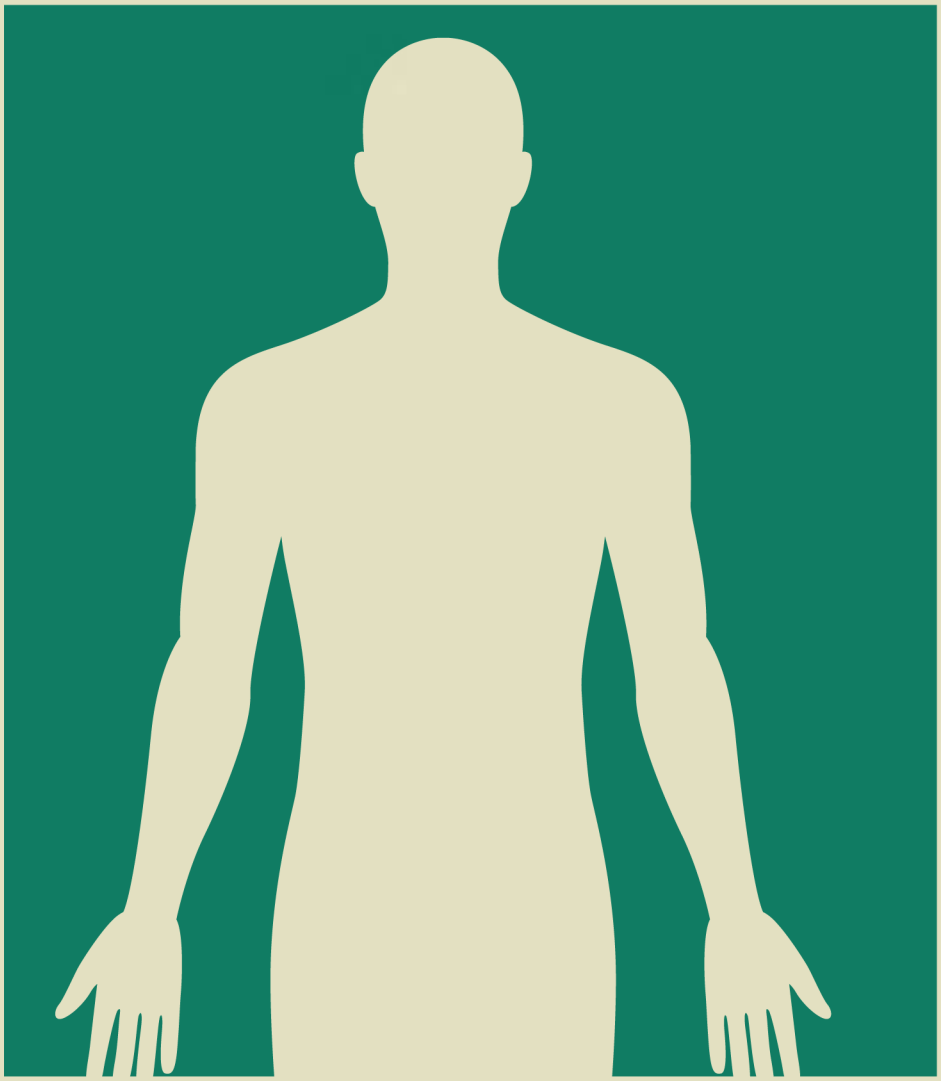
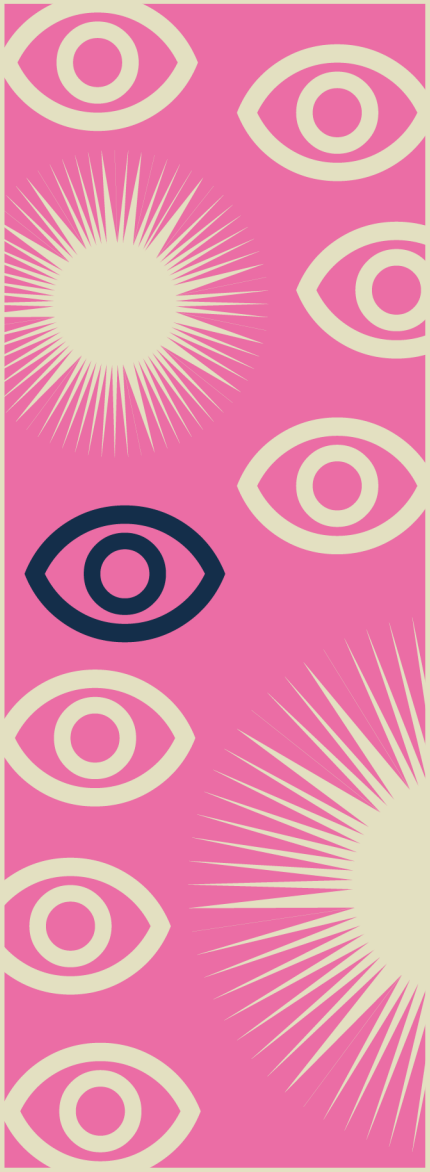




EXPONDO STALKERWARE

uma análise discursiva e técnica do ecossistema de stalkerware no Brasil

Instituto de Pesquisa em Direito & Tecnologia do Recife

UK Government

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

Expondo stalker(ware) [livro eletrônico] : uma análise discursiva e técnica do ecossistema de stalkerware no Brasil / Anicely Santos...[et al.] ; coordenação Mariana Canto. -- Recife, PE : IP.rec, 2025.
PDF

Outros autores: Carolina Branco, Luana Batista, Mariana Canto, Raquel Saraiva, Rhaiana Valois.
ISBN 978-65-982630-4-1

1. Ciência da Computação 2. Software de aplicação 3. Tecnologia - Aspectos sociais 4. Violência de gênero I. Santos, Anicely. II. Branco, Carolina. III. Batista, Luana. IV. Canto, Mariana. V. Saraiva, Raquel. VI. Valois, Rhaiana. VII. Canto, Mariana.

25-296261.0 CDD-005.8

Índices para catálogo sistemático:

1. Stalkerware : Crimes digitais : Ciência da Computação 005.8

Eliane de Freitas Leite - Bibliotecária - CRB 8/8415

FICHA TÉCNICA

REALIZAÇÃO:

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

EQUIPE:

COORDENAÇÃO:

Mariana Canto

AUTORES:

Anicely Santos
Carolina Branco
Luana Batista
Mariana Canto
Raquel Saraiva
Rhaiana Valois

PROJETO GRÁFICO:

Estúdio PUYA!

APOIO:

Programa de Acesso Digital da Embaixada
do Reino Unido no Brasil

COMO CITAR:

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

FICHA TÉCNICA

SUMÁRIO

SUMÁRIO

Sumário Executivo

O projeto de pesquisa Expondo stalker(ware) desenvolvido pelo Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec com apoio do Programa de Acesso Digital da Embaixada do Reino Unido no Brasil busca endereçar a violência de gênero facilitada por tecnologias.

Este relatório é a segunda publicação de uma série de estudos desenvolvidos no âmbito deste projeto e tem como foco a análise da distribuição e funcionamento de aplicativos utilizados para monitoramento em relações interpessoais. O estudo examina o ecossistema de promoção desses aplicativos em lojas de aplicativos, bem como redes sociais no contexto brasileiro. Além disso, a publicação oferece uma análise técnica por amostragem das funcionalidades desses aplicativos e do grau de risco associado ao seu uso abusivo. Ao articular abordagens discursivas e técnicas, o relatório busca evidenciar como narrativas que naturalizam práticas de vigilância se entrelaçam com arquiteturas digitais que favorecem o controle coercitivo e a violência de gênero no Brasil.

A análise das quatro plataformas selecionadas (Google Play, App Store, Reddit e TikTok) revelou um ambiente digital que contribui para a normalização e a disseminação de tecnologias de *stalkerware*. Nas lojas de aplicativos, ferramentas de monitoramento são amplamente disponibilizadas sob o pretexto de proteção familiar. Nas redes sociais, o problema se aprofunda com a emergência de comunidades e conteúdos que não apenas normalizam, mas também ensinam e incentivam o uso desses aplicativos.

A análise técnica revela que os aplicativos apresentam variados níveis de vulnerabilidade e riscos de uso abusivo. Enquanto alguns permitem o monitoramento silencioso sem alertas visíveis, outros possuem mecanismos técnicos que tentam mitigar riscos, mas carecem de canais de denúncia, deixando usuários vulneráveis

sem suporte efetivo.

O uso abusivo de tecnologias de monitoramento interpessoal é facilitado tanto por decisões técnicas quanto por estratégias narrativas que silenciam ou relativizam seus riscos. Este relatório evidencia a urgência de políticas públicas, diretrizes regulatórias e ações de responsabilização das empresas desenvolvedoras e distribuidoras dessas ferramentas. Também ressalta a importância de ampliar o debate público sobre violência de gênero facilitada por tecnologias, considerando suas dimensões éticas, legais e sociais, a fim de proteger os direitos de grupos vulneráveis e construir um ambiente digital mais seguro e inclusivo.

PRINCIPAIS ACHADOS

Normalização da vigilância interpessoal nas plataformas digitais:	Lojas de aplicativos bem como redes sociais promovem direta ou indiretamente o uso de tecnologias de stalkerware.
Ambiguidade discursiva e apelos emocionais como estratégias de marketing:	Muitos aplicativos de uso duplo são apresentados sob o pretexto de "proteção familiar" mas utilizam estratégias de marketing associadas a comportamentos controladores.
Prevalência de dark patterns para ocultar funcionalidades de espionagem:	Diversos aplicativos utilizam padrões de design enganosos para mascarar suas funcionalidades mais intrusivas, como esconder o ícone após a instalação ou exigir passos complexos para desativação.
Níveis variados de maturidade frente à abusabilidade:	Enquanto algumas empresas demonstram esforços técnicos limitados para mitigar abusos, outras operam com total desprezo à segurança da pessoa monitorada.
Ausência de responsabilização institucional:	Empresas transferem a responsabilidade ética e legal para o usuário final, ignorando o impacto direto de suas escolhas de design na perpetuação de práticas abusivas.
Consentimento é tratado de forma superficial ou inexistente:	Quando mencionado, o consentimento é tratado como formalidade única, desconsiderando relações de poder e contextos abusivos.

Definições e terminologias

Stalkerware: refere-se a softwares ou aplicativos usados para monitorar, rastrear ou espionar uma pessoa sem seu conhecimento ou consentimento. Essas ferramentas muitas vezes operam de forma oculta, capturando dados como localização, mensagens, chamadas, registros de tecla e atividades em redes sociais.

Aplicativos de uso duplo: são aplicativos cujo uso pode ser legítimo ou abusivo, a depender do contexto. Exemplos incluem ferramentas de controle parental ou aplicativos de rastreamento de dispositivos. Embora tenham finalidades declaradas aceitáveis, esses aplicativos podem ser facilmente adaptados para monitorar parceiros de forma coercitiva.

Abusabilidade: conceito que descreve o potencial de uma tecnologia ser usada para fins abusivos, mesmo que essa não seja sua finalidade original declarada. Refere-se também à negligência ou à postura permissiva de desenvolvedores frente aos riscos de uso indevido de seus produtos. Avaliar a abusabilidade envolve observar não apenas as funcionalidades técnicas, mas também as políticas institucionais, a comunicação com usuários e o compromisso ético das empresas com a prevenção do abuso.

