GUIA DE PROTEÇÃO DIGITAL

PARA DEFENSORAS E DEFENSORES DE DIREITOS HUMANOS

justiça global

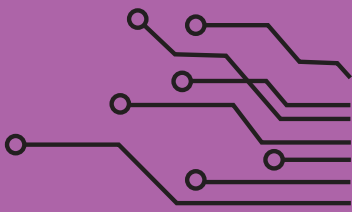
REALIZAÇÃO
Justiça Global

AUTOR
Gabriel Shiozawa Coelho

PROJETO GRÁFICO E DIAGRAMAÇÃO
Rachel Gepp

TIRAGEM
500 exemplares

ISBN
978-65-87127-06-4



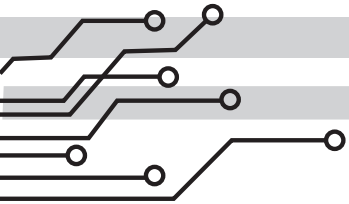
ANO 2022 - 1ª EDIÇÃO

JUSTIÇA GLOBAL
Equipe: Antonio Neto, Daniela Fichino, Daniele Duarte, Danilo Serejo, Eduardo Baker, Emily Almeida, Francisca Moura, Gizele Martins, Glaucia Marinho, Isabel Lima, Leidiane Moreno, Lourdes Deda, Melisandra Trentin, Monique Cruz, Raoni Dias e Sandra Carvalho.

+55 21 2444 2320
contrato@global.org.br
www.global.org.br

Realização

SUMÁRIO



1
INTRODUÇÃO

Segurança: ato ou efeito de segurar; estado do que se acha seguro ou firme, estável; aquilo que nos protege de agentes exteriores; condição marcada por uma sensação de paz e tranquilidade; condição ou estado do que está livre de danos ou riscos.
(Dicionário Michaelis Moderno Português Online. Ed. Melhoramentos, 2022.)

A definição do dicionário já indica que segurança é sempre relativa: **seguro contra o quê? Protegida contra o quê?** O estado de segurança depende de fatores como: quem são as pessoas, quais suas rotinas,suas atuações, com quais pautas lidam e quais interesses contrariam. Portanto, medidas de proteção não serão absolutas: é necessário avaliar as necessidades específicas de cada caso, através de uma **avaliação de risco e análise de ameaças**. Os protocolos e as ferramentas para a defesa de uma organização que lide com defensoras(es)

de direitos humanos ameaçados são diferentes, por exemplo, do que é preciso para um coletivo estudantil universitário.Não se trata de mérito ou de valorizar mais uma ou outra atuação, mas sim de compreender que **realidades, atores e cenários diferentes exigem respostas diferentes**.

Embora existam conselhos básicos de proteção que são aplicáveis em muitas situações, generalizar completamente protocolos a se utilizar pode não só dificultar o funcionamento de uma entidade como, até mesmo, trazer novos riscos – ao implementar ferramentas que o grupo não tem recursos para sustentar de maneira segura, por exemplo.

As metodologias para realização de análises de ameaças são diversas, muitas vezes mesclando diferentes técnicas como a Matriz FOFA (Forças, Oportunidades, Fraquezas e Ameaças)[1] e análises de conjuntura de maior ou menor fôlego. É preciso analisar itens **como: a si mesmo** – as características, potencialidades, vulnerabilidades, recursos e capacidades –, os **atores com quem se atua** ou se tem relação (e quais as intenções dos diferentes atores, as relações entre eles e com

1. No inglês, matriz SWOT: *Strengths, Weaknesses, Opportunities and Threats.*

você), o **cenário** em que estão atuando, **com o quê e para que estão atuando**, e a **conjuntura** geral. A ideia, assim, é **pintar um quadro com qual sua situação**, quais ameaças existem, de onde elas partem, quem são os potenciais opositores e os aliados, e, a partir disso, **traçar um planejamento de proteção**.

Não há – seja na atuação organizada ou na vida privada – um estado de completa segurança, em que não há nenhum risco e nada pode acontecer. Para morrer, há apenas um pré-requisito: estar vivo. O mesmo é válido para entidades: para sofrer algum ataque, basta existir. Enquanto houver atuação, haverá risco. Isto não quer dizer que deve-se, então, desesperar-se ou, no caminho oposto, atuar de maneira irresponsável por achar que faz pouca diferença.

Pelo contrário: sabendo que sempre haverá riscos, **toda organização deve avaliar continuamente quais são eles**, preparar-se adequadamente, tomar medidas para reduzir as chances de que uma ameaça se concretize, reduzir o impacto de possíveis ataques e ter preparadas as respostas e reações desejadas. Ou seja: **além da proteção em si, é preciso trabalhar com a redução e a contenção de danos e a mitigação de ameaças**.

Proteção é um processo continuado de responsabilização coletiva, formação, atenção e vigilância constantes. Não é apenas uma formação ou trocar um aplicativo: é uma atuação cotidiana, considerando sempre quais são os riscos envolvidos em determinada atividade e que medidas de proteção deverão ser tomadas, seja pensar no trajeto que se faz até uma reunião ou a escolha do aplicativo de mensagens para se comunicar, criando-se uma cultura de proteção.

2
A IMPORTÂNCIA DA PROTEÇÃO

As **ameaças à vida e à integridade física de defensoras(es) de direitos humanos no Brasil** são tão antigas quanto a própria luta no país. Em períodos de ditadura ou de democracia, têm feito parte da realidade brasileira tanto a repressão estatal direta quanto a violência praticada por agentes públicos ou com sua anuência, geralmente ligada a interesses de grupos locais de poder. Sejam vindas de militares e policiais ou jagunços, grupos de extermínio e milícias, **não faltam exemplos de vigilância, perseguição, ameaças, prisões, torturas, sequestros e execuções**. Tanto no contexto do campo quanto no urbano, a violência faz, infelizmente, parte do cotidiano – ainda que não de maneira igualitária. Ela atinge de maneira desproporcional jovens negros de periferia e é bastante direcionada contra pobres, negros, mulheres, LGBTQIA+ e defensores de direitos humanos.

Além dos riscos à segurança física, o panorama de vigilância e repressão se modificou de maneira drástica com o avanço do uso da internet, celulares e meios digitais, permitindo a **coleta de dados numa escala nunca antes vista**, tanto por grandes empresas de tecnologia quanto por governos – muitas vezes, atuando em conjunto.

Foi assim no caso do PRISM, programa de vigilância comandado pelos EUA e sua NSA (Agência de Segurança Nacional, na sigla em inglês) revelado ao público pelo ex-funcionário Edward Snowden. Segundo os vazamentos, entre as empresas que colaboraram ativamente com a **espionagem de cidadãos de todo o mundo** estão a Microsoft, a Google (Alphabet Inc.), o Facebook (Meta Plataformas Inc.), Yahoo!, Apple, YouTube, AOL, Paltalk e Skype.

Mesmo em casos em que não exista cooperação entre empresas de tecnologia e governos para fins de repressão, as coletas massivas de dados realizadas todos os dias pela a internet representam riscos para os direitos, como a privacidade e a dignidade das pessoas, pois invadem sua intimidade para garantir lucros e dados para anunciantes ou mesmo direcionar mensagens e agendas políticas.

Assim, **a segurança é uma necessidade primordial para todas as organizações que trabalham com a defesa de direitos humanos no Brasil**. Deve-se trabalhar para reduzir o risco tanto dos defensores e defensoras em si quanto das populações com as quais a organização atua, tendo ciência de que as atividades trazem riscos para todas e todos envolvidos.

A questão **não é assustar ou impedir estas atuações, mas sim garantir que sejam realizadas com responsabilidade**, fazendo todo o possível para que todas e todos estejam protegidos e cuidados. Esta responsabilização se dá em vários níveis, tanto coletiva quanto individualmente: da organização/entidade como um todo e dela com seus membros e as pessoas com quem atua, bem como dos próprios defensores e defensoras.

3
AMEAÇAS E PRATICIDADE X SEGURANÇA

Entre as diversas variáveis a se considerar para pensar uma política de proteção para a organização ou entidade, são fundamentais **a praticidade e a usabilidade**. As ferramentas para uma atuação segura vão, quase sempre, alterar de alguma maneira o funcionamento da organização, mas não devem afetar em demasiado e/ou de maneira desproporcional **para que não afetem o trabalho desenvolvido**, balanceando proteção e privacidade com praticidade e usabilidade.

> Um exemplo para fácil visualização é o acesso ao celular: sem nenhum tipo de bloqueio, usá-lo fica muito fácil. Mas não há nenhuma proteção para além de estar no controle físico do aparelho. Com uma senha de quatro números ou um padrão desenhado, há alguma proteção, mas o acesso leva

> algum tempo a mais – ainda que poucos instantes. Com uma senha longa, destravar o celular demora mais, mas há mais segurança. Com o aparelho com senha longa e dentro de um cofre em uma sala trancada, o celular fica bastante protegido, mas utilizá-lo para comunicação instantânea torna-se impossível.

Determinar como proceder depende de quais recursos e de quanto tempo tanto a organização tem disponível e de quantos recursos e tempo disponível um potencial adversário investiria para executar um certo ataque – o que, por sua vez, depende do valor (não necessariamente financeiro) daquilo que está sendo protegido, se há alvos mais fáceis e se há outras vulnerabilidades.

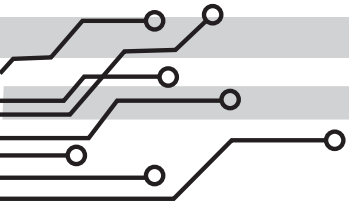
> Pode-se ilustrar com exemplos simples: se o site da entidade X tem senha forte e o da entidade vizinha é fraco, um adversário sem um alvo específico em mente vai preferir atacar a vizinha – ou, falando em vizinhos, uma casa com muros altos e arame farpado tende a ser menos visada para furtos do que uma sem qualquer tipo de cerca ou muro.

Essa adequação é muito importante no contexto de defensoras e defensores de direitos humanos

no Brasil: com acesso reduzido a internet de qualidade, limitações financeiras para comprar aparelhos, planos de celular que liberam aplicativos de mensagens como WhatsApp mas não incluem outros mais seguros como o Signal… **Implantar medidas de proteção coletivamente depende das condições de todos e todas, equilibrando as necessidades de proteção mas não impedindo que alguém que queira lutar** – não deixar ninguém para trás.

Uma medida para dialogar com as necessidades de Praticidade x Proteção é a utilização de **níveis de ameaça, estabelecendo-se procedimentos para diferentes momentos**.

Assim, no dia a dia, durante períodos de normalidade, a entidade funcionará de tais maneiras; caso se detecte uma ameaça, pode-se subir um nível, em que todas e todos utilizam procedimentos mais rígidos de proteção. A quantidade de níveis e as diferenças entre eles vão depender da situação e das necessidades de cada movimento e entidade.



4
PROTEÇÃO X PRIVACIDADE

Proteção e Privacidade caminham juntos, mas não são sinônimos. Numa simplificação extrema, dados seguros não serão roubados por agentes externos, enquanto **dados privados não serão explorados por quem os hospeda ou transmite**.

> Isso vale, por exemplo, para mensagens numa grande rede social: seguras (se a empresa protege bem seus servidores), mas não privadas (se a empresa lê as mensagens). O oposto também pode ocorrer: uma alternativa privada, construída pela comunidade, mas que pode ter um sistema de proteção menos robusto.

Para muitas entidades e organizações, este é um gargalo que deve ser observado com atenção. Pode-se desenvolver ferramentas próprias – sites, aplicativos, servidores, etc –, tendo a certeza de que a ferramenta não vai intencionalmente

compartilhar seus dados (com anunciantes, com o governo ou com quem for). No entanto, pode ser difícil para uma entidade de defesa de direitos humanos alocar recurso para desenvolver sua plataforma e a proteção destes dados e esta ferramenta tende a ser menos robusta que a de uma desenvolvida por um gigante de tecnologia, com bilhões de dólares e centenas de programadores, especialistas em segurança e pentesters (testes de invasão) que esta companhia pode mobilizar.

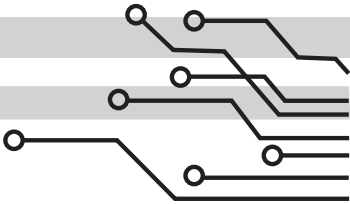
Isto não significa, claro, que não devem ser desenvolvidas alternativas próprias. É muito saudável que as comunidades e entidades desenvolvam suas plataformas e ferramentas e que assumam o controle sobre seus dados. Mas deve-se sempre **levar em conta as eventuais limitações estruturais que se enfrentarão**.

