Instituto de Pesquisa em Direito & Tecnologia do Recife

UK Government

Surveillance is not love

a guide to protection against online stalking and gender-based violence

TECHNICAL INFORMATION

Produced by:

Law and Technology Research Institute of Recife – IP.rec

Team:

Coordination:

Mariana Canto

Authors:

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

Technical Review – Psychology:

Bárbara Alves
Luisa Rique

Graphic Design:

Estúdio Puya!
Pedro Silva Neto

How to cite:

IP.REC – INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE. *Surveillance Is Not Love: A Guide to Protection Against Online Stalking and Gender-Based Violence*. Recife: IP.rec, 2025. Available at: https://ip.rec.br/en/publicacoes/survellaince-is-not-love-a-guide-to-protection-against-online-stalking-and-gender-based-violence/

Produced with the support of the Digital Access Programme of the British Embassy in Brazil

QUICK SUMMARY

UK

- Call 999
- UK National Helpline on 0808 2000 247
- Suzy Lamplugh Trust on 0808 802 0300

YOU CAN ALSO CALL YOUR:

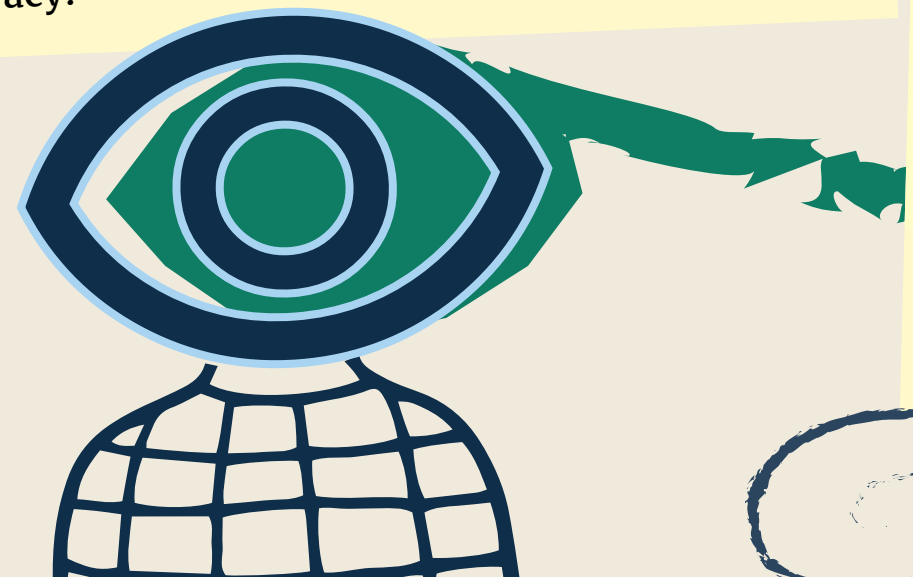
- Local domestic abuse service
- Police domestic violence unit
- General Practitioner (GP)
- Children's school

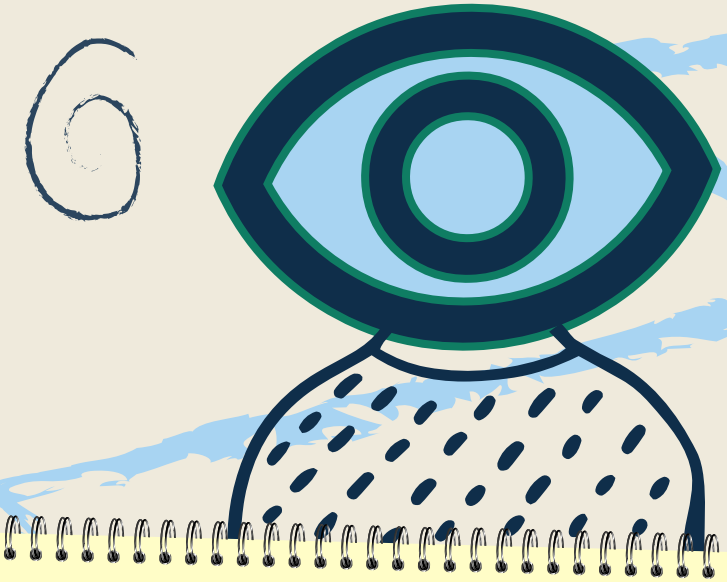
US

- Call 911
- National Domestic Violence Hotline: +1-800-799-7233
- National VictimConnect Resource Center: +1-855-4-VICTIM

