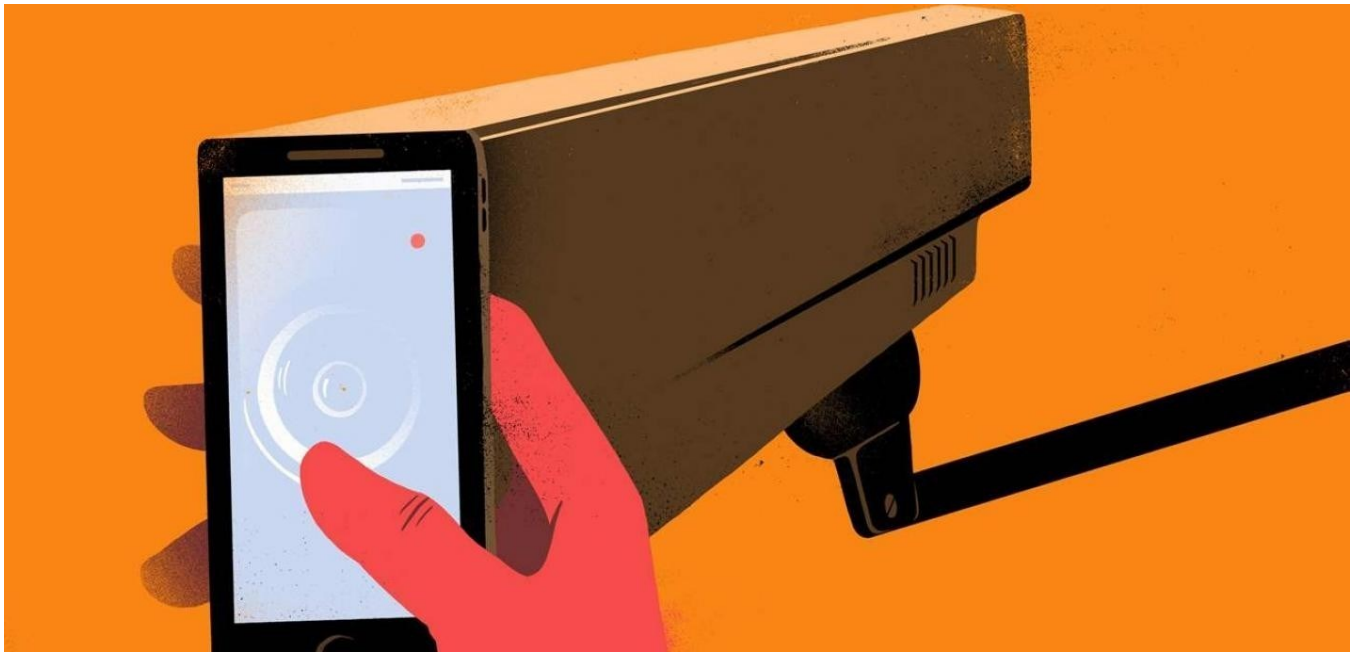
Telefonia móvel

Vigilância, fiscalização, redução de riscos



Versão 7 Janeiro de 2023

(Nota: muitos dos dados aqui apresentados se referem à França, porém muitos também são de alcance internacional)

Tabela de conteúdo

Introdução....3
I) Telefonia móvel e segurança....4
Redes de antenas telefônicas []....4
Questões específicas para telefones celulares....5
O sistema operacional do smartphone....7
II) Os inevitáveis problemas de segurança nos telefones []....10
Geolocalização do telefone []....10
Chamadas gratuitas e SMS []....10
Identificação do telefone []....11
Violações e atualizações de segurança....13
Cartão SIM e dados do telefone []....14
A comunicação é um esforço de grupo []....14
III) Ferramentas para a polícia....15
Interceptações administrativas e judiciais []....15
Caixas pretas....16
Em custódia / audiência / investigação....16
IMSI-catcher - estações rádio-base falsas []....17
Pesquisa inicial []....18
The Kiosk - extrator telefônico....18
Equipes de tecnologia da polícia []....20
Exploração de violações de segurança....21
Notebook do analista e software de análise de dados []....22
Tentativa de restaurar dados de dispositivos danificados []....23
Instalação de bugs (hardware ou software) []....23
IV) Redução de riscos....24
1) Hábitos []....24
2) Aplicativos gratuitos....25
3) Configurações do smartphone....30
4) Ter um telefone com um cartão SIM "anônimo" []....32
5) Dicas técnicas avançadas / diversas para smartphone....33
Léxico....35
Recursos adicionais....35

Introdução

Este texto baseia-se principalmente em um relatório de um curso de treinamento sobre a questão da telefonia móvel, complementado com fragmentos encontrados na Internet, pois há uma falta geral de recursos sobre essa questão nos círculos ativistas. Algumas partes tratam dos problemas de vigilância policial relacionados à telefonia em geral (e são simbolizados no início do capítulo por [📞] e no índice por []). Essas partes tratam de problemas tanto para telefones com botão quanto para smartphones. Outras partes tratam de além de smartphones (📱). As palavras com um * são explicadas em um glossário no final do folheto.

Existem mais ferramentas de redução de risco para smartphones, mas se encontram os mesmos problemas se aplicam aos telefones com botão, e os smartphones também têm outros problemas de segurança. Às vezes, as ferramentas oferecem uma sensação de segurança que faz com que você se esqueça de suas limitações e o leva a divulgar informações confidenciais que seria melhor usar por outros canais.

Embora o foco deste documento seja friamente as questões de vigilância e ferramentas de segurança em relação à repressão estatal, essas questões podem ser abordadas de outros ângulos, seja para uso coletivo ou individual:

- Ecologia e colonialismo porque são necessários 70 materiais diferentes e 70 kg de material extraído e montado por pessoas mal pagas em países colonizados pelo capitalismo para construir um smartphone que será rapidamente destruído[1]
- Resistência à pressão para usar cada vez mais essas ferramentas, para trabalho ou administração, serviços bancários, procedimentos de saúde e outros, e que muitas vezes há muitos truques para passar adiante, de modo a não ter que fornecer um número de telefone ou poder ficar desconectado·e
- Que essas ferramentas também são fontes de exclusão para as pessoas que não têm ou não desejam ter acesso a elas, ou que não possuem habilidades. É importante que nos coletivos haja discussões sobre esses assuntos para que a segurança não se torne uma ferramenta de dominação para alguns.
- Defesa de dados pessoais contra multinacionais, mesmo que algumas propostas se sobreponham (já que as multinacionais são regularmente solicitadas pelos policiais)[2].

---

[1] Para obter uma análise, consulte o artigo "L'emprunte cachée des smartphones" da France Nature Environnement, por exemplo, mesmo que as posições políticas não vão muito longe.

[2] 2 exemplos: a colaboração do Google, Facebook, Twitter e Microsoft com a Comissão Europeia na luta contra o terrorismo: https://www.laquadrature.net/2019/04/26/reglement- terrorist-first-studies-and-next-steps/, eles têm sua própria lista de pessoas ou conteúdo "terrorista". Ou no site de transparência do Google, é possível ler sobre 20.000 solicitações judiciais por ano da França, 80% das quais levam a dados enviados para o

I) Telefonia móvel e segurança

Conjuntos de antenas telefônicas [📞].

O telefone celular se conecta por meio de ondas eletromagnéticas a antenas/células. A antena então reconhece a validade do cartão SIM e do telefone. O cartão SIM contém um número de identificação (IMSI) que a operadora verifica para autorizar ou não a comunicação com outros telefones.
As antenas não se comunicam diretamente umas com as outras. Elas são o elo entre a rede da operadora e os telefones. As comunicações são transportadas de uma antena para outra por meio de cabos ou, às vezes, por outras ondas, como o Wi-Fi. Além desses cabos e ondas, nossas comunicações passam por computadores (roteadores e similares) que transportam o sinal de um lugar para outro, para novas antenas e para os telefones com os quais nos comunicamos.

Todos esses equipamentos de rede são de propriedade de empresas
empresas privadas que, como todas as empresas, querem ganhar dinheiro ou ter poder. Não se pode confiar no hardware da rede.
As novas tecnologias complementam as antigas, não as substituem.
As tecnologias GSM estão se acumulando: além do 4G e do 5G (e, em breve, do 6G), ainda há o 2G, o 3G e outros, mesmo que haja a vontade de remover o 2G um dia. Essas antenas estão presentes nas cidades, em prédios, às vezes escondidas por tecidos, se não mais geralmente em torres.

As operadoras se comunicam entre si para que você possa ligar da Orange para a Lyca, por exemplo, e vice-versa. As operadoras também têm contratos com provedores de Internet para permitir o acesso à Internet nos telefones de suas redes. Um telefone sempre tenta se conectar a várias antenas para manter a comunicação mesmo quando você se desloca. Mas se você estiver em uma área com apenas antenas livres e tiver uma assinatura da Bouygues, não terá nenhuma recepção. Quando vamos para um país diferente daquele em que temos nossa assinatura, nos conectamos a redes que têm contratos com nossa operadora, isso é chamado de roaming.

https://transparencyreport.google.com/user-data/overview.

Questões específicas para telefones celulares

Os telefones são fabricados por grandes empresas capitalistas. O equipamento fabricado não é gratuito*, não sabemos a lista exata de componentes e como ele funciona. Às vezes, há algumas instruções para consertar peças, mas nunca é possível consertar tudo. Em outras palavras, a receita não é fornecida.

