - Direito**, v. 4, n. 3, p. 59–68, 2016.

CHAI, Whistine Xiau Ting; NG, Shannon; NEO, Loo Seng. Introduction to Cyber Forensic Psychology. *In:* KHADER, Majeed; CHAI, Whistine Xiau Ting; NEO, Loo Seng (Eds.). **Introduction to cyber forensic psychology**: Understanding the mind of the cyber deviant perpetrators. Singapore: World Scientific Publishing Co. Pte. Ltd., 2021, p. 3-17.

CHATTERJEE, Rahul; DOERFLER, P.; ORGAD, H.; *et al*. The Spyware Used in Intimate Partner Violence. **2018 IEEE Symposium on Security and Privacy (SP)**, 2018.

CIRINO DOS SANTOS, Juarez. **Direito Penal: Parte geral.** São Paulo: Tirant lo Blanch, 9. ed., 2020, p. 425.

COALITION AGAINST STALKERWARE; KASPERSKY. Instituto Astronômico e Geográfico. **The State of Stalkerware in 2020**. 2020. 12 p.

COELHO, Cláudia; GONÇALVES, Rui Abrunhosa. Stalking: uma outra dimensão da violência conjugal. **Revista Portuguesa de Ciência Criminal.** Coimbra Editora, Coimbra, p. 269-302, 2007.

COLEMAN, Frances L. Stalking Behavior and the Cycle of Domestic Violence. **Journal of Interpersonal Violence**, v. 12, n. 3, p. 420-432, jun. 1997.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS - OEA. **Convenção interamericana para prevenir, punir e erradicar a violência contra a mulher**, "Convenção de Belém do Pará". 1994.

COSTA, Pedro Jorge. **A consunção no direito penal brasileiro**. Porto Alegre: Sérgio Antônio Fabris Editor, 2012.

COSTA, Helena Regina Lobo da. Crimes contra a liberdade individual: Arts.146-154-B. *In*: SOUZA, Luciano Anderson de (coord). **Código penal comentado**. São Paulo: Thomson Reuters, 2020.

CRENSHAW, Kimberlè. **Documento para o encontro de especialistas em aspectos da discriminação racial relativos ao gênero.** Estudos Feministas, Florianópolis, Centro de Filosofia e Ciências Humanas, Centro de Comunicação e Expressão, v. 7, n. 12, p. 171-188, jan./2002.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

D'AVILA, Fabio Roberto; SANTOS, Daniel Leonhardt dos. Direito Penal e criminalidade informática. Breves aproximações dogmáticas. **Revista Duc In Altum - Cadernos de Direito**, v. 8, n. 15, 2016.

DE SOUSA, Laís Lopes. Cyberstalking, violência de gênero e limites da dogmática penal. *In*: KASSADA, Daiane Ayumi; MENESES, Willians. **Cadernos do Laboratório de Iniciação Científica do Instituto Brasileiro de Ciências Criminais** (IBCCRIM): Melhores artigos do ano de 2021. Curitiba: Editorial Casa, 1. ed., 2022.

DEBERT, Guita Grin; OLIVEIRA, Marcella Beraldo de. Os modelos conciliatórios de solução de conflitos e a "violência doméstica". **Cadernos Pagu**, v. 29, jul.-dez. 2007, p. 305-337.

DEBERT, Guita Grin; GREGORI, Maria Filomena. Violência e gênero: novas propostas, velhos dilemas. **Revista Brasileira de Ciências Sociais**, v. 23, n. 66, p. 165-211, 2008.

DEIBERT, Ronald J. The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy. **Foreign Affairs**, v. 102, n. 72, 2023.

DOBRINOIU, Maxim. Criminal liability in the case of vendors of software and hardware further used in cybercrime activities. **CKS 2022 Challenges of the Knowledge Society**, 15. Ed., Bucharest, 2022.

EYALSALMAN, Ruba Taha. Android Stalkerware Detection Techniques: A Survey Study. **IEEE Jordan International Joint Conference of Electrical Engineering and Information Technology**, Amman, 2023.

FARIAS, Alexandre Ramalho de; PIEGEL, Stella Maris. § 15.2 - Soluções para o concurso aparente de normas incriminadoras: Princípio da consunção. *In:* BUSATO, Paulo César (org.). **Fundamentos de Direito Penal**. 1. ed. Curitiba: Juruá, 2013. v. 1, 314p.

FASCENDINI, Flavia; FIALOVÁ, Kateřina. **Voices from digital spaces:** Technology related violence against women. Association for Progressive Communications (APC), 2011.

FAUBERT, Camille; DÉCARY-HÉTU, David; MALM, Aili; RATCLIFFE, Jerry; DUPONT, Benoît. Law enforcement and disruption of offline and online activities: a review of contemporary challenges. *In:* WEULEN KRANENBARG, M.; LEUKFELDT, R. (coords.). **Cybercrime in Context**, 2021, p. 351-370.

FERREIRA, Ivette Senise. A criminalidade informática. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). **Direito & internet: aspectos jurídicos relevantes.** Bauru: Edipro, 2000. p. 207-237.