INTRODUCTION

If you feel that someone is watching you or trying to control what you do, you are not alone. This may be a form of violence, and no one deserves to go through this. Monitoring without your consent (through apps, messages, location tracking, or social media) is not a sign of care - it is a form of control and invasion. When someone crosses your boundaries to monitor or threaten you, this is part of gender-based violence. You have the right to privacy.





Every situation is unique, and your priority right now is to protect yourself. Seek support from trusted people and services before making any decisions. This guide was created to help victims recognize signs of digital monitoring, understand their rights, and find safe ways to seek help. **You deserve to live without fear, and you do not have to face this alone.**

WHAT IS STALKERWARE?

Stalkerware refers to spy apps and programs installed - usually without the person's consent - to monitor everything they do on their phone, including messages, calls, location, photos, videos, and even camera or microphone use.

The term combines "stalker" (someone who stalks) and "ware" (from software).

Everyday Comparisons:

- It's like someone constantly looking over your shoulder while you use your phone;
- It's like someone copying your house keys but with your phone;
- It's like someone secretly recording your calls or activating your microphone during private conversations, as if there were a hidden microphone in your pocket.

Common Situations:

An ex-partner installs an app saying it's "to protect you if your phone gets stolen," but then uses it to monitor where you are and who you talk to.

A controlling person asks to use your phone "just for a minute" and secretly installs an app that tracks your conversations and location.