1. INTRODUÇÃO

1.1. Objetivos da pesquisa e delimitação do escopo

O objetivo central desta pesquisa é investigar como aplicativos com funcionalidades de monitoramento, especialmente aqueles com potencial de uso como *stalkerware* ou aplicativos de uso duplo. O foco está na forma como esses aplicativos são apresentados em plataformas e redes sociais, bem como na análise técnica de seu funcionamento e do grau de risco para uso abusivo. A pesquisa busca compreender tanto **os discursos** que naturalizam o uso dessas ferramentas quanto a **estrutura técnica** que permite, ou mesmo incentiva, sua utilização em contextos de controle coercitivo e violência baseada em gênero no Brasil.

1.2. Metodologia

A pesquisa foi estruturada em duas etapas complementares. A primeira etapa consistiu no mapeamento de aplicativos de uso duplo e *stalkerware* no contexto brasileiro e na análise discursiva e da estratégia de distribuição de aplicativos.

O mapeamento foi realizado a partir de cinco categorias principais de palavras-chave: (1) termos diretamente associados ao *stalkerware*, como "aplicativo espião", "espionar Whatsapp" e "rastrear a localização"; (2) termos relacionados a aplicativos de uso duplo, como "controle parental" e "encontrar celular"; (3) termos emocionalmente motivados, como "rastrear namorado(a)", "rastrear esposo(a)", e "descobrir traição"; (4) termos técnicos, como "registro de teclas (*keylogger*)", "acesso remoto ao dispositivo" e "monitoramento remoto"; e (5) termos em inglês potencialmente utilizados no Brasil, como "*spy app*", "*spyware*" e "*stalkerware*".

A partir desse mapeamento inicial, foi realizada uma análise discursiva de posts, descrições, imagens e demais elementos comunicacionais relacionados aos aplicativos identificados. O objetivo foi compreender de que maneira essas ferramentas são apresentadas aos usuários, quais estratégias narrativas e persuasivas são utilizadas para legitimar seu uso e como aspectos legais e éticos são abordados ou omitidos.

A segunda etapa da pesquisa envolveu uma análise técnica por amostragem dos aplicativos mais relevantes identificados na primeira fase. A seleção considerou critérios como popularidade, recorrência nos resultados e clareza no apelo à vigilância. Cada aplicativo foi instalado e testado em ambiente controlado, com o objetivo de avaliar as exigências de instalação, funcionalidades de monitoramento e o grau de complexidade técnica envolvido em seu uso. Também foi utilizada a Escala de Maturidade de Abusabilidade, desenvolvida por pesquisadores da Universidade de Northumbria[1]. Essa

1 Angelika, Strohmayer, Slupska Julia, Bellini Rosanna, Coventry Lynne, Tara Hairston e Adam Dodge. *Trust and Abusability Toolkit: Centering Safety in Human-Data Interactions*. 2021. https://researchportal.northumbria.ac.uk/en/publications/trust-and-abusability-toolkit-centering-safety-in-human-data-inte.

métrica avalia o grau de risco de uso abusivo dos aplicativos e a postura das empresas desenvolvedoras frente a esse problema, considerando cinco dimensões: facilitação ativa de abusos (aplicativos intencionalmente voltados à espionagem), ignorância intencional (omissão consciente dos riscos), consciência organizacional (reconhecimento das vulnerabilidades do próprio produto), ação concreta (medidas efetivas para mitigar abusos) e engajamento significativo (consulta real e remunerada a sobreviventes e especialistas durante o desenvolvimento). O resumo da análise dos aplicativos pode ser encontrado no Apêndice deste relatório.

2. ANÁLISE DISCURSIVA E ESTRATÉGIAS DE DISTRIBUIÇÃO

2.1. Lojas de Aplicativos

a) Google Play

A partir da análise realizada na loja de aplicativos do Google Play, foi possível identificar diversos aplicativos que podem funcionar como facilitadores de práticas de vigilância abusiva, inclusive no contexto de violência de gênero. Termos técnicos como "monitoramento remoto" e "acesso remoto ao dispositivo", e expressões de uso dual como "controle parental" e "localizar celular" foram os que mais retornaram resultados relevantes. Termos populares como "espionar WhatsApp" e "rastrear a localização" também retornaram resultados relevantes, muitos dos quais disfarçam o nome do WhatsApp possivelmente para escapar de filtros da loja.

Entre os termos emocionalmente motivados, expressões como "rastrear esposo" e "app para vigiar marido" também geraram resultados expressivos, sugerindo que mulheres cisgênero podem ser o principal público-alvo ou usuárias desses aplicativos. Ressalta-se, contudo, que essa constatação não busca equiparar tais práticas à violência perpetrada por parceiros, em sua maioria, homens. Tal registro deve ser compreendido à luz da desigualdade estrutural de gênero, em que as formas mais graves e letais de violência atingem desproporcionalmente as mulheres, que seguem como as principais vítimas.

Na etapa de refinamento dos dados, alguns aplicativos se destacaram por sua recorrência nas buscas e alto número de avaliações e downloads, tais como: *Vincular ao Windows, Localizador do Google, TeamViewer Remote Control, Life360, Google Family Link, Find My Kids, AirDroid Parental Control, iSharing, Dual App e Rastreador de Número Celular*.

Esses aplicativos recorrem a narrativas emocionais e funcionais que associam vigilância à segurança e proteção. Em geral, quando não utilizam retóricas como "proteção de filhos" e "segurança da família" para naturalizar a vigilância constante e dinâmicas familiares disfuncionais (*iSharing, Life360, AirDroid Parental Control, Localizador do Google, Rastreador de número celular e Find My Device Kids), são apresentados como ferramentas de produtividade ou suporte técnico (Vincular ao Windows, TeamViewer e Dual App*).

Suas estratégias de marketing combinam linguagem e visual amigáveis, que retratam predominantemente pessoas brancas, para normalizar práticas de vigilância, sobretudo em contextos familiares e afetivos. Além disso, frequentemente, associam o controle excessivo a um ideal de proteção, silenciando os riscos à privacidade, ao consentimento e à autonomia.

Alguns aplicativos, como o *Dual App*, direcionam explicitamente seu apelo ao

público feminino e à suspeita de infidelidade. O material visual desse aplicativo, com uma mulher branca fazendo sinal de silêncio e mensagens sugerindo um relacionamento extraconjugal do seu parceiro, reforça o caráter oculto da vigilância e apelativo.

Do ponto de vista legal e ético, a maioria dos aplicativos analisados não esclarece, na página inicial da Play Store, como os dados são tratados ou como o consentimento é obtido. Embora essas informações constem, em tese, em suas políticas de privacidade, o baixo índice de leitura e natureza sensível dos dados coletados reforça a necessidade de alertas mais visíveis.

b) App Store

No caso da App Store, a análise dos resultados obtidos a partir dos termos selecionados revelou que a maior presença de resultados de busca relevantes estão concentrados nas categorias de termos relacionados a *stalkerware* e termos relacionados a uso duplo. A partir da catalogação dos resultados, observou-se que o aplicativo *Life360* lidera em volume de avaliações, seguido por *Google Family Link, Findo, Findup e Find My Kids*. Além da quantidade de avaliações, a variedade de termos de pesquisa associados a cada aplicativo revelou-se um fator relevante na determinação de sua visibilidade e potencial de uso duplo. Aplicativos como *iSharing, Life360 e Find My Kids*, por exemplo, aparecem indexados sob um amplo leque de termos, incluindo desde expressões relacionadas ao controle parental até aquelas com conotação de vigilância íntima, o que indica uma estratégia de ASO (*App Store Optimization*)[2] voltada a múltiplas intenções de busca. Além disso, embora aplicativos como *Google Maps* e *Google Family Link* não estejam entre aqueles com maior número de termos de pesquisa associados, sua ampla base de usuários, destaca essas ferramentas como fortes candidatas a uso duplo.

Destaca-se ainda o caso de aplicativos como *Dual messenger* + e *Whats Web - Watsapp Web*, oficialmente descritos como ferramentas para a gestão de múltiplas contas, mas que aparecem de forma recorrente em buscas por termos como "aplicativo espião" e "espionar Whatsapp". Esse padrão revela uma estratégia de marketing deliberadamente utilizada para encobrir usos abusivos reconhecidos tanto pelos usuários quanto pelos desenvolvedores.

A narrativa construída em torno desses aplicativos, assim como os da Google

2 Prática estratégica de aprimorar a visibilidade e o posicionamento de aplicativos móveis nas plataformas de distribuição digital, como App Store e Google Play, por meio da otimização de elementos como título, descrição e palavras-chave.

Play, baseia-se fortemente na ideia de segurança familiar ou de entes queridos, proteção de crianças e responsabilidade parental. O discurso predominante é o de que o rastreamento contínuo é um mecanismo de cuidado. De modo geral, os aplicativos analisados oferecem recursos como localização em tempo real, histórico de localização, notificações de chegada e saída de locais, envio de mensagens de emergência e, no caso de aplicativos de controle parental, até escuta remota do ambiente e monitoramento dos aplicativos utilizados. Essas funcionalidades são frequentemente acompanhadas de slogans publicitários como "veja onde seus familiares estão" e "proteja quem você ama", articulados dentro de uma moldura afetiva e protetiva. Essa lógica discursiva tende a naturalizar e legitimar o controle digital, ao mesmo tempo em que esvazia sua dimensão política, relacional e ética. A vigilância constante, nesses termos, é convertida em um gesto de cuidado, obscurecendo os riscos e as assimetrias de poder implicadas em seu uso cotidiano.

Tais estratégias são sustentadas por um tom comunicacional majoritariamente institucional, que combina uma linguagem profissional com apelo emocional. A comunicação empregada evita termos que remetem diretamente ao conflito, à autoridade ou à violação de privacidade, preferindo eufemismos como "localizar entes queridos". Mesmo aplicativos que oferecem funcionalidades invasivas, como escuta remota, optam por uma estética visual neutra e profissional e uma apresentação gráfica que reforça clareza e confiabilidade, projetando uma ideia de legitimidade. Comentários de usuários, entretanto, revelam percepções conflitantes: relatos de filhos e filhas que criticam o uso do *Google Family Link* por pais controladores, bem como de cônjuges que se queixam da perda de autonomia provocada por ferramentas como o *Life360*, demonstram que as tensões entre vigilância e privacidade não são invisíveis à experiência dos usuários.

A maioria dos aplicativos fornece apenas menções superficiais às políticas de privacidade, geralmente apresentadas em forma de links genéricos ao final da descrição, sem qualquer detalhamento sobre a forma como os dados são coletados, utilizados ou compartilhados. Entre os onze aplicativos com maior número de avaliações, apenas dois mencionam de forma explícita a necessidade de consentimento informado da pessoa monitorada.