Para os **telefones de botão** em geral, não há muita segurança a se esperar deles. Há telefones de botão com sistemas operacionais que permitem que eles sejam criptografados ou usem alguns aplicativos seguros[3] (nos quais, infelizmente, é difícil ou impossível confiar), e, nesse caso, os mesmos problemas que para os
Os "telefones inteligentes".

Vista explodida de um smartphone com seus diferentes componentes.

Os chamados "telefones inteligentes" ou **smartphones** fazem aquilo para o qual foram criados e nada mais. Eles não são inteligentes! Na realidade, eles são a mesma ferramenta que um telefone de botão: um pequeno computador. Só que o smartphone é mais potente e contém muitos sensores: para medir a velocidade de

[3] Você pode encontrar marcas neste site: https://dumbphones.pory.app/

do movimento, a aceleração, a frequência cardíaca (esse sensor que calcula a frequência cardíaca é tão potente que, teoricamente, poderia reconstituir o som a partir das vibrações, mesmo que o microfone estivesse fechado), a luminosidade do ambiente, câmeras, giroscópio, magnetômetro etc. Muitos smartphones são tão potentes quanto um computador de médio porte ou mais.

Os telefones têm problemas específicos de segurança digital:

- Ao contrário dos computadores, eles estão [*para a maioria dos usuários*] sempre ligados com muitos dados, alguns dos quais você não decidiu ter.

- Não há padrões de hardware para telefones celulares. Os fabricantes de telefones [Samsung, Google, Apple, ...] compram os diferentes componentes (tela, telefone celular, placa Wi-Fi, bateria, etc.) e os montam. Nos computadores, há muito mais padronização e compatibilidade de componentes entre diferentes computadores. Esses componentes são específicos para cada modelo de telefone torna mais difícil ter sistemas operacionais alternativos (mais seguros do que o originalmente instalado ou com uma ideologia menos duvidosa, por exemplo). O hardware é fabricado por empresas privadas que estão sujeitas aos Estados. Os telefones são fornecidos com software proprietário*, há pouco compromisso com a segurança e pouca documentação pública.

- Os smartphones têm várias camadas de software, cada uma com diferentes problemas de segurança:

1. **Os drivers dos vários componentes do telefone:**
   Fornecido pelos diversos fabricantes de componentes, não documentado publicamente

2. **O sistema operacional instalado no smartphone:**
   O sistema operacional é o conjunto de software que executa o telefone (ou computador). Veremos isso mais adiante.

3. **Aplicativos instalados por padrão**
   Geralmente é complicado ou impossível desinstalar/desativar sem quebrar o smartphone.

4. **Os aplicativos que estão instalados:**

Eles trabalham com permissões de acesso ao telefone. Seja no Android ou no iOS, cada aplicativo concede a si mesmo direitos de acesso ao seu telefone. No total, há até 150 permissões possíveis, com aplicativos como o Facebook que

solicita 58 delas. Como não analisamos as permissões solicitadas, eles podem solicitar qualquer coisa e ter acesso ao restante do telefone como quiserem.

Tabela de permissões possíveis no Android:

- **Sensores corporais**: obtêm informações sobre seus sinais vitais.
- **Agenda** : Ler / editar / criar eventos no calendário.
- **Registros de chamadas**: visualize e edite seu histórico de chamadas.
- **Câmera**: usando sua câmera para tirar fotos ou gravar vídeos.
- **Contatos**: acesse/edite sua lista de contatos.
- **Posição**: obtenha a posição (aproximada por GSM ou Wi-Fi, ou exata por GPS) de seu dispositivo.
- **Microfone**: para fazer gravações de áudio.
- **Dispositivos Bluetooth próximos**: os aplicativos podem detectar e se conectar a dispositivos próximos.
- **Telefone**: faça e gerencie chamadas telefônicas, leia o status do telefone, a lista de chamadas, veja quem está ligando, edite a lista de chamadas, adicione correio de voz, use VoIP (voz pela Internet),
- redirecionar/suspender chamadas, ...
- **Atividade física**: obtenha informações sobre sua atividade física (caminhada, ciclismo, número de passos, etc.).
- **SMS**: acesse SMS recebidos e envie SMS.
- **Armazenamento**: carregue/edite fotos e outros arquivos em seu telefone.

No PlayStore, há muitos aplicativos maliciosos (também chamados de malware). Por exemplo, se você pegar um aplicativo com uma conta crackeada do Spotify, poderá obtê-lo gratuitamente, mas é possível que, paralelamente ao Spotify, você tenha instalado um malware (o que não significa que ele fornecerá informações à polícia, mas sim a grupos que revenderão as informações para ganhar dinheiro).

O sistema operacional do smartphone 📱

Há vários deles: Android, iOS, Windows, Blackberry, Ubuntu Touch, /e/, LineageOS, DivestOS, ... Vamos nos concentrar aqui nos dois principais, outros são muito melhores, mas mais técnicos para instalar e não estão disponíveis para todos os modelos.

Problemas específicos dos 2 principais sistemas operacionais de smartphones

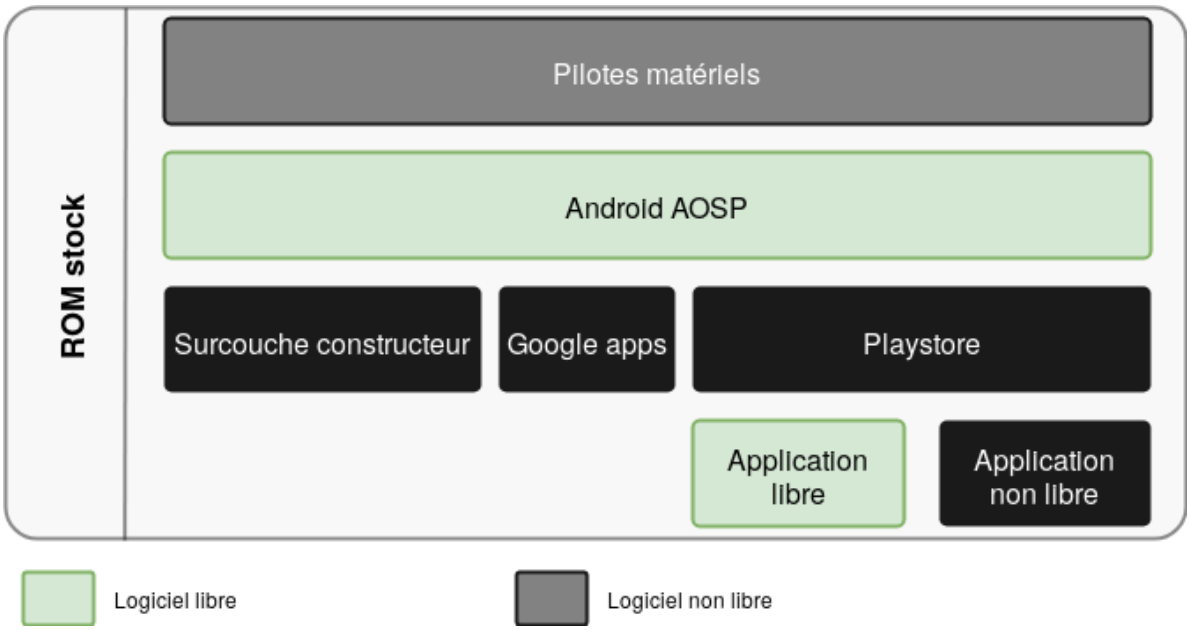
Apple

Ecossistema em que a marca controla tudo. Os engenheiros da Apple criam o iOS (o sistema operacional) e projetam os telefones, os vendedores da Apple os distribuem e as lojas da Apple os vendem e consertam. A Apple controla tudo, do design ao marketing, às atualizações e ao pós-venda...
Problema: esse sistema operacional e seus aplicativos são proprietários*. A Apple está seriamente relutante em proteger os dados do usuário quando a polícia dos EUA pede.
Vantagens: as atualizações do sistema são mantidas por mais tempo, o hardware é de boa qualidade, o sistema é consistente e funciona bem.

A Apple trabalha regularmente com o FBI, embora diga que é segura. Para um hacker, é complicado entrar em um dispositivo iOS, mas para os policiais dos EUA há possibilidades.

Android

Gerenciado pelo Google, há muitas subcamadas, algumas são proprietárias* e outras são mais ou menos gratuitas.



- A base do Android (AOSP) é gratuita, mas o resto que está dentro dela não é: o Google programou uma base gratuita* (depois de tê-la comprado), mas, para tornar seu sistema funcional, é necessário adicionar bases não gratuitas do Google* (GCM/FCM, play store, serviço de geolocalização, youtube, muitas outras coisas...).
- Além disso, os fabricantes de telefones (Samsung) pegam o software Android + Google e adicionam suas porcarias (samsung quies, MiUI, ...)
- Há partes de software dos fabricantes de componentes (geralmente proprietários*), como drivers de Wi-Fi ou outros.

- Às vezes, as operadoras telefônicas também adicionam coisas, como o Orange Music ou outros.

Isso elimina o problema de que, se um dos participantes não fornecer as atualizações, não será possível atualizar o smartphone. Muitos telefones Android não recebem atualizações logo após seu lançamento. Isso significa que as falhas de segurança descobertas ao longo do tempo não são corrigidas.

Existem outros, e isso é discutido na seção "Redução de danos".

II) Os inevitáveis problemas de segurança nos telefones [✆].