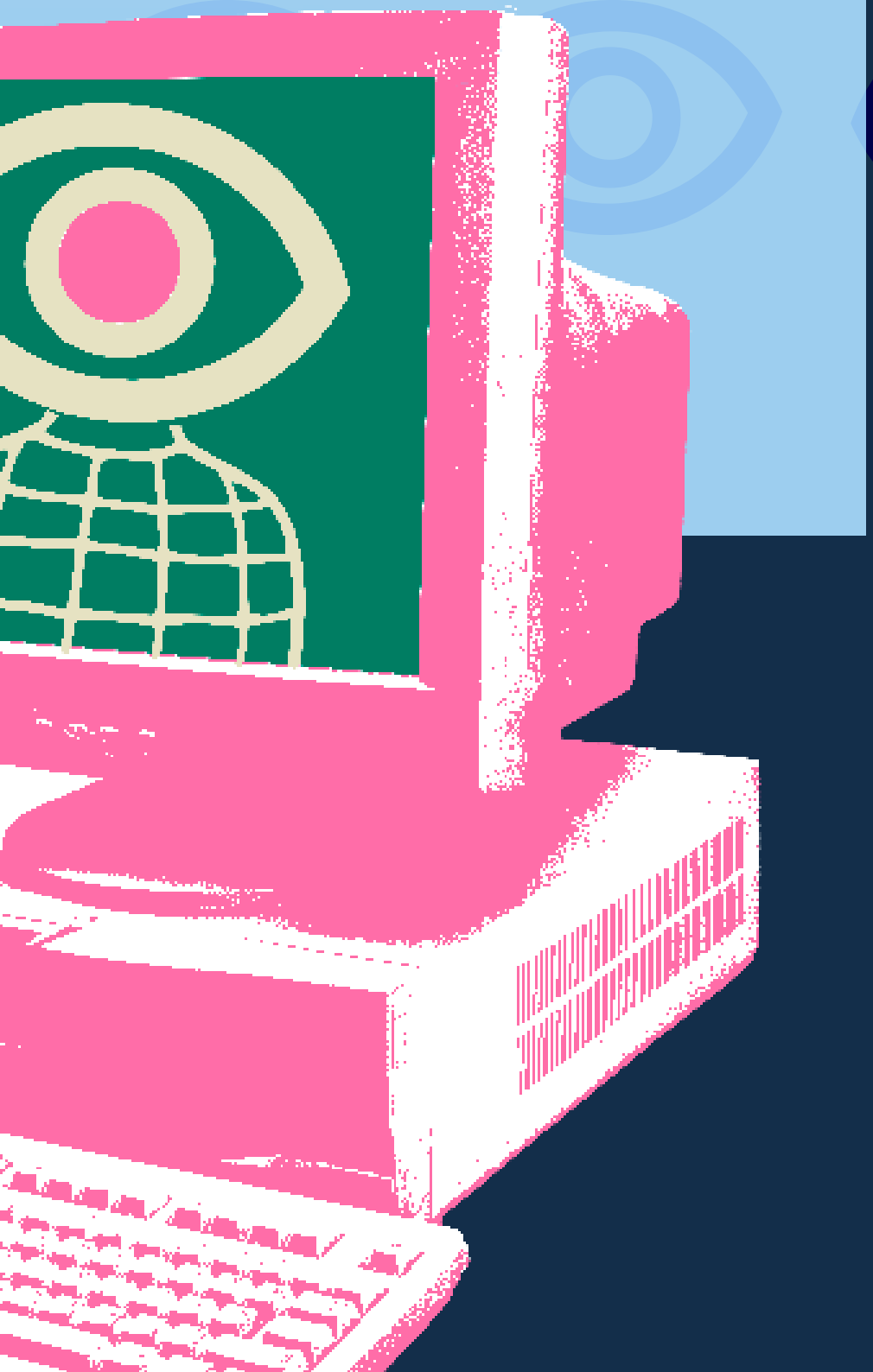
Someone uses a "parental control" app on your device to see whether you respond to messages or are online at night.

Common Types of Monitoring:

Programs installed on the phone that record or track activity;

Access via password/account (someone logs into your email, messaging apps, or social media);

Fake social media accounts or shared accounts used for monitoring.



IMPORTANT NOTE

The use of stalkerware is a form of violence and a violation of privacy.

- Even if marketed as "legitimate," installing or using this type of software without consent is illegal and may constitute the crime of stalking, in addition to other crimes related to device invasion and improper handling of personal data.
- If you suspect monitoring, do not uninstall the app immediately. Seek specialized technical and legal assistance to preserve evidence and ensure your safety.

EXAMPLES OF APPLICATIONS

Some everyday apps or tools marketed as "protection" or tracking tools can be misused for surveillance. See examples and how to reduce risks:

GOOGLE MAPS — MEDIUM RISK

MAPS AND NAVIGATION APPS

Permissions: Location, camera, contacts, nearby devices, photos and videos, microphone.

Risks: Location sharing and route history can enable tracking of movements. Gallery access may expose photos and videos taken at specific locations.

Recommendations: Enable location only while the app is in use; remove gallery and microphone access if not needed. To check with whom your location is being shared, open the app, click on the icon with your photo or initial, and select the 'Share location' option, where the list of people will be displayed.

WHATSAPP WEB — MEDIUM RISK
MESSAGING APP

Permissions: Camera, microphone, notifications.

Risks: Can be used to access your conversations without your knowledge.

Recommendations: Regularly check connected devices in Settings > Linked Devices and log out of any you don't recognize.

FIND MY KIDS — HIGH RISK
PARENTAL CONTROL APP

Permissions: Location, microphone, photos, camera, contacts, notifications.

Risks: Can operate silently and be used to listen to surroundings without consent.