Outro aspecto central diz respeito ao apagamento de experiências dissidentes. Os aplicativos analisados, tanto em suas imagens quanto em seus textos promocionais, apresentam uma homogeneidade racial, de classe e de orientação sexual, a representação predominante é de famílias brancas e heterossexuais. Essa construção evidencia não apenas um recorte específico de público-alvo, mas também uma negligência em relação aos impactos da vigilância digital sobre grupos historicamente marginalizados. Práticas de monitoramento que são naturalizadas nesses contextos podem adquirir

contornos especialmente opressivos quando direcionadas, por exemplo, a mulheres negras em relacionamentos abusivos, que enfrentam camadas adicionais de controle e invisibilização. Nesses casos, o uso de tecnologias de vigilância pode intensificar dinâmicas de poder já marcadas por assimetrias estruturais.

Por fim, cabe destacar a responsabilidade das plataformas digitais na manutenção desse cenário. A Google Play e a App Store, embora aparentemente implementem filtros que limitam parcialmente os resultados para determinados termos de pesquisa, continuam permitindo que aplicativos com alto potencial de uso abusivo sejam amplamente indexados e promovidos. A ausência de mecanismos eficazes de auditoria, moderação ou responsabilização por parte das plataformas contribui para a legitimação silenciosa dessas práticas, naturalizando o uso da vigilância digital em relações interpessoais sem a devida regulação.

2.2. Reddit

No caso do Reddit, fórum online onde os usuários criam, partilham e votam em conteúdos sobre uma gama de tópicos, discussões acerca do uso de aplicativos espiões e ferramentas de rastreamento em relacionamentos íntimos revela um cenário preocupante. O discurso é marcado por desequilíbrios de poder, abusos emocionais e invasões de privacidade. Ao se observar narrativas na plataforma, constata-se que termos como "rastrear namorada(o)" ou "espiar celular do marido/ esposa" são recorrentes. Em relação aos indivíduos relacionados com essas postagens é possível identificar três tipos predominantes de autorias: vítimas, perpetradores e facilitadores. Cada uma dessas categorias fornece uma perspectiva distinta sobre o uso dessas tecnologias, mas todas evidenciam uma naturalização crescente do uso de *stalkerware*.

No caso das vítimas, os relatos são marcados por pedidos de ajuda e sentimentos de desconfiança e ciúmes por parte do parceiro ou ex-parceiro (e até genitor) como gatilhos para a vigilância. Em muitos casos, o parceiro inicia o monitoramento sem qualquer evidência concreta de traição, guiado apenas por suposições e inseguranças. Ferramentas como *mSpy, iSpy, Life360* ou até mesmo o rastreamento via *Google Maps* são utilizadas sem consentimento, possibilitando um monitoramento constante. Há um profundo desequilíbrio de poder. Muitas vezes, as vítimas possuem sua autonomia digital obstruída, sendo submetidas a situações de abuso psicológico e medo. Além disso, a dificuldade técnica em identificar e remover esses softwares reforça a sensação de impotência, ampliando ainda mais o sofrimento.

Já no caso dos perpetradores, o discurso gira em torno da normalização da vigilância como uma resposta "natural" à suspeita. Pequenos sinais - como sorrisos durante conversas sobre terceiros ou o simples uso mais frequente do celular - são

suficientes para justificar o uso de tecnologias invasivas. Os ciúmes e a ansiedade são convertidos em ações técnicas, como a instalação de *keyloggers*, aplicativos espiões ou escutas ocultas. Em vez de refletirem sobre os próprios sentimentos ou buscarem o diálogo com o parceiro, esses indivíduos optam por práticas ilegais. Muitos ainda compartilham essas experiências com orgulho, apresentando-se como "experts" no assunto, recomendando estratégias e aplicativos com um tom de autoridade informal. O comportamento abusivo é, assim, reforçado por uma comunidade que valida a espionagem como se fosse um ato de astúcia ou sobrevivência emocional.

Os facilitadores, por sua vez, não necessariamente admitem praticar a vigilância, mas detalham com precisão como ela pode ser realizada. Os discursos frequentemente combinam frieza estratégica com um cinismo moral que relativiza a ilegalidade e os danos éticos envolvidos. Eles fornecem instruções passo a passo sobre como instalar *spyware*, apagar rastros ou enganar a pessoa monitorada, descrevendo esses atos como parte de um jogo de inteligência emocional. Embora ocasionalmente reconheçam que tais ações possam ser ilegais, continuam a apresentá-las como alternativas viáveis. Além disso, esses facilitadores frequentemente aconselham sobre como manipular emocionalmente a vítima para facilitar o acesso à informação desejada, o que amplia ainda mais os danos psicológicos causados.

Um aspecto recorrente nas falas dos perpetradores e facilitadores é a ideia de que "o fim justifica os meios". A mera suspeita de traição é usada como argumento suficiente para invadir a privacidade do outro. Há uma desumanização clara da pessoa vigiada, que passa a ser tratada como um objeto a ser manipulado, monitorado e testado, não como um sujeito com direitos. A eficácia da ferramenta se sobrepõe a qualquer questionamento moral. Comentários como "espie o celular dela, e se não encontrar nada, instale um *keylogger*" mostram a disposição para ampliar o controle mesmo diante da ausência de provas. A linguagem utilizada é técnica, fria e funcional.

Muitos dos comentários e relatos funcionam como verdadeiras demonstrações de produto, exaltando as funcionalidades das ferramentas. Esse tipo de discurso promove a mercantilização da vigilância íntima. Além disso, há uma forte presença de validação social: ao se posicionarem como especialistas, esses indivíduos fortalecem a percepção de que a vigilância é comum, legítima e até recomendada, criando uma rede informal de apoio entre perpetradores. Do ponto de vista emocional, os perpetradores demonstram uma combinação de sentimentos preocupantes: desconfiança crônica, ansiedade intensa, desejo de controle absoluto e, muitas vezes, um subtexto de ódio, misoginia ou necessidade de punição.

Apesar de algumas menções ocasionais sobre a ilegalidade dessas práticas, a questão ética é amplamente ignorada. Raramente os autores demonstram preocupação com o consentimento ou os direitos da outra pessoa. Em contrapartida, algumas vozes

dissonantes questionam a eficácia da vigilância. Também apontam para os danos emocionais causados por essa prática e sugerem, como solução mais sensata, o fim do relacionamento ao invés da persistência na tentativa de controle.

Além das dinâmicas interpessoais reveladas nesses relatos, é necessário também refletir sobre a responsabilidade da plataforma onde essas narrativas circulam. Ao permitir a circulação livre de conteúdos que ensinam, normalizam ou até promovem o uso de ferramentas de espionagem íntima, o Reddit se torna, ainda que indiretamente, cúmplice na perpetuação de práticas abusivas. Embora o Reddit possua políticas contra comportamentos prejudiciais e a violação da privacidade, a persistência de fóruns e comentários que detalham métodos ilegais de vigilância sugere uma falha na moderação eficaz desses espaços.

2.3. TikTok

No TikTok, o acesso aos conteúdos relacionados a aplicativos de monitoramento foi constatado a partir da busca direta por termos como “aplicativo espião”, “clonar WhatsApp”, “rastrear namorado” e sugestões algorítmicas baseadas em engajamento. Criadores usam frases chamativas como “esse app devia ser proibido” ou perguntas como “como saber onde ele está agora?” para capturar atenção e favorecer a viralização.

O rastreamento é apresentado como cuidado legítimo. Em contextos parentais, os aplicativos são tratados como ferramentas de proteção. Em relações afetivas, são associados à manutenção do vínculo e à preocupação com o bem-estar, especialmente em situações cotidianas de ausência ou deslocamento.

A suspeita de infidelidade motiva o uso de *stalkerwares* por criadores de conteúdo. O conteúdo promete acesso a conversas, localização e arquivos apagados, reforçando que o domínio técnico oferece “verdade” e controle, mesmo sem consentimento. A legalidade raramente é discutida. Termos como “modo psicopata” ou “brincadeira” indicam consciência parcial da gravidade das práticas, mas funcionam como atenuantes que viabilizam sua continuidade. O humor opera como dispositivo de aceitação, e a crítica superficial, quando presente, atua mais como escudo retórico do que como resistência.

Os vídeos assumem o formato de passo a passo instrucional, com visual chamativo e linguagem acessível. Os criadores ocupam o lugar de especialistas informais e transformam o saber técnico em ferramenta de autoridade, normalizando práticas invasivas sob o verniz da competência. A dor causada por ciúmes, abandono ou experiências anteriores é mobilizada como justificativa.

A vulnerabilidade de quem sofre é instrumentalizada por perfis que se apresentam como “técnicos” ou “detetives digitais”, oferecendo serviços pagos e prometendo acesso irrestrito ao dispositivo de terceiros. Nos comentários, há uma promoção disfarçada de interação espontânea: usuárias recomendam técnicos por nome, sempre com elogios e

emojis, criando um ambiente de confiança e familiaridade. Há inclusive indícios de atuação de bots, com padrões replicados e linguagem artificial, que ampliam o alcance das ofertas.

As estratégias de marketing nos vídeos envolvem uso de frases sensacionalistas, promessas de gratuidade, dramatização e apelo ao segredo revelado ("ninguém quer que você saiba disso"). O uso de nanoinfluenciadoras[3] é comum: criadoras com poucos seguidores, linguagem íntima e perfil "gente como a gente" compartilham tutoriais como se fossem conselhos pessoais. Esse formato facilita a viralização e reduz a percepção de risco.

Essa rede de comercialização ilegal se apoia no próprio funcionamento da plataforma. O TikTok não apenas falha em moderar vídeos que ensinam práticas ilícitas, como invasão de privacidade, violação da LGPD e uso de *spyware*, como também os impulsiona por meio de sua lógica algorítmica baseada em engajamento. Conteúdos com milhares de interações seguem ativos por semanas. Mesmo vídeos que ensinam abertamente a espelhar o WhatsApp ou instalar localizadores não são sinalizados.

O enquadramento ético e legal é praticamente ausente. Criadores evitam menções à ilegalidade, e quando o fazem, suavizam o impacto com justificativas emocionais ("só faço porque ele me traiu", "uso com meu filho para protegê-lo"). Comentários críticos aparecem pontualmente, denunciando golpes ou alertando para o caráter criminoso, mas são minoritários frente ao discurso hegemônico de normalização.

A interseccionalidade está ausente nos conteúdos analisados. Os vídeos são protagonizados por mulheres e homens brancos e voltados a um público branco, heteronormativo e de classe média. Não há representação de corpos racializados, pessoas LGBTQIA+ ou experiências periféricas, tampouco tematização das vulnerabilidades específicas desses grupos frente ao monitoramento. A vigilância é retratada como prática segura, legítima e universal, apagando os efeitos desiguais que ela pode gerar em contextos marcados por violência estrutural.

A análise de vídeos e comentários no TikTok sobre o uso de *stalkerware* revela um ecossistema digital em que a vigilância íntima é naturalizada, convertida em conteúdo de entretenimento e rentabilizada. A ausência de moderação efetiva, somada a estratégias de marketing disfarçadas de espontaneidade, sustenta um mercado informal altamente ativo, promovido por uma ecologia de discursos que minimiza os riscos legais, apaga marcadores sociais e estimula a vigilância como prática desejável.

---

3 Criadoras de conteúdo digital que possuem entre 1.000 e 10.000 seguidores em redes sociais. Apesar de terem um público relativamente pequeno em comparação com influenciadoras maiores, elas geralmente mantêm um alto nível de engajamento com seus seguidores.

