RESUMO EM 6 LINHAS

1. Signal por defeito, com nome de utilizador e número escondido.
2. SimpleX quando o número é um problema.
3. Briar como rede de reserva sem internet.
4. Telegram e WhatsApp só para o que já é público.
5. Mensagens temporárias em todos os grupos do movimento.
6. O mais sensível diz-se ao vivo.

Informação geral, revista a 25 de Outubro de 2026. As apps mudam depressa: confirma antes de confiar.

Inspirado livremente em guias de segurança digital de outros movimentos. Texto original, escrito para um movimento não-violento pela habitação. Outras fontes: páginas de apoio do Signal, SimpleX, Cwtch, Briar e Element, imprensa especializada.

Série Prevenção Anti-Censura: n.º 1 O Telemóvel é um Bufo, 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 2 DE 4

MENSAGENS ENCRIPTADAS 101

Escolher bem onde falamos

LÊ · COPIA · PARTILHA

PREVENÇÃO ANTI-CENSURA

PORQUÊ ESTA ZINE?

Organizamo-nos por mensagens: assembleias, GT, grupos de afinidade, turnos, boleias.

Lutar por casa é legal. Associar-nos é um direito. Mas as conversas guardam muita coisa: quem somos, onde vivemos, quem conhece quem.

Para algumes de nós isto pesa mais: pessoas migrantes, com processos de residência por resolver, a viver sem contrato, em quartos, na rua.

Nenhuma app é perfeita. Cada uma protege umas coisas e expõe outras. Esta zine ajuda a escolher a ferramenta certa para cada conversa, e a usá-la bem.

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

TRÊS PERGUNTAS ANTES DE ESCOLHER

1. Com quem falo?
2. O que estou a dizer?
3. Quem fica em risco se isto sair daqui?

Regra de ouro: **a melhor mensagem sensível é a que se diz ao vivo.**

REGRAS DO GRUPO (ASSEMBLEIA E GT)

Leiam juntes, adaptem e fixem no chat.

1. **Um grupo, um objectivo.** Avisos da assembleia num grupo só de leitura. Discussão em grupos de GT. Coisas sensíveis: ao vivo.
2. **Entrada com aprovação.** Link de convite com aprovação por admin. Repõe o link se circular fora do grupo.
3. **Quem entra, alguém conhece.** Cada pessoa nova é apresentada por alguém do GT.
4. **Revisão mensal.** Quem já não está no GT sai do grupo, sem drama.
5. **Mensagens temporárias sempre ligadas.**
6. **Nada de listas:** nomes, moradas, situação de residência, saúde. Nunca.
7. **Sem prints.** O que se diz no grupo fica no grupo.
8. **Fotos com consentimento**, sem caras, enviadas pelo Signal.
9. **Fala por ti.** Não digas onde outras pessoas estiveram ou vão estar.
10. **Duas ou mais pessoas admin.**
11. **Telemóvel perdido?** Avisa e sai do grupo até estar resolvido.
12. **Dúvida? Pergunta.** Aqui ninguém é julgade por não saber.

CONFIRMA QUEM ESTÁ DO OUTRO LADO

NÚMEROS DE SEGURANÇA (SIGNAL)

Cada conversa tem um código único. Se for igual nos dois telemóveis, ninguém está no meio.

- Conversa > nome da pessoa > **Ver número de segurança**. Em pessoa, lê o QR do outro telemóvel.
- Algumas conversas já mostram um visto verde "encriptação verificada". Se não aparecer, verifica à mão.
- Aviso de que o número de segurança mudou? Normalmente é telemóvel novo. Confirma ao vivo antes de falar de coisas sensíveis.

MENSAGENS TEMPORÁRIAS

- Definições > Privacidade > **temporizador predefinido**. Uma semana para começar. Um dia para grupos de afinidade.
- Em grupos, admins podem definir quem muda o temporizador.
- Não impedem capturas de ecrã. São uma ajuda, não uma garantia.