Não há respostas certas e absolutas neste caso, mas diversos questionamentos são pertinentes: qual o grau de proteção e privacidade que os dados exigem? Há diferentes graus de sensibilidade e confidencialidade? Há disponíveis recursos necessários para criar, manter e atualizar ferramentas e plataformas próprias? Há alternativas? Elas pertencem a grandes empresas de tecnologia e potencialmente comprometidas por governos? Há alternativas

criadas por voluntários, entidades de defesa de direitos, com código aberto, que passaram por auditorias?

Os critérios para escolha de ferramentas virtuais são diversos. Passam não só pelos técnicos e pelas necessidades de proteção e privacidade como também pela comodidade, pela facilidade do acesso e do uso, pelos custos e por decisões políticas – como boicotar ou utilizar ferramentas que pertençam a empresas que violam direitos e privacidade continuamente.

Na maioria das vezes, o uso de uma plataforma própria não parte do zero: podem ser utilizadas ferramentas e bases criadas por outras entidades de defesa de direitos e por comunidades que se importam com a privacidade e a proteção dos usuários. Muitas dessas alternativas estão disponíveis na internet, com o código aberto e com licenças que permitem seu uso irrestrito sem fins lucrativos.



5
CONTROLE SOBRE SEUS DADOS

Muitos dados pessoais hoje estão disponíveis na internet, seja porque foram postados pelas próprias pessoas nas redes sociais, coletados pelas gigantes de tecnologia, cadastrados em sites enganosos ou vazados por *hackers*. Esses dados podem ser usados de infinitas maneiras para uma porção de fins nefastos: anúncios, repressão, golpes financeiros, roubo de identidade, intimidação, perseguição, vigilância… Assim, **tomar controle sobre os próprios dados é fundamental para todo mundo, em especial para quem está na defesa dos direitos humanos**.

> Existem alguns cuidados básicos a serem tomados. Não **forneça dados sem necessidade. Proteja suas informações**, revelando só o estritamente necessário – evitando revelar sua própria rotina, intimidade,

> contatos, datas importantes, endereços e imagens que exponham sua casa e as pessoas próximas a você. É importante refletir sobre os conteúdos que serão postados, se realmente são necessários e se é preciso postar naquele momento: pode ser mais prudente postar um story ou tuíte de um lugar que você foi depois de sair de lá, não enquanto ainda está presente, por exemplo.

Pense bem no que vai publicar, especialmente nas mídias sociais. **Evite o excesso de exposição**, limitando apenas para seus amigos e conhecidos. Novamente, é necessário avaliar o contexto: algumas pessoas são figuras públicas e necessitam postar publicamente. Nestes casos, é fundamental uma análise de ameaças específicas. Uma saída é manter redes sociais separadas: uma aberta, onde qualquer pessoa – inclusive desconhecidos – tem acesso e uma fechada, apenas para pessoas próximas.

Cada rede social tem diferentes mecanismos de controle de visibilidade e privacidade. É importante checá-los constantemente, alterando conforme necessário. Além das **opções para limitar a visibilidade de suas postagens para outros usuários, existem opções para limitar**

o que as próprias redes coletam sobre você. Um exemplo é pausar o histórico do Google, que constantemente coleta informações de pesquisas, e-mails, vídeos assistidos e de localização (registrando por onde você andou). Cabe mencionar que a localização é muitas vezes coletada mesmo com opções de "Local" e/ou "GPS" desligado no celular, através de dados como redes *wi-fi* utilizadas.

O controle de seus dados não é apenas para redes sociais: evite entregar informações para qualquer cadastro, inclusive comerciais e de compras. Não se cadastre em sites suspeitos, preferindo sempre serviços com reputação e confiança pública. Mantenha seus cadastros atualizados e exclua contas desnecessárias ou que você não usa mais. **Desconfie sempre!** Tome cuidado com links, convites, anexos, mesmo que venham de contatos supostamente conhecidos – pode ser um golpista se passando por um amigo, colega ou familiar.

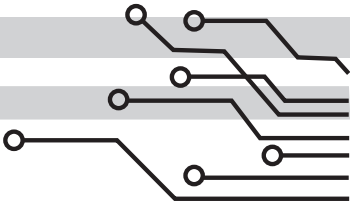
Alguns golpes de WhatsApp, por exemplo, usam apenas três informações para tentar extrair dinheiro: seu nome, sua foto de perfil e alguns de seus contatos, utilizando estas informações para criar um perfil duplicado, tentando se passar por você para pedir dinheiro a seus familiares e/ou amigos.

Algumas medidas podem dificultar golpes e vazamentos, como **senhas fortes e verificação em duas etapas** (falaremos mais sobre isso adiante). Outras medidas podem ajudar a descobrir se você foi vítima de um, como consultas ao **Registrato**[2], do Banco Central do Brasil (**https://www.bcb.gov.br/cidadaniafinanceira/registrato**), que permite checar quais contas, chaves Pix ou empréstimos estão vinculadas ao CPF (ou CNPJ). ***O have i been pwned?*** (**https://haveibeenpwned.com/**)[3] revela – através de consulta via seu e-mail ou telefone celular – se os seus dados estão entre os que apareceram em algum vazamento.

O controle das informações não é só virtual: **agendas ou cadernos de anotações, por exemplo, são fontes valiosas de dados**. Podem conter calendário de atividades, contatos, nomes, atas, táticas e estratégias planejadas… Convém não concentrar informações demais em poucos registros físicos e sempre mantê-los sempre em locais seguros ou sob sua guarda – não deixando-os guardados em um carro estacionado, por exemplo.

---

2. Atualmente, a ferramenta exige que login seja feito através do gov.br, a plataforma digital de relacionamento do cidadão com o governo federal brasileiro, e com o padrão de segurança prata ou ouro (o qual exige autenticação através da vinculação a uma conta bancária, à CNH, ou ao cadastro de servidor público federal.
3. A página está disponível apenas em inglês. Mas é possível usar ferramentas de tradução, como o Google Translate, para acessar o conteúdo.



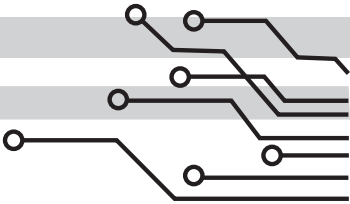
6
COMPARTIMENTALIZAÇÃO

A concentração de informações pode trazer riscos graves. Um sistema, uma conta, um servidor, um caderno ou uma pessoa que reúna um número muito grande de informações sobre a entidade/organização e as suas atividades aumenta consideravelmente seu valor enquanto alvo para um potencial adversário. No caso de um ataque bem-sucedido, a quantidade de informações perdidas será muito maior, podendo comprometer o funcionamento de toda a entidade/organização.

Assim, **evitar a circulação irrestrita de informações sensíveis** entre todas as pessoas que fazem parte da entidade/organização pode ser uma interessante medida de proteção. **Trata-se da compartimentalização: cada um só sabendo apenas do que é necessário para o cumprimento de suas funções, evitando a centralização de informações e que dados sensíveis sejam compartilhados desnecessariamente**.

Para a compartimentalização ou segmentação funcionar, no entanto, se faz necessária confiança mútua entre as pessoas e transparência nos critérios adotados: o sigilo é importante, mas não pode ser utilizado para compartilhar ou reter informações com base em interesses individuais ou disputas internas. Em algumas organizações, aplicar princípios de compartimentalização pode ser difícil, por conta dos processos internos e externos de comunicação, e aí torna-se necessário avaliar e equilibrar as necessidades de proteção com as de transparência e de debate interno.

Ainda assim, qualquer que seja o caso e a cultura organizacional, evitar a centralização de informações em ferramentas e plataformas – contas de e-mail, servidores, sites, cadernos, documentos – tende a ser bastante prudente e aplicável, mesmo que as informações circulem de maneira mais irrestrita entre as pessoas.



7
PROTEÇÃO DIGITAL

No meio digital, é importante ter **controle sobre o que aplicativos, sistemas e aparelhos estão fazendo, para que não executem escondidos algo que você não queira**. As mais diversas coisas podem ser feitas sem seu conhecimento em determinadas situações. Algumas dessas vêm diretamente dos sistemas operacionais e programas de empresas conhecidas – como o envio constante de informações de uso, horários de utilização, programas abertos, localização… Em alguns desses casos, o usuário até é informado desta coleta, mas pode não ter a possibilidade de impedi-la.

Por sua vez, programas maliciosos podem executar diferentes ataques: captura de tudo que é digitado, uso indevido de câmera ou microfone, envio de seus registros ou documentos para quem está o atacando, criptografar todos os seus arquivos e exigir dinheiro para descriptografá-los ou mesmo transformar seu aparelho em um "zumbi"

para atacar outros sistemas ou *minerar*[4] moedas virtuais criptografadas.

Está entre as mais eficientes medidas para buscar maior controle sobre seus aparelhos: o uso de programas e sistemas com **código aberto, softwares livres e auditados**, que tenham compromisso com privacidade e mostram como funcionam.

Explicando por partes…
O **código aberto** (*Open Source*) é um software ou aplicativo, que deixa acessível seu código-fonte – o conjunto de instruções computacionais para que um programa funcione. Diferente de softwares proprietários/privados, em que só quem o desenvolveu conhece seu funcionamento, a disponibilidade do código do programa permite que outros usuários que conheçam a linguagem de programação possam usá-lo, modificá-lo e melhorá-lo, incentivando a **colaboração** entre diferentes pessoas e comunidades.

---

4. De maneira resumida, minerar dados (ou Data Mining, em inglês) significa sistematizar dados obtidos em grande volume para analisar, identificar padrões e, assim, obter informações valiosas. No caso de moedas virtuais criptografadas, seu funcionamento é baseado em "blockchain" (em tradução livre, "corrente de blocos"), uma base de dados de registros distribuída por toda a rede. Para criar novos registros e novos blocos, é necessário realizar cálculos complexos e é aí que entra a mineração: computadores com alta capacidade de processamento realizam esses cálculos e são recompensados com valores da moeda da rede para qual trabalharam.

Já o "**Software livre**"é uma definição do projeto GNU (lê-se guinú) e da FSF (Fundação para o Software Livre, na sigla em inglês). Diz respeito a um **"software que respeita a liberdade e senso de comunidade dos usuários". De grosso modo, isso significa que os usuários possuem a liberdade de executar, copiar, distribuir, estudar, mudar e melhorar o software. Assim sendo, 'software livre' é uma questão de liberdade, não de preço.[5]"**

Ou seja, você deve ter a **liberdade para utilizar e modificar o programa da maneira que quiser**, sem restrições, independente de ter adquirido o programa/sistema de maneira gratuita ou paga[6]. Todo software livre possui código aberto, mas nem tudo que tem código aberto se encaixa nas definições de software livre.

Mesmo com o código-fonte público, **não há como esperar que todas as pessoas e entidades tenham a capacidade de vasculhar todas as linhas**

---

5. Saiba mais em "O que é o software livre?": https://www.gnu.org/philosophy/free-sw.pt-br.html).
6. Em inglês, existe a necessidade de diferenciar que software livre não quer dizer gratuito ("pensar em livre como em liberdade de expressão, não como cerveja grátis"), já que "free" significa tanto "livre" quanto "gratuito", o que leva a existência dos conceitos diferentes – ainda que similares – de "free and open-source software" (FOSS) e "free/libre and open-source software" (FLOSS ou F/LOSS). A FSF prefere o uso do termo "free/libre".

de programação de todos os programas que vão utilizar e possam garantir que são seguros e privados. É aí que entra o terceiro conceito, de **auditados**, que quer dizer os programas foram testados por pessoas que sabem o que estão fazendo e nas quais você confie. Passar por auditorias não quer dizer que os programas são perfeitos, mas que – a depender das avaliações, evidentemente – tem padrões adequados de proteção, estabilidade e privacidade.

Juntando estes conceitos, temos **programas e sistemas desenvolvidos de forma pública, avaliados e alterados constantemente conforme estas avaliações, e, de maneira geral, com grande atenção para proteção e privacidade**.

Algumas indicações de programas e sistemas que sigam estes conceitos podem ser encontrados em sites como o PRISM Break (https://prism-break.org/pt/), o Privacidade Digital (https://www.privacidade.digital/), o Privacy Guide (https://privacyguides.org/, em inglês), o Autodefesa Contra Vigilância (https://ssd.eff.org/pt-br) e o AlternativeTo (https://alternativeto.net, em inglês).

Para além destes conceitos, também é fundamental **manter os programas e sistemas atualizados**.