3. ANÁLISE TÉCNICA POR AMOSTRAGEM

3.1. Life360: Rastreador de Celular

a) Instalação, Permissões e Funcionamento

O aplicativo *Life360* é desenvolvido pela empresa de mesmo nome, sediada nos Estados Unidos. A empresa oferece serviços baseados em geolocalização e lançou sua primeira versão do aplicativo após a catástrofe causada pelo furacão Katrina. A versão analisada neste relatório é a 25.28.0, disponibilizada gratuitamente.

A instalação segue o procedimento comum, sendo realizada através da loja de aplicativos. O processo de instalação é padrão, acompanhado de uma tela explicativa intuitiva. Após a instalação, o ícone do aplicativo torna-se visível.

No primeiro acesso, durante a etapa de configuração inicial, são solicitados dados pessoais do usuário, como número de telefone, email e data de nascimento. A coleta da data de nascimento visa atender às regulações sobre acesso de menores de idade a aplicativos, havendo mecanismos automáticos de bloqueio caso o usuário informe uma idade inferior a 13 anos.

As permissões solicitadas para o funcionamento do aplicativo incluem: Atividade física (para indicar deslocamento), Localização (para ativar o mapa e compartilhar localização), Notificações (para indicar *check-ins* e alertas), Câmera, Contatos, Dispositivo por perto, Microfone e Telefone. Além disso, o aplicativo recomenda que a permissão de Localização seja definida na opção "Sempre permitir" para obter melhor precisão.

Quanto ao tratamento de dados, os desenvolvedores coletam informações sobre identificadores de dispositivos, atividades realizadas no aplicativo, fotos e vídeos, dados de desempenho, informações pessoais, contatos e mensagens. Os dados podem ser compartilhados com outras empresas ou organizações dados sobre saúde/fitness e localização, mas não explicita quem são essas empresas e organizações e de quais maneiras elas utilizam essas informações.

Sobre o funcionamento, o aplicativo permite o monitoramento de outros dispositivos de forma relativamente simples, exigindo apenas a inserção de um código no dispositivo alvo. Esse procedimento viabiliza a inclusão rápida de novos dispositivos, desde que haja acesso físico a eles. O processo de desinstalação também é simples e pode ser executado tanto pela loja de aplicativos quanto diretamente nas configurações do sistema operacional do dispositivo.

b) Abusabilidade

Apesar de não permitir o ocultamento como fazem os *stalkerware* típicos, não há qualquer evidência de que o *Life360* adote medidas ativas e estruturais para prevenir ou coibir abusos cometidos por seus usuários. Ao contrário, a análise dos termos de uso, da política de privacidade e de publicações no blog oficial da empresa sugere uma abordagem superficial e performativa diante do problema.

A sinalização de uma suposta preocupação ética aparece sem lastro em mecanismos concretos de proteção, o que sugere um caso de lavagem ética, quando valores éticos são proclamados, mas não sustentados por ações técnicas ou institucionais.

Um exemplo disso aparece no artigo *Can You Track Someone on Life360 Without Them Knowing?* [4], em que o aplicativo afirma que o aceite de um convite para participar de um "Círculo" equivale a um consentimento informado e contínuo. Embora se mencione que o iOS envia notificações sobre o compartilhamento de localização, não há qualquer referência a alertas no Android que informem de forma recorrente ao usuário que está sendo rastreado.

Embora o aplicativo exija instalação no dispositivo da pessoa rastreada, nada impede que essa instalação seja feita por terceiros com acesso físico ao celular, o que é especialmente preocupante em contextos de violência doméstica. Um agressor pode facilmente instalar o *Life360* no dispositivo da vítima, criar uma conta em nome dela e ativar o rastreamento com todas as permissões necessárias.

Além disso, usuários com baixo domínio técnico podem sequer perceber que continuam com o rastreamento ativo, especialmente se não acessarem regularmente as configurações do aplicativo. Em contextos de relações abusivas, como em dinâmicas entre parceiros controladores ou pais coercitivos, esse consentimento também pode ser obtido sob coação, medo ou manipulação emocional. O aplicativo não diferencia consentimento livre de consentimento forçado, tampouco parece demonstrar mecanismos para detectar padrões de uso abusivo.

Não foram identificadas, nos documentos analisados, funcionalidades desenhadas especificamente para prevenir, mitigar ou denunciar o uso abusivo do aplicativo. Além disso, não há qualquer indicação pública de que a empresa mantenha diálogo com sobreviventes de violência, especialistas em trauma, pesquisadores de privacidade ou grupos de apoio, seja durante o desenvolvimento do produto, seja em seu monitoramento posterior. Não há menção a testes de abusabilidade, modelagem de ameaças com foco em violência interpessoal, nem à incorporação de feedback especializado em abusos no design do

---

4 "Can You Track Someone on Life360 Without Them Knowing?" Life360. Acesso em 9 de agosto de 2025. https://intl.life360.com/learn/can-life360-track-you-without-you-knowing.

aplicativo.

A ausência de atenção sistemática a potenciais impactos desproporcionais sobre mulheres, pessoas LGBTQIA + ou vítimas de violência doméstica também chama atenção, com exceção de referências a crianças, mencionadas na política de privacidade e nos termos de uso.

Ao listar uma série de "usos proibidos" em seus termos de uso, mas sem apresentar ferramentas técnicas eficazes ou mecanismos auditáveis de prevenção, o *Life360* parece transferir integralmente a responsabilidade pelo uso ético aos usuários, mesmo diante de um conjunto de funcionalidades que, sem salvaguardas adequadas, pode ser facilmente utilizado para fins abusivos. O fato de o aplicativo não ser oculto, nem utilizar técnicas de persistência, apenas o distancia da definição técnica clássica de um *stalkerware*, mas não o exime da responsabilidade por facilitar dinâmicas de vigilância coercitiva.

A ausência de barreiras técnicas mínimas abre brechas incompatíveis com qualquer compromisso ético robusto e verificável. Diante disso, à luz da escala adotada da Escala de Maturidade de Abusabilidade, o *Life360* poderia ser classificado no nível -1 (Ignorância Intencional), categoria em que a inação diante de riscos previsíveis se apresenta como uma escolha consciente.

3.2. Google Maps

a) Instalação, Permissões e Funcionamento

O *Google Maps* é desenvolvido pela empresa Google LLC, subsidiária controlada pela empresa Alphabet Inc. Lançado em 2005, o aplicativo atua como um serviço gratuito de pesquisa e visualização de mapas, incluindo imagens de satélite e outros recursos de navegação. Neste estudo analisamos a versão 25.30.03.785163646.

Por integrar a suíte de aplicativos do Google, o *Google Maps* já vem pré-instalado na maioria dos dispositivos Android. Essa prática está inserida no contexto do chamado *bloatware*, que consiste na instalação prévia de aplicativos pelo fabricante sem solicitação do usuário, muitas vezes impossibilitando sua remoção por métodos convencionais.

Dentre as muitas funcionalidades do aplicativo, destaca-se o compartilhamento de localização, que possibilita visualizar em tempo real a posição de um usuário, bem como o acesso ao histórico de deslocamentos, como está viajando (dirigindo ou andando) e informações do dispositivo. O aplicativo permite ainda habilitar notificações sobre chegadas e saídas de locais específicos.

Para que o compartilhamento de localização funcione, é necessário que as notificações estejam ativadas e a localização habilitada. Adicionalmente, o aplicativo solicita permissões opcionais para acesso à câmera, contatos, dispositivos por perto, fotos e vídeos e microfone.

No compartilhamento de localização entre contas Google, é necessário que o usuário esteja conectado à sua conta, tenha adicionado o destinatário aos seus contatos e defina o período de tempo em que deseja compartilhar sua localização (de algumas horas até a opção "até ser desativado"). Já o compartilhamento via link é destinado a pessoas que não possuem uma conta Google. Nesse caso, o link gerado permite acesso à localização em tempo real por até 24 horas e pode ser enviado por e-mail, mensagem ou outros meios.

Apesar de notificações mensais, caso o compartilhamento ocorra entre contas Google por tempo indeterminado, ao utilizar o recurso de compartilhamento via link, não é possível identificar se a localização está sendo monitorada por terceiros. Isso cria uma vulnerabilidade, pois não há uma indicação clara e constante de que a localização está sendo compartilhada com outras pessoas nem quem são estas pessoas.

No âmbito dos dados coletados, observa-se que a lista de informações captadas é extensa, incluindo áudio, arquivos e documentos, recursos que são desnecessários para o cumprimento da função principal do aplicativo.

b) Abusabilidade

O *Google Maps* é amplamente utilizado como ferramenta de navegação e localização, mas sua funcionalidade de compartilhamento em tempo real com links anônimos apresenta riscos significativos de abusabilidade. O recurso permite que a localização de uma pessoa seja compartilhada por até 24 horas por meio de um link acessível mesmo a quem não possui conta Google, sem autenticação. Essa facilidade pode ser explorada por agressores, especialmente em contextos de relacionamentos abusivos ou controle coercitivo, quando o link é ativado sem o conhecimento ou consentimento informado da vítima, por exemplo.

Durante a análise, observou-se que a ativação do compartilhamento pode ocorrer de forma silenciosa, e, embora notificações mensais aconteçam no caso do compartilhamento por tempo indeterminado entre contas Google, não há alertas ativos no caso de compartilhamentos que ocorrem por links por 24h. A transparência sobre quem tem acesso à localização é limitada, especialmente se o link for copiado ou reenviado, o que reduz o controle da pessoa afetada sobre o próprio rastreamento.

Apesar de existirem funcionalidades básicas entre compartilhamento de contas Google como interrupção do compartilhamento, bloqueio de contatos e ocultação da própria localização, esses recursos atuam de forma reativa e dependem da ação consciente da vítima. Não há orientações para contextos de violência doméstica, nem mecanismos proativos de alerta, denúncia ou proteção para usuários em risco.

Com base na Escala de Maturidade de Abusabilidade, o aplicativo Google Maps se

enquadra no nível 0, já que há uma consciência organizacional limitada. O aplicativo oferece mecanismos de notificação e interrupção no caso do compartilhamento entre contas Google. Entretanto, o design da funcionalidade de compartilhamento via links permite exploração silenciosa por agressores. Também não foi possível identificar por meio de documentos públicos disponíveis a consulta a especialistas em abuso tecnológico ou sobreviventes no desenvolvimento do aplicativo. Isso reforça um ciclo de design que negligencia impactos sociais graves.

3.3. AirDroid Parental Control

a) Instalação, Permissões e Funcionamento

O *AirDroid Parental Control* é desenvolvido pela AirDroid Sand Studio, empresa que está no mercado desde 2011 e especializada em soluções de Gerenciamento de Dispositivos Móveis[5]. Nesta análise, foi investigada a versão 2.5.0.0, disponibilizada gratuitamente.

De acordo com a desenvolvedora, o *AirDroid Parental Control* tem como objetivo garantir a segurança e proteção de crianças, possibilitando o monitoramento, em tempo real, de seus dispositivos móveis. Entre as funcionalidades associadas, destacam-se o controle remoto da câmera, espelhamento da tela e o acesso ao microfone, este último permitindo a captação do som ambiente.

