



Instituto de  
Pesquisa em  
Direito & Tecnologia  
do Recife



UK Government



# **vigilância não é amor**

guia de proteção contra perseguição  
e violência de gênero online

# FICHA TÉCNICA

## Realização:

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

## Equipe:

### Coordenação:

Mariana Canto

### Autoras:

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

### Revisão técnica – Psicologia:

Bárbara Alves  
Luisa Rique

### Projeto Gráfico:

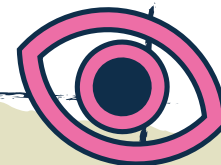
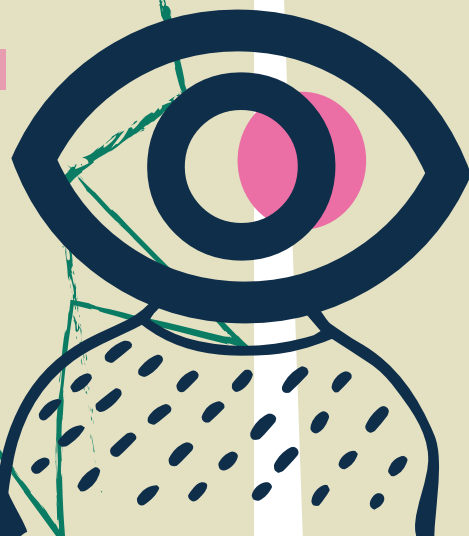
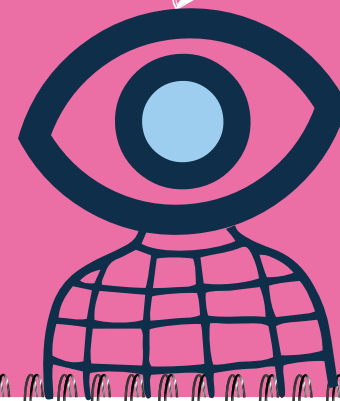
Estúdio Puya!

## Como citar:

IP.REC – INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE. **Vigilância não é amor:** guia de proteção contra perseguição e violência de gênero online. Recife: IP.rec, 2025. Disponível em: <https://ip.rec.br/publicacoes/vigilancia-nao-e-amor/>

Produzida com apoio do Programa de Acesso Digital da Embaixada do Reino Unido no Brasil

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



# SUMÁRIO RÁPIDO

Procure ajuda pelos canais de emergência:

**180**

Central de Atendimento à Mulher;

**190**

Polícia Militar;

**100**

Disque Direitos Humanos;

Delegacia da Mulher (DEAM) da sua cidade;

Delegacia de Crime Cibernético da sua cidade;

Centros de apoio à mulher da sua cidade;



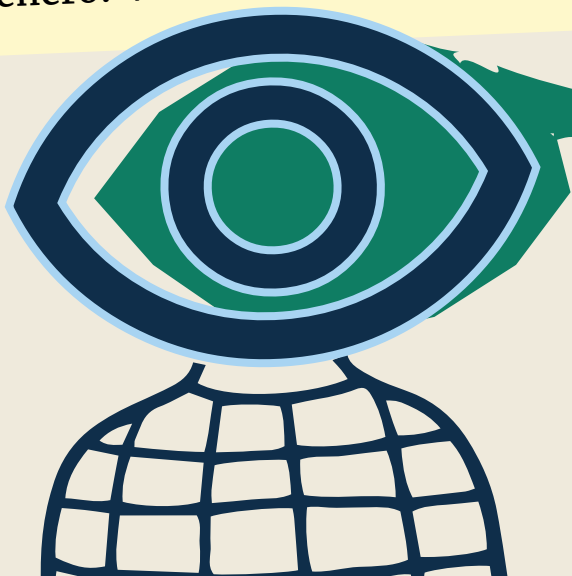
Centros de apoio à população LGBTQIAPN+ da sua cidade;

Canal de Ajuda da MariaLab  
(<https://mariadajuda.org/>);