O que não pode ser resolvido com telefones no momento:

Geolocalização do telefone [✆]

Um telefone que está ligado (mesmo sem um cartão SIM) é geolocalizado de forma muito simples pelas empresas que controlam as antenas (e, portanto, a polícia pode solicitar determinadas informações a elas).
Em teoria, em um ambiente plano, a geolocalização tem precisão de 50 cm no 4G, de alguns metros a algumas dezenas de metros no 2G e no 3G (mas não temos essas condições teóricas o tempo todo), e o 5G deve permitir uma localização infinitamente mais precisa. Essa geolocalização é independente do GPS. O modo avião corta qualquer conexão com as antenas, de modo que a localização pela operadora se torna impossível.

Diferentes tipos de localização por smartphone

Como o GPS funciona: Os satélites transmitem sua posição. Ativar a localização significa pedir ao telefone que capte esses sinais e, assim, saiba exatamente onde está localizado (estar no subsolo ou em um prédio pode distorcer ou impossibilitar a localização). Os aplicativos podem recuperar essa localização, que tem precisão de poucos metros, mas os satélites não têm conhecimento da localização dos dispositivos.
Antenas telefônicas (2G, 3G, 4G, 5G): o telefone e as antenas estão em comunicação contínua, desde que o telefone esteja ligado (e não no modo avião, com ou sem cartão SIM). As antenas sabem a distância em que o telefone está localizado, ou seja, um raio ao redor da antena. Uma triangulação com 3 antenas permite a localização. Sem essa triangulação, a precisão é baixa (várias 100enas de metros).
Localização por wi-fi: o telefone é localizado pela posição conhecida das redes wi-fi.

Chamadas telefônicas gratuitas e mensagens de texto [✆].

As chamadas e os SMS que enviamos são transmitidos de forma transparente* na rede. Isso significa que seu conteúdo, bem como os metadados* referentes a eles, podem ser interceptados. Na realidade, é um pouco mais complicado porque as comunicações são criptografadas, mas essa criptografia foi projetada para ser desativada por agentes estatais. Seja em 2G, 3G, 4G ou 5G.
Os policiais estão interessados principalmente em metadados, pois isso lhes permite fazer gráficos relacionais, saber quem está "no centro" de um grupo, etc.

Condições para que o telefone pare de se comunicar com as antenas

No modo avião, os telefones não se comunicam mais com as antenas e, portanto, não há geolocalização possível a partir das antenas. Entretanto, é possível imaginar um software mal-intencionado coletando a geolocalização via GPS e transmitindo-a quando o telefone se reconectar à rede.

Quando desligado, o telefone não se comunica com as antenas. Entretanto, às vezes ele pode voltar a funcionar, por exemplo, alguns telefones ligam quando um despertador toca. Ou nosso bolso pode pressionar o botão liga/desliga do telefone... Também podemos imaginar um software malicioso instalado no telefone que o liga novamente ou faz com que pareça estar desligado. Mesmo que não pareça ser frequente, a melhor maneira de se proteger contra isso é remover a bateria. Alguns modelos de telefone não permitem que a bateria seja removida. Você também pode embrulhar o telefone em cerca de quinze camadas de papel-alumínio para isolá-lo das ondas.

Observe que um telefone ligado sem um cartão SIM ainda se conecta à rede telefônica, para que possa pedir ajuda. Na França, essa função foi desativada pela maioria das operadoras há muitos anos, mas o telefone ainda se conecta à rede.

Identificação do telefone [📞] IMEI / IMSI

Quando o telefone se conecta a uma antena, ele transmite os identificadores IMSI do cartão SIM, bem como os identificadores IMEI do telefone. O IMSI (International Mobile Subscriber Identifier, Identificador Internacional de Assinante Móvel) é um dos identificadores que permitem que a operadora verifique se o cartão SIM está autorizado a se comunicar em sua rede.

O número IMEI (International Mobile Equipment Identity) é um identificador exclusivo por slot de cartão SIM de cada telefone. Ele está vinculado à marca do telefone, bem como ao modelo específico, às vezes até à cor da caixa. É usado para bloquear um telefone quando ele é dado como roubado (embora isso raramente seja implementado).

Esse identificador é armazenado permanentemente no telefone. Ao contrário dos endereços MAC das placas WiFi ou ethernet dos computadores, não é possível falsificar o IMEI de um telefone (bem, é *quase* impossível, embora estejam começando a surgir possibilidades). Você pode descobrir os números IMEI de um telefone discando *#06#. O IMEI é uma sequência de 15 a 17 dígitos que inclui :

- Os dois primeiros dígitos indicam o país de fabricação
- Os seis dígitos a seguir representam o número de série

- O último dígito é um dígito de autenticação e, portanto, serve como uma chave de segurança.

Na França, as operadoras mantêm as informações de conexão por um ano. Isso significa que as informações sobre qual IMSI estava em qual IMEI são mantidas durante todo esse tempo. Junto com isso, a lista de antenas às quais um telefone foi conectado e as datas e horários correspondentes também são mantidos. Outras informações são mantidas, mas falaremos sobre isso mais tarde.

Portanto, é fácil para as operadoras (e, portanto, para a polícia) ter a lista de telefones que foram usados para tal e tal cartão SIM ou tal e tal número, bem como a lista de cartões SIM que foram conectados a tal e tal telefone.

Se houver vários slots SIM em um telefone, eles devem ser considerados vinculados. Na Internet[4] é possível encontrar os diferentes IMEIs do mesmo telefone e, às vezes, também a cor da capa, a marca, as dimensões, as informações básicas do telefone etc. Portanto, se houver 2 cartões SIM no mesmo telefone, as operadoras poderão saber facilmente que é o mesmo telefone que usa os 2 cartões SIM

As operadoras de telefonia são legalmente obrigadas a excluir essas informações de identificação após um ano. Não há 100% de garantia de que isso será feito e, se as informações das operadoras tiverem sido fornecidas a serviços de inteligência, como a DGSI (Direction Générale de la Sécurité Intérieur), é provável que esse órgão mantenha os dados por mais tempo.

A partir do número de telefone, pode ser possível estimar a operadora com a qual você está, os 4 dígitos após 06 / 07 são atribuídos a estes[5]. Entretanto, com a portabilidade do número, pode ser mais complicado do que isso, pois é possível mudar de operadora mantendo o mesmo número.

Faturas detalhadas

Essas são todas as informações que não são o conteúdo real da conversa: as faturas detalhadas mencionam números, datas, horários e durações da comunicação. As operadoras mantêm as "faturas detalhadas" por 5 anos porque se trata de outra legislação: a legislação tributária. Esse tempo corresponde ao período durante o qual as faturas podem ser contestadas. Mas a estrutura jurídica não permite, em teoria, que os policiais solicitem acesso além de um ano.

30.000 policiais tiveram acesso ao software *DeveryAnalytics Telephony Data* desde junho de 2022 que pode ajudar na análise de fadettes e outros dados de massa[6].

---

4 Por exemplo: https://www.imei.info/

5 Consulte a lista de prefixos de operadoras telefônicas: https://fr.wikipedia.org/wiki/Liste_des_pr%C3%A9fixes_des_op%C3%A9rateurs_de_t%C3%A9l%C3%A9phonie_mobile_en_France

A nova jurisprudência da Cour de Cassation de 12 de julho de 2022 pode permitir que o uso de provas obtidas de fadettes seja contestado em determinados contextos.[7]

Violações e atualizações de segurança 📱

Nenhum software é perfeito e, enquanto houver software, haverá falhas de segurança. A existência de falhas não significa que as pessoas as estejam explorando, mas é preciso ter em mente que o software sempre foi atacado e será novamente. Mesmo o melhor software de segurança, mesmo que os melhores engenheiros do mundo tenham trabalhado nele.

Alguns exemplos de falhas de segurança descobertas nos últimos anos:

Em 2015: no Android, era possível receber um MMS adulterado que dava acesso a áudio e vídeo e ao cartão SD do telefone.

Em 2019: no iOS, quatro falhas de segurança permitiam que um telefone fosse controlado, levando o usuário a se conectar a um site malicioso; no Android, era possível acionar um sinal de atendimento de chamadas [8]

Em 2020: no Android 8 e 9 e na maioria dos Linux, com o bluetooth ligado, mas não conectado, um invasor poderia assumir o controle e sugar todos os dados. Essa falha foi corrigida, mas muitos telefones nunca recebem atualizações e, portanto, continuam vulneráveis... Para se proteger disso, é preciso desligar o bluetooth.

Como já mencionado, as falhas de segurança sempre serão descobertas. Às vezes corrigidas antes de se tornarem públicas, às vezes usadas por adversários por vários anos antes de serem corrigidas. É por isso que é extremamente importante aplicar atualizações sempre que possível, seja em nossos computadores ou em nossos telefones. É importante que os aplicativos e o sistema operacional que usamos sejam monitorados ao longo do tempo, que a equipe de desenvolvimento corrija todas as falhas de segurança que forem descobertas. Em termos de confiança, podemos descobrir a capacidade de resposta dos desenvolvedores quando uma falha é conhecida e como eles se comunicam sobre ela. Isso pode ser um fator determinante na escolha do sistema operacional ou dos aplicativos.