No caso do Android, o dispositivo-alvo requer a instalação de um aplicativo disponível na Google Play, obtido exclusivamente no site oficial da desenvolvedora no formato APK. Essa instalação demanda acesso físico ao dispositivo e é indispensável para habilitar funções avançadas de monitoramento. Já no iOS, tanto o aplicativo do dispositivo de controle quanto o do dispositivo-alvo estão disponíveis na App Store, sendo este último identificado como *AirDroid Kids - Screen Time*. Essa distribuição restrita se deve ao fato de que o sistema operacional da Apple permite a instalação de aplicativos apenas pela loja oficial, impedindo o uso de fontes externas sem procedimentos adicionais, como o *jailbreak*[6].

No processo de instalação via APK no Android, o arquivo funciona como um instalador intermediário[7], responsável por permitir a instalação da aplicação principal.

---

5 Do inglês Mobile Device Management, tecnologia usada para monitorar, controlar e proteger dispositivos móveis (como celulares, tablets e laptops) usados por funcionários ou usuários.

6 Processo de remover as restrições impostas pelo sistema operacional iOS da Apple com o objetivo de obter acesso irrestrito ao sistema, incluindo permissões root que normalmente não são concedidas ao usuário.

7 Também conhecido como Dropper, quando o objetivo do app instalador é driblar defesas para instalar o app principal.

Durante esse processo, o instalador solicita ser reconhecido como um aplicativo seguro pelo usuário, burlando proteções padrão do dispositivo. Após essa validação, o aplicativo principal é baixado e instalado normalmente. Por padrão, este não é exibido na gaveta de aplicativos, embora seja possível torná-lo visível manualmente. Ambas as instalações, tanto no dispositivo de controle quanto no dispositivo-alvo, ocorrem de forma convencional, sem necessidade de acesso root.

Nem todos os recursos de monitoramento estão disponíveis para iOS devido às restrições do sistema operacional, não sendo possível, por exemplo, ouvir o áudio ambiente ao redor do aparelho.

Além disso, o aplicativo adota práticas que podem ser enquadrados como padrões obscuros de design, combinando *Obfuscation* [8] e *Forced Continuity* [9]. Isso se manifesta quando o aplicativo, após ser instalado, não aparece na gaveta de aplicativos e permanece ativo em segundo plano, sem o conhecimento, consentimento ou controle do usuário monitorado.

O processo de desinstalação no dispositivo-alvo deve ser realizado manualmente e requer a senha de administrador definida no dispositivo de controle.

b) Abusabilidade

O *AirDroid*, conforme mencionado, possibilita o ocultamento total do aplicativo. Em cenários de abuso, isso significa que um agressor pode, com acesso físico ao celular da vítima, realizar a instalação do aplicativo silenciosamente. O aplicativo pode operar em modo visível ou oculto. Essas características o tornam compatível com práticas de vigilância não consentida.

Ao analisar a política e os termos de uso da empresa, observa-se a invocação frequente de uma suposta "neutralidade do *software*". A responsabilidade pelo uso ético é inteiramente transferida ao usuário, enquanto a empresa se resguarda sob cláusulas genéricas que proíbem atividades ilegais e eximem-se de responsabilidade por quaisquer danos decorrentes de uso indevido. Em uma das cláusulas, a empresa afirma que, "devido à neutralidade inerente do *software* e da tecnologia", não consegue prever os propósitos e expectativas dos usuários, e que o uso de equipamentos de terceiros só seria permitido mediante "permissão e autorização explícitas", uma formalidade ineficaz

8 Quando o aplicativo esconde funcionalidades, informações ou acessos importantes do usuário de forma deliberada, mesmo que tecnicamente estejam presentes no sistema.

9 Se o app permanece ativo e funcionando (rastreando, gravando ou acessando dados) mesmo sem ícone ou acesso visível, mantendo uma continuidade forçada de operação sem controle do usuário.

em contextos de abuso, em que o consentimento raramente é livre ou informado.

A empresa ainda afirma comunicar os padrões de confidencialidade e segurança aos seus funcionários e monitorar rigorosamente sua implementação. No entanto, tais declarações parecem limitadas a garantir a integridade da infraestrutura de dados da empresa, sem repercussão prática sobre a proteção das pessoas monitoradas, especialmente quando o próprio design técnico do serviço permite que usuários instalem e ocultem o aplicativo em dispositivos alheios.

Embora o *AirDroid* mencione, pontualmente, riscos legais associados à vigilância e gravações não autorizadas, como na advertência de que tais práticas podem configurar crimes, não há qualquer iniciativa visível de enfrentamento efetivo do problema. A empresa se limita a avisos legais, sem demonstrar preocupação em identificar ou prevenir formas de uso abusivo, como o monitoramento coercitivo disfarçado de "controle parental", vigilância de ex-parceiros ou imposições em contextos de vulnerabilidade.

Não há qualquer reconhecimento público de que seu design técnico possa facilitar, direta ou indiretamente, o controle coercitivo ou excessivo. Recursos como escuta ambiental, gravação de tela, acesso remoto à câmera e monitoramento de localização, por exemplo, são tratados como neutros, sem qualquer contextualização sobre os riscos quando usados contra pessoas sem seu consentimento livre e informado. Controle e vigilância excessiva são tratadas como sinônimos de proteção, especialmente em contextos familiares.

Além disso, não se identificam reflexões da empresa sobre quais grupos sociais podem ser mais afetados por tais práticas, como adolescentes LGBTQIA+ vigiados por familiares, mães solos que têm seus dispositivos comprometidos por ex-parceiros ou sobreviventes de violência doméstica. Também não há evidências de que a empresa realize consultas públicas, estudos sobre impactos sociais ou diálogos com especialistas, pesquisadores e organizações da sociedade civil.

Do ponto de vista técnico e institucional, faltam políticas voltadas à análise de abusabilidade ou modelagem de ameaças com foco em controle coercitivo. Não foram encontradas barreiras técnicas capazes de impedir o uso indevido do serviço.

Diante de tais elementos, o *AirDroid* não apenas ignora os riscos inerentes ao seu modelo de funcionamento, como viabiliza ativamente cenários de abuso. Por essa razão, considerando a escala adotada nesta análise, poderia ser classificado no nível -2 (Facilita Ativamente o Abuso) da Escala de Maturidade de Abusabilidade.

3.4. Find My Kids: GPS rastreador

a) Instalação, Permissões e Funcionamento

O aplicativo *Find My Kids* é desenvolvido pela empresa LETEM LTD, situada na República do Chipre. O aplicativo declara ter como principal objetivo ser um localizador familiar, oferecendo recursos para garantir segurança e tranquilidade para toda a família[10]. Nesta análise, foi examinada a versão 2.9.41.

A instalação do aplicativo ocorre por meio da loja de aplicativos. O *software* destinado ao dispositivo-alvo também é obtido dessa forma, porém apresenta um nome distinto: *Pingo*. Ambos, após a instalação, exibem ícones visíveis, o que tem sido alvo de críticas por parte de usuários controladores (pais, responsáveis ou administradores)[11], pois a visibilidade permite que o usuário monitorado perceba o aplicativo e, consequentemente, desative funcionalidades ou o desinstale.

Quanto às funcionalidades, é possível desativar diversos recursos de monitoramento diretamente no aplicativo *Pingo*, o que oferece ao usuário monitorado certo grau de controle e consentimento — ainda que mínimo.

Ambos os aplicativos coletam os mesmos tipos de dados, como informações pessoais, localização e atividade no aplicativo. A principal diferença está na coleta de dados financeiros realizada pelo aplicativo *Find My Kids*, uma vez que este oferece funcionalidades pagas.

Quanto ao processo de desinstalação, ele segue o procedimento padrão do sistema operacional, podendo ser efetuado tanto pela loja de aplicativos quanto diretamente nas configurações do aparelho.

b) Abusabilidade

A análise do *Find My Kids* não conseguiu identificar nenhuma medida para dificultar a detecção ou a remoção do aplicativo do dispositivo. Entretanto, as funcionalidades disponibilizadas por ele podem facilmente ser utilizadas em contextos de relacionamentos tóxicos e abusivos.

O aplicativo é descrito nos canais oficiais como "aplicativo de celular desenvolvido para pais cuidadosos", propagando a ideia de que vigilância é sinônimo de cuidado, em especial com as crianças e adolescentes. Ocorre que a propagação dessa ideia pode

10 Informações extraídas da página do aplicativo na Play Store.

11 Comentários presentes nas avaliações do aplicativo nas lojas e em vídeos tutoriais na internet.

levar ao uso disfuncional das ferramentas. Ou seja, num cenário de abuso, o agressor pode baixar o aplicativo no celular da vítima e obrigá-la a compartilhar sua localização de forma ininterrupta. Mesmo com a possibilidade de detecção e remoção do aplicativo, a vítima pode se sentir coagida a mantê-lo em operação no dispositivo, pois a interrupção do compartilhamento ou qualquer outra medida neste sentido pode escalar ainda mais a violência dentro do relacionamento.

Analisando os termos de uso, verifica-se a proibição do uso da ferramenta para exploração e abuso sexual infantil, mas o documento silencia sobre o uso para monitoramento de outras pessoas que não crianças, o que pode configurar ingorância intencional da empresa sobre essa possibilidade, pois não há qualquer tipo de barreira técnica nem sequer um aviso ou proibição sobre esse tipo de uso.

Além disso, não há qualquer evidência de manifestações públicas da empresa sobre abusos cometidos por pessoas em uso do aplicativo, tampouco menção a riscos para mulheres, população LGBTQIAP+ ou outras categorias sociais em vulnerabilidade.

Também não foram encontradas evidências de medidas de mitigação da possibilidade de abusos, como por exemplo o bloqueio de agressores. No mesmo sentido, não há registro de engajamento da empresa em ações de abordagem de abusos ou a incorporação de relatos de sobreviventes e defensores no design do produto. Com base na Escala de Maturidade de Abusabilidade, o aplicativo poderia ser classificado no nível -1 (Ignorância Intencional).

3.5. Rastreador de Celular iSharing

a) Instalação, Permissões e Funcionamento

O *iSharing* é desenvolvido pela iSharingSoft, Inc., empresa fundada em 2010 e sediada nos Estados Unidos[12], especializada em soluções de localização e segurança voltadas para grupos familiares ou pessoas próximas[13]. O aplicativo atua como um rastreador de celular via GPS e, segundo os desenvolvedores, foi projetado para garantir a segurança de crianças e proporcionar tranquilidade aos pais[14]. Nesta análise, foi considerada a versão 12.7.14.1 do aplicativo.

A instalação do aplicativo segue o procedimento padrão das lojas oficiais de

12 "iSharingSoft". IT History Society. Acesso em 8 de agosto de 2025. https://www.ithistory.org/db/companies/isharingsoft.

13 "iSharingSoft Overview". PitchBook. Acesso em 8 de agosto de 2025. https://pitchbook.com/profiles/company/151138-81.

14 Informações coletadas da página do aplicativo na Play Store

aplicativo. Durante a configuração inicial, dois pontos chamam atenção: a solicitação da data de nascimento e a obrigatoriedade de ativar todas as notificações. A coleta da data de nascimento poderia, em tese, ser utilizada para restringir o uso por menores de 13 anos — como ocorre em outros aplicativos analisados neste relatório. No entanto, verificou-se que, mesmo com a inserção de uma data correspondente a um usuário com apenas um ano de idade, o processo de configuração prossegue sem apresentar qualquer alerta ou bloqueio. Já a exigência de ativar todas as notificações no Android, impede a recusa seletiva pelo usuário, caracterizando um padrão conhecido como *Privacy Zuckering* [15].