Canal de Ajuda da SaferNet Brasil  
(<https://new.safernet.org.br/helpline>);

# APRESENTAÇÃO

Se você sente que alguém está lhe vigiando ou tentando controlar o que você faz, você não está só. Isso pode ser uma forma de violência, e ninguém merece passar por isso. O monitoramento sem o seu consentimento (seja por aplicativos, mensagens, localização ou redes sociais) não é demonstração de cuidado, é uma forma de controle e invasão. Quando alguém ultrapassa seus limites para lhe vigiar ou lhe ameaçar, isso faz parte da violência de gênero. Você tem direito a sua privacidade.



Cada situação é única e o mais importante agora é se proteger. Procure apoio de pessoas e serviços em quem confie antes de tomar qualquer decisão. Esta cartilha foi feita para ajudar vítimas a reconhecer sinais de monitoramento digital, entender seus direitos e encontrar caminhos seguros para buscar apoio. **Você merece viver sem medo e não precisa enfrentar isso só.**

# O QUE É STALKERWARE?

Refere-se a aplicativos e programas espões instalados, geralmente sem o consentimento da pessoa, para monitorar tudo o que ela faz no celular, desde mensagens, chamadas, localização, fotos, vídeos até o uso da câmera ou do microfone.

É um termo formado pela junção de dois termos: “stalker”, que do inglês quer dizer perseguidor/perseguidora e “ware” que é relativo a software.



## Paralelos do dia dia:

- É como se alguém ficasse olhando por cima do seu ombro enquanto você usa o celular;
- Pense em alguém que copia as chaves da sua casa, só que com o seu celular;
- Ou como alguém que pode gravar ligações ou ativar o microfone quando você está em uma conversa privada, como se houvesse um microfone oculto no bolso.



## Situações comuns:

Um ex-parceiro instala o app dizendo que é “para te proteger se roubarem o celular”, mas depois passa a monitorar onde você está e com quem fala.

Uma pessoa controladora pede o celular “só um minuto” e, sem que você perceba, instala um aplicativo que mostra suas conversas e localização.

Alguém usa um “app de controle parental” no seu aparelho para ver se você responde mensagens ou está online à noite.



## Tipos comuns:

Programas que aparecem no celular e gravam/acompanham;

Acesso por senha/conta (alguém entrou no seu e-mail, apps de mensagens, redes sociais);

Uso de redes sociais falsas ou contas compartilhadas para vigiar.



## OBSERVAÇÃO IMPORTANTE

**O uso de stalkerware é uma forma de violência e violação de privacidade.**

☞ Mesmo que o aplicativo seja vendido como “legítimo”, instalar ou usar esse tipo de software sem consentimento é ilegal e pode configurar crime de perseguição (art. 147-A do Código Penal), além de outros delitos relacionados à invasão de dispositivo e tratamento indevido de dados pessoais.

☞ Se houver suspeita de monitoramento, não desinstale o app imediatamente, busque ajuda técnica e jurídica especializada para preservar provas e garantir sua segurança.

# EXEMPLOS DE APLICATIVOS

Alguns aplicativos, sejam de uso cotidiano ou ferramentas para ajudar a “proteger” e rastrear, podem acabar sendo usados para vigiar pessoas. Veja alguns exemplos e como reduzir os riscos:

## GOOGLE MAPS – RISCO MÉDIO

### APLICATIVO DE MAPAS E NAVEGAÇÃO

**Permissões:** localização, câmera, contatos, dispositivos por perto, fotos e vídeos e microfone.

**Riscos:** o compartilhamento de localização e o histórico de trajetos podem permitir controle dos deslocamentos de alguém. O acesso à galeria pode expor fotos e vídeos tirados em determinados locais.