Vulnerabilidades, de maior ou menor impacto, são descobertas todos os dias em diversos programas. Muitas das atualizações são desenvolvidas justamente para resolver essas falhas e impedir que sejam exploradas. Por isso, também é importante verificar se o programa/sistema utilizado ainda recebe **suporte do desenvolvedor** (ou da comunidade que o desenvolveu). Todas as versões do Windows 7 para baixo, por exemplo, já não têm mais suporte da Microsoft.

Há um porém na questão das atualizações que são **os ataques de cadeia de suprimentos**. Aqui, a invasão é feita contra um sistema que oferece, por exemplo, serviços a terceiros, que por sua vez, acabam também comprometidos.

Foi o caso do *Sunburst*, descoberto em 2020. A SolarWinds, empresa que fornece sistemas para outras empresas, entidades e governos, sofreu um ataque e o *hacker* enviou, sem seu conhecimento, atualizações que também comprometaram os sistemas de seus clientes.

Estes ataques, entretanto, são de **grande complexidade** – realizados, via de regra, por um Estado contra outro – e não significam, de maneira alguma, que não seja importante manter

os sistemas atualizados: os riscos de manter programas desatualizados é muito maior do que ser vítima de um ataque que exige tantos recursos.

Por outro lado, riscos muito mais comuns e que também envolvem ataques não diretos, **via fornecedores**, são riscos com **assistências técnicas**. Aparelhos enviados para consertos, manutenção no local ou instalação de sistemas e assistências podem – seja por motivos financeiros, ideológicos, sórdidos (como no vazamento de *nudes*) ou por descuido e negligência – acabar sendo um ponto para vazamento de informações, dados e/ou comprometimento dos sistemas.

Algumas formas de contornar ou minimizar esse risco são: a **criptografia** de disco dos dispositivos, a realização dos serviços de manutenção e/ou instalação por pessoas que sejam da entidade/organização e a contratação apenas de empresas de assistência técnica confiáveis, com referências e avaliações consistentes.

Os itens a seguir dizem respeito à **proteção digital** mas, como em toda proteção, não devem ser usados isoladamente: é preciso avaliar contexto, ameaças específicas e condições materiais para implantar o que mais faz sentido em cada caso.

É também importante se **manter atualizado em novidades e alterações no cenário: o que é seguro e privado hoje pode não ser mais amanhã**.

SISTEMAS OPERACIONAIS DE COMPUTADORES

Entre computadores, os sistemas operacionais (SO) que cumprem melhor os requisitos de código aberto, softwares livres e auditados e com atenção especial para proteção e privacidade são, em geral, distribuições **GNU/Linux**.

É interessante buscar a troca de sistemas operacionais privados como Windows e MacOS (Apple), por uma das opções aqui listada, caso o foco seja **privacidade e proteção**. A troca de sistemas operacionais em computador não é uma operação particularmente difícil e as opções elencadas possuem tutoriais próprios para facilitar o processo.

O número de distribuições GNU/Linux é imenso e não há como listar todas e suas diferenças neste guia, com muitas delas sendo voltadas para públicos e aplicações específicas. É possível pesquisar informações sobre diversas versões em sites como o *DistroWatch* (https://distrowatch.com/?language=PT, majoritariamente em inglês).

Algumas indicações que podem ser feitas são:

FEDORA
Bastante utilizada e base para outros sistemas, é desenvolvida pelo projeto Fedora com patrocínio da Red Hat, é estável e fácil de utilizar;

DEBIAN
Também muito utilizada, é uma distribuição baseada completamente em software livre e código aberto, sendo razoavelmente fácil de utilizar;

UBUNTU
É outra distribuição com significativo número de usuários, suporte constante e facilidade para uso. Em 2012, houve uma polêmica com propagandas e cooperação com a Amazon. Depois de alguns anos, a situação foi alterada, mas alguns guias (como o PRISM Break) seguem não recomendando mais Ubuntu como alternativa;

QUEBES
É uma distribuição mais difícil de usar, mas focada especialmente na privacidade e na proteção, sendo um dos sistemas mais seguros existentes hoje. Não é muito recomendada para iniciantes, mas uma excelente opção para usuários mais avançados;

TAILS

Diferente das distribuições acima, o Tails não precisa ser instalado no disco rígido, rodando a partir de um pendrive ou CD. É focado em proteção e privacidade, buscando não deixar rastros no computador em que foi utilizado, contendo ferramentas para criptografar e fazendo todas as conexões com a internet pela rede Tor. É uma opção interessante para quem está utilizando um computador em que não pode alterar o sistema, mesmo não confiando no instalado – como no caso de um computador emprestado ou da família;

WHONIX

É uma distribuição que roda através de máquinas virtuais, sendo utilizada dentro de outro sistema – como, por exemplo, uma distribuição GNU/Linux, Windows e macOS – também focado em privacidade.

SISTEMAS OPERACIONAIS DE CELULARES

Celulares, por diversas razões, são plataformas **mais difíceis para que o usuário saiba e controle tudo que está acontecendo**. Há menos maneiras de acompanhar todos os processos, sejam do sistema ou de programas instalados.

Alterar o sistema operacional de celulares não é algo impossível – longe disso ,mas isto é consideravelmente mais complexo do que num computador, inclusive com maiores riscos para o funcionamento normal do smartphone e a estabilidade do sistema. Além disso, o número de sistemas alternativos é bem mais reduzido, e não há suporte para todos os aparelhos e modelos.

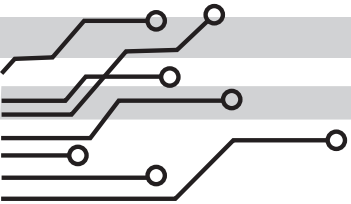
O Android, apesar de ser baseado em Linux e possuir código aberto, é financiado pela empresa Google (do conglomerado Alphabet Inc.) e os aparelhos celulares com este sistema vêm com aplicativos privados pré-instalados, estando longe de padrões ideais de privacidade. Existem algumas alternativas, desenvolvidas a partir do código-fonte do próprio Android.

Entre essas alternativas, três com maior foco na privacidade são **LineageOS**, **GrapheneOS** e **CalyxOS**. Os modelos de celular que suportam cada um dos sistemas são variados, e é preciso checar caso a caso.

Um possível risco é que com estes sistemas as atualizações de proteção podem ser menos frequentes que o sistema original, comprometendo a proteção em nome da privacidade.

REQUISITOS MÍNIMOS

Para rodar Tails, um computador precisa de pelo menos 2 GB de memória RAM e um processador de 64-bit. Para o Debian, o mínimo é mais leve: 512 MB de RAM e 10 GB de espaço no HD (Disco Rígido). Para celular, os requisitos variam muito de acordo com o fabricante e o sistema, mas o recomendável é, ao menos, 2 GB e – no caso de um celular Android – um modelo que seja de um sistema que ainda receba atualizações oficiais de proteção – no momento, Android do 8.1 ao 11.



8
SENHAS

A senha é o elemento mais básico na proteção digital e é muito comum ouvir recomendações de uso de **"senhas fortes"**. Mas o que exatamente isto significa?

Primeiramente, as senhas devem ser capazes de resistir ao modo mais simples – porém muito eficaz – de quebra: **a adivinhação**.

Senhas óbvias – como seu nome ou de familiares, ídolos, celebridades, jogadores, animais de estimação, apelidos, datas importantes ou outros dados pessoais facilmente acessíveis – podem ser descobertas por alguém em poucas tentativas, mesmo sem nenhuma ferramenta sofisticada.

Senhas muito comuns também entram nesta categoria de facilmente adivinhadas. Para referência do que não fazer, as dez senhas mais comuns do mundo são, nesta ordem: "123456", "123456789", "qwerty"(a sequência das primeiras letras de

muitos teclados), "password", "111111", "12345678", "abc123", "1234567", "password1" e "12345"[7].

A adivinhação não é um método apenas artesanal: com a tecnologia, é possível tentar centenas de milhares de variações por minuto, em **ataques de força bruta**. Senhas comuns são as primeiras testadas e alguns dos software especializados em quebrar senhas podem ser configurados com palavras e termos específicos para cada pessoa – colocando, por exemplo, o nome de seus familiares e cachorros para serem testados primeiro.

Assim, suas senhas devem ser bem diferentes das senhas óbvias e comuns, bem como não serem diretamente relacionáveis com você. Uma alternativa é o uso de conjuntos diferentes de caracteres – letras, números, variações de maiúsculas e minúsculas e caracteres especiais (!@#$%, por exemplo). No entanto, em senhas curtas, diferentes caracteres acabam fazendo pouca diferença. Por isso, é importante que as **senhas sejam longas**.

Mesmo assim, surge um problema: senhas grandes

7. A lista completa, com as 100 mil senhas mais comuns do mundo está disponível no site do NCSC (Centro Nacional de Cibersegurança, na sigla em inglês) do Reino Unido: https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt

e com vários caracteres diferentes tendem a ser muito mais difíceis de lembrar. Para auxiliar, existem duas alternativas – que se complementam e, idealmente, são usadas em conjunto:

A primeira é a utilização de **"frases-senha"** ou **"frases-passe"**: uma sequência de palavras, criando senhas longas, mas relativamente fáceis de lembrar. O ideal é que sejam ao menos seis palavras e que não seja uma frase com sentido – muito menos uma citação, letra de música ou poema –, escolhendo termos aleatórios, chegando a um resultado como "LanternaQuedaMedicoPortaTelevisãoGarrafa".

A segunda ferramenta são os **gerenciadores de senhas**, que podem ser utilizados para criar e guardar, de forma segura, diferentes senhas. Dois gerenciadores de senhas livres e código aberto são o **KeePassXC** e o **Bitwarden**. Ambos oferecem suporte para diferentes sistemas.

Existem ainda alguns outros cuidados com senhas: **devem ser únicas**, não reutilizando as mesmas em diferentes contas e, assim, se algum serviço ou rede tiver os dados vazados, suas

8. O termo surgiu por analogia ao inglês, onde "senha" é "password" – que quer dizer, em tradução literal, "palavra-passe/chave", enquanto "passphrase" é "frase-senha/passe".

outras contas continuam seguras[9]. Um segundo risco de senhas iguais (ou com poucas variações) é que um adversário que tenha você como alvo específico pode utilizar senhas vazadas para entender sua lógica de criação de senhas e ter maior facilidade para quebrar outras senhas suas.

No caso de ter suas **informações de login vazadas** em um serviço, **troque-a imediatamente**, assim como em outros locais em que você usa a mesma senha. Outros casos que demandam troca imediata de senhas são **perda, roubo ou furto** de equipamentos eletrônicos com logins seus, **atividades suspeitas** (como acessos não reconhecidos) e **comprometimento** da conta.

Há ainda recomendações sobre **trocas periódicas de senhas**. No entanto, esta é uma medida que deve ser avaliada caso a caso. Por um lado, ela **diminui o valor relativo de uma senha obtida por um adversário** – já que ela perderá a utilidade mais rapidamente – mas por outro **pode gerar senhas mais fracas** (por cansaço ou preguiça de elaborar constantemente senhas boas), além de um **armazenamento inseguro**

9. É possível checar vazamentos em serviços como o have i been pwned? (https://haveibeenpwned.com/).

(como escrever senhas em papéis colados em monitores). No caso de implantar a troca de senhas periódicas, deve-se **garantir que as senhas novas sejam seguras e que sejam armazenadas de modo adequado**.

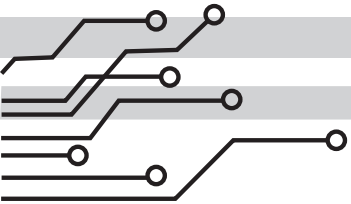
VERIFICAÇÃO EM DUAS ETAPAS

Em diversos serviços, é possível ativar a **verificação/autenticação em duas etapas/fatores** (ou 2FA, do inglês "two factor authentication"), que é a exigência de um outro código além de sua senha para realizar o login. Este código pode ser gerado de diversas formas, como por um aplicativo específico, através de uma chave USB, enviando-se um código via SMS ou com verificação biométrica.

Os SMS (torpedos) são vulneráveis e não costumam ser recomendados como método primário – embora sejam melhores do que não ativar a verificação em duas etapas. Aplicativos específicos, como o **Aegis** e o **andOTP**, são preferíveis. Chaves USB são boas alternativas, mas têm com algum custo e são menos comuns.

Qualquer que seja o método, é importante ativar a verificação em duas etapas nos serviços em

que for possível. Lembre-se de fazer o backup de códigos de recuperação de uma maneira segura, como em um gerenciador de senhas, para o caso de perder o dispositivo/aplicativo que gera os códigos.