Outro requisito é a necessidade de manter a permissão de Localização configurada como "Sempre permitir". Nos testes realizados, ao selecionar outra opção — como "Durante o uso do aplicativo" — o processo de configuração não avançava, forçando a aceitação do padrão imposto pelo desenvolvedor.

Semelhante ao *Life360*, o monitoramento ocorre por meio do compartilhamento de um link ou código, sendo necessário que ambos os dispositivos tenham o aplicativo instalado. Em ambos os casos, o ícone do aplicativo permanece visível.

Os dados coletados incluem informações como atividades no aplicativo, localização, fotos e vídeos, e dados pessoais. Contudo, os desenvolvedores indicam que parte dessas informações — como ID do dispositivo, ID do usuário e localização — pode ser compartilhada com empresas ou organizações terceiras, sem identificar quem são essas entidades ou como utilizam os dados. Cabe ainda salientar que em 2024, uma falha de segurança no sistema do aplicativo comprometeu os dados pessoais dos usuários[16].

b) Abusabilidade

A análise do *iSharing* também não conseguiu identificar nenhuma medida para dificultar a detecção ou a remoção do aplicativo do dispositivo. Mas, assim como o *Find My Kids*, as funcionalidades disponibilizadas por ele podem facilmente ser utilizadas em contextos de relacionamentos tóxicos e abusivos.

Chama a atenção o blog oficial da empresa que traz artigos que incentivam e dizem como e com que ferramentas pode ser feita a espionagem de pessoas. Apesar de brevemente mencionar a necessidade de consentimento da pessoa vigiada, o consentimento é tratado como formalidade única, abordagem que ignora completamente os princípios de consentimento informado e contínuo, desconsiderando

15 Um tipo de *dark pattern* onde o usuário é induzido ou forçado a aceitar todas as permissões, sob pena de não conseguir usar o aplicativo.

16 Whittaker, Zack. "Security bugs in popular phone-tracking app iSharing exposed users' precise locations | TechCrunch". TechCrunch, 24 de abril de 2024. https://techcrunch.com/2024/04/24/security-flaws-isharing-tracking-app-exposed-millions-precise-locations/.

relações de poder e contextos abusivos.[17] Trata-se, aqui, da normalização de um comportamento de vigilância, tanto em relacionamentos amorosos quanto de amizade, o que demonstra uma total complacência da empresa com as condutas de rastreamento ostensivo e vigilância.[18] Para alguém que tem o desejo de implementar essas medidas contra parceiros, amigos ou parentes, encontrar de forma fácil e acessível esse tipo de informação, ainda com a chancela de uma empresa destacada no mercado, é a chance de engajar num comportamento abusivo e violento, o que deve ser completamente rechaçado.

Além disso, não há qualquer evidência de manifestações públicas da empresa sobre abusos cometidos por pessoas em uso do aplicativo, tampouco menção a riscos para mulheres, população LGBTQIAP+ ou outras categorias sociais em vulnerabilidade. Também não foram encontradas evidências de medidas de mitigação da possibilidade de abusos, como por exemplo o bloqueio de agressores. No mesmo sentido, não há registro de engajamento da empresa em ações de abordagem de abusos ou a incorporação de relatos de sobreviventes e defensores no design do produto. Com base na Escala de Maturidade de Abusabilidade, o aplicativo poderia ser classificado no nível -1 (Ignorância Intencional).

3.6. Whatsapp Web

a) Instalação, Permissões e Funcionamento

O *WhatsApp Web* é uma extensão do aplicativo *WhatsApp Messenger*, desenvolvido pelo WhatsApp LCC., que pertence ao grupo Meta Platforms Inc., sediado nos Estados Unidos. Lançado em 2015, o *WhatsApp Web* permite o uso do mensageiro em navegadores de internet, espelhando as mensagens do celular no computador. Neste estudo analisamos o comportamento da versão web acessada via navegador Chrome em agosto de 2025.

Por ser uma extensão do aplicativo móvel, o *WhatsApp Web* não requer instalação direta no computador, basta acessar o link e escanear o QR Code exibido na tela com a câmera do aplicativo *WhatsApp Messenger* no celular. Após isso, o computador e o celular permanecem conectados enquanto ambos estiverem com acesso à internet.

---

17 "Will I be able to track someone without their knowledge?" iSharing, junho de 2025. https://help.isharingsoft.com/hc/en-us/articles/360057089674-Will-I-be-able-to-track-someone-without-their-knowledge.

18 "How to track someone by their phone number". iSharing, 29 de dezembro de 2021. https://isharingsoft.com/how-to-track-someone-by-their-phone-number/.

Embora prático, esse funcionamento apresenta riscos de segurança e privacidade quando há acesso físico ao celular sem supervisão. Qualquer pessoa que consiga acesso ao celular desbloqueado pode parear uma sessão no *WhatsApp Web* em poucos segundos. Não há notificação constante sobre sessões ativas no navegador, e o sistema permite que essa conexão permaneça funcionando por tempo indefinido, se a opção "manter conectado" for marcada. A única forma de verificar se há navegadores conectados à conta é acessando a opção "Dispositivos conectados", disponível no aplicativo do *WhatsApp Messenger* no celular, em Configurações > Dispositivos conectados. Se o usuário não acessar essa opção manualmente, nenhum alerta é exibido, o que pode permitir que sessões permaneçam ativas sem seu conhecimento.

Ao ser utilizado, o *Whatsapp Web* solicita permissões à medida que o usuário tenta utilizar determinados recursos. Essas permissões são controladas diretamente pelo sistema de permissões do próprio navegador. As principais são: Câmera: utilizada tirar fotos, gravar vídeos e realizar chamadas de vídeo; Microfone: necessário para o envio de áudios e para a realização de chamadas de voz ou vídeo; E notificações: assim que o login é realizado, o site pode solicitar permissão para enviar notificações pelo navegador, como alertas de novas mensagens.

Para encerrar uma sessão ativa, o usuário precisa desconectar a conta manualmente pelo site ou pelo aplicativo no celular, acessando Configurações > Dispositivos conectados e encerrando a sessão desejada.

b) Abusabilidade

No contexto da violência de gênero digital, o *WhatsApp Web* se apresenta como uma funcionalidade particularmente vulnerável à abusabilidade. Embora projetado para facilitar o uso do aplicativo em dispositivos não móveis, seu desenho técnico cria condições para que essa ferramenta seja explorada como forma de vigilância íntima, muitas vezes sem o conhecimento da vítima.

Do ponto de vista técnico, o *WhatsApp Web* permite que uma vez estabelecida a conexão, não há qualquer mecanismo ativo e contínuo de notificação no dispositivo monitorado que alerte sobre sessões em andamento. A única forma de detectar que a conta está sendo acessada por outro dispositivo é visitar manualmente a aba "Dispositivos conectados".

A única menção oficial a essa verificação aparece em um trecho pouco visível da central de ajuda, onde o *WhatsApp Messenger* recomenda que o usuário habilite as notificações push no celular para ser alertado caso um dispositivo não reconhecido se conecte à conta, além de sugerir que se "confira com frequência os dispositivos que

estão conectados". Embora essa orientação institucional represente um gesto no sentido da proteção do usuário, ela permanece restrita a um material técnico localizado fora do aplicativo, sem destaque nas interfaces principais do sistema. Trata-se, portanto, de uma recomendação pouco acessível e de baixa visibilidade, especialmente para usuários em situação de vulnerabilidade, que não têm familiaridade com os mecanismos de segurança da plataforma.

Quando contrastada com os termos de uso, essa permissividade técnica não encontra enfrentamento robusto. O documento não menciona o uso da plataforma como instrumento de vigilância interpessoal nem reconhece o fenômeno do *stalkerware*. A categoria de "acesso não autorizado" é tratada apenas como algo externo, associado a ataques por *malware* ou a *softwares* de espionagem desenvolvidos por empresas especializadas, como exemplificado pelo processo movido contra o grupo NSO.[19] No entanto, é importante salientar que muitas formas de espionagem íntima não dependem de softwares maliciosos, mas sim da exploração de funcionalidades legítimas de plataformas populares. A vigilância perpetrada por parceiros íntimos se utiliza, muitas vezes, de relações de confiança prévias e acesso físico autorizado em algum momento.

O *WhatsApp Messenger* possui uma posição de destaque como um serviço centrado na privacidade e segurança de seus usuários. Sua comunicação institucional destaca com ênfase a criptografia de ponta a ponta como salvaguarda contra interceptações, reforçando a ideia de que apenas remetente e destinatário têm acesso ao conteúdo das mensagens. No entanto, cabe salientar que a maior ameaça à privacidade dos usuários nem sempre está na interceptação de dados por agentes externos, mas no acesso silencioso por pessoas próximas, autorizado por funcionalidades que não exigem habilidades técnicas avançadas.

A permissividade da interface cria um ambiente propício para que o *WhatsApp Web* seja utilizado como ferramenta de uso duplo. A análise reconhece que há um reconhecimento institucional acerca dos riscos postos por *spywares* de uma forma geral, assim como a adoção de algumas orientações preventivas como a checagem de dispositivos conectados. Entretanto, a falta de medidas técnicas e de um suporte adequado a vítimas de monitoramento interpessoal leva a classificação na Escala de Maturidade de Abusabilidade ao nível 0 (Consciência Organizacional).

19 "Winning the Fight Against Spyware Merchant NSO". Meta Newsroom, 6 de maio de 2025. https://about.fb.com/news/2025/05/winning-the-fight-against-spyware-merchant-nso/.

3.7. Find Hub e Buscar (Find My)

a) Instalação, Permissões e Funcionamento

O aplicativo do *Google Find Hub*, anteriormente denominado *Find My Device*, passou a adotar a nova nomenclatura em 2025. Já o serviço da Apple *Find My* (Buscar) adquiriu este nome em 2019, sendo resultado da junção de dois outros recursos pré-existentes: *Find My Phone* e *Find My Friends*.

Ambos os aplicativos têm como finalidade o rastreamento de dispositivos e acessórios, incluindo produtos de terceiros, como garrafas de água e malas. As versões analisadas correspondem à 3.1.348-2 (*Find Hub*) e à versão integrada ao iOS 18.5 no caso do Buscar.

O *Find Hub*, por fazer parte da suíte Google,vem pré-instalado na maioria dos dispositivos Android, mas, diferentemente dos demais aplicativos da suíte, pode ser removido tanto pela loja oficial quanto diretamente pelas configurações do dispositivo. De forma semelhante, o aplicativo *Buscar* já vem pré-instalado nos dispositivos iOS e pode ser desinstalado manualmente nas configurações. O acesso ao Buscar requer autenticação de segurança (senha ou biometria) configurada no próprio aparelho do usuário. Esse recurso adiciona uma camada extra de proteção, mas não elimina completamente a possibilidade de uso indevido por terceiros.