---

6 O site do produtor do software: https://deveryware.com/marches/securite-interieure/data- analytics/

7 https://www.courdecassation.fr/toutes-les-actualites/2022/07/12/enquetes-penales-conservation-et-access-to-login-data

8 Fonte: https://www.cvedetails.com/cve/CVE-2019-17191/

Você pode saber por quanto tempo alguns sistemas operacionais são rastreados neste site: https://endoflife.date/android

Cartão SIM e dados do telefone [📞]1

Em caso de acesso físico ao cartão SIM e ao telefone:
- A ativação do código PIN do cartão SIM pode dificultar o acesso dos policiais básicos a determinadas informações. Entretanto, esse código PIN é facilmente contornado pelo código PUK que os policiais podem solicitar às operadoras. Os dados armazenados no cartão SIM podem então ser recuperados. Não é possível proteger com segurança os dados armazenados em um cartão SIM (IMSI, contatos, etc.).

- Os dados de um telefone não criptografado* podem ser acessados por ferramentas que veremos no próximo capítulo.

A comunicação é algo de grupo [📞]

Em geral, a comunicação é algo grupal. As ferramentas e práticas que você escolhe usar em seu lado não são necessariamente as mesmas para os outros. Se eu tiver o telefone mais seguro do mundo, mas meus colegas me ligarem para perguntar se vou a uma reunião hoje à noite, as práticas deles podem tornar as minhas obsoletas.

- Não se sinta infalível por ter criptografado seu telefone ou por ter boas práticas a seu favor.
- As práticas coletivas devem ser discutidas em conjunto e é importante apoiar uns aos outros na criação de ferramentas.
- A seguir, há uma série de dicas de autodefesa digital; talvez seja mais cômodo seguir passo a passo para que seja acessível aos poucos.

III) Ferramentas da polícia

Interceptações administrativas e judiciais [↘]

Temos elementos de práticas usadas em processos judiciais para tudo relacionado à polícia, mas é complicado conhecer as práticas reais dos serviços de inteligência[9].

A polícia pode requisitar operadores, seja durante um evento ou depois. Há uma série de opções disponíveis para eles[10]. Elas podem se aplicar:

- em uma antena específica: identificadores IMEI e/ou IMSI que foram vinculados a tal e tal antena em tal e tal momento.
- em um telefone ou cartão SIM específico: dados fornecidos à operadora, como endereço de e-mail, dados bancários ou identidade, geolocalização em tempo real, histórico de cartões SIM colocados em tal telefone, lista de telefones que foram usados para um determinado cartão SIM, histórico de chamadas e SMS enviados (mas não o conteúdo, se não houve escuta), escuta em tempo real (envia a chamada de volta para o telefone de um policial em paralelo), faturas detalhadas, sites visitados (nem sempre é possível e, em muitos casos, diz respeito apenas aos domínios visitados, não às páginas exatas), código PUK, etc.
- em uma pesquisa de cada operadora para obter o número de telefone a partir da identidade de uma pessoa. Isso exige que os policiais verifiquem os números recuperados por esse método (homônimos, nomes falsos...)
- para identificação em massa: a polícia solicita a identidade associada a várias centenas de números de telefone ao mesmo tempo, por exemplo. Os atrasos são da ordem de uma hora.

Essas requisições devem passar pela PNIJ: plataforma nacional de interceptações judiciais - que automatizou e simplificou muitos procedimentos[11].

---

9 É possível pesquisar os relatórios da CNTCR - Commission nationale de contrôle des techniques de renseignement - para obter as informações que eles desejam fornecer: https://www.cnctr.fr/8_relations.html

10 Você pode se divertir examinando as diferentes possibilidades oferecidas aos policiais, com os preços de cada operação aqui, por exemplo, para a data de 2016: https://docplayer.fr/72431284-Memoire-recapitulatif-de-f frais-de-justice.html

11 Em um comentário do Ministro da Justiça no final de 2018, que dá a dimensão da plataforma: "O PNIJ está agora totalmente operacional e é usado por mais de 60.000 juízes, investigadores e funcionários do tribunal. Ele processa mais de 11.000 interceptações simultâneas e 6.000 solicitações de

Dados facilmente obtidos remotamente pela polícia

- Dados de identificação
- Identificador do cartão SIM
- Faturas detalhadas
- Escutas

Marcação de limites e geolocalização

Embora as operadoras de telefonia sejam obrigadas a monitorar as antenas às quais um telefone está conectado - e, portanto, uma geolocalização aproximada -, elas não são obrigadas a monitorar automaticamente os locais das transmissões telefônicas simples para localizá-lo. Para a operadora, há um local associado a cada mensagem de texto, chamada ou pacote de dados (ou seja, todas as conexões telefônicas com a Internet) enviado ou recebido. Além da geolocalização em tempo real e do coletor de IMSI, as localizações obtidas por requisição policial estão vinculadas às comunicações (com outros telefones ou servidores).

Caixas pretas 📱

As caixas-pretas são equipamentos de vigilância algorítmica que estão sendo gradualmente desenvolvidos e usados por agências de inteligência (Direction Générale de la Sécurité Intérieure). Esses algoritmos estão sendo desenvolvidos para telefonia e também para tecnologia digital. Eles realizam vigilância em massa da população e emitem alertas, e em 2020 emitiram 1.739 alertas de pessoas com comportamento "suspeito".[12].

De modo geral, elas são usadas para obter uma lista dos sites que visitamos. As caixas pretas fazem o processamento automatizado de dados. Não está claro como elas funcionam, mas elas não podem saber exatamente quais páginas você visita quando o site está em https (com o s[ecurised] no final - a maioria dos sites). Juntamente com outros métodos de monitoramento, isso pode ser usado para criar gráficos de perfil.

Em custódia / audiência / investigação 📱

Durante a custódia policial, nosso direito ao silêncio é limitado pela "obrigação de fornecer o acordo de criptografia". Essa obrigação se aplica especialmente a

serviços por dia. Ele intercepta cerca de 800.000 chamadas e 1,2 milhão de mensagens SMS por semana. https://questions.assemblee-nationale.fr/q15/15-13319QE.htm

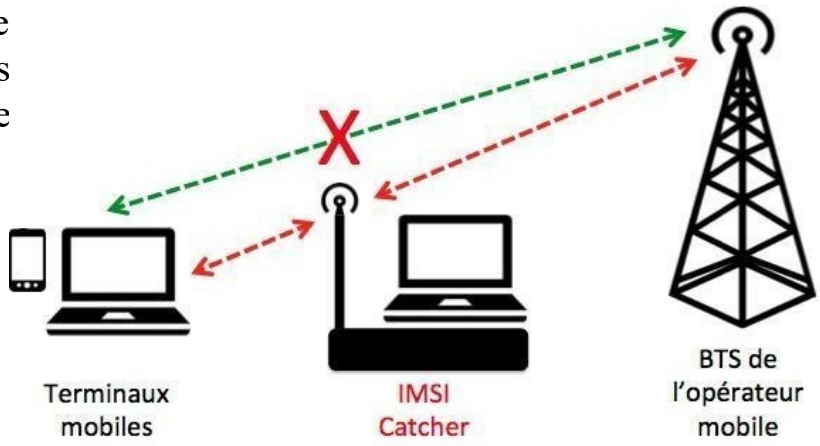
12 https://www.nextinpact.com/article/69817/6-000-comptes-informatiques-sont-connectes-aux-grandes-teaching-ears

telefones, se a solicitação for feita dentro de sua estrutura. Nesse caso, a recusa em fornecer as senhas pode, por si só, acarretar o risco de ação legal. A estrutura para tal solicitação a ser feita a nós é a seguinte:

- a solicitação deve ser feita por um oficial de polícia judicial (não um policial "básico") supervisionado por um magistrado - um promotor ou juiz de instrução.
- deve ser justificada, deve ser demonstrado que o telefone usa métodos de criptografia e que o desbloqueio poderia fornecer acesso a material relevante para a investigação em andamento (por exemplo, "a investigação deve ter identificado a existência de dados processados por meios criptográficos que possam ter sido usados para preparar, facilitar ou cometer um crime ou delito"). Se não parecer que houve uma investigação completa, não deve ser possível condenar por isso.
- é necessário demonstrar que você conhece esse código de desbloqueio.

Tudo isso deve ser explicitamente formulado para que seja aceito em uma estrutura legal. Se a evolução judicial não for na direção certa com o passar do tempo, **ainda assim é aconselhável aplicar as mesmas regras que normalmente se aplicam à custódia policial "não tenho nada a declarar" no caso de uma solicitação de código de desbloqueio** (e não "não sei" ou qualquer outra coisa)[13]. Esses processos não parecem ser frequentes, e geralmente são usados como uma acusação para complementar outras acusações. A vantagem de exercer seu direito ao silêncio é que você poderá escolher sua defesa em caso de processo, pois há muitas possibilidades.

Esse é um dispositivo que se disfarça de relé antena, que capta todas as conexões telefônicas em um raio definido. Ele pode ser transportado em um veículo.
Sua função é listar os dispositivos telefônicos aparelhos telefônicos



[13] Consulte o artigo de maio de 2021 "New developments on the obligation to give one's telephone code in police custody: how to avoid the trap" (Novos desenvolvimentos sobre a obrigação de fornecer o código telefônico sob custódia policial: como evitar a armadilha) https://paris-luttes.info/du-nouveau-sur-l-obligation-de-15018 disponível em formato de brochura em https://rajcollective.noblogs.org/materiaux-a-diffuser/

em torno dele. Ele também pode interceptar conteúdo não criptografado*, como chamadas e SMS, mas é usado principalmente para recuperar metadados*: qual telefone Isso pode ser feito por meio do uso de um "terminal" (presente no raio definido), que telefone liga para qual outro telefone e em que horário, etc.