**Recomendações:** deixar ativado a permissão de localização só quando o aplicativo estiver em uso; remova o acesso à galeria e ao microfone se não utilizar esses recursos. Para verificar com quem sua localização está sendo compartilhada, acesse o aplicativo, clique no ícone com sua imagem ou inicial e selecione a opção “Compartilhar local”, onde será exibida a lista de pessoas.



## **WHATSAPP WEB — RISCO MÉDIO**

### **APLICATIVO DE MENSAGERIA**

**Permissões:** câmera, microfone e notificações.

**Riscos:** pode ser usado para acessar suas conversas sem que você saiba.

**Recomendações:** verifique periodicamente os dispositivos conectados em Configurações > Dispositivos conectados e saia de todos que não reconhecer.

## **FIND MY KIDS — RISCO ALTO**

### **APLICATIVO DE CONTROLE PARENTAL**

**Permissões:** localização, microfone, fotos, câmera, contatos e notificações.

**Riscos:** pode operar de forma silenciosa e ser usado para ouvir o ambiente e vigiar sem consentimento.

**Recomendações:** desative funções potencialmente abusivas, como escuta de ambiente; limite o acesso à permissões sensíveis que podem violar a privacidade, como fotos câmera e microfone.

## **LIFE 360 — RISCO ALTO**

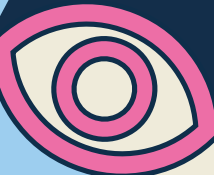
### **APLICATIVO DE LOCALIZAÇÃO FAMILIAR**

**Permissões:** localização, câmera, contatos, dispositivos por perto, microfone, telefone e atividade física.

**Riscos:** pode permitir rastreamento constante e revelar rotinas e hábitos pessoais, mesmo fora do contexto familiar ou de proteção.

**Recomendações:** revise quem pode ver sua localização e dados; desligue o rastreamento em tempo real quando não for necessário e limite o acesso a outros recursos do celular que podem violar a privacidade, como câmera, fotos e microfone.

# SE LIGUE NOS SINAIS



Seu celular/computador fica quente mesmo sem uso.



Bateria acaba muito rápido do nada.



Apps abrem sozinhos ou você vê mensagens “lidas” que você não abriu.



Mensagens de verificação (SMS/e-mail) chegando quando você não pediu.



Conta de rede social com acesso em locais que você não esteve.



Chamadas estranhas ou pessoas perguntando sobre seus passos.



Você nota mudanças na sua conta bancária / preços subindo sem explicação.



Recebe perguntas pessoais que só alguém próximo poderia saber.



Esses sinais podem indicar que alguém está tentando lhe monitorar, mas, sozinhos, não significam uma certeza. Eles são indícios, e precisam ser observados junto com o contexto da sua vida, especialmente se existe um histórico de controle, invasão de privacidade, ciúmes excessivo, ameaças ou outras formas de violência.



# O QUE NÃO FAZER



**NÃO**

confronte a pessoa se isso te coloca em risco.

**NÃO**

apague aplicativos, arquivos, provas ou resete o celular por conta própria imediatamente por medo. Isso pode lhe colocar em risco e dificultar ações futuras de denúncia.

**NÃO**

compartilhe sua localização em redes sociais e, se possível, torne suas redes privadas.

**NÃO**

entregue suas senhas, códigos de acesso ou de desbloqueio.

# MEDIDAS DE SEGURANÇA



## TELEFONE / APARELHO CELULAR

= A PORTADA DA SUA CASA:

quem tem acesso ao seu aparelho pode ter acesso a tudo sobre você;

## SENHA NUMÉRICA

= CHAVE:

dá acesso a casa, mas dependendo do nível de segurança (se é forte ou fraca) pode facilitar o acesso;

123



## BIOMETRIA

= FECHADURA ELETRÔNICA:

é uma camada a mais de segurança, mas assim como fechaduras eletrônicas podem falhar;

## AUTENTICAÇÃO EM 2 FATORES

= FECHO COM CORRENTE

camada extra de segurança. Mesmo que alguém descubra sua senha, ainda vai precisar destrancar essa segunda “fechadura”;