No *Find Hub*, o compartilhamento de localização é feito por meio de um link, de forma semelhante ao *Google Maps*. Ao ativar essa função, o aplicativo exibe um alerta informando quais dados estarão visíveis para quem tiver acesso ao link. Há a possibilidade de selecionar a opção "Não mostrar novamente" para este aviso, podendo levar o usuário a não ter ciência no futuro sobre que informações estão sendo compartilhadas. Além disso, não é possível saber quem está visualizando a localização, a tela principal exibe o status do compartilhamento, sem informações claras sobre como encerrá-lo. Para quem recebe o link, a interface permite visualizar informações detalhadas de localização. A única forma de identificar quem está monitorando é se o compartilhamento for feito de forma nominal, como por exemplo via email.

No *Buscar*, o compartilhamento de localização é feito exclusivamente com contatos previamente cadastrados no ecossistema Apple. Essa abordagem permite que o usuário identifique de forma explícita quem possui acesso à sua localização, mas não elimina a possibilidade de que o compartilhamento permaneça ativo sem o conhecimento contínuo do titular, caso não haja revisão periódica das configurações.

Em ambos os serviços, os dados coletados incluem informações pessoais e de localização. Segundo os desenvolvedores, essas informações não são compartilhadas com terceiros.

b) Abusabilidade

O aplicativo *Buscar* oferece funcionalidades como rastreamento e compartilhamento de localização entre dispositivos Apple e usuários, além da possibilidade de localizar objetos pessoais via *AirTags*. Embora essas ferramentas tenham sido desenvolvidas com foco em conveniência e segurança, elas também apresentam potenciais significativos de uso abusivo. Um parceiro abusivo, por exemplo, pode acessar a conta Apple da vítima para rastrear a localização de seus dispositivos ou forçá-la a compartilhar sua localização em tempo real. Também é possível que o rastreamento ocorra por meio de *AirTags* ocultas, sem o conhecimento da pessoa monitorada.

Nesse contexto, a Apple implementou medidas técnicas para mitigar alguns desses riscos, como alertas para *AirTags* desconhecidos se movendo com o usuário, possibilidade de reprodução de som no rastreador, bloqueio de ativação de dispositivos vinculados, além da opção de desativar certos recursos, interromper o compartilhamento de localização ou mesmo deixar de usar o aplicativo *Buscar* e desativá-lo. No entanto, essas ações são reativas e restritas ao plano técnico-operacional. Não foram identificados mecanismos de denúncia integrados ao aplicativo, e a vítima não é notificada quando alguém apenas consulta sua localização, exceto em casos específicos, como o uso da função "Busca Precisa" em modelos de iPhone 15 ou superiores.

Institucionalmente, a Apple reconhece, ainda que de forma discreta, que suas ferramentas podem ser exploradas em contextos de abuso, perseguição ou assédio. Esse reconhecimento está presente no Manual de Segurança Pessoal[20], um guia com orientações sobre como revisar permissões de privacidade e proteger dados em situações de risco. No entanto, esse material não é de fácil acesso, não está diretamente vinculado ao app Buscar, e não foi identificado em políticas de privacidade ou descrições públicas do aplicativo, mesmo ele sendo um dos principais recursos que aborda o potencial de uso do aplicativo para vigilância. Dessa forma, embora exista uma iniciativa institucional relevante, ela permanece pouco visível e pouco acessível para usuários em situação de vulnerabilidade.

Diante desse cenário, o aplicativo Buscar apresenta características associadas tanto ao nível -1 (Ignorância Intencional) quanto ao nível 1 (Tomada de Ação) da Escala de Maturidade e Abusabilidade. Por um lado, a Apple adota ações técnicas relevantes para mitigar riscos; por outro, não assume um posicionamento institucional claro e acessível sobre os perigos de uso abusivo dessas funcionalidades. Assim, a classificação

20 "Manual de Segurança Pessoal da Apple". Apple Support. Acesso em 8 de agosto de 2025. https://support.apple.com/pt-br/guide/personal-safety/ipse14bfadaf/1.0/web/1.0.

mais adequada recai sobre o nível 0 (Consciência Organizacional). Embora não atenda integralmente os critérios formais dessa categoria, este é o nível que melhor reflete o estágio atual de abusabilidade do aplicativo. A Apple demonstra alguma consciência institucional sobre os riscos de uso abusivo, mas essa percepção ainda não se traduz em uma resposta pública clara, acessível e integrada à experiência do usuário.

No caso do *Find Hub*, recursos de rastreamento de dispositivos e objetos por meio de tecnologias como Bluetooth e localização GPS são oferecidos. Embora tenha sido projetado para segurança e conveniência, como encontrar aparelhos perdidos ou rastrear pertences, o serviço também apresenta riscos significativos de uso abusivo. Um agressor pode, por exemplo, esconder um rastreador vinculado à conta Google em um objeto pessoal da vítima ou utilizar o acesso à conta para monitorar a localização de forma não consentida.

Na Central de Ajuda para Androids, a plataforma deixa claro que é proibido usar o serviço para rastrear pessoas sem consentimento ou para obter a localização de alguém sem seu conhecimento[21]. Também informa que tais condutas podem configurar crime, o que representa um importante passo no reconhecimento do problema e na definição de responsabilidade legal e moral. A política inclui orientações úteis, como o fato de que alguns rastreadores, ao serem desativados, podem perder seu vínculo com o proprietário original, o que pode comprometer futuras investigações[22]. O alerta de que autoridades podem não conseguir mais informações após resetar o dispositivo é direto e relevante para uma tomada de decisão informada, especialmente por pessoas em situação de risco. Além disso, a recomendação de manter o rastreador ativo em casos de possível retaliação demonstra uma compreensão, ainda que incipiente, da dinâmica de controle coercitivo.

Algumas funcionalidades adicionais, como a possibilidade de pausar temporariamente o compartilhamento de localização por até 24 horas, podem ser úteis em contextos de emergência, permitindo que a pessoa interrompa momentaneamente o rastreamento. No entanto, esse recurso está disponível apenas para rastreadores compatíveis com a rede *Find Hub*, o que limita sua acessibilidade. A orientação para entrar em contato com as autoridades locais pode ser importante, mas é insuficiente quando o sistema não fornece suporte técnico estruturado. A dependência de uma iniciativa individual da vítima para registrar e proteger evidências enfraquece a possibilidade de responsabilização dos abusadores.

---

21 "Find Hub acceptable use policy - Google Pixel Tablet Help". Google Help. Acesso em 8 de agosto de 2025. https://support.google.com/googlepixeltablet/answer/14799569.

22 "Find unknown trackers". Google Help. Acesso em 8 de agosto de 2025. https://support.google.com/android/answer/13658562.

Apesar desses avanços, persistem lacunas importantes. A plataforma alerta sobre riscos, mas não os resolve de forma técnica ou institucional. Não há garantias de preservação de informações forenses mínimas após o reset de fábrica, o que favorece a impunidade em casos de rastreamento abusivo. Além disso, o Google não exige que parceiros (como fabricantes de rastreadores) adotem padrões mínimos de responsabilidade. Isso transfere toda a responsabilidade para o usuário e fragiliza sua proteção.

Embora haja um reconhecimento textual dos riscos, ele não se traduz em mecanismos acessíveis de mitigação. É importante destacar que em relação a recursos de apoio, que são brevemente mencionados no seu Centro de Ajuda[23], a empresa menciona organizações nos Estados Unidos (*Safety Net Project*), Reino Unido (*Refuge UK*) e Austrália (*WESNET Safety Net Australia*), priorizando usuários no Norte Global, já que nenhuma menção é feita em relação a organizações de apoio localizadas no Sul Global. Há uma disparidade entre o discurso de responsabilidade e a ausência de ações práticas robustas. Não há integração entre o alerta de risco e ações técnicas automáticas que poderiam proteger a vítima (como preservação de evidências, bloqueio remoto, ou encaminhamento facilitado às autoridades). Recursos como pausar a localização ou buscar apoio policial são oferecidos, mas são manuais, limitados e dependem da ação individual do usuário, o que não configura "ação concreta" por parte da empresa.

Considerando que há um reconhecimento institucional moderado e a adoção de algumas orientações preventivas, mas sem medidas técnicas e de suporte adequadas, a classificação mais apropriada na Escala de Maturidade de Abusabilidade é o nível 0 (Consciência Organizacional). O aplicativo reconhece o problema em sua documentação, mas falha em integrar esse entendimento à experiência do usuário e à estrutura técnica do serviço, limitando sua eficácia na prevenção e responsabilização de abusos.

23 Ibidem.

3.8. Eyezy

a) Instalação, Permissões e Funcionamento

O *Eyezy* é desenvolvido pela empresa Fortunex Limited, sediada na República do Chipre. O aplicativo é voltado ao monitoramento parental, permitindo rastrear a localização em tempo real[24]. A versão analisada neste relatório é a 1.4.0, sendo este o único aplicativo pago entre todos os avaliados.

Entre os aplicativos analisados, este é o que apresenta o maior potencial de dano à privacidade e autonomia do usuário monitorado. Isso porque seus recursos permitem praticamente clonar o dispositivo-alvo, concedendo controle total ao usuário que realiza o monitoramento.

O processo de instalação no Android não requer acesso root, mas em dispositivos iOS é necessário realizar *jailbreak*. Assim como o *AirDroid Parental Control*, o ícone do aplicativo permanece oculto após a instalação. O *Eyezy* funciona trabalhando secretamente em segundo plano para coletar todos os dados necessários e enviá-los para o painel do administrador[25]. As declarações encontradas no site oficial do aplicativo evidenciam o uso deliberado de padrões obscuros no design do aplicativo e a violação da autonomia do usuário monitorado sobre o seu aparelho, sob o pretexto de proteção.

Entre as funcionalidades disponíveis, destacam-se: bloqueio de redes *Wi-Fi*, registro de teclas, monitoramento de atividades em redes sociais e a configuração de "cercas proibidas", que disparam alertas sempre que o dispositivo monitorado entra em determinadas áreas geográficas. Para quem realiza o monitoramento, o aplicativo disponibiliza um painel de controle com diversos recursos que permitem executar ações e alterar configurações no dispositivo monitorado de forma remota.

No que diz respeito à coleta e compartilhamento de dados, destaca-se a coleta de áudio — que pode incluir gravações de voz ou sons do ambiente — entre os dados sensíveis que podem ser compartilhados com outras empresas ou organizações. Embora haja uma lista de informações que podem ser repassadas a terceiros, a página do aplicativo menciona apenas a coleta de dados de mensagens, sem esclarecer sobre os dados compartilhados dos demais itens listados[26]. Há a possibilidade de solicitar ao desenvolvedor a exclusão da conta e dos dados associados a ela.

---

24 Informações extraídas da página do aplicativo na Play Store.

25 "Eyezy". Eyezy Phone Monitoring App | See Everything, Everywhere | FAQ. Acesso em 8 de agosto de 2025. https://www.eyezy.com/faq.

26 Informações extraídas da página do aplicativo na Play Store.

b) Abusabilidade

O aplicativo *Eyezy* é promovido como uma ferramenta de controle parental, mas oferece funcionalidades típicas de *stalkerware*, com alto potencial de uso abusivo. Entre seus recursos estão o rastreamento em tempo real, histórico de localização, monitoramento de mensagens e chamadas, captura de teclas e tela, além da visualização de arquivos e aplicativos instalados. O aplicativo também pode operar em modo oculto, sem ícone e sem qualquer notificação visível à pessoa monitorada, permitindo que seja instalado e usado sem o seu conhecimento.