A polícia coleta os números IMSI e IMEI e pode fazer consultas às operadoras para descobrir quem é o proprietário. Eles também podem ver os sites que você visita (mas o https protege o que é feito nos sites que você visita, quando funciona). Um capturador de IMSI não permite que você assuma o controle de um telefone ou extraia dados dele remotamente. O preço de um capturador IMSI de qualidade profissional é de cerca de 2.000 euros. Por 50 euros, você pode fazer um para si mesmo, mas ele terá um raio pequeno de eficiência e ferramentas precisarão ser encontradas para decifrar o comunicações, mas será fácil ver os IMEIs e outras informações ao redor.

Pesquisa inicial [📞]

Existem várias estruturas legais para uma busca, portanto, quando isso acontecer, talvez valha a pena perguntar em qual estrutura você está (investigação preliminar, flagrante, instrução). Se for uma investigação preliminar, você pode recusar a busca, o que os policiais não especificarão. Não vamos nos aprofundar nessa parte, mas há um guia chamado "Preparing for a search" (Preparando-se para uma busca) disponível aqui: https://rajcollective.noblogs.org/materiaux-a-diffuser/. O que não foi atualizado nesse guia é que, há alguns anos, é possível ter um advogado presente durante uma busca (no entanto, o momento em que ele chega não suspende a busca).

The Kiosk - extrator telefônico

Fabricado pela empresa israelense Cellebrite, O Kiosk é vendido para agências estatais. É uma versão com tudo incluído de sua ferramenta "UFED". 500 Kiosks foram comprados na França para os policiais, a 8.000€ cada um, para serem instalados até 2023. Como resultado,

ele não é usado o tempo todo. É um computador com tela sensível ao toque, com botões grandes e muitos fios: ele tentará sugar o conteúdo do telefone e gerar relatórios que sejam válidos aos olhos dos magistrados (análise forense). Em seu site, você pode encontrar as "notas de lançamento"[14]que contêm listas de telefones que eles conseguem quebrar, listas de aplicativos compatíveis com a extração de dados e outras coisas divertidas.

Para funcionar, o UFED explora brechas de segurança na parte do sistema operacional que lida com a porta USB. Essas falhas de segurança podem já ser públicas ou descobertas pelos engenheiros da Cellebrite. Outros podem ser comprados na Internet p o r valores que variam de algumas dezenas de milhares a vários milhões de euros, o que não é muito para esse tipo de empresa.

A empresa promete muitas coisas com esse dispositivo, inclusive ignorar o código de desbloqueio de tela na maioria dos telefones (portanto, quando o telefone estiver ligado). Ele também promete descriptografar muitos telefones, especialmente os da marca Samsung. Entretanto, sua comunicação é muito mercadológica, e parece que muitas de suas promessas não são realmente aplicáveis.

O que é certo é que o UFED pode ignorar os códigos de desbloqueio de telefones não criptografados* ou criptografados*, mas ligados, e clonar o cartão SIM.

Le tableau ci-après montre des exemples d'informations susceptibles d'être collectées dans différents matériels de téléphonie :

Téléphone portable	Smartphone (iPhone, Android…)	Tablette (iPad, Android…)
- Liste de contacts - Messages GSM (SMS) - Journal d'appels - Calendrier - Notes personnelles - Photographies …	- Liste de contacts - Messages GSM (SMS-MMS) - Messageries Internet (WhatsApp, Skype, Facebook Messenger, Telegram, SnapChat, Signal…). - Journal d'appels - Photographies - Vidéos - Géolocalisation - Traces de navigation Internet - Agendas - Notes personnelles - Documents - Messagerie électronique …	- Liste de contacts - Messageries Internet (WhatsApp, Skype, Messenger, Telegram, SnapChat…). - Photographies - Vidéos - Géolocalisation - Traces de navigation Internet - Documents - Agendas - Notes personnelles - Messagerie électronique …

[14] https://cellebrite.com/fr/mises-a-jour-des-produits/

Equipes de tecnologia da polícia [].

Ao longo deste texto, falamos sobre policiais, mas, na realidade, há muitos órgãos diferentes dentro da polícia e do sistema judiciário, que têm diferentes significados em termos técnicos.

A maioria dos órgãos técnicos precisa extrair informações do telefone sem degradar o telefone ou deixar vestígios da invasão no telefone, o que é chamado de "análise forense".

Tipo de rota possível durante uma investigação: Há uma célula trabalhando em uma instrução, que envia o IRCGN (Institut de Recherche Criminelle de la Gendarmerie Nationale) para o departamento de informática e eletrônica, cuja missão é extrair o conteúdo de um telefone e armazená-lo em um disco rígido. Ele também pode viajar e estar presente durante as buscas. Se essa instituição for bloqueada por uma mídia criptografada, ela pode decidir enviá-la ao CTA (centro de assistência técnica). Se as informações forem extraídas, elas serão enviadas de volta à unidade de investigação.

- O **Institut de Recherche Criminelle de la Gendarmerie Nationale**, que tem status militar e inclui o Departamento de Informática, é a única instituição do país a ter um sistema de informática. (INL). "*Este último lida com evidências digitais em todos os tipos de mídia, especialmente em discos rígidos e telefones celulares. Fornece perícia forense e exames científicos para magistrados e investigadores, e também pode auxiliá-los em campo ou remotamente, durante buscas ou audiências em ambientes complexos.* Possui investigadores de tecnologia digital (N- Tech), que são gendarmes, com treinamento de policial e também em 14 meses na UTT em Troyes.

- **O Centro de Assistência Técnica** :
"[...] *o Estado teve um*
O Centro de Assistência Técnica (CTA) é um órgão interministerial vinculado ao Ministério do Interior e agora está sob a autoridade da DGSI. Ele está a serviço dos magistrados e investigadores que o solicitam e constitui um nível superior de intervenção técnica disponibilizado a eles para aumentar as chances de sucesso de suas investigações quando delinquentes e criminosos têm usa criptografia. . O CTA está coberto pelo sigilo de defesa e tem o direito de usar técnicas que podem destruir o material a ser estudado.

O IRCGN pode ser substituído por empresas de engenharia subcontratadas, como

- Tracip: https://www.tracip.fr/
- Computação jurídica https://informatique-legale.com/
- Laboratoire évidences SAS: https://evidences-lab.com/

Mais informações sobre as equipes técnicas:

- "Blog de um ex-especialista em informática": https://zythom.fr/

- "the french intelligence", compilação de textos sobre a inteligência francesa: https://infokiosques.net/spip.php?article1821

Exploração de brechas de segurança 📱

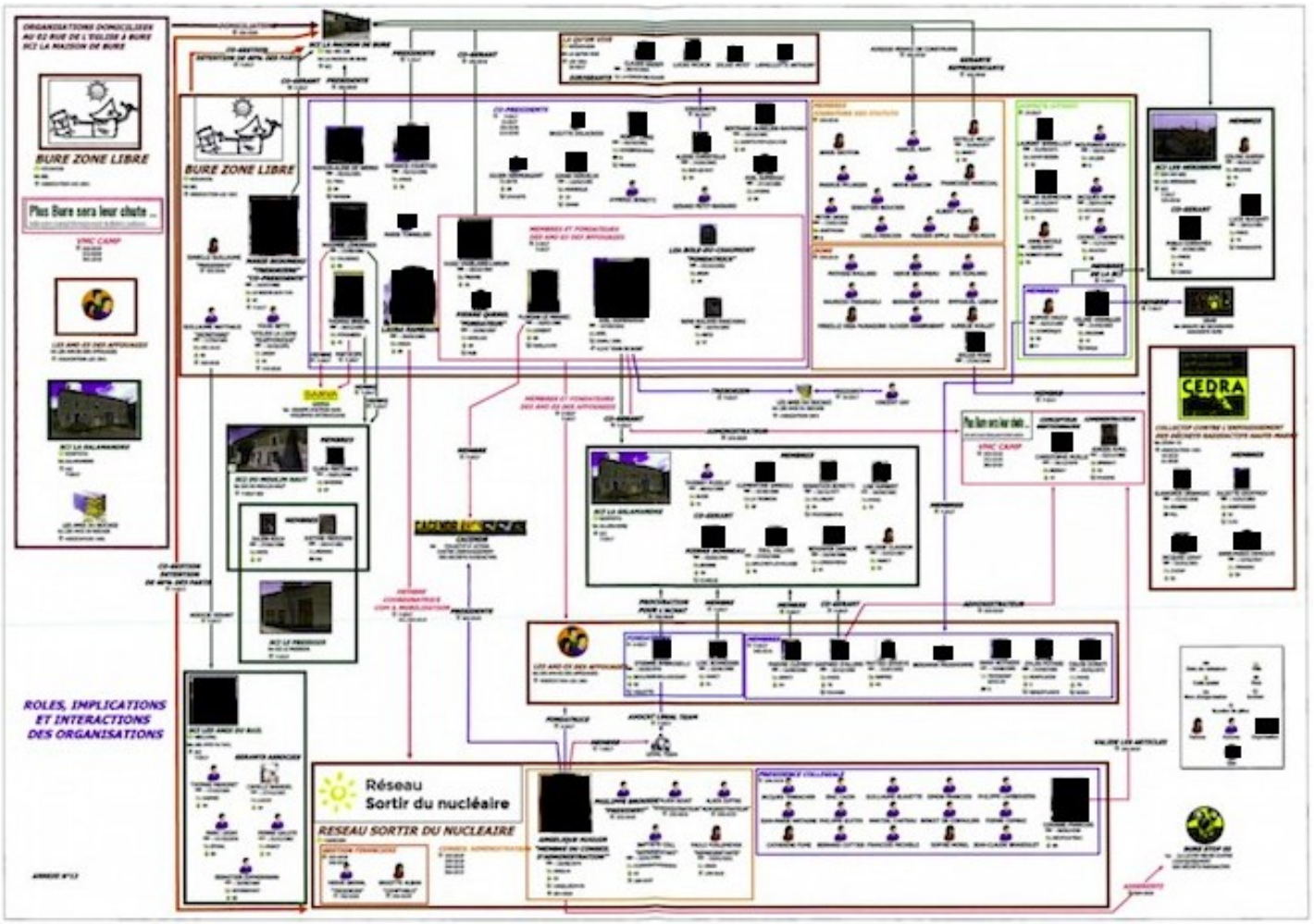
Parece que isso é bastante praticado pelo Centro de Assistência Técnica (CTA). Por exemplo, o CTA pode extrair determinadas informações de Iphones 5 a X criptografados (imagens ou informações de geolocalização de determinados aplicativos, informações de conexão com redes Wifi ou Bluetooth etc.).[15]