9
INTERNET, REDES E TOR

Quando você se conectar à internet, o ideal é que os dados só sejam vistos por você e o que está sendo acessado. No entanto, **alguns outros atores podem, de maneira legal ou ilegal, acabar tendo acesso ao que está sendo navegado**, como seu provedor de internet (inclusive móvel – 3/4/5G), o administrador da rede *wi-fi* ou alguém que intercepte a comunicação. Para diminuir riscos, o ideal é não confiar em redes *wi-fi* públicas e usar ferramentas que protejam sua navegação.

O primeiro instrumento de proteção de sua navegação é o uso do **HTTPS** (Protocolo de Transferência de Hipertexto Seguro, na sigla em inglês) ao invés do HTTP ao acessar sites (Ex.: https://www.global.org.br/ no lugar de *http://*). Este protocolo gera uma camada de proteção ao autenticar a conexão entre o navegador e o site/servidor, protegendo os dados acessados, com certificação SSL/TLS.

Ao acessar um site utilizando HTTPS e com **certificados** em dia, os navegadores avisam o usuário, geralmente com um símbolo de cadeado ao lado do endereço. Clicar neste cadeado permite que você verifique o certificado do site. Alguns navegadores, como o **Firefox**, apresentam a opção de exigir conexões via HTTPS, bloqueando o acesso automático e exigindo confirmação do usuário para entrar em sites com HTTP. Extensões como o **HTTPS Everywhere** fazem um trabalho semelhante.

Também importante no acesso à internet é o **DNS** (Sistema de Nomes de Domínio, na sigla em inglês), o sistema responsável por relacionar os endereços que digitamos (os domínios) com os endereços de IP[10] em que estão os sites que queremos acessar. Como é função deste sistema conectar você com o conteúdo que você quer acessar, é algo sensível para sua privacidade, pois podem ser coletados os registros de onde você navega. É também sensível para sua proteção, pois uma interferência maliciosa no sistema pode fazer você acessar um site falso no lugar do verdadeiro.

10. Do inglês "Internet Protocol" (protocolo de rede), o IP é uma série de números que identifica cada dispositivo (como celular ou computador) conectado a uma rede. É ele que contém as informações de localização e torna o dispositivo acessível para comunicação.

Desta maneira, há recomendações para alterar o provedor de DNS (geralmente fornecido pelo provedor de internet) e para o uso de técnicas de encriptar (ou cifrar) o DNS. Assim como em outros casos, a alteração de DNS precisa ser feita para provedores em que se confie – **caso contrário, você pode acabar se expondo a mais riscos em vez de se proteger**.

Algumas listas de serviços DNS são:

MOZILLA
(https://wiki.mozilla.org/Security/DOH-resolver-policy);

PRIVACYTOOLS
(https://www.privacidade.digital/provedores/dns/);

PRISM.BREAK
(https://prism-break.org/en/categories/gnu-linux/#dns).

Outra ferramenta de proteção ao navegar na internet é a **rede Tor**. O nome é uma sigla em inglês para "o roteador cebola", fazendo referência às **várias camadas de proteção providas pela rede**. De maneira simplificada, usar a rede Tor faz com que sua conexão conte com razoável privacidade e anonimidade, criando uma espécie de "túnel" entre você e o que você acessa, o que faz com que

sua conexão "pule" entre diferentes pontos e servidores, mascarando sua identidade e localização.

Assim, se tudo estiver configurado corretamente, nem quem está na rede com você, nem seu provedor, nem um ator malicioso no meio do caminho será capaz de interceptar os dados e detectar o que você acessa – apenas saberá que você está acessando a rede Tor. O próprio site ou servidor que você acessa não saberá sua identidade ou de onde você se conectar – para ele, você é um usuário anônimo do Tor.

O Tor pode ser usado apenas nas conexões do próprio navegador – com o **Navegador Tor** –, ou para todas as **conexões do sistema, como no Tails e no Whonix**. A rede Tor não é uma solução perfeita, possuindo alguns poucos pontos negativos. Primeiramente, ela não está acima de erros e possui vulnerabilidades – que, no entanto, além de continuamente pesquisadas e resolvidas, são exploráveis apenas por atores com muitos recursos (como Estados e grandes empresas). Em segundo, alguns sites e serviços proíbem ou limitam o acesso feito via Tor – desde a Wikipédia bloqueando edições, até *internet bankings* travando contas que tentem acessar pela rede.

Outro problema é que, embora o que você acesse (ou transmita) pelo Tor fique oculto para alguém monitorando sua internet (como seu provedor ou administrador da rede wi-fi), provavelmente será possível saber que você está usando Tor. Em alguns casos específicos, isto pode trazer riscos. Há, por fim, um risco que não vem diretamente da Tor, mas sim de seu uso: se você loga em contas diretamente associadas a você ou tem hábitos de navegação idênticos aos quando você está utilizando uma rede normal, não há como ser anônimo. De qualquer maneira, outras proteções – como contra sua exata localização – vão seguir funcionando.

Uma outra ferramenta de acesso de redes são os **VPNs** (Redes Privadas Virtuais, na sigla em inglês). Existem diferentes tipos de VPNs, com diversas aplicações, como para acesso de redes de empresas ou universidades fora de suas sedes ou para fingir acesso de outro país e driblar proteções de *copyright*[11] de serviços de *streaming*[12].

Na proteção digital, os VPNs que interessam são com criptografia e técnicas para proteger

11. Direito autoral ou direitos de reprodução de uma obra intelectual.
12. Serviço de transmissão contínua de determinados tipos de dados, como áudios e vídeos.

sua navegação, levando a um resultado semelhante ao do uso da rede Tor (ainda que de maneiras muito distintas): uma espécie de "túnel" protegendo sua navegação. No entanto, há uma diferença muito grande em relação à Tor que precisa ser destacada: o provedor de VPN será capaz de ver seu tráfego. Assim, no lugar de ter seu provedor de internet, administrador da wi-fi ou um ator malicioso vendo o que você vê, haverá o provedor de VPN sendo capaz de saber – e registrar – o que você está acessando e enviando.

Por isso (de maneira simplificada, já que o debate é longo), muitas pessoas da comunidade de privacidade e proteção digital são **contra o uso e recomendação de VPNs, preferindo o uso do Tor**. Alguns dos argumentos são que para ser anônimo, o Tor é suficiente; para proteção, há também um debate do uso de Tor combinado com VPN, também sem consenso: há quem diga que aumenta sua proteção e há quem defenda que prejudica sua proteção e privacidade, possivelmente reduzindo a eficácia de usar Tor.

De qualquer maneira, se você optar pelo uso de um VPN, deve ter **muito cuidado com qual serviço de VPN será escolhido** – afinal, o provedor possivelmente vai ver e registrar tudo que você acessa.

A EFF (em inglês, Electronic Frontier Foundation) tem um guia para ajudar na escolha de VPNs: (https://ssd.eff.org/pt-br/module/escolhendo-vpn-rede-virtual-privada-mais-adequada-para-voc%C3%AA) e há listas do PrivacyTools (https://www.privacidade.digital/provedores/vpn/), Prism.Break (https://prism-break.org/en/categories/gnu-linux/#vpn) e da comunidade /r/VPN do Reddit (https://docs.google.com/spreadsheets/d/1ijfqfLrJWLUVBfJZ_YalVpstWsjw-JGzkvMd6u2jqEk/edit#gid=231869418 – https://www.reddit.com/r/VPN/)

DIMINUA SEUS RISCOS NA INTERNET

É sempre importante repetir alguma recomendações básicas: não clique em **links suspeitos**, não baixe **arquivos desconhecidos**, não instale **programas que não sejam de confiança**, não insira **USBs ou CDs desconhecidos** em seus aparelhos. Mantenha seus **sistemas e programas atualizados**, utilize um serviço de antivírus e o mantenha atualizado – embora qual programa específico vá variar conforme a necessidade, em muitos sistemas, o básico, que vem junto com o sistema, é suficiente, não sendo necessário comprar ou baixar um extra.

Preste atenção e sempre confira se o **site que você está acessando é o oficial daquele serviço** e não um tentando se passar por ele – assim como se a **pessoa que você está conversando é ela mesmo** e não alguém tentando se passar por ela. **Navegue desconfiado:** não faltam golpistas e agentes de vigilância online.

Caso acredite que seu aparelho foi infectado, tente executar escaneamentos para descobrir a fonte da infecção e a limpar. Em muitos casos, pode ser necessário formatar o computador, limpando HD e reinstalando o sistema. É válido notar que, eventualmente, mesmo a formatação pode não ser suficiente, em casos de ataques mais avançados.

Como sempre na proteção, é preciso adequar suas medidas de proteção com sua necessidade de proteção. Quais são suas ameaças determina quais são as ferramentas e técnicas necessárias para uma utilização minimamente segura e privada das redes.

Procure evitar atalhos, preguiça e cair em hábitos inseguros e que comprometam sua privacidade: a proteção não se dá simplesmente instalando um ou outro programa recomendado para se proteger, mas sim usando-os de maneira

consciente, dentro de uma estratégia de proteção. Às vezes, pode ser interessante simplificar alguns procedimentos para garantir que você os seguirá (sem sacrificar sua privacidade e proteção).

NAVEGADORES

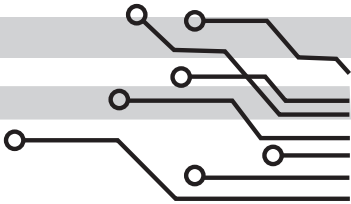
Para navegação segura e privada, o ideal é buscar soluções que sejam naturalmente de código aberto, livres e que venham de empresas (ou comunidades) que valorizam a privacidade. Os navegadores que melhor atendem a esses requisitos atualmente são: o **Mozilla Firefox** e o **Navegador Tor** (que é, em si, baseado no Firefox e utiliza,portanto, a rede Tor).

Algumas **extensões** podem ser utilizadas para melhorar a proteção de sua navegação. O problema é que extensões no navegador Tor podem, eventualmente, trazer problemas e revelar sua identidade ao fazerem conexões por fora da rede Tor. Outra observação importante é que extensões podem aumentar a "impressão digital" do seu navegador, com configurações e hábitos muito específicos que podem ajudar a revelar sua identidade, além de reduzir a velocidade e a usabilidade de sua navegação.

Algumas das extensões mais recomendadas são **uBlock Origin**, como um eficiente bloqueador de anúncios; o **HTTPS Everywhere**, ainda que possivelmente redundante, com as opções de apenas permitir conexões HTTPS no Firefox; o **ClearURLs**, que retira rastreadores das URLs (endereços eletrônicos) em que você navega; o **Cookie AutoDelete**, para deletar cookies (dados armazenados de preferências em sites) entre uma sessão e outra – opções semelhantes podem ser configuradas diretamente no navegador, sem a extensão; bloqueadores específicos de alguns rastreadores, como o **Facebook Container** e o **Firefox Multi-Account Containers** (ambas da Mozilla); e o **CanvasBlocker** para diminuir a "impressão digital" coletada por sites.

Há dezenas de outras extensões, mas algumas são desnecessárias e outras podem trazer riscos ou, como dito acima, reduzir sua velocidade ou sua usabilidade e mesmo ajudar a te identificar. Listas (e discussões sobre motivos de usar ou não algumas extensões) podem ser conferidas em sites como o PrivacyTools (https://www.privacidade.digital/navegadores/), o Riseup (https://riseup.net/pt/security/network-security/better-web-browsing) e em fóruns do GitHub (https://github.com/arkenfox/user.js/wiki/4.1-Extensions).

Várias opções do Firefox podem também ser alteradas para aumentar sua proteção e privacidade. Um guia completo pode ser conferido no PrivacyTools (https://www.privacidade.digital/navegadores/#about_config) e no link acima do Riseup.



10
CRIPTOGRAFIA

A criptografia é um campo ou conjunto de técnicas e ferramentas que tem como objetivo **manter informações seguras contra um adversário**. A ideia básica é a de trancar conteúdos e **só permitir o acesso de quem possui as chaves**. A criptografia pode assumir formas muito simples, como a alteração da ordem das letras (transformando "mensagem simples" em "gemsamen plessim", por exemplo) ou substituindo letras por outras (como trocar a por b, b por c e assim por diante).

Mesmo nestas maneiras mais simples, decifrar as mensagens pode ser razoavelmente difícil para uma pessoa, dependendo das escolhas de alterações e/ou substituições. No entanto, como estas técnicas são conhecidas desde a Antiguidade, quebrar códigos criptografados de maneiras mais básicas tornou-se cada vez mais fácil, em especial com o auxílio de computadores. Ao mesmo tempo, as

fórmulas matemáticas que protegem as informações também se tornaram muito mais complexas, e também são desenvolvidas por computadores.