## PASSKEY

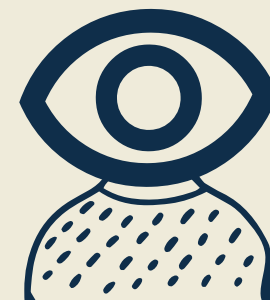
= CHAVES NO ESTILO TAG:

É uma chave única e segura que confirma que é realmente você;

## ENGENHARIA SOCIAL

= “JEITINHO” DE SABER INFORMAÇÕES

Sabe quando a gente começa a conversar com alguém e, sem perceber, acaba contando um monte de coisas sobre a vida? Pessoas mal-intencionadas podem usar essas informações contra você, ainda mais se suas senhas tiverem algo pessoal, como data de aniversário ou idade.



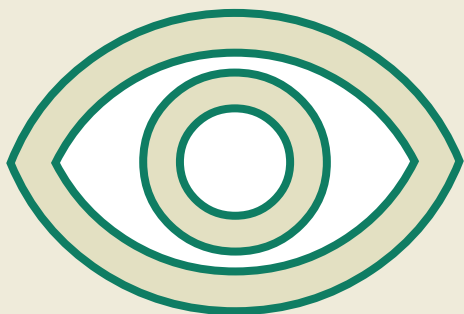
Pensando nisso, tem algumas situações que podem acontecer e jeitos simples de resolver:

### Situação:

“Como é que essa pessoa sempre sabe onde eu estou?”

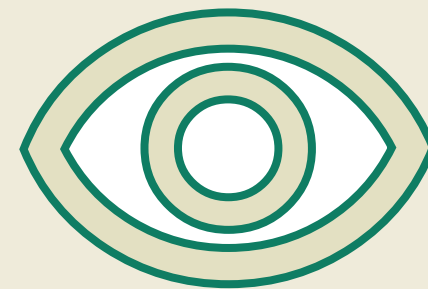
### O que pode estar acontecendo:

Pode ser que sua localização esteja sendo compartilhada sem você saber. Dá uma olhada nas configurações do celular e veja quais apps têm permissão para acessar sua localização e controle quem realmente pode ver onde você está. Também vale prestar atenção no que está sendo compartilhado nos aplicativos de localização.



### Situação:

“Estão me chantageando com fotos que nunca compartilhei, estou em desespero. E agora?”

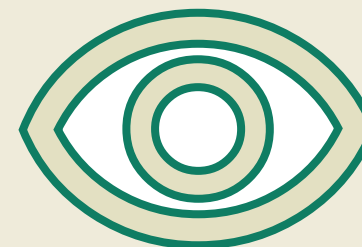


### O que pode estar acontecendo:

Calma! Não apaga nada. Tira print das mensagens e documenta tudo como prova. Procura uma delegacia de crimes cibernéticos, da mulher ou LGBTQIAPN+ e faz um boletim de ocorrência. Também é importante buscar ajuda psicológica.

### Situação:

“Que estranho... minhas mensagens aparecem como lidas, mas eu nem cheguei a abrir a conversa.”



### O que pode estar acontecendo:

Pode ser que tenha mais de uma sessão do seu app de mensagens aberta ou que ele tenha sido clonado. Dá uma olhada nas configurações do aplicativo para confirmar. Se for no e-mail, pode ser que alguém tenha sua senha. Nos dois casos, troque as senhas e saia de todos os dispositivos. E no e-mail, aproveita e ativa a autenticação em dois fatores e/ou *passkey*.



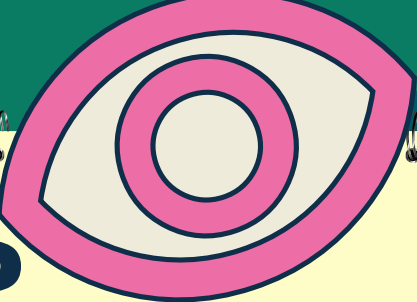
## RISCOS ALÉM DO MONITORAMENTO INTERPESSOAL

Vazamento de dados pessoais ➤ Informações expostas podem levar a constrangimento e chantagem.