Durante a investigação, não foi identificada nenhuma medida técnica de prevenção ou mitigação contra esses riscos. Todas as funcionalidades operam de forma silenciosa, sem alertas, sem consentimento verificável e sem mecanismos de controle por parte da pessoa monitorada. A instalação pode ser realizada com acesso físico breve ao dispositivo da vítima, e o aplicativo permanece ativo em segundo plano, de forma invisível.

Embora os Termos de Uso afirmem que o *software* deve ser utilizado com consentimento e apenas para fins legais, na prática, isso representa uma transferência de responsabilidade legal ao usuário, uma vez que não há qualquer controle técnico efetivo para impedir o uso indevido. Além disso, o site oficial e os materiais promocionais não reconhecem explicitamente o potencial de uso abusivo, nem oferecem canais de denúncia, recursos informativos ou orientações para vítimas.

O design e as funcionalidades do aplicativo são compatíveis com práticas de vigilância e controle digital, e não há qualquer esforço institucional ou técnico para limitar seu uso como ferramenta de abuso. Ainda que o aplicativo seja apresentado como controle parental, não há diferenciação clara entre supervisão legítima e vigilância coercitiva, nem reconhecimento público do impacto potencial para pessoas em situação de vulnerabilidade. Trata-se, portanto, de um produto com risco extremo de abusabilidade, sem mecanismos de proteção mínimos para os usuários monitorados. Com base na Escala de Maturidade de Abusabilidade, o *Eyezy* se enquadra no nível -2 (Facilita Ativamente o Abuso).

4. CONSIDERAÇÕES FINAIS

A pesquisa realizada evidencia como tecnologias de monitoramento interpessoal, embora disfarçadas sob discursos de cuidado e proteção, se inserem em uma lógica mais ampla de controle e vigilância, muitas vezes em contextos marcados por violência de gênero e assimetrias de poder. A articulação entre práticas de design, estratégias publicitárias ambíguas e ausência de regulação eficaz contribui para um ecossistema permissivo ao uso abusivo desses aplicativos. Ao invisibilizar os riscos e transferir a responsabilidade ética para o usuário final, empresas e plataformas digitais colaboram para a naturalização de comportamentos invasivos e para a perpetuação de relações de dominação e coerção.

Frente a esse cenário, é indispensável adotar uma abordagem multidimensional que envolva regulação estatal, responsabilização corporativa e educação digital crítica. O enfrentamento ao uso abusivo de tecnologias de monitoramento não deve se limitar a soluções técnicas ou reativas, mas incorporar políticas públicas estruturais que reconheçam as especificidades de gênero, as desigualdades sociais e o papel das plataformas na disseminação dessas ferramentas. Tais medidas devem atuar tanto na prevenção quanto na reparação dos danos, assegurando proteção real para as vítimas e desestimulando práticas abusivas por meio da responsabilização efetiva de todos os agentes envolvidos.

RECOMENDAÇÕES

Para formuladores de políticas públicas:

- Criar regulações específicas para aplicativos que permitam o monitoramento interpessoal, com critérios claros de transparência, consentimento e limites de funcionalidade.
- Estabelecer sanções para empresas que permitam ou incentivem o uso abusivo dessas tecnologias.
- Integrar políticas de proteção digital aos programas de enfrentamento à violência de gênero.

Para desenvolvedores e plataformas:

- Adotar padrões de design que adotem análises de abusabilidade, isto é, que foquem em seguridade (garantindo direitos e bem-estar) e não apenas em segurança cibernética.
- Construir mecanismos eficazes de auditoria e moderação de conteúdo. Incluindo em seus aplicativos e plataformas alertas visíveis sobre riscos de uso indevido, canais de denúncia acessíveis e mecanismos de cooperação com autoridades.
- Revisar e restringir estratégias de marketing que utilizem apelos emocionais ambíguos ou que incentivem práticas de controle.

Para a sociedade civil:

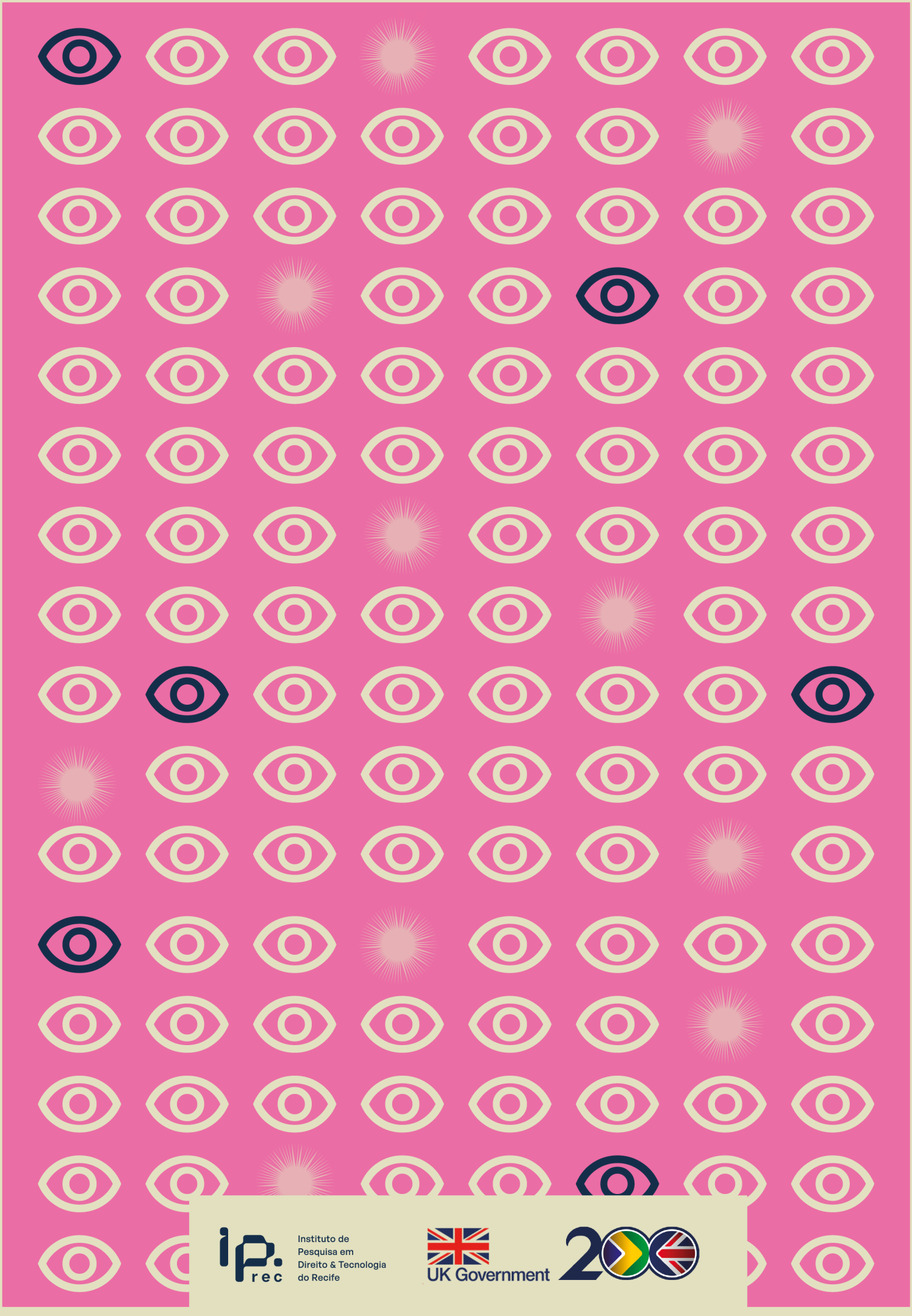
- Promover a conscientização sobre os riscos associados ao uso de tecnologias de monitoramento interpessoal, especialmente em contextos de violência de gênero.
- Cobrar transparência e responsabilidade de empresas e governos quanto à regulação, uso e fiscalização dessas tecnologias.
- Fortalecer redes de apoio comunitárias, com foco na escuta, acolhimento e orientação de vítimas de violência digital.

Para vítimas de violência digital:

- Buscar apoio junto a organizações especializadas em direitos digitais e enfrentamento à violência de gênero.
- Denunciar aplicativos suspeitos de violar sua privacidade em plataformas e órgãos de defesa do consumidor.
- Reivindicar seus direitos e exigir respostas efetivas das plataformas e autoridades.

Apêndice

Aplicativo	Grau de Maturidade (de -2 à +2)	Justificativa
Life 360	**-1**	Apesar de não ser oculto, nem utilizar técnicas de persistência, a ausência de medidas ativas e estruturais para prevenir ou coibir abusos demonstra uma escolha consciente de ignorar riscos previsíveis e facilitar a vigilância coercitiva.
Google Maps	**0**	Embora não promova ativamente o abuso, o design da funcionalidade permite exploração silenciosa. Possibilidade de bloqueios e notificações mensais acontecem no caso do compartilhamento por tempo indeterminado entre contas Google, entretanto, não há alertas ativos no caso de compartilhamentos que ocorrem via links por 24h.
AirDroid Parental Control	**-2**	Permite a instalação oculta e o controle remoto sem consentimento, somado à postura da empresa que se exime de responsabilidade e não adota medidas eficazes para prevenir abusos.
Find My Kids: GPS rastreador	**-1**	Apesar de não ser oculto nem dificultar detecção ou remoção do aplicativo, as funcionalidades do aplicativo podem ser utilizadas para perseguir uma pessoa dentro de uma relação tóxica, além da postura da empresa de ser eximir de responsabilidade e não adotar medidas para prevenir e coibir abusos.
Rastreador de Celular iSharing	**-1**	Apesar de brevemente mencionar a necessidade de consentimento da pessoa vigiada, o consentimento é tratado como formalidade única (lavagem ética). Desconsidera relações de poder e contextos abusivos.
Whatsapp Web	**0**	Há um reconhecimento institucional acerca dos riscos postos por *spywares* de uma forma geral, assim como a adoção de algumas orientações preventivas como a checagem de dispositivos conectados. Entretanto, há uma falta de medidas técnicas e de um suporte adequado a vítimas de monitoramento interpessoal.
Buscar	**0**	Possui medidas técnicas para mitigar rastreamento não autorizado. Há também um manual de segurança pessoal que reconhece riscos de abuso, mas é pouco visível e não está integrado ao aplicativo. Falta um posicionamento institucional claro, acessível e diretamente relacionado ao aplicativo.
Find Hub	**0**	Há uma consciência sobre o abuso tecnológico em sentido amplo resultando na adoção de algumas orientações preventivas, disponibilizadas, entretanto, de forma não integrada ao aplicativo.
Eyezy	**-2**	Oferece funcionalidades típicas de *stalkerware*, sem mecanismos de consentimento verificável ou alertas à pessoa monitorada. A empresa transfere a responsabilidade legal ao usuário e não adota medidas preventivas ou políticas contra o uso indevido.



Instituto de Pesquisa em Direito & Tecnologia do Recife

UK Government