FERREIRA, Renan Azevedo Leonessa. **Crimes informáticos estudados a partir da vítima**. São Paulo: Editora Dialética, 2023, 284 p.

FLAUZINA, Ana Luiza Pinheiro. Lei Maria da Penha: entre os anseios da resistência e as posturas de militância. In: FLAUZINA, Ana Luiza Pinheiro et al. **Discursos Negros:** legislação penal, política criminal e racismo. Brasília: Brado Negro, 2015, pp. 115-144.

FLORES, Carlos Pereira Thompson. **A Tutela Penal do Stalking**. Porto Alegre: Elegantia Juris, 2014, 81 p.

FRASER, Cynthia; OLSEN, Erica; LEE, Kaofeng; SOUTHWORTH, Cindy; TUCKER, Sarah. **The New Age of Stalking: Technological Implications for Stalking Juvenile and Family Court Journal,** v. 61, n. 4, 2010.

FREED, Diana *et al*. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. **Proceedings of the ACM on Human-Computer Interaction**, v. 1, n. 46, p. 1-22, 2017.

FREED, Diana *et al*. "Is my phone hacked?" analyzing clinical computer security interventions with survivors of intimate partner violence. **Proceedings of the ACM on Human-Computer Interaction**, v. 3, n. CSCW, p. 1-24, 2019.

GRANATO, Fernanda Rosa de Paiva. **A influência do discurso midiático e do clamor popular na recente produção legislativa penal brasileira:** os delitos eletrônicos e a Lei

12.737/12 (Lei Carolina Dieckmann). Monografia (Bacharel em Direito), Faculdade de Direito da Universidade Federal de Juiz de Fora, 2015.

GREGORI, Maria Filomena. **Cenas e Queixas:** Um Estudo sobre Mulheres, Relações Violentas e a Prática Feminista. Rio de Janeiro, Paz e Terra, 1993.

GILLESPIE, Alisdair A.. **Cybercrime: Key issues and debates**. Abingdon, Oxon: Routledge, 2019.

GOMES, Mariângela Gama de Magalhães. **Teoria geral da parte especial do direito penal**. São Paulo: Atlas, 2014.

GUDÍN RODRÍGUEZ-MAGARIÑOS, Faustino. Cyberstalking frente a una regulación penal inconclusa. **Revista de Derecho Penal**, n. 2, p. 47-83, 2014.

GRECO, Luís; LEITE, Alaor. Concurso de delitos: uma primeira tentativa de reorientação. **Revista do Instituto de Ciências Penais**, Belo Horizonte, v. 7, n. 1, p. 131-158, 2022.

HARKIN, Diarmaid; MOLNAR, Adam; VOWLES, Erica. The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. **Crime, Media, Culture**, v. 16, ed. 1, p. 33-60, 2020.

HARKIN, Diarmaid; MERKEL, Robert. Technology-Based responses to Technology-Facilitated Domestic and Family Violence: An Overview of the Limits and Possibilities of Tech-Based "solutions". **Violence Against Women**, v. 29, n. 3-4, 2023, p. 648–670.

HASSEMER, Winfried; MUÑOZ CONDE, Francisco. **Introducción a la Criminología y al Derecho Penal**. Valencia: Tirant lo Branch, 1989.

HASSEMER, Winfried. Das Symbolische am symbolischen Strafrecht. *In*: SCHÜNEMANN, Bernd; ACHENBACH, Hans; BOTTKE, Wilfried; HAFFKE, Bernhard; RUDOLPHI, Hans-Joachim (Coords.). **Festschrift für Claus Roxin zum 70**. **Geburtstag**. Berlin: De Gruyter, 2001, p. 1001-1020.

HOFFMANN, Jens; WONDRAK, Isabel. Stalking und Häusliche Gewalt – Eine allgemeine Einführung. Zum Management derartiger Fälle. *In*: WEISS, Andrea (Hrsg.). **Stalking und häusliche Gewalt -** Interdisziplinäre Aspekte und Interventionsmöglichkeiten. Freiburg, 2005, p. 13-22.

HORTA, Frederico Gomes de Almeida. **Do concurso aparente de normas penais**. Rio de Janeiro: Lumen Juris, 2007.

HUTCHINGS, Alice; CHUA, Yi Ting. Gendering cybercrime. *In*: HOLT, T. J. (Ed.), **Cybercrime through an Interdisciplinary Lens**. Oxon: Routledge, 2017, p. 167-188.

IBGE. 2024. **Estatísticas de Gênero:** Indicadores sociais das mulheres no Brasil. Estudos e Pesquisas: Informação Demográfica e Socioeconômica, n. 38, 3. ed., ISBN 978-85-240-4605-6. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv102066_informativo.pdf>. Acesso em: 03 jun. 2024.

KASPERSKY. 2021. Stalking online em relacionamentos. **Relatório**. Disponível em: <https://media.kasperskydaily.com/wp-content/uploads/sites/86/2021/12/17102010/Kaspersky_Digital-stalking-in-relationships_Report_FINAL_BR-PT.pdf>. Acesso em: 03 jun. 2024.