Impacto financeiro ➤ Dados comprometidos podem permitir clonagem/aceso indevido a contas, compras fraudulentas ou golpes, por isso monitore bancos e cartões.

Aumento de preços/discriminação ➤ dados vazados podem ser usados por empresas para ajustar preços, direcionar anúncios abusivos ou limitar ofertas.

**O que fazer sobre isso:** contatar banco, bloquear cartões comprometidos, monitorar notificações, alterar senhas de serviços financeiros e e-mail periodicamente, ativar a autenticação de dois fatores e remover permissões desnecessárias de aplicativos.



# GUIA RÁPIDO PARA PROFISSIONAIS



Para advogados/as

## a) Procedimentos recomendados

Oriente a vítima a registrar o Boletim de Ocorrência (B.O.) imediatamente, presencialmente na Delegacia da Mulher ou Delegacia de Crimes Cibernéticos, ou online pelo site da Polícia Civil;

Relatar todos os atos de perseguição, com datas, meios utilizados e impacto à vítima

Solicitar a instauração de inquérito e, quando aplicável, medida protetiva de urgência.

Encaminhar a vítima para atendimento psicológico e assistência social.

Evitar revitimização e garantir acompanhamento humanizado.

**Obs1:** O crime de perseguição (stalking), previsto no art. 147-A do Código Penal, é de ação penal pública condicionada à representação, devendo a vítima manifestar vontade de ver o autor processado, no prazo de 6 meses a contar da identificação do agente.

**Obs2:** Eventualmente, essas práticas podem ser avaliadas cumulativamente ou em relação a tipos penais mais específicos, como no crime de invasão de dispositivo informático, disposto no art. 154-A do Código Penal.

**Obs3:** Se a vítima não souber quem é o agressor:

I. Proponha uma ação de exibição de documentos ou obtenção de dados contra a plataforma onde o assédio ocorreu (redes sociais, aplicativos, sites etc.), requerendo judicialmente a identificação do IP vinculado às contas, postagens ou mensagens ofensivas.

II. Após a obtenção do número de IP, ajuíze nova ação, desta vez, contra a provedora de conexão responsável por aquele endereço IP, solicitando a quebra de sigilo dos dados cadastrais do usuário (nome, CPF, endereço, e-mail, entre outros).

### III. De posse da identificação completa, você poderá:

- 1) Propor ação cível indenizatória, buscando reparação por danos morais e materiais; e/ou
- 2) Representar criminalmente o agressor, instruindo o inquérito ou a ação penal com todas as provas obtidas nas etapas anteriores.

### IV. Medidas Protetivas

Aplicáveis quando há relação íntima, familiar ou afetiva (Lei Maria da Penha, art. 22).

Podem incluir:

- Proibição de contato ou aproximação (presencial e virtual);
- Afastamento do lar ou local de trabalho;
- Restrição ao uso de redes sociais ou comunicação com a vítima.

O pedido pode ser feito na delegacia ou diretamente ao Ministério Público. Em alguns estados, é possível solicitar a aplicação de uma medida protetiva de urgência de forma remota.

É necessário acompanhar o cumprimento e comunicar eventuais descumprimentos ao juízo.

## V. Coleta de Provas Digitais

Oriente à vítima:

- a nunca apagar mensagens, e-mails, prints, perfis ou ligações.
- Registrar URLs completas, datas e horários.

Considere a lavratura de ata notarial (documento feito por tabelião que certifica o conteúdo das mensagens). Mais caro, porém garante maior legitimidade para a prova digital.

Mantenha registro cronológico da coleta e, se possível, guarde cópias das provas em mídias externas (pendrive ou HD).