As formas de gerar chaves e quebrar criptografia são inúmeras. Muitas vezes, ao usar a internet, a criptografia está sendo utilizada para a sua comunicação, protegendo suas informações, mesmo que você não perceba – com que grau de proteção vai variar – em compras virtuais, internet banking, senhas em sites, envio de informações… são muitas as aplicações normais de criptografia.

Para o uso cotidiano e a partir de coisas que você mais facilmente pode alterar para aumentar sua segurança e privacidade nos meios digitais, duas das mais importantes aplicações possíveis de criptografia são a de **disco** e de **ponta a ponta**.

CRIPTOGRAFIA DE DISCO

Nem só quando são transmitidas as informações precisam ser protegidas: é aí que entra a criptografia (ou encriptação)[13] dos **dados armazenados**,

13. Há distinção entre os termos, com a encriptação sendo parte do campo de criptografia, mas, em nome da simplicidade e da facilidade do entendimento, optamos por não incluir as diferenciações neste guia.

em repouso. De forma básica, significa **proteger os dados em dispositivos** – como computador, celular, servidor, *pendrive*, HD externo – contra acesso não autorizado.

As senhas de usuário no Windows, por exemplo, não garantem qualquer proteção contra acesso dos arquivos num computador: acessar o HD inteiro e todos os dados presentes nele é uma tarefa trivial, com métodos simples como conectar o HD em outro dispositivo ou ligar o computador utilizando um outro sistema que não o Windows (inclusive o Tails, recomendado acima). **Boa parte dos bloqueios de dispositivos não tem relação direta com a encriptação de disco**, deixando os dados vulneráveis.

A ideia de criptografar os dados no dispositivo é impedir que eles sejam acessados por qualquer pessoa que não possua as chaves. Esta encriptação pode ser feita de diversas maneiras: pode-se criptografar apenas um único arquivo (ou alguns arquivos específicos), uma parte (partição de disco) ou o disco inteiro. É possível, inclusive, combinar estas formas diferentes – encriptando todo o disco, uma partição dentro dele e arquivos dentro dessa partição, criando camadas de proteção para informações com diferentes graus de sensibilidade.

A criptografia/encriptação de disco inteira é uma recomendação básica da segurança digital. Com ela, seu sistema e seus arquivos não podem ser acessados sem suas chaves – ou sem a quebra da criptografia, algo muito difícil de realizar se a encriptação foi bem-feita e a senha é forte. Criptografar apenas partes ou arquivos específicos deixa o sistema mais vulnerável e, via de regra, deve ser feito apenas em conjunto com a criptografia de disco, não no lugar dela.

Com a encriptação de todo o disco, seus dados estarão muito mais protegidos – seja após um furto, uma força de repressão, um familiar enxerido, uma assistência técnica inescrupulosa… A criptografia de disco pode ser feita em diversos dispositivos, mas tem eficácias diferentes: em computadores, pendrives e HDs externos, elas são mais seguras, estáveis e difíceis de quebrar.

Em celulares, por conta de sua arquitetura, a encriptação do disco segue sendo uma recomendação básica – e capaz de impedir muitos acessos não autorizados –, mas é mais vulnerável a quebras e acessos, especialmente por parte de atores estatais.

Um programa bastante recomendado para encriptação é o **VeraCrypt**. Com suporte para vários

sistemas (Windows, macOS, diversas distribuições GNU/Linux), livre, código aberto e derivado do TrueCrypt, o VeraCrypt é bastante intuito e capaz de criptografar discos inteiros ou partes deles. Ao criptografar o disco inteiro, a única diferença no dia a dia para o usuário é que, ao ligar o computador, é preciso digitar uma senha – que, obviamente, deve ser forte, já que uma senha fraca diminui muito a proteção provida pela encriptação de disco.

Em diversas **distribuições Linux/GNU, a criptografia de disco é uma opção apresentada no momento de instalação**. Há ainda opções de softwares privados de criptografia nativa em alguns sistemas, como Windows e macOS, que possivelmente comprometam sua privacidade.

CRIPTOGRAFIA DE PONTA A PONTA

Enquanto a encriptação de disco é de dados em repouso, a criptografia de ponta a ponta é uma ferramenta para proteger informações que estão sendo transmitidas. Com ela, **os dados são criptografados na hora do envio (uma ponta) e só podem ser abertos pelo destinatário correto (a outra ponta), impedindo que sejam lidos por qualquer um no**

meio do caminho, incluindo o servidor que envia as mensagens, o provedor de internet ou qualquer interceptação que possa ocorrer no meio do caminho.

É um recurso **fundamental para a comunicação mais segura** que pode ser usado, por exemplo, em e-mails ou aplicativos de mensagem. Um dos conceitos importantes para diversas ferramentas que contam com criptografia de ponta a ponta são as chaves: para, por exemplo, enviar um e-mail criptografado com PGP (Pretty Good Privacy, em português: privacidade muito boa). É frequentemente utilizado para assinar, encriptar e descriptografar textos, e-mails, arquivos, diretórios e partições inteiras de disco e para incrementar a segurança de comunicações via e-mail. Foi desenvolvido por Phil Zimmermann em 1991. Nele, você utiliza uma chave pública do destinatário e a mensagem só poderá ser decifrada com a chave privada e secreta da pessoa que vai receber esta mensagem, sem poder ser lida por alguém que intercepte o e-mail.

Para aumentar a confiança no sistema, existem as ***fingerprints*** – as "impressões digitais", um código longo único (ou mesmo um QR code) que **garante que aquela chave pertence a pessoa que você quer conversar**. Para funcionar, você deve conferir esta impressão através de um modo seguro –

preferencialmente, pessoalmente – e aí saber que as mensagens seguintes enviadas vêm da pessoa certa.

Um ponto importante a se observar na criptografia de ponta a ponta é que, em muitas das técnicas e plataformas que a utilizam, o que fica encriptado é apenas o conteúdo da mensagem, com os **metadados – os dados sobre a mensagem – ainda passíveis de serem lidos**. Assim, é possível que, ao interceptar a mensagem, mesmo que alguém não saiba exatamente o que você conversou, saiba com quem você falou, que horas e por quanto tempo.

11
METADADOS E ARMAZENAMENTO

Os arquivos têm informações que os identificam – são os metadados, dados sobre os dados, como e quando ele foi criado ou em que dispositivo... Programas como o **ExifCleaner** e o **MAT2** buscam deletar estes metadados e preservar sua privacidade ao compartilhar arquivos.

Arquivos deletados no computador não somem completamente e podem ser recuperados. Por isso, é bom apagar arquivos sensíveis de maneiras mais seguras, usando aparelhos como o **BleachBit**, que fragmenta o arquivo ao deletá-lo. Isso serve também para registros físicos: deve-se ter cuidado ao descartar documentos, agendas, cadernos, atas… fragmentadoras podem também ser usadas com os impressos ou manuscritos.

Além da destruição de arquivos individuais, é possível limpar HDs inteiros, com ferramentas

específicas. Há debates sobre a eficácia de programas como o **Darik's Boot and Nuke (DBAN)** e a capacidade ou não de recuperar arquivos após limpezas completas – este é mais um motivo que ressalta a importância da criptografia de disco, já que é virtualmente impossível recuperar algo de um disco encriptado corretamente e depois limpo. Em **SSDs**[14], é mais difícil garantir uma limpeza com qualidade razoável, com alguns fabricantes disponibilizando métodos específicos para seus produtos.

Há quem recomende, para além da destruição via software, a destruição de hardware – ou seja, a destruição física dos discos, incluindo desfragmentação, incineração, cortes, perfurações, dobras e até mesmo atirar no HD no caso de uma necessidade emergencial de eliminar arquivos.

A menção a atirar é do National Institute of Standards and Technology (NIST)[15], equivalente ao INMETRO nos EUA – com a nota de que alguns destes métodos podem apenas danificar

14. A sigla significa Solid State Drive ou Unidade de Estado Sólido, em português. É uma tecnologia de armazenamento ou memória de dados mais recente que o HDD (Unidade de Disco Rígido, em português) para computadores, a princípio, mais rápida e silenciosa.
15. Guidelines for Media Sanitization | NIST Special Publication 800-88 Revision 1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

parte dos discos e manter algumas informações recuperáveis, se não feito de forma adequada. Cabe dizer que, segundo arquivos divulgados por Snowden, o NIST colabora com a NSA e nem todos os seus métodos podem garantir destruição que impeça peritos forenses da comunidade de inteligência dos EUA de lerem os arquivos.

12
REUNIÕES E LIVES

Para reuniões onlines e chamadas, há diversos aplicativos e programas disponíveis, com diferentes graus de segurança e privacidade. Uma solução com razoável número de recomendações é o **Jitsi Meet**, livre e código aberto, com opções para criptografia ponta a ponta e podendo ser utilizado em computadores e celulares. Ele pode ser utilizado diretamente do site (https://meet.jit.si/) ou hospedado pela entidade. Pelo site, há limitações de quantas pessoas conseguem acompanhar a reunião antes de problemas de conexão aparecerem – não há limite exato, até por depender também da conexão dos próprios usuários, mas eventos com mais de 30 pessoas encontram complicações. No caso de se hospedar num servidor próprio, os limites vão de acordo com a qualidade da conexão existente.

Outras ferramentas incluem o **Element** (antigo **Riot**), o **Mumble** (apenas áudio, sem criptografia

de ponta a ponta – então fazer a própria hospedagem é fundamental), o **Jami** e o **BigBlueButton** (também para fazer a própria hospedagem). Boa parte destas ferramentas não é tão acabada ou refinada quanto soluções de grandes empresas de tecnologia, mas o foco aqui recai mais em privacidade e segurança que na usabilidade. A solução mais adequada para qual entidade depende das necessidades específicas.

Para lives e apresentações, algumas dicas básicas podem melhorar a experiência e aumentar sua segurança:

1. ESCOLHA BEM A PLATAFORMA EM QUE VAI REALIZAR A LIVE E TESTE-A ANTES
   Decidir em cima da hora pode trazer muitos problemas, como dificuldades de conexão, incompatibilidades de navegador ou falta de recursos necessários para sua atividade – como limite de tempo, participantes ou apresentação de telas.

2. RESTRIÇÃO DAS PESSOAS NA SALA DA ATIVIDADE
   Dentro da sala em que está sendo realizada a atividade, só devem estar presentes a organização e os participantes. Quem vai acompanhar a live deve assistir numa plataforma pela qual

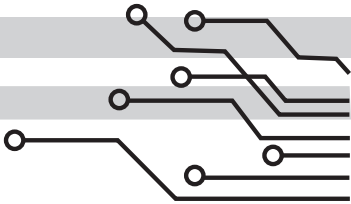
não tenha como interromper ou atrapalhar a transmissão. Exemplificando: Num debate, as pessoas que vão compor a mesa entram numa sala do Jitsi. Nesta sala, além delas, só estão membros da organização da atividade e uma delas usa um aplicativo como o OBS Studio para transmitir o que acontece na sala para uma plataforma de transmissão – como o YouTube, Facebook ou Instagram. Quem vai assistir a live só tem acesso a este link público e, assim, não tem como interromper a atividade.

3. PROTEJA A SALA ORIGINAL
   A sala privada da atividade deve ser protegida com uma senha forte, conhecida apenas por quem está participando, e mesmo o link deverá ser protegido, não sendo compartilhado nem exibido na transmissão pública.

4. PROTEJA AS CONTAS
   As contas que vão realizar a transmissão publicamente – no Youtube, Facebook, Instagram, etc – devem ser protegidas para que não sejam invadidas e a atividade seja interrompida. Assim, é fundamental que as contas possuam senhas fortes, utilizem autenticação em dois fatores e que os logins sejam monitorados, impedindo acessos não autorizados.

5. ACOMPANHE O PÚBLICO E MODERE OS COMENTÁRIOS

É preciso que alguém da organização da atividade esteja monitorando atentamente o público assistindo à live. Comentários com mensagens de ódio ou que busquem atrapalhar o andamento do evento devem ser ocultados e seus autores retirados. Caso aconteça um ataque coordenado, com muitos comentários simultâneos e eventualmente até uso de bots, pode ser necessário desativar completamente os comentários, ao menos até que seja possível retirar todos os atacantes da transmissão.



13
REDES SOCIAIS, NUVEM, DRIVES E E-MAILS

Grandes empresas de tecnologia não só armazenam uma gigantesca quantidade de dados para fins comerciais como têm agendas políticas próprias e podem ter relações com agências de inteligência e vigilância – como revelou Snowden. Assim, é fundamental **não usar redes sociais corporativas para se organizar, reservando-as apenas para fins de divulgação e agitação**.