KHOO, Cynthia; ROBERTSON, Kate; DEIBERT, Ronald. Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications. **Citizen Lab Research Report No. 120**, University of Toronto, 2019.

KÖVER, Chris. Der Feind in der eigenen Tasche: Stalkerware und digitale Überwachung im Kontext von Partnerschaftsgewalt. *In*: PRASAD, N. (Ed.). **Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung:** Formen und Interventionsstrategien. Bielefeld: transcript Verlag, 2021, pp. 227-238.

LEITÃO, Roxanne. Technology-facilitated intimate partner abuse: A qualitative analysis of data from online domestic abuse forums. **Human–Computer Interaction**, v. 36, n. 3, p. 203-242, 2021.

LENHART, Amanda; YBARRA, Michele; ZICKUHR, Kathryn; PRICE-FEENEY, Myeshia. **Online harassment, digital abuse, and cyberstalking in America.** Data and Society Research Institute Report, 21 nov. 2016.

MACHADO, Jessika Milena Silva; MOMBACH, Patrícia Ribeiro. Stalking: Criminalização necessária sob a indubitável afronta ao direito fundamental à vida privada. **Revista da ESMESC**, v. 23, n. 29, p. 207-230, 2016.

MARTINS, Ana Paula Antunes; CERQUEIRA, Daniel; MATOS, Mariana Vieira Martins. A institucionalização das políticas públicas de enfrentamento à violência contra as mulheres no Brasil (versão preliminar). **IPEA**, vol. nº 13, 2015, pp. 1-37.

MANNAN, Mohammad; YOUSSEF, Amr. Privacy Analysis of Technologies Used in Intimate Partner Abuse. **Final Report for OPC Contributions Program 2022-2023**, University of Concordia, 2023.

MISKOLCI, Richard. Novas conexões: notas teórico-metodológicas para pesquisas sobre o uso de mídias digitais. **Revista Cronos**, v. 12, n. 2, p. 09-22, jul./dez. 2011. Disponível em: <https://periodicos.ufrn.br/cronos/article/view/3160>. Acesso em: 03 jun. 2024.

MPDFT. **Diretivas resultantes da Oficina sobre o novo crime de stalking e suas repercussões.** 25 jun. 2021. Disponível em: < https://www.mpdft.mp.br/portal/images/pdf/nucleos/nucleo_genero/publicacoes/Diretivas_Oficina_Lei_14132_21.pdf>. Acesso em: 06 jun. 2024.

NUCCI, Guilherme de Souza. **Manual de Direito Penal:** volume único. Rio de Janeiro: Forense, 19. ed., 2023.

O'BRIEN, Wendy; MARAS, Marie-Helen. Technology-facilitated coercive control: response, redress, risk, and reform. **International Review of Law, Computers & Technology**, p. 1-21, 2024.

PARSONS, Christopher; MOLNAR, Adam; DALEK, Jakub; KNOCKEL, Jeffrey; KENYON, Miles; HASELTON, Bennett; KHOO, Cynthia; DEIBERT, Ron. The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry. **Citizen Lab Research Report No. 119**, University of Toronto, jun. 2019.

PASCOLATI JUNIOR, Ulisses Augusto. A utilização do malware como ferramenta da infiltração virtual na investigação da criminalidade organizada: uma realidade normativa possível?. **Revista Judicial Brasileira**, Brasília, v. 2, n. 1, p. 544-571, jan./jul. 2022.

PASINATO, Wânia. Acesso à justiça e violência doméstica e familiar contra as mulheres: as percepções dos operadores jurídicos e os limites para a aplicação da Lei Maria da Penha. **Revista Direito GV**, v. 11 n. 2, p. 407-428, jul,-dez. 2015.

PIOVESAN, Flávia; PIMENTEL, Sílvia. A Lei Maria da Penha na perspectiva da responsabilidade internacional do Brasil. *In*: CAMPOS, Carmem Hein de. **Lei Maria da Penha comentada em uma perspectiva jurídico-feminista**. Rio de Janeiro: Lumen Juris, 2011.

PISCITELLI, Adriana. Interseccionalidades, categorias de articulação e experiências de migrantes brasileiras. **Sociedade e Cultura**, Goiânia, v. 11, n. 2, 2008.

PRASAD, Nivedita (Ed.). **Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung: Formen und Interventionsstrategien.** Bielefeld: transcript, 2021.

RAMOS JÚNIOR, Hélio Santiago. Invasão de dispositivo informático e a Lei nº 12.737/12: comentários ao art. 154-A do Código Penal. **Revista Jurídica do Ministério Público Catarinense**, v. 9, n. 20, jan./jun. 2012.

REALE JÚNIOR, Miguel (Coord.). **Código Penal Comentado**. São Paulo: Saraiva Jur, 2ª ed., 2023.