15 Se você quiser obter mais informações técnicas sobre esse assunto, trata-se do método "BFU" (Before First Unlock) https://blog.elcomsoft.com/2019/12/bfu-extraction-forensic-analysis-of-locked-and-disabled-iphones/

Analyst's Notebook e software de análise de dados [↘]

Software oferecido pela I2, um subgrupo da IBM, a gigante dos microprocessadores. É usado pelo Serviço Central de Inteligência Criminal com o nome de ANACRIM para “analista criminal” (cujo nome é frequentemente confundido entre o da equipe da gendarmaria e o do software).

Os policiais usam uma ferramenta de análise que lhes permite fazer gráficos de quem fala com quem e injetam no software todas as informações coletadas principalmente de comunicações telefônicas (seja sobre pessoas, lugares, eventos ou materiais). Assim, nas investigações sobre ativistas, eles tentam destacar os "organizadores" de tal e tal movimento que estão em contato com muitos ativistas, ou pessoas que fazem ligações entre vários universos.



Exemplo de um gráfico feito pelo software Analyst's Notebook em uma pesquisa em Bure.[16] Esse gráfico, baseado nas comunicações entre as pessoas, permite classificar cada pessoa em supostos papéis com relação à luta.

[16]Informações disponíveis no artigo https://reporterre.net/La-justice-a-massivement-surveille-les-militants-antinucleaires-de-Bure, que desenvolve as ferramentas de vigilância usadas na estrutura da investigação da associação de malfeitores em Bure, incluindo muitas sobre telefonia.

Tentativa de restaurar dados de dispositivos danificados [↘]

Dar detalhes específicos sobre isso é complexo, mas há forças policiais que tentam recuperar dados de mídias digitais quebradas ou parcialmente queimadas[17]. Essas técnicas parecem ser usadas em casos maiores.

Instalação de bugs (hardware ou software) [↘].

É possível que isso seja feito no contexto da inteligência. Por exemplo, a instalação de um bug que monitora o que está acontecendo em outros aplicativos ou a ativação de microfones remotamente. As falhas podem ser de hardware, o que requer acesso ao dispositivo, ou de software, instalando malware remotamente ou a partir do dispositivo.

17 https://www.nextinpact.com/article/29762/108071-la-nouvelle-arme-anti-cryptographie-gendarmerie

IV) Redução de riscos

Cuidado: este capítulo evolui de forma particularmente rápida ao longo do tempo. Acompanhe como ele evolui ao longo do tempo.

Você pode encontrar essa parte no wiki https://telmob.0id.org/. Esse é um wiki, portanto, é possível contribuir/modificar.

A segurança absoluta para telefones é impossível, o que queremos é reduzir o risco de roubo de dados.

O importante é pensar/entender as ameaças que se aplicam a nós individual e coletivamente. Para reduzir os riscos e ter mais controle sobre nossas comunicações, temos várias ferramentas à nossa disposição.

Essas ferramentas podem ser divididas em algumas categorias:

- hábitos, formas de usar o telefone, usos de questionamentos

- escolha de aplicativos

- Configurações do telefone

- ter um telefone "anônimo

- coisas de nerd (técnicas)

1) Hábitos [✎]

O nível de hábito é o mais importante, pois, como vimos, o uso de telefones celulares envolve muitos problemas inevitáveis.

* O primeiro hábito é fazer as perguntas certas. A "modelagem de ameaças" é uma ferramenta que nos permite escolher respostas adaptadas às nossas necessidades. É uma ferramenta que deve ser experimentada e usada individual e coletivamente, pois nossas escolhas terão consequências para as pessoas ao nosso redor.

→ Quem são nossos inimigos em potencial (policiais sob custódia, agente de inteligência atrás de seu computador, agente na mira, fascistas, vizinhos, coabitantes...)

→ O que queremos ocultar deles (lista de contatos, membros de um grupo de sinal, conteúdo de mensagens, localização, sites visitados, documentos salvos...)

→ O que arriscamos se falharmos (sermos repreendidos, perdermos nossos dados, sermos multados, irmos para a cadeia...)

→ Que recursos nossos inimigos estão dispostos a colocar contra nós ou contra nossas atividades (conformidade legal ou não, quantidade de dinheiro disponível, proteção legal...)
→ Quanta energia precisamos investir para nos proteger?

Alguns hábitos para colocar em prática, se isso fizer sentido para nós:

* Pergunte a si mesmo todas as vezes como passar sem o telefone, se possível (também conhecido como "Deixe o telefone em casa")
* Tornar alguns usos inhabituais, como o modo avião, algo habitual
* Armazene o mínimo possível no telefone (documentos, fotos, contatos, mensagens). Pense na transferência de fotos e arquivos e coloque-os em um computador confiável ou em um dispositivo USB criptografado*.
* Faça monitoramento político e tecnológico, treine-se ou tenha um coletivo que se forme. Os telefones evoluem muito rapidamente!
* Treinamento coletivo em caso de custódia policial: história em quadrinhos "Não tenho nada a declarar" em https://infokiosques.net, ou "Manual de sobrevivência em custódia policial", livro "Como a polícia questiona e como se defender" em https://projet-evasions.org/
* Ter telefones diferentes para finalidades diferentes. Tenho um telefone de trabalho, um telefone militante que não ligo em casa, de preferência. Complexo de aplicar, mas interessante. Também é possível que isso possa ser resolvido coletivamente: que o coletivo forneça telefones anônimos para uma tarefa específica na luta.
* A NSA disse "reinicie seu telefone uma vez por semana". Se houver uma vulnerabilidade explorada, mas não gravada no telefone, ao reiniciar, a vulnerabilidade não estará mais lá.
* Não ter um telefone :)

2) Aplicativos gratuitos 📱

Como vimos, os aplicativos têm grande poder de monitoramento. É por isso que se pode optar por usar aplicativos "confiáveis".
Mas então precisamos definir o que significa "confiança" e como ganhar essa confiança. A confiança em um aplicativo pode se manifestar em diferentes lugares:
* segurança "o aplicativo faz o que diz e diz o que faz"
* Confiabilidade ao longo do tempo: as pessoas continuam a trabalhar nele para corrigir vulnerabilidades?
* Verifique a reputação das pessoas que desenvolvem o software.
* Verifique o modelo de negócios do software.

Uma tendência quando se trata de segurança é usar software gratuito*. Por que isso acontece?
* Com um aplicativo proprietário, não será possível verificar profundamente a qualidade do aplicativo em termos de segurança, e os desenvolvedores podem decidir interromper o desenvolvimento do aplicativo sem aviso prévio. Um aplicativo de código aberto* permitirá que uma comunidade examine sua operação e, com sorte, retome o desenvolvimento se a equipe original sair.
* Um aplicativo não gratuito* pode estar deliberadamente buscando causar danos (de forma ampla ou específica), sem ser notado sem ser instalado, porque sua receita não é tornada pública. Os exemplos incluem: Skype, malware e ransomware escondidos em jogos, etc.

/Cuidado, gratuito* ≠ seguro, um aplicativo gratuito* pode conter código malicioso (intencionalmente ou não).
Além disso, alguns aplicativos têm uma reputação baseada em vários elementos:
* a qualidade do aplicativo ao longo do tempo
* Capacidade de resposta à correção de vulnerabilidades
* a reputação da equipe de desenvolvimento
* O modelo de negócios
* fenômenos da moda
Por fim, é importante manter seus aplicativos sempre atualizados para se beneficiar das correções de segurança.

Vamos dar uma olhada em alguns aplicativos, nem todos confiáveis, nem todos atualizados regularmente, mas todos gratuitos*.

Loja de aplicativos :

* F-Droid (oferece apenas aplicativos gratuitos*)
* Aurora Store (interface gratuita* da Google Play Store, que permite usá-la sem uma conta do Google) (lembrete: os aplicativos da Play Store são, em sua maioria, não gratuitos* e podem ser modificados pelo Google).