DISPOSITIVOS

- Signal no computador? Revê os dispositivos ligados todos os meses.
- Telemóvel perdido, roubado ou apreendido: avisa o grupo, para te retirarem até teres outro telemóvel seguro.

Confiança constrói-se ao vivo. A app só a confirma.

A CARTA E O ENVELOPE

ENCRIPTAÇÃO PONTA-A-PONTA (E2EE)

Só tu e quem recebe conseguem ler. A empresa que gere a app não. É como uma carta fechada que só se abre com a chave certa.

METADADOS

São o envelope: quem fala com quem, quando, quantas vezes, de onde, o tamanho dos ficheiros. Muitas apps encriptam a carta, mas deixam o envelope à vista.
Com envelopes dá para desenhar o mapa de um colectivo sem ler uma única mensagem.

SERVIDOR CENTRAL

As mensagens passam por computadores de uma empresa. Funciona bem, mas temos de confiar nela.

PEER-TO-PEER (P2P)

As mensagens vão directamente de aparelho para aparelho. Menos gente pelo meio, mas as duas pessoas costumam ter de estar online.

TOR

Uma rede que esconde de onde te ligas. Algumas apps usam-na por defeito.

Atenção: encriptação não protege um telemóvel desbloqueado na mão de outra pessoa. Código forte e mensagens temporárias contam tanto como a app.

QUAL É O NOSSO RISCO?

Não precisamos todes da mesma protecção. Pensa no que pode correr mal:

- **Recolha comercial:** empresas que guardam com quem falas para vender publicidade ou treinar sistemas.
- **Pedidos de autoridades:** a empresa recebe uma ordem judicial e entrega o que tiver. Se não tiver nada, não entrega nada.
- **Telemóvel perdido, roubado ou apreendido:** quem o abre vê conversas, grupos e números.
- **Pessoa infiltrada ou print partilhado:** a encriptação não ajuda se a mensagem chega a quem não devia.

O QUE ISTO QUER DIZER NA PRÁTICA

- Escolhe apps que **guardam pouco** sobre ti.
- Esconde o teu **número de telefone**: é a chave que liga a conta à tua identidade.
- Usa **mensagens temporárias**: o que já não existe não se pode ler.
- Cuidado com **quem entra** nos grupos.

Uma assembleia aberta e um grupo de afinidade não têm o mesmo risco. Não usem a mesma ferramenta nem as mesmas regras.

PORQUE NÃO TELEGRAM (E CUIDADO COM O RESTO)

TELEGRAM

- Grupos **sem encriptação ponta-a-ponta**. Nunca. A empresa pode ler.
- Os "chats secretos" são só entre duas pessoas, não vêm ligados e ficam presos a um aparelho.
- Desde Setembro de 2024, a política de privacidade prevê entregar **IP e número de telefone** a autoridades com ordem judicial.
- Serve para: canal público de anúncios. Nada mais.

WHATSAPP

- O conteúdo é encriptado. Mas a Meta sabe **com quem falas, quando e de onde**, e a tua lista de contactos. Um documento do FBI de 2021 indica que estes dados podem ser entregues quase em tempo real.
- Cópias de segurança no Google Drive ou iCloud só são encriptadas se activares essa opção.

ELEMENT / MATRIX

- Encriptado nas salas privadas, mas o servidor vê **nomes das salas e quem lá está**. Servidor de confiança e nada sensível.

SMS e chamadas normais: sem encriptação. Só para coisas banais.

BRIAR E CWTCH: QUANDO É PRECISO MAIS

Briar (Android)

- Funciona **sem internet**: as mensagens passam de telemóvel em telemóvel por **Bluetooth e Wi-Fi**. Óptimo para uma acampada com rede fraca.
- Com internet, usa Tor. Sem número de telefone: adicionam-se contactos por link ou QR.
- Atenção: desde Julho de 2026 está em **modo de manutenção** (só correcções essenciais). Gasta muita bateria e não envia ficheiros.
- **Ideia:** um pequeno grupo de apoio instala-o antes de uma acampada ou manifestação longa, como rede de reserva.