Relatório de CPI propõe seis projetos de lei para combater a violência cibernética contra a mulher. **O Dia**, Rio de Janeiro, 7 mar. 2024. Disponível em: <https://odia.ig.com.br/rio-de-janeiro/2024/03/6805927-relatorio-de-cpi-propoe-seis-projetos-de-lei-para-o-combate-a-violencia-cibernetica-contra-a-mulher.html>. Acesso em: 06 jun. 2024.

RIFIOTIS, Theophilos. Judiciarização das relações sociais e estratégias de reconhecimento: repensando a violência conjugal e a violência intrafamiliar. **Revista Kata**, v. 11, n. 2, p. 225-236, 2008.

ROYER, Sofie; VANLEEUW, Rune. Criminal Law and Technology. *In*: BROŻEK, Bartosz; KANEVSKAIA, Olia; PAŁKA, Przemysław. **Research Handbook on Law and Technology**. Edward Elgar, 2023, p. 190-213.

ROXIN, Claus. Que comportamentos pode o Estado proibir sob ameaça de pena? Sobre a legitimação das proibições penais. **Revista Jurídica**, Porto Alegre, v. 52, n. 317, p. 69-81, mar. 2004.

ROXIN, Claus. O tipo penal de stalking: questões de legitimidade e interpretação. **Revista do Instituto de Ciências Penais**, Belo Horizonte, v. 6, n. 1, p. 09–25, 2021.

SAFFIOTI, Heleith; ALMEIDA, Suely Souza de. **Violência de gênero – Poder e Impotência**. Rio de Janeiro: Revinter, 1995.

SAFFIOTI, Heleieth I. B. **Gênero, Patriarcado, Violência**. São Paulo, Editora Fundação Perseu Abramo, 2004.

SAFFIOTI, Heleieth. Contribuições feministas para o estudo da violência de gênero. **Cadernos Pagu**, Campinas, n. 16, p. 115-136, 2016.

SANTOS, Cecília MacDowell; PASINATO IZUMINO, Wânia. Violência contra as Mulheres e Violência de Gênero: Notas sobre Estudos Feministas no Brasil. **Estudios Interdisciplinarios de América Latina y El Caribe**, v. 16, nº 1, p.147-164. Israel: Universidade de Tel Aviv, 2005.

SANDYWELL, Barry. On the globalisation of crime: the Internet and new criminality. *In:* JEWKES, Yvonne; YAR, Majid (Eds.), **Handbook of Internet Crime**. London: Willan Publishing, 2010, p. 38-66.

SEVERI, Fabiana Cristina; CAMPOS, Carmen Hein. Violência contra mulheres e a crítica jurídica feminista: breve análise da produção acadêmica brasileira. **Revista Direito e Práxis**, [S. l.], v. 10, n. 2, p. 962–990, 2019.

SILVA SÁNCHEZ, Jesús María, **La expansión del Derecho penal**: Aspectos de la Política criminal en las sociedades postindustriales. Buenos Aires-Montevideo: B de F, 2006.

SILVA, Mariana Almeida da. A internet como ambiente facilitador à violência de gênero: cyberstalking, sextorsão e revenge porn. **Revista do Ministério Público do Estado do Rio de Janeiro**, Rio de Janeiro, n. 86, p. 109-131, out./dez. 2022.

SHAHANI, Aarti. Smartphones Are Used To Stalk, Control Domestic Abuse Victims. **NPR**, 2014. Disponível em: <https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims>. Acesso em: 22 nov. 2023.

SOTO, C. A. A. et al.. Violencia digital de género en Chile: un estudio durante la pandemia de COVID-19. **Sexualidad, Salud y Sociedad**, Rio de Janeiro, n. 39, p. e22306, 2023.

SOUZA, Luciano Anderson de. **Direito penal - vol. 2:** parte especial: arts. 121 a 154-A do CP. 3. ed. São Paulo: Revista dos Tribunais, Thomson Reuters, 2022.

SPONCHIADO, Jéssica Raquel. Título I: Dos Crimes contra a Pessoa. Capítulo I: Dos Crimes contra a Vida. *In*: SOUZA, Luciano Anderson de (coord). **Código penal comentado**. São Paulo: Thomson Reuters, 2020, p. 447-486.

STRAWHUN, Jenna; ADAMS, Natasha; HUSS, Matthew T.. The assessment of cyberstalking: an expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse. **Violence and victims,** v. 28, n. 4, p. 715-730, 2013.

SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade Por Omissão 84 - Distrito Federal. Min. Relator Cristiano Zanin, Data de Publicação: 17 abr. 2024. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15366173525&ext=.pdf>. Acesso em: 06 jun. 2024.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. São Paulo, Saraiva, 2015.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático**: Partes Geral e Especial. Salvador: Editora JusPodivm, 2022.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, São Paulo, v. 30, n. 86, p. 269–285, 2016.

VALENTE, Mariana. **Online Gender-Based Violence in Brazil.** New Data Insights. Supporting a Safer Internet Paper No. 4. Centre for International Governance Innovation, 2023. Disponível em: https://www.cigionline.org/static/documents/SaferInternet_Paper_no_4.pdf. Acesso em: 20 mai. 2024.