Aplicativos para proteger a confidencialidade das comunicações:

* Signal (protocolo de criptografia do Signal, conta vinculada a um número de telefone)
* Briar (protocolo de criptografia Briar, não vinculado a um telefone, usa o Tor se você quiser, também funciona sem internet (via Bluetooth)
* Conversations (protocolo de criptografia XMPP/Jabber, originalmente para PC, o aplicativo para Android é, na verdade, melhor do que seus equivalentes para PC)
* Element (protocolo de criptografia de matriz)

* Silence (protocolo de criptografia para SMS - esteja ciente de que o contato permanece visível na rede, ao contrário de outros softwares).

Há também uma comparação de aplicativos feita pelo site nothing2hide de comunicação em vários critérios interessantes (atenção, há alguns erros no comparador, por exemplo, o código-fonte do servidor do telegrama não é absolutamente gratuito* nem de código aberto, por exemplo). Esta página compara o software : briar, conversas, delta chat, Element, Imessage, Jami, Signal, Telegram, Threema, Whatsapp, Wire sobre segurança e privacidade, durabilidade, funções e modos de armazenamento: https://wiki.nothing2hide.org/doku.php?id=formations:smartphones:appcommunications-securisees

Aqueles destinados a proteger a identidade de seus usuários:

* Navegador Tor (para navegar na Web)
* Briar (para trocar mensagens instantâneas criptografadas sem fornecer um número de telefone ou e-mail)
* Conversations (para trocar mensagens instantâneas criptografadas)

Para SMS :

* QKSMS
* Mensageiro SMS simples
* Silence (excelente porque criptografa SMS de Silence para Silence, mas cuidado com o fato de que, durante o uso, alguns SMS não criptografados* se perdem...)
* O aplicativo básico de SMS do Android Open-Source Project

Para e-mails:

* Correio K-9

VPN :

* RiseupVPN
* Mullvad VPN
* CalyxVPN
* Orbot: para configurar outros aplicativos para passar pelo tor (não funciona para todos os aplicativos)

Outros aplicativos de segurança :

* exodus: o εxodus analisa aplicativos Android para listar rastreadores incorporados. Um rastreador é um software cuja finalidade é coletar dados sobre você e seu uso. Assim, os relatórios do εxodus revelam a você os ingredientes do bolo. Também disponível no F-cold.

* Hypatia : Scanner de malware, funciona off-line : https://github.com/Divested-Mobile/Hypatia/blob/stable/README.fr.md

Fotos:

* Câmera aberta
* Obscuracam: que pode ser configurado para desfocar rostos automaticamente.
* Exif misturado
* Cryptocam + OpenKeyChain (criptografia direta de fotos e vídeos com OpenPGP. Requer "Cryptocam Companion GUI/CLI" para abrir vídeos no computador. Requer algum conhecimento e leitura de tutoriais em inglês, em https://cryptocam.gitlab.io)

Vídeos:

* VLC

Leitura de documentos:

* Librera (para ler livros eletrônicos)
* MuPDF (para exibir PDF e outros)
* Visualizador de documentos (para visualizar PDF e outros)
* Bônus: ebooks em massa para download em trantor.is (prefira .onion) e z-lib.org

Conferências audiovisuais:

* Jitsi (áudio/vídeo para vários usuários)
* Plumble (protocolo Mumble, somente áudio)

Calendário/agenda:

* Calendário simples (funciona off-line)
* DAVx⁵ (sincronização remota de calendário, com o Nextcloud, por exemplo. Compatível com o Simple Calendar)

Observações:

* Notas simples (off-line, com um ótimo widget)
* Nextcloud Notes (para sincronizar com um nextcloud)

Firewall:

* Netguard

Isolamento de aplicativos:

* Insular
* Abrigo

Navegação na Web:

* Firefox Focus (por meio do aplicativo FFUpdater; inclui bloqueador de anúncios e rastreador)
* Navegador Tor
* Navegador de privacidade DuckDuckGo

Alternativas ao Youtube/Bandcamp/Soundcloud/Framatube:

* NewPipe
* SkyTube

Mapas:

* Mapas orgânicos (com base no Openstreepmap)
* OsmAnd (idem)

Backup

* OandBackup: permite um backup exaustivo, por aplicativo, do telefone. Mesmo que sua interface seja um pouco austera, você pode fazer backup de tudo com ele, desde que tenha um telefone com root.
* SMS Backup + : complemento do OandBackup para fazer backup de sms

Jogos:

* Lona (espécie de jogo de cobra)
* TowerJump
* Quebra-cabeças (muitos quebra-cabeças estilosos)
* Fuga de coelhos
* Sokoban
* Shattered Pixel Dungeon (exploração)

Uma série de ótimos aplicativos disponíveis no F-Droid: Simple Mobile Tools (https://simplemobiletools.com). Há um calendário, um gerenciador de contatos, um aplicativo de SMS, um aplicativo de notas, uma galeria etc.

Vários aplicativos têm versões para computador, que devem ser consideradas para comunicações entre computador e telefone: Signal (Signal- desktop, axolotl.chat), Conversations (Dino, Pidgin, Gajim, ...), Element (https://element.io/get-started), Tor Browser, RiseupVPN, etc. etc.

Vamos voltar ao Signal

Defeitos :

→ Possível sensação de segurança perfeita (ilusória) que faz com que a pessoa não preste mais atenção ao que está enviando

→ Vinculado a um número de telefone que não pode ser ocultado
→ Centralizado

Opções :

- Nome, Sobre, Foto ⇒ fornecer informações mínimas
- Habilitar mensagens efêmeras e definir um valor padrão
- Defina um PIN (/!\ ) e ative o bloqueio de registro
- Não gerencie SMS/MMS e use um aplicativo dedicado (para evitar confusão)
- Ativação da opção "Always relay calls" (é importante entender as implicações: ela permite que não divulguemos o endereço IP de nossa conexão para os destinatários de nossas chamadas)
- Opção "Link previews" a ser desativada
- Opção "Teclado anônimo" a ser ativada
- Número de segurança a ser verificado com seu correspondente·e·s
- Bloqueio de tela a ser ativado no smartphone
- Segurança da tela a ser ativada

Certifique-se de que as notificações não sejam exibidas se o telefone estiver bloqueado. Verifique regularmente os dispositivos conectados.
No caso de uma ordem judicial contra a Signal, a Signal alega ter apenas a data em que a conta foi criada e a data em que a conta foi acessada pela última vez[18].

3) Configurações do smartphone 📱

Um bom código de criptografia telefônica

Evitaremos o reconhecimento facial (problemático como tecnologia e há falhas) e a impressão digital (é possível forçar a pessoa a colocar o dedo). Esquemas, muitas vezes há traços deixados na tela que permitem que eles sejam refeitos.

Frase-senha: melhor em termos de segurança, mas pode ser difícil de digitar (ajuste o tempo de bloqueio da tela).

Digicode: bom se você tiver um código longo o suficiente. É ainda melhor se você ativar a opção "layout aleatório" disponível em alguns sistemas.

O problema é que o código de criptografia é o mesmo que o código de desbloqueio da tela, o que muitas vezes o obriga a criar códigos mais curtos, pois

18 Em seu site, o sinal diz que fornece às instituições judiciais: https://signal.org/bigbrother/

deve ser digitado com frequência. **Lembre-se de desligar um telefone criptografado antes de digitar para ativar a criptografia**.

Se você quiser salvar seu código em algum lugar, é melhor usar um cofre de senhas como o keepassxc.

Criptografia de rede e comunicação

No nível da rede, é melhor criptografar suas comunicações de ponta a ponta (consulte as dicas de aplicativos) para que o conteúdo não seja divulgado e, para ocultar os sites visitados, use uma VPN ou a rede Tor.

O Android 7 ou superior oferece suporte a um "VPN killswitch" e está disponível sem a necessidade de instalar aplicativos de terceiros. Esse recurso impede vaza se a VPN estiver desconectada. Ele pode ser encontrado em ⚙ Configurações → Rede e Internet → VPN → ⚙ → Bloquear conexões sem VPN.

Desativar recursos não utilizados

Sempre que possível, desative o Bluetooth e os serviços de localização. Às vezes, há botões de alternância para a câmera e o microfone. Quando não estiverem em uso, é melhor desativar esses recursos. Os aplicativos não podem usar os recursos desativados (mesmo que tenham recebido permissão individual) até que sejam ativados novamente.

Android

* Modo USB padrão: somente carregamento
* Depuração USB desativada
* Defina um bloqueio rápido de tela + um bom código de desbloqueio
* Optar por sair do identificador de publicidade direcionada que coleta dados pessoais ou em Configurações → Google → Anúncios ou em ⚙ Parâmetros → Privacidade → Anúncios
* Criptografia do telefone (ativada por padrão desde o Android 10)
* Notificações discretas
* Use as Contas de usuário para separar determinados usos, ou um aplicativo para isolar aplicativos como Insular ou Shelter.

iOS

* Bom código de desbloqueio
* Desativar backups do iCloud
* Desativar a ID de publicidade

* Cuidado com as notificações

⇒ O telefone é criptografado* por padrão, mas às vezes essa criptografia pode ser contornada.

4) Ter um telefone com um cartão SIM "anônimo" [📞]

É possível ter um telefone "anônimo" usando cartões pré-pagos. Há várias marcas: Lycamobile, Lebara, Syma (outras operadoras oferta, a ser testada).

Você recebe um novo cartão SIM e paga em dinheiro em uma tabacaria pelo crédito para abastecer o telefone.