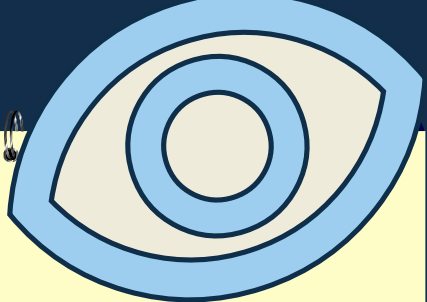
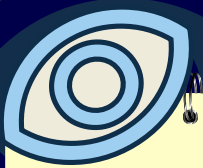
## **b) Responsabilidade civil e medidas judiciais complementares**

É possível processar o agressor nas esferas criminal e cível simultaneamente.

A vítima pode ingressar com ação de obrigação de não fazer, pedindo proibição de contato ou aproximação (inclusive via perfis falsos).

Também é possível requerer indenização por danos morais e psicológicos, comprovando o impacto emocional e reputacional.

Medidas liminares urgentes podem ser solicitadas com base no art. 497 do Código de Processo Civil.



# GUIA RÁPIDO PARA PROFISSIONAIS



de Saúde Mental

## **a) Acolhimento com foco em segurança emocional e validação**

Crie um espaço de escuta empática e validação do sofrimento, reconhecendo a especificidade da violência digital como forma de controle e violência psicológica.

Evite minimizar a experiência da vítima ou sugerir soluções técnicas imediatas sem compreender o impacto emocional e psicológico produzido pela violência digital.

Quando a vítima não tiver clareza sobre a problemática do que está vivenciando, você deve clarificar e nomear como cyberstalking. Acolher os sentimentos conflitantes que possam surgir e apoiar a vítima na construção de possibilidades.

Atente-se ao diagnóstico diferencial de sintomas ou transtornos psicóticos e avalie discurso sobre outras áreas da vida, sintomas anteriores e associados, contexto familiar, social e laboral.

Considere que a violência digital costuma ocorrer em conjunto com outras modalidades de violência. Essa informação deve orientar sua avaliação clínica do risco e seu diálogo sobre segurança com a vítima.

## **b) Coordenação com a rede de proteção e preservação de provas**

Mantenha articulação constante com a rede de apoio e proteção, respeitando o sigilo profissional e a vontade da vítima.

Oriente sobre preservação de evidências digitais (salvar mensagens, registros de localização, capturas de tela) sem estimular a exposição ou revitimização.