VALENTE, Mariana; NERIS, Para falar de violência de gênero na Internet: uma proposta teórica e metodológica. In: NATANSOHN, Graciela; ROVETTO, Fiorencia (Orgs.). **Internet e feminismos: olhares sobre violências sexistas desde a América Latina**. Salvador: EDUFBA, 2019.

VANDER, Sascha. Stalking - Aktuelle Entwicklungen und Tendenzen zur Schaffung eines speziellen Tatbestandes. **Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft**, v. 89, n. 1, 2006, p. 81-99.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Imprenta: Belo Horizonte, Fórum, 2013.

VINAGRE, Nuno. **Da Reforma Dogmática do Concurso de Crimes**: O repensar à luz do complexo sistema dialéctico entre o crime de coação sexual e o crime de violação. Coimbra: Coimbra Editora, 1. ed., 2011.

WALL, David S., **Cybercrime:** The Transformation of Crime in the Information Age. POLITY, 2007.

WILSON, Chanelle; SHERIDAN, Lorraine; GARRATT-REED, David. What is Cyberstalking? A Review of Measurements. **Journal of Interpersonal Violence**, v. 37, n. 11-12, 2022, NP9763-NP9783.

WILSON, Chanelle; SHERIDAN, Lorraine; GARRATT-REED, David. Examining Cyberstalking Perpetration and Victimization: A Scoping Review. **Trauma, Violence, & Abuse**, v. 24, n. 3, 2023, p. 2019-2033.

WINNER, Langdon. **The Whale and the Reactor:** A Search for Limits in an Age of High Technology. Chicago: University of Chicago Press, 1986.

WINTERER, Heidi. Stalking und Häusliche Gewalt - Erfahrungen bei der Staatsanwaltschaft Freiburg. *In*: WEISS, Andrea (Hrsg.). **Stalking und häusliche Gewalt** - Interdisziplinäre Aspekte und Interventionsmöglichkeiten, Freiburg, 2005, p. 97-109.

WOODHAMS, Samuel. **Spyware:** An Unregulated and Escalating Threat to Independent Media. Center for International Media Assistance, 2021.

WOODLOCK, Delanie. The Abuse of Technology in Domestic Violence and Stalking. **Violence Against Women**, v. 23, n. 5, p. 584-602, abr. 2017.

YARDLEY, Elizabeth. Technology-Facilitated Domestic Abuse in Political Economy: A New Theoretical Framework. **Violence Against Women**, v. 27, n. 10, 2021, p. 1479–1498.

ZAND, Elina van ‘t; MATTHIJSSE, Sifra; FISCHER, Tamar; WAGEN, Wytske van der. Interventions for cyber offenders. *In*: OERLEMANS, J. J.; KRANENBARG, M. Weulen (Eds.). **Essentials in cybercrime:** A criminological overview for education and practice. The Hague: Eleven, 2021, p. 255-283.

ANEXO A

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO

Registro: 2020.0000475252

ACÓRDÃO

Vistos, relatados e discutidos estes autos de Apelação Criminal nº 0000534-35.2017.8.26.0070, da Comarca de Batatais, em que é apelante ANDRE LUIS ALVES CARNEIRO, é apelado MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO.

ACORDAM, em sessão permanente e virtual da 3ª Câmara de Direito Criminal do Tribunal de Justiça de São Paulo, proferir a seguinte decisão: **Negaram provimento ao recurso. V. U.**, de conformidade com o voto do relator, que integra este acórdão.

O julgamento teve a participação dos Desembargadores RUY ALBERTO LEME CAVALHEIRO (Presidente sem voto), LUIZ ANTONIO CARDOSO E TOLOZA NETO.

São Paulo, 26 de junho de 2020.

CESAR MECCHI MORALES
Relator
Assinatura Eletrônica

Este documento é cópia do original, assinado digitalmente por CESAR MECCHI MORALES, liberado nos autos em 26/06/2020 às 18:33 .
Para conferir o original, acesse o site https://esaj.tjsp.jus.br/pastadigital/sg/abrirConferenciaDocumento.do, informe o processo 0000534-35.2017.8.26.0070 e código 17b17WYa.

Apelação nº 0000534-35.2017.8.26.0070
Comarca: Batatais
Apelante: André Luiz Alves Carneiro
Apelado: Ministério Público

Voto nº 14.688

LESÃO CORPORAL – VIOLÊNCIA DOMÉSTICA – Apelo do réu – Pretendida absolvição – Alegação de ausência de dolo - Impossibilidade – Autoria e materialidade delitivas amparadas nas declarações das vítimas, nos relatos do informante e no exame pericial que atestou a agressão física perpetrada pelo recorrente – Condenação de rigor.
RECURSO DESPROVIDO.

1. Ao relatório da r. sentença de fls. 109/114, de lavra da MM. Juíza Adriana Aparecida de Carvalho Pedroso, acrescenta-se que **André Luiz Alves Carneiro** foi condenado ao cumprimento de três meses de detenção, em regime aberto, como incurso nos artigos 129, § 9º, do Código Penal.

