RESUMO EM 6 LINHAS

1. Menos dados, menos risco.
2. Telemóvel em casa sempre que der.
3. Se vai contigo: código forte, sem biometria, actualizado.
4. Signal com mensagens temporárias e número escondido.
5. Sem consentimento, não há cara nem nome.
6. Cuidamos umes des outres.

Informação geral, revista a 25 de Outubro de 2026. A tecnologia e a lei mudam. Não substitui aconselhamento jurídico.

Inspirado livremente em guias de segurança digital de outros movimentos. Texto original, escrito para um movimento não-violento pela habitação. Outras fontes: Lei 18/2024, imprensa portuguesa.

Série Prevenção Anti-Censura: n.º 2 Mensagens Encriptadas, n.º 3 GrapheneOS, n.º 4 Tails.

Copia, imprime, partilha. Assembleia Popular / Acampada, Lisboa.

ACAMPADA
ASSEMBLEIA POPULAR

LISBOA · OUT. 2026



SÉRIE PREVENÇÃO ANTI-CENSURA
N.º 1 DE 4

O TELEMÓVEL É UM BUFO 101

Prevenção anti-censura para quem luta pela habitação

LÊ · COPIA · PARTILHA

PREVENÇÃO ANTI-CENSURA

PORQUÊ ESTA ZINE?

Lutar por casa é legal. Juntar-nos é um direito.
Mas há dados que podem pôr pessoas em risco.

Algumes de nós são migrantes. Algumes vivem em casas sem contrato, em quartos, em ocupações, na rua. Algumes têm processos de residência por resolver.

Para estas pessoas, uma lista de nomes, uma foto ou um registo de localização pode ter consequências sérias: no trabalho, na casa, nos papéis.

O telemóvel sabe muito: onde estás, com quem falas, a que horas, quem está na tua lista de contactos. Guarda isto e partilha-o com empresas. Em certos casos, com autoridades.

Não é preciso ter medo. É preciso ter cuidado.

Esta zine não é sobre esconder nada. É sobre privacidade, liberdade de associação e cuidar umes des outres.

Regra de ouro: **os dados que não existem não podem ser usados contra ninguém.**

CUIDAR DO COLECTIVO

A segurança digital é colectiva. Um grupo é tão forte como o telemóvel menos protegido.

NO GRUPO

- Grupos pequenos para assuntos sensíveis. Grupos grandes só para avisos públicos.
- Não partilhes listas com nomes, moradas ou situação de residência. Nunca.
- Não digas quem esteve onde. Nem em brincadeira.
- Quem entra no grupo? Quem sai? Revejam de vez em quando.
- Mensagens temporárias activas em todos os grupos do movimento.

PESSOAS EM MAIOR RISCO

- Migrantes e pessoas em situação de habitação precária decidem o seu próprio nível de exposição. Não decides por elas.
- Pergunta sempre antes de fotografar, gravar ou nomear.
- Não as ponhas em listas, actas ou formulários sem necessidade e sem consentimento.

CONVERSA IMPORTANTE?

Melhor ao vivo, sem telemóveis na sala ou com eles desligados noutra divisão.

Ninguém sabe tudo. Aprendemos juntes, sem culpa e sem julgamento.

ORGANIZAR COM MENOS ECRÃ

Antes dos smartphones também havia movimentos. E funcionavam.

ENCONTROS

- Combina hora e sítio antes. Define um **ponto de encontro de reserva**.
- Combina uma regra: "se não estás lá às 19h15, esperamos 15 minutos e seguimos".

CAMINHOS

- Mapa em papel ou mapa offline. Vê o caminho antes de sair.

EMERGÊNCIAS

- Números importantes em papel, no bolso.
- Quase sempre alguém empresta um telemóvel para uma chamada urgente.
- Combina com a tua dupla onde vão estar e quando dão notícias.

Burocracias (Segurança Social, AIMA, banco, arrendamento)

- Isto não precisa de ser encriptado. Pode ser feito de casa, com telemóvel ou chamada pela internet.

Telemóveis "básicos" (de teclas)

- Gastam pouca bateria e têm menos apps a recolher dados.
- Mas **não encriptam** chamadas nem SMS e continuam ligados às antenas. Não servem para conversas sensíveis.

O QUE O TELEMÓVEL CONTA

Mesmo parado no bolso, o telemóvel fala.

- **Antenas.** Para teres rede, o telemóvel liga-se às antenas mais próximas. A operadora sabe por onde andas: na cidade, muitas vezes com uma precisão de poucas centenas de metros.
- **Identificadores.** O cartão SIM e o próprio aparelho têm números únicos. Mudar de SIM não muda o aparelho.
- **GPS.** Apps de mapas, redes sociais, meteorologia, fotos: muitas guardam a localização exacta.
- **Wi-Fi e Bluetooth.** Ligados, podem revelar onde estiveste e que aparelhos estavam perto.
- **Fotos.** Cada foto pode levar data, hora e coordenadas escondidas.
- **Contas.** Google, Apple, Meta: fazem cópias de segurança de contactos, mensagens e fotos nos servidores delas.

O telemóvel faz o diário por ti.

CHECKLIST RÁPIDA

☐ Vê que apps têm acesso à localização. Tira a quem não precisa.
☐ Desliga Wi-Fi e Bluetooth quando não usas.
☐ Revê o que vai para a "nuvem".

METADADOS: O ENVELOPE DIZ MUITO

O conteúdo é a carta. Os metadados são o envelope: quem enviou, para quem, quando, de onde, quanto tempo.

Parece pouco. Não é.

Com metadados dá para saber:

- quem fala com quem, e com que frequência;
- quem esteve no mesmo sítio à mesma hora;
- quem faz parte de um grupo, mesmo sem ler uma única mensagem.