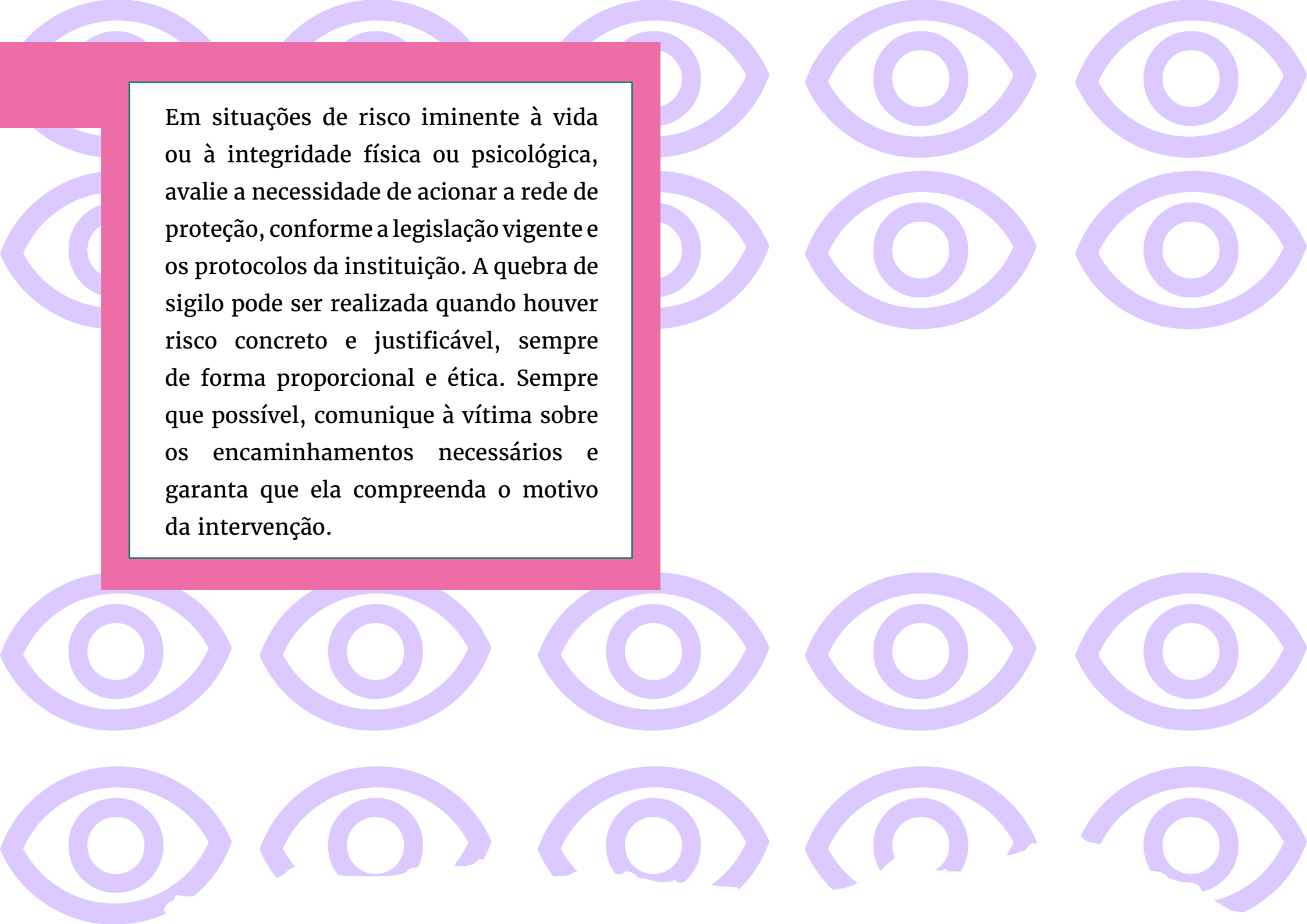
Não oriente a vítima a desinstalar o aplicativo suspeito ou a alterar configurações em seu celular, pois o agressor pode perceber e reagir de forma violenta.

Explique à vítima que existem serviços especializados em segurança digital e violência de gênero, e ofereça informações confiáveis caso ela manifeste desejo de acessá-los. Evite realizar intervenções técnicas no dispositivo da vítima e mantenha sempre o foco no cuidado clínico, na autonomia e na avaliação de risco.

Se necessário, busque essas instituições junto à vítima e apresente as possibilidades a ela. O tempo do atendimento pode ser utilizado para esse fim, é inclusive uma estratégia de fortalecimento.

Em casos de risco elevado, comunique a rede técnica (CREAS, Ministério Público, Delegacia Especializada) conforme protocolos institucionais.

Trabalhe o processo de reconstrução da autonomia digital e afetiva, apoiando o reestabelecimento da rotina e dos vínculos sociais.



Em situações de risco iminente à vida ou à integridade física ou psicológica, avalie a necessidade de acionar a rede de proteção, conforme a legislação vigente e os protocolos da instituição. A quebra de sigilo pode ser realizada quando houver risco concreto e justificável, sempre de forma proporcional e ética. Sempre que possível, comunique à vítima sobre os encaminhamentos necessários e garanta que ela compreenda o motivo da intervenção.

### **c) O que não fazer:**

Não manipule o celular ou computador da vítima (não busque aplicativos suspeitos, não altere configurações, não instale antivírus). Isso pode aumentar o risco.