Irresignado, apela o réu, postulando desate absolutório por *"total ausência de dolo"* (razões de fls. 122/124).

O recurso foi respondido (fls. 139/141).

A ilustrada Procuradoria de Justiça Criminal manifesta-se pelo desprovimento do apelo (fls. 148/152).

É a síntese do necessário.

2. O reclamo não comporta acolhimento.

Este documento é cópia do original, assinado digitalmente por CESAR MECCHI MORALES, liberado nos autos em 26/06/2020 às 18:33 .
Para conferir o original, acesse o site https://esaj.tjsp.jus.br/pastadigital/sg/abrirConferenciaDocumento.do, informe o processo 0000534-35.2017.8.26.0070 e código 17b17WYa.

3. Narra a denúncia que em 02 de janeiro de 2017, por volta das 23h, na Rua José Benedito Moreira, nº 207, na cidade de Batatais, **André Luiz Alves Carneiro** ofendeu a integridade corporal de sua esposa J.S.F., causando-lhe lesões corporais de natureza leve.

4. A autoria e materialidade delitivas foram cabalmente comprovadas, sobretudo pelo boletim de ocorrência (fls.4/5), pela ficha de atendimento ambulatorial (fls. 13), pelo laudo pericial (fls. 20/21) e pela prova oral coligida (fls. 6/7, 8/9 e mídias digitais).

Interrogado em ambas as fases da persecução penal, **André** negou a imputação alegando que apenas segurou o pulso da vítima para retirar o aparelho celular de suas mãos e que o braço da ofendida teria sido, na verdade, arranhado pelos adornos de *"strass"* colados na capa de seu celular (fls. 17 e mídia digital).

Sua escusa, todavia, restou infirmada pela prova dos autos.

De forma harmônica e segura, a vítima narrou os fatos descritos na inicial. Esclareceu que apesar de, à época dos fatos, morar com **André**, estavam separados. Esclareceu que o apelante instalou um *"aplicativo espião"* em seu telefone celular para monitorá-la e que, na data do crime, trocava mensagens com um amigo quando o recorrente entrou no quarto acusando-a de traição. Narrou que **André** retirou o aparelho de suas mãos e quando tentou recuperar o telefone móvel o apelante a agrediu, apertando com força seus pulsos. Esclareceu, por fim, que o recorrente somente interrompeu a agressão pois o filho do casal *"começou a gritar"* (fls. 6/7 e mídias digitais).

No mesmo sentido, o depoimento do informante A.A.S.C, filho do casal, que estava no quarto e a tudo presenciou, destacando não ter sido a primeira oportunidade em que o apelante *"brigou"* com sua genitora (fls. 8/9 e mídias digitais).

E, de fato, o laudo pericial atestou que a vítima apresentava lesões corporais de natureza leve, consistentes em *"pequenas escoriações na região do antebraço esquerdo"* causadas por *"agente contundente"* (fls. 20/21), ferimentos plenamente compatíveis com a descrição fática por ela ofertada.

Incogitável a absolvição por ausência de dolo, tendo em vista que a prova oral coligida, bem como o laudo pericial juntado aos autos, indicam que o recorrente ofendeu a integridade física da vítima ao *"apertar"* seus braços com força e não

Este documento é cópia do original, assinado digitalmente por CESAR MECCHI MORALES, liberado nos autos em 26/06/2020 às 18:33 .
Para conferir o original, acesse o site https://esaj.tjsp.jus.br/pastadigital/sg/abrirConferenciaDocumento.do, informe o processo 0000534-35.2017.8.26.0070 e código 17b17WYa.

ao retirar o aparelho celular de suas mãos, como tentou fazer crer a Defesa.

A propósito: "*no âmbito dos crimes previstos na Lei n. 11.340/06, a palavra da vítima possui especial relevância, mormente quando corroborada por outros elementos de prova, tal como ocorreu na espécie.*" (STJ, AgRg no AREsp 936222 / MG, 5ª Turma, rel. Min. Jorge Mussi, j. 25.10.2016).

5. Enfim, justo o desfecho condenatório.

6. O procedimento dosimétrico, bem ainda a fixação do regime aberto, não comportam alteração, tanto que ausente inconformismo quanto a tais aspectos.

7. Diante do exposto, pelo meu voto **nega-se provimento** ao apelo.

CESAR MECCHI MORALES
Relator

Este documento é cópia do original, assinado digitalmente por CESAR MECCHI MORALES, liberado nos autos em 26/06/2020 às 18:33 .
Para conferir o original, acesse o site https://esaj.tjsp.jus.br/pastadigital/sg/abrirConferenciaDocumento.do, informe o processo 0000534-35.2017.8.26.0070 e código 17b17WYa.

ANEXO B

SUPERIOR TRIBUNAL DE JUSTIÇA

AGRAVO EM RECURSO ESPECIAL Nº 1721099 - DF (2020/0159437-9)

RELATOR	**:**	**MINISTRO PRESIDENTE DO STJ**
AGRAVANTE	:	BRUNO MOTA AVELAR ALMEIDA
ADVOGADOS	:	TATIANA NUNES VALLS - DF021521
		LENDA TARIANA DIB FARIA NEVES - DF048424
AGRAVADO	:	MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS

DECISÃO

Trata-se de agravo apresentado por BRUNO MOTA AVELAR ALMEIDA contra a decisão que não admitiu seu recurso especial.