Recommendations: Disable potentially abusive features such as ambient listening; limit sensitive permissions like camera, photos, and microphone.

LIFE 360 — HIGH RISK
FAMILY LOCATION APP

Permissions: Location, camera, contacts, nearby devices, microphone, phone, physical activity.

Risks: Enables constant tracking and reveals routines and personal habits, even outside protective or family contexts.

Recommendations: Review who can see your location; disable real-time tracking when unnecessary and limit access to camera, photos, and microphone.

WATCH FOR THE SIGNS

- **Your phone/computer gets hot even when not in use.**
- **Your battery drains very quickly without explanation.**
- **Apps open on their own or messages appear as "read" when you didn't open them.**
- **You receive verification codes (SMS/email) you didn't request.**
- **Social media logins appear in locations you haven't been.**
- **Strange calls or people asking about your whereabouts.**
- **Unexplained changes in your bank account.**
- **Someone asks personal questions only someone close to you would know.**

These signs may indicate monitoring, but alone they are not proof. They must be considered in the context of your life, especially if there is a history of control, invasion of privacy, excessive jealousy, threats, or other forms of violence.

WHAT NOT TO DO

DO NOT confront the person if it puts you at risk.

DO NOT delete apps, files, evidence, or reset your phone out of fear. This may increase risk and hinder future legal action.

DO NOT share your location on social media; make accounts private if possible.

DO NOT share passwords, access codes, or unlock codes.

SECURITY MEASURES

TWO-FACTOR **AUTHENTICATION**

= **SAFETY CHAIN** ON THE DOOR:

an additional layer of protection. Even if someone discovers your password, they will still need to unlock this second "lock";

PHONE / MOBILE DEVICE

= THE **FRONT DOOR** OF **YOUR HOME:**

whoever has access to your device may have access to everything about you;

PASSKEY

= DIGITAL TAG-STYLE **KEY**

a unique and secure key that confirms it is really you;

NUMERIC **PASSWORD**

= **KEY**:

it gives access to the house, but depending on how strong or weak it is, it may make access easier;

SOCIAL **ENGINEERING**

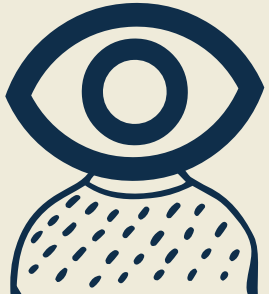
= **A "TRICK" TO OBTAIN** INFORMATION

You know when you start talking to someone and, without realizing it, end up sharing many details about your life? Malicious people can use this information against you - especially if your passwords include personal details like your birthdate or age.

BIOMETRICS

= ELECTRONIC **LOCK**:

an extra layer of security, but like electronic locks, it can fail;



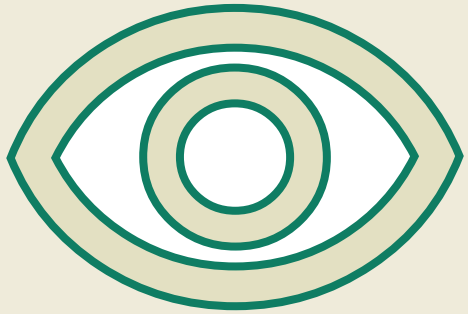
With that in mind, here are some situations that may happen and simple ways to handle them:

Situation:

"How does this person always know where I am?"

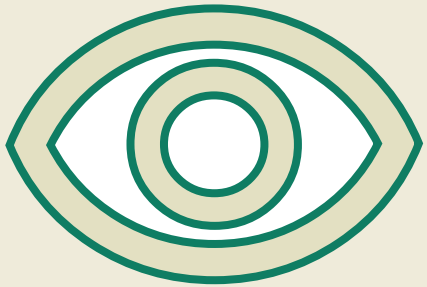
What may be happening:

Your location may be shared without you realizing it. Check your phone's settings to see which apps have permission to access your location and control who can actually see where you are. Also pay attention to what is being shared in location-based apps.