Isso vale também para e-mails, redes, sites para escrever textos, fazer questionários, planilhas, armazenamento de arquivos na nuvem… o **PrimsBreak** (https://prism-break.org/en/categories/gnu-linux/#email) e o P**rivacidade.Digital** (https://www.privacidade.digital/provedores/) apresentam algumas alternativas mais privadas e seguras.

Entre alguns exemplos, estão o coletivo Riseup

tem serviço de **e-mail, VPN, lista de e-mails, editor de textos, compartilhamento de arquivos e rede social**. Provedores como ProtonMail, Disroot e Tutatona têm opções gratuitas de e-mail, focadas na privacidade. O CryptPad e o EtherCalc têm ferramentas de texto e tabelas online (e armazenamento, no caso do CryptPad).

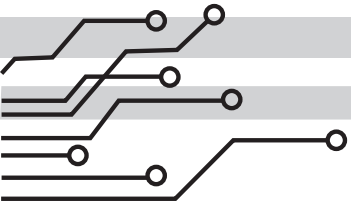
Também existem **soluções que podem ser hospedadas pela própria entidade** e trazem diversos serviços, como o Nextcloud e EteSync. Para **compartilhar arquivos**, sem necessariamente armazená-los por muito tempo, há opções como o **OnionShare** (com envio e recebimento através da rede Tor) e, do Riseup, o share.riseup.net (também com versão acessível pela rede Tor).

Também para envio de arquivos de forma segura e privada, existe o **SecureDrop** (https://securedrop.org/), ferramenta desenvolvida para proteger fontes e denunciantes (*whistleblowers*) e utilizada por diversos veículos de imprensa.

As opções são **diversas e cabe analisar, dentre as ferramentas disponíveis, as mais adequadas para as necessidades da entidade** – tanto as organizacionais e de trabalho quanto de segurança e privacidade.

Para **e-mails**, há uma ferramenta fundamental para segurança e privacidade para além da escolha de um provedor de confiança: o uso de **criptografia ponta a ponta, através do protocolo PGP**. Com esta ferramenta, seu e-mail é encriptado com uma **chave pública** de quem você quer se comunicar, mas só pode ser aberto com a **chave privada** que esta pessoa possui.

Para enviar e receber e-mails com **PGP**, uma boa opção é o **Mozilla Thunderbird**, em conjunto com a extensão **Enigmail**. Você pode conferir um guia de como gerar as chaves e utilizar o programa no Securityinabox (https://securityinabox.org/pt/guide/thunderbird/linux/) e no Riseup (https://riseup.net/pt/security/message-security/openpgp).



14
CELULAR

VULNERABILIDADES

Boa parte da vida hoje passa por celulares inteligentes ou smartphones – conversas, trabalho, ativismo/militância, relacionamentos… essa concentração é perigosa, pois se o aparelho é comprometido ou extraviado, informações de todas estas áreas podem ser obtidas. Por isso, é bom manter o celular criptografado, com uma boa senha e **evitar concentrar dados nele**. Isso pode ser feito de duas maneiras: **não usando o celular para tratar de assuntos sensíveis, minimizando o uso do celular** e **rotineiramente limpando os arquivos**, mensagens e fotos do aparelho.

Além de concentrar dados, **celulares também podem ser usados diretamente na vigilância** de alguém. Os dados de localização, por exemplo, podem ser continuamente coletados, seja por

aplicativos, pelo sistema ou mesmo pelas torres de celular que o aparelho se conectar.

Muitos dos **dados são coletados de maneira aberta** (ainda que não necessariamente legal) por **sistemas e programas de grandes empresas de tecnologia** e, por isso, é importante pensar nas possibilidades de usar **sistemas operacionais alternativos** (como LineageOS, GrapheneOS e CalyxOS), diminuir ou **evitar programas que violem sua privacidade, limitar as permissões** destes aplicativos e buscar ferramentas de código aberto, livre e com respeito aos direitos digitais. Diversos destes programas podem ser obtidos através de plataformas como **F-Droid**, para Android e alguns derivados – ainda que nem todos os programas na loja cumpram estes requisitos.

Celulares também podem ser **comprometidos por programas maliciosos**, que podem ser instalados **disfarçados como aplicativos inofensivos**, ou instalados de **maneira oculta**, através de métodos como **arquivos**, anexos e links **contaminados**. Há também programas desenvolvidos para suposto **controle de pais ou de empresas**, que podem ser usados de forma abusiva para vigilância – inclusive de parceiros/as e em situações de relacionamentos abusivos.

Com **programas voltados para vigilância**, as possibilidades de coleta de dados aumentam, com aplicativos capazes de registrar as **chamadas**, ler as **mensagens**, ouvir indevidamente o **microfone**, abrir a **câmera** ou mesmo **alterar** coisas dentro do aparelho.

É o caso de celulares infectados com o **Pegasus**, *malware/spyware* desenvolvido pela israelense **NSO Group**, vendido a diversos atores e utilizado para monitorar, entre outros alvos, jornalistas e defensoras(es) de direitos humanos. Sobre o caso, a Anistia Internacional publicou um resumo do assunto, em português (https://anistia.org.br/informe/projeto-pegasus-vazamento-massivo-de-dados-revela-spyware-da-nso-group-usado-para-atingir-ativistas-jornalistas-e-lideres-politicos-em-todo-o-mundo/) e um relatório forense, de maneira muito mais completa, em inglês (https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/).

Utilize bloqueio de tela e uma senha forte, mantenha sempre o sistema atualizado, desative o *wi-fi* e o Bluetooth quando não estiver usando, não baixe arquivos e aplicativos desconhecidos e não conceda permissões desnecessárias para programas – um app para jogar paciência não deve ter acesso ao microfone, por exemplo.

Mesmo com um celular não comprometido e com boas práticas de segurança, os dados dele podem ser usados para apontar sua localização – às vezes, convém deixá-lo em casa.

A proteção do aparelho também conta e, por isso, é importante, por exemplo, não deixá-lo exposto, fora da sua guarda, usá-lo enquanto caminha ou com as janelas do carro abertas. Recomenda-se bloquear, em caso de iPhones, o acesso ao iCloud pelo celular para que ninguém além de você possa mudar a sua senha e trocar seu FaceID / TouchID. É recomendado ainda, para qualquer tipo de smartphone, o uso de senhas para acessar aplicativos que possam dar acesso a dados sensíveis, como e-mail, bancos e até aplicativos que tenham o cartão de crédito cadastrado (como o BitWarden e outros).

APLICATIVOS DE MENSAGENS

Para **troca de mensagens e ligações**, é fundamental contar com **criptografia ponta a ponta** em um aplicativo com **código aberto, auditado** e baseado na **privacidade**. Além disso, é importante que o aplicativo conte com uma razoável **usualidade** (ou seja, é usado comumente, por várias pessoas) e, para que sirva para comunicação, que pessoas o tenham instalado e saibam usar – afinal, é preciso

que quem você queira falar também esteja usando o aplicativo.

Dentro destes requisitos, a recomendação mais comum hoje é o **Signal**, com criptografia de ponta a ponta, código aberto, **foco na privacidade e segurança**, bastante fácil de usar e com um número razoável de usuários. Uma de suas desvantagens, no entanto, é a de, por enquanto, exigir um número de telefone para uso. Outra é que ele é **"centralizado"** – ou seja, as mensagens, ainda que criptografadas, passam pelo servidor do Signal. Mesmo que o servidor não consiga ler, algumas pessoas preferem evitar este problema.

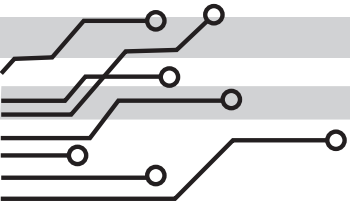
Uma maneira de contornar isto é com **servidores federados**, permitindo que você controle seu próprio servidor. Um aplicativo que funciona nesta lógica é o **Element** (antigo Riot), que utiliza a rede **Matrix**. Outra alternativa é o uso de mensageiros P2P, o *peer to peer*, como o **Jami** e o **Briar**.

Cada uma das opções listadas têm **vantagens e desvantagens**, cabendo a cada organização e defensor avaliar o que é mais adequado para sua realidade. Existem diversas outras também, em diferentes graus de desenvolvimento e recursos para segurança e privacidade.

Alguns dos aplicativos mais conhecidos não são recomendáveis do ponto de vista da segurança e/ou da privacidade: são os casos do WhatsApp e do Telegram. Mesmo com criptografia de ponta a ponta, o código do WhatsApp é fechado e ele pertence à Meta (mesmo conglomerado do Facebook e Instagram), uma empresa que não tem a privacidade dos seus usuários como foco. Além disso, mesmo sua criptografia parece não ser de tanta ponta a ponta assim, com relatos de funcionários da empresa tendo acesso a mensagens de usuários[16]. No caso do Telegram, sua criptografia própria, falta de auditorias e não ter a criptografia de ponta a ponta ativada por padrão motivam sua não-recomendação.

Independente do aplicativo utilizado, convém usar recursos como o de **mensagens temporárias**, deletando automaticamente mensagens antigas (assim como arquivos de mídia) ou deletá-las manualmente de quando em quando, reduzindo a quantidade de informações armazenada no aplicativo e/ou no celular.

16. Em setembro de 2021, o ProPublica, portal de jornalismo investigativo independente dos EUA, revelou que a empresa monitora e compartilha regularmente informações pessoais com promotores. (https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users).



15
GRAMPOS EM LIGAÇÕES E AMBIENTE

No Brasil, **grampos – legais e ilegais – são bastante comuns em telefones**. Assim, deve-se **evitar tratar de assuntos sensíveis por ligaçõe**s. De maneira geral, é válido **trocar chamadas normais por ligações via internet**, desde que por **aplicativos seguros** (como o Signal).

Há diferentes tipos de grampos. O mais tradicional é o feito **diretamente na linha telefônica**. Teoricamente, devem ser feitos apenas com autorização judicial e sob necessidade extrema, mas tornaram-se prática corriqueira em investigações criminais. Além disso, há o risco de grampos ilegais ou irregulares, como os feitos com autorização judicial mas sob falsos pretextos – inserindo números de adversários políticos em investigações sem nenhuma relação com estes alvos, por exemplo. Apesar de "lendas urbanas"

sobre cliques, ruídos e ecos, em quase todos os grampos feitos na linha, não há alteração para quem está na chamada.

Além do uso em investigações, existe o recurso de **divulgação de eventuais gravações** – independente da legalidade da gravação ou de sua divulgação – muitas vezes com fins de **influenciar o debate público**. Estes registros divulgados podem inclusive ser fruto não de grampo, mas de simples gravação por parte de um dos participantes da conversa. Os registros podem também passar por **edição ou descontextualização**. Avanços em tecnologias, como ***deepfakes***[17], tendem a agravar consideravelmente este problema.

Outro método é **comprometer diretamente os aparelhos** – desde rudimentares gravadores em telefones fixos de ontem até ***malwares*** em celulares de hoje. Variam muito de acordo com o método utilizado, podendo ser de baixa complexidade (como programas "espiões" instalados por parceiros abusivos) até mais complexos, que demandam mais recursos e costumam partir de atores maiores, como Estados.

17. *Deepfake* é um tipo de manipulação ou edição de conteúdos como áudios e vídeos através da inteligência artificial e que permite, por exemplo, substituir o rosto de uma pessoa pelo de outra, sincronizar um áudio como os movimentos labiais e outras possibilidades.

Como podem ser utilizadas ferramentas muito diferentes, não há uma única recomendação, cabendo seguir as orientações de segurança apresentadas neste guia e **adaptá-las para sua realidade**. Um adendo é que no caso de comprometimento do celular por um programa malicioso avançado, não há diferença na ligação normal ou via internet/aplicativos, já que o próprio microfone pode estar comprometido.

Os **microfones de celulares** são, inclusive, fonte de desconfiança para muitos defensores e defensoras de direitos humanos. Seu uso como grampos ambientais é plausível, do ponto de vista técnico, mas não prático do ponto de vista do que é necessário para a vigilância dos celulares de todas as defensoras(es) em todos os momentos. Os recursos para essas operações são grandes, então tendem a ser mais direcionados e utilizados apenas por grandes atores. A chance de um celular de uma liderança estar comprometido é consideravelmente maior do que a de defensoras(es) com atuação não-pública, ainda que não necessariamente grande em nenhum dos casos. **Por precaução, diversos movimentos e organizações preferem realizar reuniões com os celulares fora do ambiente**.