Ou seja: dá para desenhar o mapa de um colectivo.

Por isso, cuidar de ti é também cuidar da tua rede. O teu telemóvel tem o número das tuas pessoas. Se ele for vigiado, elas também ficam visíveis.

Um telemóvel que vai sempre a todo o lado cria um padrão muito detalhado da tua vida: casa, trabalho, assembleias, casa de amigues.

Pensa assim: se alguém visse só o "envelope" da tua semana, o que ficava a saber?

NO LOCAL: FOTOS, CARAS E CÂMARAS

Uma foto bonita da assembleia pode tornar-se uma lista de presenças.

ANTES DE FOTOGRAFAR

- Pergunta. Sem consentimento, não há cara.
- Fotografa costas, mãos, faixas, cartazes, o espaço.
- Desfoca caras, tatuagens, roupa marcante. O Signal tem ferramenta de desfocar.
- Para tirar metadados: faz screenshot da foto, ou envia-a pelo Signal antes de publicar.
- Não publiques em directo. Espera que todes tenham saído.

CÂMARAS NA CIDADE

Segundo a imprensa (Maio 2026), Lisboa tem cerca de 96 câmaras de videovigilância (Bairro Alto, Santa Catarina, Cais do Sodré, Campo das Cebolas) e quer chegar a 251, incluindo Martim Moniz, Almirante Reis, Restauradores e Saldanha. São autorizadas pelo Governo, com parecer da CNPD, e geridas pela PSP.

Não é razão para não ir. É razão para não juntar a isso mais imagens nossas.

ANTES DE SAIR DE CASA

Se levas o telemóvel, prepara-o.

CHECKLIST

☐ **Código forte**: 6 dígitos no mínimo, melhor uma frase-passe. Nada de padrões.

☐ **Desliga a impressão digital e o desbloqueio facial.** O teu dedo ou a tua cara desbloqueiam o telemóvel num segundo, até sem quereres.

☐ Confirma que o telemóvel está **encriptado** (nos modelos recentes vem por defeito, com código activo).

☐ **Signal** para conversas do movimento, com **mensagens temporárias**.

☐ No Signal: **nome de utilizador** e **número escondido**.

☐ Desliga a localização e o histórico de localização ("Cronologia" no Google Maps, "Locais significativos" no iPhone).

☐ Notificações sem conteúdo no ecrã bloqueado.

☐ Sai de sessões que não precisas (email, redes sociais).

☐ Bateria carregada e números importantes **escritos em papel**.

Se puderes, usa um telemóvel só para o movimento, com poucas apps e sem contas pessoais.

E A LEI EM PORTUGAL?

Notícia boa: em Portugal a guarda de metadados tem limites.

- Em 2022, o **Tribunal Constitucional** (acórdão 268/2022) chumbou a lei antiga, que guardava dados de tráfego de toda a gente e não avisava as pessoas.
- Em 2023, voltou a travar uma tentativa de guardar tudo durante 3 meses (acórdão 800/2023).
- A **Lei 18/2024** é a regra actual. Em resumo:
- dados de identificação do cliente e endereços IP: guardados **1 ano**;
- dados de tráfego e localização: só com **autorização judicial** (uma formação do Supremo Tribunal de Justiça) e só para **crimes graves**;
- a pessoa deve ser **notificada**, mas isso pode ser adiado.

O que isto quer dizer:

- Ir a uma assembleia ou manifestação legal não é crime.
- Mas as operadoras e as apps continuam a recolher dados por razões comerciais.

A lei protege. Menos dados protege mais.

Este é um resumo simplificado. Não substitui aconselhamento jurídico.

SPYWARE: O BUFO DENTRO DO BUFO

Há programas espiões, como o **Pegasus** ou o **Graphite**, que tomam conta de um telemóvel inteiro: mensagens, microfone, câmara, localização.

Alguns são "zero-click": não é preciso carregar em nenhum link. Em 2025 foram noticiados ataques destes a jornalistas e pessoas da sociedade civil em vários países da UE.

São caros e usados contra poucas pessoas. Mas há coisas simples que dificultam muito:

CHECKLIST

- ☐ Faz **todas as actualizações** do sistema e das apps, logo que saem.
- ☐ **Reinicia** o telemóvel todos os dias. Alguns ataques não sobrevivem a um reinício.
- ☐ Apaga apps que não usas.
- ☐ Não instales apps a partir de links ou sites desconhecidos.
- ☐ Em situações de maior risco: activa o **Modo de Isolamento** (Lockdown Mode, iPhone) ou a **Protecção Avançada** (Android 16 ou mais).
- ☐ Telemóvel muito antigo, sem actualizações? É hora de o reformar.

MODO AVIÃO, DESLIGADO OU EM CASA?

Não é a mesma coisa.

MODO AVIÃO

Corta a rede móvel. Mas o GPS pode continuar a funcionar e as apps podem guardar a localização e enviá-la mais tarde. Wi-Fi e Bluetooth às vezes voltam a ligar-se sozinhos.

DESLIGADO

Muito melhor. Atenção: muitos iPhones recentes continuam a dar sinal por Bluetooth à rede "Encontrar" (Find My) durante horas depois de desligados. Isto desactiva-se nas definições do "Encontrar".

BOLSAS FARADAY

Bloqueiam o sinal se forem boas e bem fechadas. Muitas baratas não funcionam. Testa: põe o telemóvel lá dentro e liga-lhe. Se tocar, não serve.

EM CASA

A opção mais segura. Um telemóvel que fica em casa não diz por onde andaste.

Ideia para o colectivo: em vez de deixar o telemóvel em casa só "nos dias importantes", experimenta sair sem ele mais vezes. Ganhas tempo, atenção e privacidade. E protegemos todes da mesma forma.