Cwtch (Android e computador, sem iPhone)

- Tudo por Tor, peer-to-peer, sem número. Das apps que menos envelope deixam.
- As duas pessoas têm de estar online para o primeiro contacto.
- Para grupos é preciso um servidor. Os novos "grupos híbridos" são experimentais e quem aloja o grupo vê as mensagens.
- Mantém-no actualizado: a versão 1.17.2 (Outubro 2026) corrige falhas de segurança.

Pedem mais esforço. Valem a pena para grupos pequenos com mais risco.

TABELA: QUAL APP PARA QUÊ?

APP	E2EE	METADADOS	PEDE NÚMERO?	SEM INTERNET?	BOM PARA
Signal	Sim, sempre	Guarda muito pouco	Sim (sem número: só beta Android)	Não	Quase tudo: GT, afinidade, chamadas
Molly (Android)	Sim (rede Signal)	Como o Signal	Sim	Não	Maior risco, com Android
SimpleX	Sim, sempre	Muito bom: sem ID de conta	Não	Não	Contacto público da assembleia
Cwtch	Sim, via Tor	Muito bom	Não	Não	Texto entre poucas pessoas
Briar (Android)	Sim, via Tor	Muito bom	Não	**Sim** (Bluetooth, Wi-Fi)	Rede de reserva no local
Element / Matrix	Sim, salas privadas	Fraco: servidor vê salas e membros	Não	Não	Comunidades grandes, nada sensível
WhatsApp	Sim (conteúdo)	Fraco: a Meta recolhe muito	Sim	Não	Quem só tem WhatsApp, avisos públicos
Telegram	Não nos grupos	Fraco	Sim	Não	Só canais públicos

Resumo: Signal por defeito. SimpleX quando o número é um problema. Briar como plano B. Telegram e WhatsApp só para o que já é público.

SIGNAL: A BASE DO MOVIMENTO

Gratuito, sem publicidade, de uma fundação sem fins lucrativos. Perante ordens judiciais, só consegue entregar a data de criação da conta e a última ligação.

O ponto fraco é o **número de telefone**. Resolve assim:

CHECKLIST

☐ Cria um **nome de utilizador** (Definições > Perfil) e partilha esse, não o número.

☐ Definições > Privacidade > Número de telefone: quem pode **ver** o número: **Ninguém**; quem te pode **encontrar** pelo número: **Ninguém**.

☐ Nome e foto de perfil que não te identifiquem logo.

☐ Activa o **bloqueio de registo** com PIN (Definições > Conta).

☐ **Bloqueio de ecrã** da app activo.

☐ Privacidade > Avançado: **reencaminhar sempre as chamadas** (esconde o teu IP).

☐ Revê **dispositivos ligados**. Desliga o que não reconheces.

Em teste (2026): contas **sem número**, só em beta Android, pagas via Google Play. Espera pela versão final.

Molly: Signal reforçado para Android (frase-passe, bloqueio automático). Mesmos contactos.

SIMPLEX: SEM NÚMERO, SEM NOME

O SimpleX não tem número de telefone, nem email, nem sequer um código de conta. Cada contacto é ligado por um convite próprio. Os servidores não sabem quem fala com quem.

BOM PARA

- Pessoas que não querem, ou não podem, dar o número.
- **Contacto público da assembleia:** um endereço SimpleX num cartaz. Quem está em risco de despejo escreve-nos sem se expor. Desliga a "aceitação automática" e alguém do GT responde.

CUIDADOS

- Define uma **frase-passe** para a base de dados.
- Não há cópia na nuvem: se perderes o telemóvel, perdes as conversas. Exporta uma cópia de vez em quando, para um sítio seguro.
- Convites de uso único: envia-os por um canal de confiança ou mostra o QR em pessoa.
- Em contas públicas: permite **só texto**.
- Grupos grandes: testem antes de mudar a assembleia inteira.
- Pode usar Tor, mas não vem ligado.

Funciona em Android, iPhone e computador.