Há também o debate em torno de gravações do **som ambiente por celulares (ou outros aparelhos inteligentes, como TVs, assistentes virtuais e até mesmo geladeiras)** por aplicativos e sistemas legítimos. Embora não existam conclusões definitivas sobre seu uso para vigilância e/ou para marketing, a depender do grau de ameaça, pode ser interessante evitar debates sensíveis em ambientes com qualquer um destes aparelhos, bem como buscar alterar as configurações para desativar compartilhamento de dados e solicitar privacidade aos fabricantes – ainda que com poucas garantias de ser atendido.

Ainda em grampos e vigilância de conversas, existem os **grampos ambientais, as escutas ambientais**. Campo muito famoso nos filmes de espionagem – e na espionagem real – há grampos ambientais dos mais variados sistemas e funcionamentos: dos que transmitem continuamente, os que gravam quando há atividade, os que não transmitem e devem ser recuperados para se ouvir os registros… A detecção destes pode ser trivial ou muito difícil, a depende da complexidade dos aparelhos.

É importante buscar o **controle de acesso do ambiente**, para impedir a instalação e/ou

recuperação destes aparelhos. Existem ferramentas para detecção de microfones e câmeras ocultas, mas as realmente eficazes são bastante custosas. As baratas, vendidas em lojas online, tem eficácia no máximo dúbia, com muitos falsos positivos (e, possivelmente, falsos negativos).

Por fim, a **vigilância por áudio** pode também ser feita a **distância**, com **microfones de diferentes métodos de funcionamento – como microfones direcionais ou microfones a laser**. Sua eficácia depende de diversos fatores, como o próprio aparelho, se há **linha direta de visão**, se quem está vigiado está num **ambiente aberto**, fechado mas com **janelas**, **fechado**, se há **isolamento acústico**. Como exigem presença física de pessoas participando de uma operação de vigilância, são **muito mais direcionados** e para alvos considerados mais valiosos por quem está vigiando.

MEDIDAS FÍSICAS DE PROTEÇÃO DIGITAL

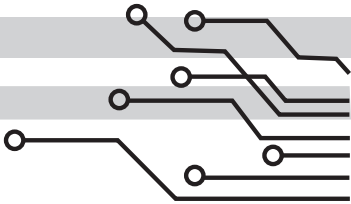
Além de medidas digitais para proteção e privacidade nos dispositivos eletrônicos, existem medidas físicas que podem ser tomadas. A mais evidente delas é a retirada dos aparelhos da equação, seja colocando-os em ambientes

diferentes das em que estão sendo feitas reuniões, ou o não uso deles para troca de algumas informações sensíveis ou deixar por completo de usá-los (ou não os carregar para algumas atividades). Uma mediação feita por algumas pessoas é usar aparelhos "burros", evitando-se dispositivos inteligentes, mais complexos e que podem se conectar a redes – sejam geladeiras, televisões, carros, aspiradores, celulares ou quaisquer outros – numa **tentativa de evitar ou reduzir possíveis coletas de dados e vigilância**.

No caso de celulares, por exemplo, há uma diminuição na "superfície de ataque" – ou seja, de vulnerabilidades que os adversários podem explorar – mas não se zeram os riscos: mesmo aparelhos que não são smartphones ainda podem fornecer dados como localização e estarem sujeitos a grampos.

Em computadores, pode-se usar táticas como computadores que nunca se conectam na internet para dados sensíveis, com outros aparelhos seguros fazendo eventuais envios e recebimentos. Alguns sistemas permitem segregação dentro do próprio aparelho. É o caso do Qubes OS, por exemplo, que busca separar o computador em diversos ambientes isolados entre si, impedindo que ataques em uma parte se espalhem para o todo.

Uma outra tática comum é o uso de barreiras físicas, tais como o bloqueio, a desativação e o desligamento de dispositivos. O exemplo mais comum é o de tapar webcams e câmeras frontais com adesivos, fitas ou tampas. Alguns aparelhos permitem também o corte de energia para dispositivos como câmeras ou microfones. Há quem conecte microfones, fios ou conectores quebrados/rompidos nas entradas de áudio numa tentativa de dificultar a escuta de um adversário – uma medida que ganhou alguma notoriedade após Mark Zuckerberg postar uma foto fazendo isso. Sua eficácia, no entanto, é controversa, e depende bastante do aparelho e do possível ataque.



16
SEGURANÇA DE INSTALAÇÕES

Assim como na segurança física, a **segurança das instalações vai depender de muitas coisas**, como as características do movimento ou entidade, como é seu funcionamento, quais são as ameaças existentes, quem são os potenciais adversários e quais recursos os dois lados têm disponíveis.

Assim, cabe fazer a **avaliação caso a caso**, e medidas muito efetivas para uma entidade podem ser desaconselháveis para outra – ou mesmo dois imóveis da mesma organização podem ter necessidades muito diferentes.

A primeira coisa a se considerar ao pensar na segurança de um imóvel é sua **localização**. É um local **isolado** ou há **vizinhos**? Se há vizinhos, são imóveis residenciais, comerciais, industriais, rurais? A presença de um grande número de

vizinhos pode tornar um ataque mais custoso para um adversário, por aumentar o número de testemunhas e possivelmente reação, enquanto um imóvel isolado pode possivelmente ser atacado sem que ninguém veja. No entanto, no imóvel isolado a vigilância torna-se muito mais difícil, já que há menos imóveis a partir dos quais se pode vigiar – ou vizinhos que podem colaborar com o adversário que monitora o imóvel.

Ainda sobre vizinhos, uma outra consideração é a **altura dos imóveis** ao redor: são mais altos? Possibilitam ver seu imóvel, as movimentações, quem chega e quem sai, se há pessoas dentro? Também podemos pensar no grau de segurança deles: é possível invadir seu imóvel a partir de um dos vizinhos? Há cercas, muros altos, arame farpado? Há câmeras e outros dispositivos de segurança? **Seu imóvel destoa dos outros** – e vai chamar mais atenção caso instale dispositivos de segurança? O imóvel também pode ser uma **sala ou apartamento dentro de um condomínio**, exigindo atenção para **características e procedimentos específicos** daquele local (como se há porteiro, vigilante, número de condôminos, horários de maior movimento, o controle de acesso de visitantes e funcionários, etc).

Na localização, também cabe avaliar o **bairro**, a distância para delegacias, quartéis e órgãos de segurança pública no geral, índices de criminalidade, fluxo de veículos e pessoas, iluminação, **acesso** e **saídas**: Há diversas entradas para a rua? É possível entrar e sair do imóvel por variados caminhos? Além da segurança contra adversários, vale ainda avaliar as chances de **desastres naturais**, inundações, deslizamentos, quedas de árvores, animais peçonhentos, **incêndio**, falta de luz… uma **enormidade de fatores que deve ser pensada dentro do contexto das necessidades e recursos da entidade**.

Na segurança da instalação em si, um **ponto que demanda grande atenção é o perímetro**. O imóvel está murado? Tem cerca? É possível ver de fora para dentro e de dentro para fora? É possível pular as **barreiras perimetrais** (muros, cercas)? Algum ponto é mais baixo, em maior desnível, mais próximo de árvores escaláveis? Pode-se colocar arame farpado ou isso destoaria muito na rua – ou, ainda, poderia parecer muito agressivo para o ambiente desejado? A depender dos recursos disponíveis e do tipo de imóvel, é possível pensar em barreiras organicamente dispostas no imóvel, ficando menos expostas e diminuindo o ar agressivo – no entanto, em alguns imóveis, pode

ser melhor exibir os itens de segurança, em vez de disfarçá-los.

Alguns itens servem mais para **aviso e monitoramento** do que impedimento físico – como sensores de presença e alarmes, inclusive em muros. Apesar de alertarem os ocupantes do imóvel e, dependendo do caso, dissuadir invasores, eles não impedem por si próprios que o muro seja pulado. Outros buscam cumprir as duas funções, como algumas cercas eletrificadas que contam com alarmes. Já dispositivos como arame de concertina tem como objetivo **dificultar ou retardar uma invasão**.

É importante notar o **"dificultar ou retardar" entre aspas pois nenhuma ferramenta vai impedir completamente adversários obstinados, com recursos e tempo sobrando** – até um fosso com jacarés e muros de castelos podem ser vencidos, ainda que demore. As ferramentas de segurança, no entanto, podem dificultar o suficiente para transformar um ataque em impraticável, de pouca valia ou facilmente frustrado.

Diretamente relacionado ao perímetro estão os **acessos ao imóvel, como portões e portas**. Via de regra, um número **maior de camadas de proteção** é ideal – como portões duplos,

sistemas de **eclusas**, trancamento de portões externos do terreno e portas do imóvel em si. Também é importante observar os **métodos de abertura** de portões (manuais, eletrônicos), se é possível ver de fora para dentro e de dentro para fora, se há locais que alguém pode se esconder para tentar emboscar alguém entrando ou saindo. O número de portões é outra consideração a se levar em conta: um único portão diminui os locais que podem ser atacados ou mesmo arrombados, mas dificulta a fuga e torna as rotinas de entrada/saída mais óbvias.

Nas **portas**, é interessante que sejam **reforçadas**, com dobradiças não acessíveis por fora e mais de uma chave e/ou contem com uma outra ferramenta como grades em conjunto. Um número grande de trancas para abrir, no entanto, diminui consideravelmente a velocidade com que a pessoa conseguirá entrar no imóvel, potencialmente **deixando-a exposta por mais tempo** para um eventual ataque. **Janelas e sacadas** também são possíveis pontos de acesso e convém instalar **trancas e grades**, principalmente em andares mais baixos. Grades e número maior de trancas dificultam a entrada de um adversário, mas podem dificultar também a saída da pessoa – inclusive num momento emergencial de, por exemplo, fuga de um ataque ou de incêndio.

Câmeras são um dispositivo bastante utilizado na segurança de instalações, com diferentes aplicações. Em primeiro lugar, buscam servir de **dissuasão** contra potenciais adversários. Em segundo, servem para **monitoramento** constante, para reação em caso de ataque. Por fim, servem para **registro** de ocorrências, investigação e responsabilização posterior. Quais são as necessidades da organização (e em qual prioridade) vão ditar muitas coisas na eventual escolha de câmeras.

Uma entidade que pretenda **dissuadir** vai preferir **câmeras visíveis** e avisos de que elas existem, enquanto uma que prefira manter um perfil mais discreto do imóvel vai ocultá-las – é possível inclusive combinar as duas coisas, usando algumas câmaras chamariz (de "isca"), enquanto outras ficam menos à vista.

Para **monitoramento**, é preciso decidir se haverá **alguém assistindo** às imagens 24 horas por dia, ou durante o período de atividades, se será contratada **empresa de segurança** para prestar este serviço (no local ou remotamente) ou se as câmeras serão apenas para registro. Uma empresa monitorando a todo momento certamente melhora as condições de reagir a um ataque, mas **pode também representar um risco à privacidade**,

com uma companhia alheia sabendo sempre quem está lá, quando chegou e com quem está.

Na questão dos **registros**, novamente a privacidade entra em jogo: os **arquivos serão armazenados apenas localmente**? Serão enviados para uma **nuvem**? Esta nuvem é **segura e criptografada**? Uma empresa de segurança terá **cópias remotas**? Manter a gravação apenas no local evidentemente tem vantagens de privacidade, mas pode ser desastroso para a segurança: numa **invasão**, os **arquivos** podem ser **danificados**, **apagados** ou mesmo **roubados** – inclusive por um adversário que deseje ver as filmagens e quem esteve no imóvel em outros dias.

Várias destas considerações a respeito de câmeras também se aplicam a **sistemas de alarmes**: estarão conectados a uma empresa? Apenas disparam uma sirene no local? Pode-se monitorar remotamente? Muito comum em residências e menos em imóveis institucionais, está o uso de cães de guarda. Ainda que com uma série de ramificações, debates e recursos necessários para manter, segue sendo uma medida com eficácia razoável.

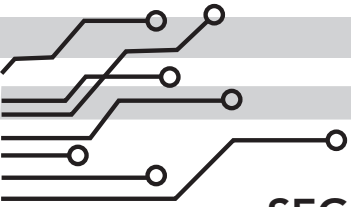
A **visibilidade no e do imóvel** é outro ponto importante. A visibilidade no imóvel vem de pontos

como conseguir monitorar a rua – fundamental para saber se é possível entrar ou sair com segurança, se há pontos cegos e se há locais para se esconder. A visibilidade do imóvel diz respeito à facilidade ou à dificuldade que alguém monitorando terá de saber se há pessoas presentes, onde estão, se vão sair em breve, se é possível vigiar sem ser visto.

Os "comos" disto variam muito de imóvel para imóvel, mas incluem itens como altura dos muros, iluminação pública e do próprio imóvel (inclusive com sensores de movimento), vegetação, paisagismo, arborização, estruturas no jardim ou rua (como de gás, de correspondência ou de lixo), material e estado de portas, portões, existência de olhos mágicos, janelas, cortinas e persianas.