O apelo nobre, fundamentado no art. 105, inciso III, alínea "a", da CF/88, visa reformar acórdão proferido pelo TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS, assim ementado:

> APELAÇÃO CRIMINAL INVASÃO DE DISPOSITIVO INFORMÁTICO FORMA QUALIFICADA TIPICIDADE CONFIGURADA CONDENAÇÃO MANTIDA DOSIMETRIA CONSEQUENCIAS DO CRIME ANÁLISE ESCORREITA QUANTUM READEQUAÇÃO PENA PECUNIÁRIA EXCLUSÃO IMPOSSIBILIDADE REDUÇÃO PROPORCIONALIDADE COM A PENA CORPORAL SUBSTITUIÇÃO POSSIBILIDADE

Quanto à **controvérsia em exame**, alega a defesa violação do art. 154-A do CP, associada à dicção do art. 386, inciso III, do CPP, ao raciocínio de que como não houve, nos autos, a demonstração das elementares do tipo penal em testilha, máxime de dolo na conduta denunciada, a absolvição o increpado - em homenagem ao postulado da legalidade, conjugada à vedação à analogia *in malam partem* - é medida de rigor.

Para tanto, traz à colação o(s) seguinte(s) argumento(s):

> Conforme consta no relatório do voto da decisão recorrida, o Recorrente teria, em 28.08.2013, instalado aplicativo espião no computador de sua então namorada com o objetivo de obter informações não autorizadas. (fl. 429).
>
> No decorrer do processo (defesa e apelação), o Recorrente demonstrou que não é qualquer dispositivo informático invadido que conta com a proteção legal e que, para que seja configurado o crime, **é necessário que ele conte com "mecanismo de segurança"**, como antivírus, firewall, senhas, etc. **e que**, **no caso**, **o computador não possuía qualquer** - a perícia realizada também não apontou a existência ou violação dos citados dispositivos de segurança. (fl. 429 - g.n.).
>
> Sucedeu-se a interposição de apelo pela ora Recorrente, que arguiu que a sentença mereceria reforma em virtude da conduta ser atípica, pois os requisitos caracterizadores do delito previsto no artigo 154-A do Código Penal não se fazem presentes: (fl. 430).

Documento eletrônico VDA26205439 assinado eletronicamente nos termos do Art.1º §2º inciso III da Lei 11.419/2006
Signatário(a): MINISTRO Presidente do STJ Assinado em: 10/08/2020 19:36:54
Publicação no DJe/STJ nº 2970 de 13/08/2020. Código de Controle do Documento: 105e5de4-994e-44bc-991f-278bee4642fc

> [...] porque **não houve violação a mecanismos de segurança**; (fl. 430 - g.n.).
>
> [...] porque **havia autorização tácita da Ofendida** para que o Recorrente utilizasse seu computador; e (fl. 430 - g.n.).
>
> [...] porque não houve qualquer "obtenção de vantagem ilícita; (fl. 430).
>
> **Demonstrou**, **ainda**, **a ausência de *animus nocendi* do Recorrente**, **não restando configurado o tipo subjetivo** (**dolo**) [...] (fl. 430 - g.n.).
>
> Não há nos autos demonstração das elementares do tipo penal do crime de invasão a dispositivo informático. Muito embora a sentença recorrida tenha, exaustivamente, analisado o conceito do objeto da conduta dispositivo informático - nada foi analisado quanto às demais elementares do tipo. (fl. 435).

É o relatório. Decido.

No que concerne à **controvérsia em apreço**, o Tribunal de origem, ao desprover o apelo defensivo, manifestou-se nos seguintes termos:

> Na fase de inquérito, a vítima N.L.H. relatou que namorou o réu Bruno Mota Avelar Almeida por cerca de dois anos e meio e que, em outubro de 2015, terminou o relacionamento, ao perceber que ele tinha todas as suas senhas pessoais e conversas do aplicativo *WhatsApp*. Narrou que descobriu esse fato quando o réu deixou a conta de e-mail dele aberta no seu computador, o que possibilitou que ela verificasse tal fato. Disse que inicialmente não quis registrar ocorrência sobre o fato, mas, depois de algum tempo, **descobriu que ele havia instalado em seu computador um programa chamado "*Netspy Pro*"**, **por meio do qual ele teria acesso às suas senhas e tudo que ela fizesse em seu computador**, **e que o e-mail do réu estava cadastrado como recebedor de tais informações** [...].
>
> O *notebook* da vítima **foi submetido a perícia** (Laudo de Exame de Informática n° 16.292/16 - fls. 21/29), **que constatou a existência de três softwares** "**espiões**", a saber: "*kgb keylogger spy*", "*Refog Keylogger*" e "*Netspy Pro*", **pelos quais** "**era possível obter informações sem autorização expressa ou tácita do titular do dispositivo**, sendo possível monitorar não apenas as teclas digitadas pelos usuários, mas praticamente todo tipo de atividade como: utilização de salas de bate papo, e-mails, páginas da internet com *Facebook*, aplicativos de mensagens como MSN, senhas utilizadas e capturas de telas do dispositivo. Além disto também era possível o envio dos dados capturados remotamente" [...].
>
> **O laudo apontou ainda que**, com relação ao programa "*Netspy Pro*", **o e-mail cadastrado como destinatário dos dados coletados bruno**mota.avelar@gmail.com [...]
>
> **Em Juízo** (mídia de fl. 182) **a vítima confirmou que o réu**, **sem o seu conhecimento**, **instalou software "espião" em seu *notebook***. **Disse que nunca desativou *firewall***, [...]. **Afirmou que ele não tinha acesso irrestrito a seu computador** [...]
>
> De todo o exposto, vê-se que o apelante, num primeiro momento, praticou a conduta descrita na parte final do dispositivo, ou seja, instalou uma vulnerabilidade, no caso, um programa espião, que lhe permitia monitorar todas as conversas e atividades do *notebook* da vitima.
>
> [...] **o próprio recorrente admite que instalou o referido programa** para ter acesso às conversas e mensagens trocadas pela sua então namorada e terceiros, para averiguar se "valeria a pena investir" no relacionamento o que, indubitavelmente, pode ser **caracterizado como ganho pessoal**.
>
> Pois bem, a instalação do referido programa "espião" pelo recorrente, conduta que, por si só, já configura a figura típica prevista no artigo 154- A do Código Penal, viabilizou a prática da segunda conduta prevista no referido dispositivo, qual seja, a da invasão em si.
>
> [...]
>
> Outrossim, conforme assinalado pela ilustre Procuradoria de Justiça, o

Documento eletrônico VDA26205439 assinado eletronicamente nos termos do Art.1º §2º inciso III da Lei 11.419/2006
Signatário(a): MINISTRO Presidente do STJ Assinado em: 10/08/2020 19:36:54
Publicação no DJe/STJ nº 2970 de 13/08/2020. Código de Controle do Documento: 105e5de4-994e-44bc-991f-278bee4642fc

> recorrente instalou o software "espião" pra ter acesso às conversas e mensagens justamente em razão da ausência de autorização para tanto, sendo certo que **se ela existisse** ou, ainda, se o réu tivesse acesso à máquina pelo perfil da vitima, conforme sustentado no interrogatório, **não seria necessário que ele se valesse do programa para obter tais informações**.
>
> Dessa forma, restou satisfatoriamente demonstrado que o réu instalou vulnerabilidade no computador da vitima com fim de obter proveito contrário ao direito e, mediante a violação indevida dos mecanismos de segurança, acessou e-mail e redes sociais dela, obtendo o conteúdo de suas comunicações privadas e outras informações pessoais, condutas que se amoldam perfeitamente ao tido descrito no artigo 154-A, §3°, do Código Penal. (fls. 406-412 - g.n.)

Da compreensão dos excertos transcritos, infere-se incidir o óbice da Súmula n. 7 do STJ ("A pretensão de simples reexame de prova não enseja recurso especial") sobre a aspiração absolutória alhures, porquanto a revisão das premissas assentadas perante as instâncias ordinárias demandaria necessário reexame do acervo fático-probatório carreado aos autos, mister incabível na via eleita.

Nesse sentido: "O recurso especial não será cabível quando a análise da pretensão recursal exigir o reexame do quadro fático-probatório, sendo vedada a modificação das premissas fáticas firmadas nas instâncias ordinárias na via eleita (Súmula n. 7/STJ)" (AgRg no REsp n. 1.773.075/SP, relator Ministro Felix Fischer, Quinta Turma, DJe de 7/3/2019).

Confiram-se ainda os seguintes precedentes: AgRg no AgRg no AREsp n. 1.374.756/BA, relatora Ministra Laurita Vaz, Sexta Turma, DJe de 1º/3/2019; AgInt nos EDcl no AREsp n. 1.356.000/RS, relator Ministro Luis Felipe Salomão, Quarta Turma, DJe de 6/3/2019; e REsp n. 1.764.793/RJ, relator Ministro Herman Benjamin, Segunda Turma, DJe de 8/3/2019.

Ante o exposto, com base no art. 21-E, V, do Regimento Interno do Superior Tribunal de Justiça, **conheço do agravo para não conhecer do recurso especial**.

Publique-se. Intimem-se.

Brasília, 10 de agosto de 2020.

MINISTRO JOÃO OTÁVIO DE NORONHA
Relator

Documento eletrônico VDA26205439 assinado eletronicamente nos termos do Art.1º §2º inciso III da Lei 11.419/2006
Signatário(a): MINISTRO Presidente do STJ Assinado em: 10/08/2020 19:36:54
Publicação no DJe/STJ nº 2970 de 13/08/2020. Código de Controle do Documento: 105e5de4-994e-44bc-991f-278bee4642fc