Não oriente a desinstalação de apps ou mudanças imediatas no dispositivo. O agressor pode perceber.

Não questione a veracidade da experiência.

Não confronte o agressor nem faça contato em nome da vítima.

Não realize investigações paralelas (procurar perfis, IPs, localização, prints de terceiros).

Não pressione a vítima a denunciar. Respeite o tempo, o medo e a avaliação de risco dela.

Não acione familiares ou contatos pessoais sem análise cuidadosa de risco.

Não salve evidências em seus próprios dispositivos.

Não tome decisões pela vítima, exceto em risco iminente e seguindo protocolos legais.

# CHECKLISTS IMPRIMÍVEIS

## DICAS PARA AUMENTAR A SUA SEGURANÇA DIGITAL:

### 1. Fortaleça suas senhas:

- Não compartilhe suas senhas.
- Use senhas fortes e diferentes para cada conta.

### 2. Proteja suas contas e informações pessoais:

- Ative a autenticação de dois fatores e/ou passkeys em redes sociais, e-mails e aplicativos bancários.
- Evite salvar senhas em navegadores ou aparelhos compartilhados.
- Revise regularmente os dispositivos conectados às suas contas e saia dos que não reconhecer.

### 3. Cuide do acesso aos seus aparelhos:

- Evite compartilhar a senha de desbloqueio do celular ou do computador.
- Evite deixar seus dispositivos desbloqueados e sozinhos.

### 4. Revise permissões:

- Nas configurações, verifique as permissões de cada app e retire o que for desnecessário.
- Evite conceder todas as permissões ao instalar um aplicativo.

### 5. Preste atenção aos sinais de vigilância:

- Desconfie se alguém parece saber detalhes da sua vida que você não contou.
- Confira regularmente os apps instalados e veja se há algum que você não reconhece.
- Observe se o celular está mais lento, esquenta rápido ou a bateria acaba depressa sem motivo.

Se houver suspeita de monitoramento, não desinstale o app imediatamente, busque ajuda técnica e jurídica especializada para preservar provas e garantir sua segurança.



# CHECKLISTS IMPRIMÍVEIS

- # Disque 180 - Central de Atendimento à Mulher  
(<https://www.gov.br/mdh/pt-br/ligue180>)
- # Disque 190 - Polícia Militar
- # Disque 100 - Disque Direitos Humanos
- # Canal de Ajuda da SaferNet Brasil  
(<https://new.safernet.org.br/helpline>)
- # Canal de Ajuda da MariaLab  
(<https://mariadajuda.org/>)
- # Delegacia da Mulher da sua cidade
- # Delegacia de Crimes Cibernéticos da sua cidade
- # Centros de apoio à mulher da sua cidade
- # Centros de apoio à população LGBTQIAPN+ da sua cidade
- # Mapa Saúde Mental do Instituto Vita Alere  
(<http://mapasaudemmental.com.br/>)
- # Disque 188 - Centro de Valorização à Vida  
([www.cvv.org.br](http://www.cvv.org.br))



## COMO PROCURAR AJUDA

Se você está sendo ou já foi vítima de monitoramento, lembre-se de duas coisas importantes: a culpa não é sua e você não está sozinha. Faz parte do ciclo da violência tentar colocar a culpa na vítima, mas não deixe que isso lhe faça duvidar de si. Se você conhece alguém passando por essa situação, ofereça apoio: escute, acompanhe e ajude essa pessoa a buscar profissionais e tomar as medidas certas para se proteger. Se o seu foco agora é se manter segura, use esta cartilha como guia, monte um protocolo de segurança e siga-o com frequência para reduzir os riscos. A seguir, você encontra alguns lugares e números úteis que podem ser utilizados a qualquer momento. **Fique bem!**



expondo

# STALKERWARE

vigilância

não é

amor

ip.  
rec

Instituto de  
Pesquisa em  
Direito & Tecnologia  
do Recife



UK Government



@ip.rec



ip.rec.br



@ukinbrazil