A **visibilidade** também conta na **parte interna**: pessoas na rua ou vizinhos conseguem ver dentro dos cômodos? As pessoas no imóvel ficam de costas para janelas e demais aberturas? É possível monitorar, gravar ou ouvir conversas e reuniões em ambientes do imóvel? Principalmente em imóveis abertos ao público, é importante garantir que seja possível ver quem está vindo, sem ser pego de surpresa ou de costas para a entrada, e, se possível, ter uma recepção que não dê acesso imediato ao restante do imóvel.

Dentro do imóvel, pode-se também aplicar a lógica de mais **camadas de proteção**, com alguns cômodos mais protegidos de acordo com a necessidade – como um quarto com porta reforçada, uma sala de arquivos com trancas, um espaço de reuniões com acesso controlado, sem janelas e com isolamento acústico.



17
SEGURANÇA FÍSICA DAS PESSOAS

A segurança física das pessoas deve ser sempre a prioridade, para preservar integridade e vida de toda defensora e todo defensor. Trata-se de um processo coletivo, mas em que também os indivíduos assumem responsabilidades. É preciso que as pessoas evitem exposição e riscos desnecessários, evitem a previsibilidade, variem como possível as rotinas e rotas e mantenham-se em comunicação constante com camaradas.

Por outro lado, as entidades devem buscar prover condições para que as pessoas consigam aplicar procedimentos e utilizar ferramentas para sua proteção, monitorar as ameaças aos indivíduos, dar apoio e acolher quem foi ameaçado e atuar de maneira proativa para evitar que ameaças se concretizem em ataques.

A redução dos riscos no cotidiano passa por,

antes de tudo, realizar análises de ameaças individualizadas e buscar adequar sua realidade a ela – defensoras(es) em diferentes graus de atuação e exposição precisam adotar diferentes medidas de proteção. Alguns procedimentos bastante aplicáveis incluem evitar andar sozinho e/ou com vestuário que a identifique enquanto defensora e defensor (como camiseta, adesivos e bottons), planejamento prévio da rotina – evitando locais inseguros, vazios, mal iluminados –, prestando atenção no cotidiano e tomando nota de atividades suspeitas ou sinais de vigilância.

Em relação à proteção física individual, há diversos debates sobre, por exemplo, formações em defesa pessoal e/ou artes marciais. Embora não sejam um problema em si, não são aplicáveis para todas as pessoas, podem causar uma equivocada sensação de segurança e certamente não são substitutivos para outras medidas de proteção – inclusive porque a ideia é evitar confrontos e, caso inevitável, desvencilhar-se o mais rápido possível, não se alongando neles.

Em paralelo, há discussões sobre aparelhos para defesa pessoal, nas quais cabem alguns rápidos comentários e dois gerais: todos eles podem acabar sendo tomados pelo agressor e utilizados

contra quem se defende; as chances de reação bem-sucedida a ataques de pessoas surpreendidas são baixas e tentativas frustradas de reação podem causar mais dano. A prevenção para evitar a situação é mais importante do que a reação quando o ataque já está dado.

Aparelhos contundentes (como cassetetes e bastões) são difíceis de portar – principalmente velados – e ainda mais difíceis de utilizar, com chances razoáveis de serem tomados de quem está se defendendo. Podem ainda extrapolar os limites éticos e legais da defesa pessoal.

Aparelhos cortantes (como facas) são mais fáceis de portar, porém mais difíceis de manusear e, ao introduzi-los em uma situação de confronto, se escalona a situação para o uso de força letal, já que facas são, mesmo que não intencionalmente, instrumentos letais. Possibilidades de serem tomadas de quem se defende também são razoáveis.

Aparelhos de choque podem ser divididos em dois. O primeiro grupo é o de lançamento de dardos, como nos casos de Taser e Spark. Seu uso é restrito para forças de segurança pública e, portanto, não cabem para defesa pessoal. Aparelhos de choque direto por contato têm legalidade e

eficácia dúbia, com a maioria dos modelos tendo pouca capacidade de frear injusta agressão.

Aparelhos com agentes químicos existem em diversas versões. Excluindo-se aqueles que têm uso restrito por forças de segurança, como o spray de pimenta, existem ainda alguns produtos de uso simples e eficácia razoável, mas não necessariamente incapacitam o agressor, apenas atrapalhando-o. No entanto, podem ser o suficiente para conseguir desvencilhar-se e escapar da situação.

18
AMEAÇAS E ACOLHIMENTO

Para a proteção das pessoas, é importante monitorar constantemente as defensoras(es) e registrar conforme ocorrem incidentes de segurança, ameaças feitas ao defensor, pessoas próximas ou à entidade. O que deve ser feito depende, evidentemente, de cada caso, mas entre as medidas mais comuns – que não são necessariamente excludentes – estão o aprimoramento ou o reforço da segurança da pessoa (como escolta ou reformas para segurança da residência), a denúncia e/ou a exposição das ameaças (com aumento do perfil público das defensoras(es), por exemplo) e a retirada da pessoa do território ou da localidade.

Em qualquer um dos casos e mesmo sem ameaças específicas (na militância no Brasil, sentir-se com medo ou acuado é perfeitamente compreensível, mesmo sem ser ameaçado individualmente) é

importante pensar no processo de cuidado, acolhimento e recebimento das defensoras(es), mostrando-o que ele não está sozinho, que faz parte de um coletivo, buscando apoiá-lo – se necessário, com atendimento especializado para saúde mental e/ou física.

MANIFESTAÇÕES

Em atos, é importante se preparar previamente: saber como será o clima, o tamanho da rota, o ânimo dos presentes e ficar atento a uma possível repressão. Se você está na organização do ato, isso se torna ainda mais importante, sendo necessário planejar bem a rota, os locais para dispersão, ter advogados de sobreaviso, destacar pessoas para a comunicação e para primeiros socorros.

É recomendável evitar chegar, permanecer ou ir embora de um ato sozinha/o e é importante sempre avisar outras pessoas que você está indo, inclusive pessoas que não estarão na manifestação. É interessante formar duplas/trios, que não devem se perder de vista em nenhum caso. Convém levar documento de identificação, contatos de advogados (se tiver), água, algo leve para comer e remédios que faça uso constante. Também é importante fazer uma limpeza prévia dos dados e arquivos do celular.

Se possível, use calçados firmes e fechados. Roupas de algodão reagem pior aos agentes químicos, assim como lentes de contato, então é recomendável não utilizá-las – assim como acessórios e roupas que possam se enganchar ou serem usadas para puxar você. Importante levar remédios, caso utilize, e não levar armas de qualquer tipo, nem objetivos do cotidiano que podem ser enquadrados enquanto ofensivos (tesouras, estiletes, etc).

Entre o arsenal das forças de repressão, é possível dividir entre alguns diferentes tipos de instrumentos mais utilizados. Os primeiros são os contundentes, de contato físico direto – cassetetes, escudos, o próprio corpo de agentes da repressão. Os segundos são projéteis, sejam letais ou menos letais, como os de borracha. Há os espargidores, que são basicamente de onde se lançam agentes químicos como spray de pimenta. Ainda existem as granadas, com finalidades múltiplas – como conter agentes químicos ou serem apenas para desorientar (como as de efeito moral e de atordoamento). Granadas podem ainda ser lançadas diretamente com as mãos ou através de lançadores específicos. Por fim, há alguns outros, como o uso de aparelhos de choque, veículos (especialmente motos) e de animais (cachorros e cavalos).

CONTUNDENTES

Não há muito segredo em seu uso – são basicamente as mesmas armas que a humanidade usa desde a primeira guerra da História, há milhares de anos. Em atos maiores, forças de repressão tendem a preferir manter a distância, utilizando outros meios para forçar a dispersão e usando instrumentos como cassetetes contra manifestantes que ficaram para trás e/ou para efetuar prisões.

PROJÉTEIS

Os letais teoricamente não deveriam ser utilizados em manifestações, mas há casos de seu uso – por vezes com tiros para o alto e de intimidação. Os de borracha são utilizados de maneira corriqueira, contrária inclusive ao manual do fabricante (a Condor) e da maioria das corporações: seu uso deveria ser contra indivíduos específicos, identificados pelo agente da repressão como ameaça e deveriam ser disparados a pelo menos 20 metros, na direção da perna – não é o que ocorre, com casos repetidos, infelizmente, de tiros na cabeça e nos olhos. Há diferentes tipos de projéteis, possuindo focos como precisão, alcance, dispersão e fragmentação. Costumam ser disparados de armas calibre 12, embora existam outras versões.

ESPARGIDORES

Tanto o gás lacrimogêneo (CS – 2-Clorobenzilideno malononitrilo) quanto o agente pimenta (OC – Oleoresin Capsicum) são agentes químicos que atuam nas vias respiratórias, olhos, peles e mucosas, causando ardência, irritação, dificuldade para respirar e para enxergar. São armazenados pressurizados dentro dos espargidores e lançados em jatos, com raio de alcance variando de acordo com o tempo do jato e o tamanho do espargidor. Há também uma versão gel de agente de pimenta, para uso em ambientes fechados.

GRANADAS

A Condor, fabricante da imensa maioria dos equipamentos menos letais utilizados por forças de repressão no Brasil, possui um grande catálogo de granadas, para usos diferentes. As mais utilizadas são a de efeito moral (com barulho alto e pó inerte, para distrair e atordoar) e as de gás lacrimogêneo. Há inúmeras variações das de CS, como as inteiras, as com três ou cinco pastilhas, a "bailarina" (projetada para fazer movimentos aleatórios e dificultar que seja lançada de volta nos agentes). Quase todas as granadas da Condor possuem tanto uma versão que pode ser arremessada com as mãos quanto uma que é atirada por um lançador específico.

APARELHOS DE CHOQUE

O Taser é o mais famoso e a Condor fabrica o Spark. Ambos têm funcionamento semelhante, com lançamento de dardos conectados a arma, dando choques elétricos incapacitantes em quem for atingido. Podem também ser usadas diretamente por contato.

VEÍCULOS

Podem ser utilizados para empurrar ou forçar manifestantes para determinada rota, com veículos avançando para cima das pessoas, quando não atingindo-as.

ANIMAIS

A cavalaria é bastante utilizada para barrar manifestantes ou executar "cargas" sobre o ato, buscando dispersá-lo (geralmente em conjunto com uso de bombas e agentes químicos). Cachorros costumam ser usados mais especificamente contra algumas pessoas ou para bloquear acessos pequenos (como uma porta).

As táticas e procedimentos operacionais padrões de diferentes corporações variam conforme a localidade, e não é possível dar respostas simples que sirvam para tudo em todo o país. É importante observar a quantidade do efetivo deslocado

para o ato, bem como sua composição (são apenas do batalhão local ou incluem unidades especializadas, como Choque?), suas movimentações e possíveis preparações para um ataque, seja para forçar a dispersão da manifestação ou prender alguns presentes no ato.

Para alívio da ação dos agentes químicos, o mais recomendado é água corrente – só água (de uma garrafa, por exemplo) pode até piorar a situação, dependendo de qual agente foi utilizado. Leite de magnésia parece aliviar efeitos de gás lacrimogêneo, mas não há comprovação científica. Vinagre é mais uma lenda urbana do que uma medida realmente efetiva.

Segundo a Condor, estes são os procedimentos para primeiros socorros:

> *"Para alívio e descontaminação das pessoas afetadas, as seguintes providências devem ser tomadas: 1) Remover a pessoa da área contaminada; 2) Estimular a pessoa a remover as lentes de contato. Se necessário, solicitar ajuda médica para remoção das lentes; 3) Não deixar que a pessoa contaminada esfregue os olhos; 4) Submeter a pessoa a ventilação prolongada; 5) Lavar as*

partes afetadas com água em abundância e sabão neutro, ou solução de bicarbonato de sódio a 10%; 6) Troque as roupas da pessoa contaminada; 7) Persistindo os sintomas, procure um médico."

No ato em si, é importante ficar calma/o, na medida do possível, **evitando o pânico**, buscando respirar fundo – às vezes, figurativamente, para evitar inspirar agentes químicos – e raciocinando quais os próximos passos. Neste ponto, o planejamento prévio é fundamental: se você pensou antes no que fazer, é mais fácil executar no momento, mesmo que esteja difícil pensar.

Justiça Global. Guia de proteção digital para
defensoras e defensores de direitos humanos
Rio de Janeiro: Justiça Global, 2022.

Facebook: /justicaglobal
Twitter: @justicaglobal
Instagram: @justicaglobal

ISBN: 978-65-87127-06-4