Situation:

"They're blackmailing me with photos I never shared. I'm desperate. What now?"

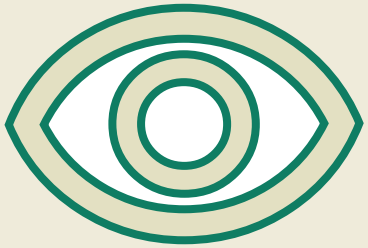


What may be happening:

Stay calm! Don't delete anything. Take screenshots of the messages and document everything as evidence. Go to a cybercrime police station, women's police station, or LGBTQIAPN+ police station and file a police report. It is also important to seek psychological support.

Situation:

"That's strange... my messages show as read, but I didn't even open the conversation."



What may be happening:

There may be more than one active session of your messaging app, or your account may have been cloned. Check the app's settings to confirm. If it's your email, someone may have your password. In both cases, change your passwords and log out of all devices. For email, also enable two-factor authentication and/or a passkey.

RISKS BEYOND INTERPERSONAL MONITORING

Personal data leaks ⪢ Exposed information may lead to embarrassment or blackmail.

Financial impact ⪢ Compromised data may allow account cloning, unauthorized access, fraudulent purchases, or scams. Monitor your bank accounts and cards.

Price increases/discrimination ⪢ Leaked data may be used by companies to adjust prices, target abusive advertising, or limit offers.

What to do: Contact your bank, block compromised cards, monitor notifications, regularly change financial service and email passwords, enable two-factor authentication, and remove unnecessary app permissions.

QUICK GUIDE FOR PROFESSIONALS

For Lawyers

a) Recommended Procedures

Advise the victim to file a police report immediately, either in person at a Women's Police Station or Cybercrime Police Station, or online through the Police website.

Report all acts of stalking, including dates, methods used, and impact on the victim.

Request the opening of a criminal investigation and, when applicable, urgent protective measures.

Refer the victim for psychological care and social assistance.

Avoid revictimization and ensure humane follow-up.

Note: If the victim does not know who the aggressor is:

I. File a legal request against the platform where the harassment occurred (social networks, apps, websites, etc.), seeking court-ordered identification of the IP address linked to the accounts, posts, or offensive messages.

II. After obtaining the IP address, file a new action against the internet service provider responsible for that IP address, requesting disclosure of the user's registration data (name, ID number, address, email, etc.).

III. With full identification, you may:

1) File a civil lawsuit seeking compensation for moral and material damages; and/or

2) Initiate criminal proceedings against the aggressor, providing all evidence gathered.

IV. Protective Measures

Applicable when there is an intimate, family, or affective relationship.

May include:

- Prohibition of contact or approach (in person or online);
- Removal from the home or workplace;
- Restriction on social media use or communication with the victim.

V. Collection of Digital Evidence

Advise the victim to:

- Never delete messages, emails, screenshots, profiles, or call records.
- Record complete URLs, dates, and times.
- Consider a notarial record (an official document certifying digital content). Though more expensive, it strengthens digital evidence.
- Keep a chronological record of evidence collection and store copies on external devices (USB drive or external hard drive).

b) Civil Liability and Additional Legal Measures

The aggressor may be sued in both criminal and civil courts simultaneously.

The victim may file a restraining order action requesting prohibition of contact or approach (including through fake profiles).

Compensation for moral and psychological damages may be requested, demonstrating emotional and reputational impact.

Urgent preliminary injunctions may be requested when necessary.

QUICK GUIDE FOR PROFESSIONALS

For Mental Health Professionals

a) Support Focused on Emotional Safety and Validation

Create a space for empathetic listening and validate the suffering, recognizing digital violence as a form of control and psychological abuse.

Avoid minimizing the experience or suggesting immediate technical solutions without understanding the emotional impact.

If the victim lacks clarity about what they are experiencing, help name it as cyberstalking. Welcome conflicting feelings and support the victim in building possibilities.