Na primeira vez, é necessário registrar seu telefone: por telefone ou pela Internet. Sempre lhe serão solicitados dados pessoais, mas você pode fornecer informações imaginárias ou fantasiosas, não há verificação. Se for solicitada uma fotocópia da sua carteira de identidade, você pode colocar uma foto falsa ou de uma montanha, que funciona (a ser verificada pela operadora), e se for solicitado o número da sua carteira de identidade, você diz o número correto, mas o altera.

Às vezes, demora um pouco (algumas horas) para entrar em vigor, por isso é bom preparar o telefone com antecedência. Em seguida, você insere um código para obter um pacote. Por exemplo, você pode inserir 40 euros de crédito comprado em uma tabacaria e, com o código, ele debitará mensalmente uma parte do crédito até que não seja suficiente (nesse caso, você terá que inserir o crédito novamente).

Às vezes, é preciso procurar as melhores ofertas. No caso da lycamobile, por exemplo, é preciso digitar *139*3004# para obter um pacote de 5 euros por mês, com telefone e sms ilimitados, mas sem internet, e *139*4099# para obter um pacote de 10 euros ilimitado e um pouco de internet.

Pequenos tipos a serem observados:

- Não use um cartão SIM que tenha sido usado anteriormente com uma identidade que esteja vinculada a você, não coloque seu novo cartão SIM em um telefone que você tenha usado no passado.
- No caso de uma busca, a polícia pode descobrir em qual tabacaria o pacote foi comprado.
- Pense no nível de anonimato que você deseja. Já é importante e não inútil ter um telefone que não esteja vinculado à sua identidade, pois as buscas

  Os primeiros policiais simplesmente farão uma solicitação às operadoras para descobrir a identidade das pessoas por trás de um número IMSI ou IMEI. Eles podem estabelecer outros métodos para descobrir quem está por trás de um número IMSI ou IMEI.

Eles podem conseguir grampear o telefone (escutas, estudar os números contatados com o telefone etc.) ou podem grampear seus parentes para descobrir seu novo número quando você ligar para eles. Mas isso requer mais recursos, portanto, depende do modelo de ameaça.

- Convidar mais pessoas para usar essas técnicas é proteger-se em massa. Se em uma demonstração houver apenas um telefone com cartão pré-pago, isso pode parecer suspeito no caso de uma investigação.

5) Dicas técnicas avançadas / diversas para smartphones

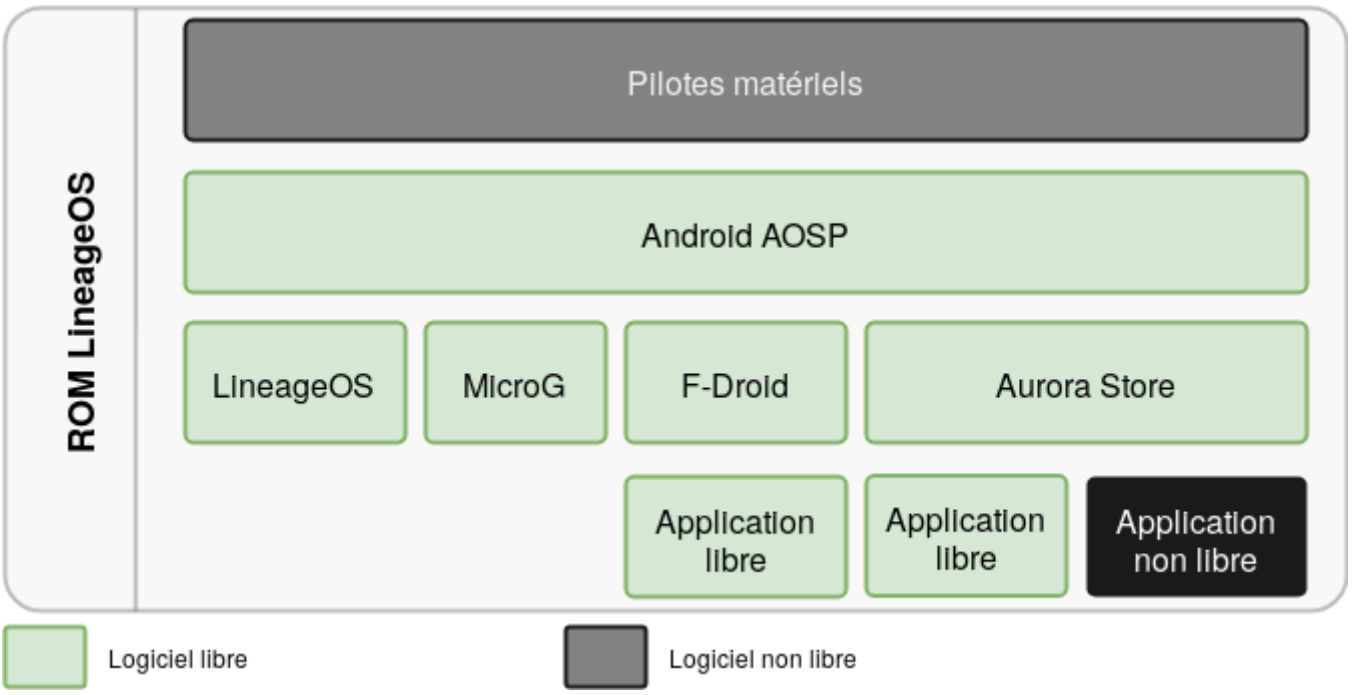
Esse material não é potencialmente muito acessível sem um pouco de habilidade técnica, dedicação ou recursos financeiros. Se houver coletivos de nerds em sua região, vale a pena pedir conselhos a eles.

Alterar o sistema operacional:

⇒ Requer um telefone compatível (lista disponível nos sites dos sistemas operacionais)

⇒Cuidado, isso não resolve os problemas inevitáveis

⇒Sistemas operacionais de código aberto* existentes: LineageOS[19]CalyxOS, GrapheneOS, CarbonROM, /e/, DivestOS Mobile[20], ...



19 Um tutorial muito bom que explica por que e como instalar o LineageOS em um smartphone está disponível nesta página: https://linuxfr.org/news/installer-lineageos-sur-son-appareil-android

20 Modelos de telefones disponíveis: https://divestos.org/index.php?page=devices&base=LineageOS

Use um telefone vendido com um sistema operacional de código aberto*:

* Murena, em https://murena.com, a partir de €330, garantia de 4 anos

Usando um telefone com drivers gratuitos* :

* Fabricar um telefone com material aproximadamente livre*: https://www.instructables.com/ArduinoPhone-20-an-Open-Source-MobilePhone-Based-/

* Compre um telefone grátis*: https://www.pine64.org/pinephone/

* (Não testamos essas duas possibilidades)

Aplicativo SnoopSnitch

Somente para telefones Android: o SnoopSnitch verifica o firmware do seu telefone em busca de patches de segurança do Android instalados ou ausentes. Para telefones Android com root, esse software pode detectar o IMSI catcher.

Raspe o número marcado no SIM (IMSI ou outro) Raspe o(s) número(s) marcado(s) no telefone (IMEI, interno)

Léxico

Software livre vs. software proprietário
Antes de continuar, é importante entender a diferença.
Software livre ou de código **aberto** é aquele em que você tem acesso ao código-fonte, ou seja, pode acessar a receita do software para saber como ele funciona (o software livre vai além, pois oferece a liberdade de modificar, redistribuir, alterar o software, além de ter acesso à receita).
O software proprietário não oferece acesso ao código-fonte. Isso significa que não pode haver aconselhamento externo por parte da empresa que fornece o software proprietário; entregamos 100% da nossa confiança à empresa que criou o software em termos de segurança e respeito aos nossos dados pessoais.

Informações em linguagem simples vs. informações numéricas
Diz-se que a informação é "**clara**" se qualquer pessoa/máquina que tenha acesso a ela puder acessar o conteúdo diretamente.
Diz-se que o conteúdo está **criptografado** se houver uma linguagem (em termos numéricos, um algoritmo matemático) que torne impossível (ou complicado) para pessoas/máquinas que não conheçam o algoritmo descriptografar o conteúdo. Há várias tecnologias/linguagens para criptografia, cujas qualidades variam enormemente.

Metadados : Metadados são o que descreve o contexto em torno dos dados. Em uma mensagem de texto, há os dados que são a própria mensagem de texto, os metadados são o tamanho da mensagem de texto, quem está escrevendo para quem, a que horas, etc.

Recursos adicionais

* Site da La quadrature du net sobre a evolução das leis digitais: https://laquadrature.net
* Surveillance Self-Defense (nem sempre traduzido para o francês): https://ssd.eff.org/
* Segurança de telefones celulares para ativistas e agitadores Segurança de celulares para ativistas e agitadores
* U m guia de autodefesa digital para todos os aspectos do computador: https://guide.boum.org
* Lista softwares livres alternativos (software livre não significa seguro para este que você deseja fazer):

- https://technopolice.be/autodefense-numerique/
- https://www.chatons.org/
- https://prism-break.org/fr/
- https://riseup.net/fr/security/resources/radical-servers

Este livreto tem como objetivo identificar questões relacionadas à vigilância policial de telefones e dar dicas sobre como reduzir os riscos associados a ela.

Esta é a primeira versão deste folheto. Ela contém erros, atalhos, incertezas - além disso, tudo relacionado à tecnologia digital evolui rapidamente. Não hesite em fazer críticas para que este texto evolua, entrando em contato com :

autodefense-numerique@riseup.net