Pay attention to differential diagnosis of psychotic symptoms or disorders and assess other areas of life, previous symptoms, and family, social, and work context.

Consider that digital violence often occurs alongside other forms of violence. This should guide clinical risk assessment and safety discussions.

b) Coordination with Protection Networks and Evidence Preservation

Maintain coordination with support and protection networks, respecting professional confidentiality and the victim's wishes.	In high-risk cases, notify appropriate institutional networks according to protocols.
Guide the preservation of digital evidence (saving messages, location records, screenshots) without encouraging exposure or revictimization.	Support the rebuilding of digital and emotional autonomy, helping restore routines and social connections.
Do not advise uninstalling suspected apps or changing device settings, as the aggressor may notice and react violently.	In cases of imminent risk to life or physical/ psychological integrity, assess the need to activate protection networks according to legislation and institutional protocols. Confidentiality may be breached when there is concrete and justifiable risk, always proportionally and ethically. Whenever possible, inform the victim about referrals and ensure they understand the reason for intervention.
Inform the victim about specialized digital security and gender violence services if they wish to access them. Avoid technical interventions on the victim's device and maintain focus on clinical care, autonomy, and risk assessment.	

c) What Not to Do

- Do not manipulate the victim's phone or computer (do not search for suspicious apps, change settings, or install antivirus software).
- Do not advise immediate app uninstallation or device changes.
- Do not question the truthfulness of the experience.
- Do not confront the aggressor or contact them on the victim's behalf.
- Do not conduct parallel investigations (searching profiles, IPs, locations, third-party screenshots).
- Do not pressure the victim to report. Respect their timing, fear, and risk assessment.
- Do not contact family members or personal contacts without careful risk analysis.

PRINTABLE CHECKLISTS

TIPS TO INCREASE YOUR DIGITAL SECURITY:

1. Strengthen your passwords:

- Do not share them.
- Use strong and different passwords for each account.

2. Proteja suas contas e informações pessoais:

- Enable two-factor authentication and/or passkeys on social media, email, and banking apps.
- Avoid saving passwords on shared browsers or devices.
- Regularly review connected devices and log out of unrecognized ones.

3. Control access to your devices:

- Do not share your unlock password.
- Avoid leaving devices unlocked and unattended.

4. Review app permissions:

- Check each app's permissions in settings and remove unnecessary ones.
- Avoid granting all permissions when installing new apps.

5. Watch for signs of surveillance:

- Be cautious if someone seems to know details about your life that you did not share.
- Regularly review installed apps and look for unfamiliar ones.
- Notice if your phone becomes slower, overheats, or the battery drains quickly without reason.

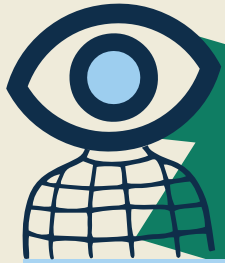
PRINTABLE CHECKLISTS

United Kingdom

- Call 999
- UK National Helpline on 0808 2000 247
- Suzy Lamplugh Trust on 0808 802 0300
- Your local domestic abuse service
- Police domestic violence unit
- GP
- Social worker
- Children's school

United States

- Call 911
- National Domestic Violence Hotline: +1-800-799-7233
- National VictimConnect Resource Center: +1-855-4-VICTIM



HOW TO SEEK HELP

If you are being monitored or have been a victim of monitoring, remember two important things: it is not your fault, and you are not alone. Blaming the victim is part of the cycle of violence, but do not let that make you doubt yourself. If you know someone going through this situation, offer support: listen, stay by their side, and help them seek professional assistance and take the appropriate steps to protect themselves. If your focus right now is staying safe, use this guide as a reference, create a safety plan, and follow it regularly to reduce risks. Below, you will find helpful places and contact numbers that can be used at any time.

Take care!

exposing STALKERWARE