

Como documentar durante bloqueios da internet

Índice:

[Introdução: como documentar durante bloqueios da internet](#)

[Configurando um telefone para documentar quando não há internet](#)

[Quais aplicativos devo usar para documentar?](#)

[Como garantir que sua mídia possa ser verificada por outras pessoas durante um bloqueio da internet](#)

[Como fazer backup da mídia do telefone sem internet ou computador](#)

[Como compartilhar arquivos e se comunicar durante um bloqueio da internet](#)

Introdução: como documentar durante bloqueios da internet

Em junho de 2019, à medida que os abusos dos direitos humanos e uma crise humanitária continuavam em Mianmar, o Ministério de Transporte e Comunicação do país [ordenou que as empresas de telecomunicações](#) encerrassem o seu serviço de internet móvel em partes do estado de Rakhine e no estado vizinho de Chin. Citando "distúrbios da paz" e "atividades ilegais", o governo de Mianmar afirma ter decretado o bloqueio da internet ["para o benefício do povo"](#). Na realidade, os cortes impediram que [mais de um milhão de pessoas](#) tivessem acesso a informações e comunicações essenciais e interrompeu esforços humanitários. Como [afirmou](#) Matthew Smith, da organização [Fortify Rights](#), "Este bloqueio acontece no contexto do genocídio em curso contra os rohingya e de crimes de guerra contra Rakhine, e mesmo que tivesses a intenção de mirar em combatentes, é algo flagrantemente desproporcional".

O bloqueio foi [parcialmente suspenso em cinco dos municípios](#) em setembro de 2019, mas não acabou. Durante o mesmo mês, no país vizinho, Bangladesh, para onde muitos rohingya fugiram, as autoridades ordenaram que as operadoras de telefonia móvel suspendessem [os serviços de 3G e 4G](#) nos campos de refugiados rohingya e parassem de vender cartões SIM de celular para membros do grupo étnico. À medida que entramos em 2020, [quatro distritos em Rakhine](#) ficaram isolados do mundo, e Bangladesh [continuava a limitar o serviço](#) nos campos de refugiados. Periodicamente, as autoridades de Mianmar cortam o serviço, e milhões no país ficam na escuridão.

Documentando durante bloqueios da internet

As suspensões propositais da internet estão aumentando globalmente. De acordo com a [campanha #KeepItOn, da AccessNow](#), houve 128 cortes intencionais da internet entre janeiro e julho de 2019, em comparação a 196 em todo o ano de 2018, e um aumento

acentuado dos 106 cortes de 2017 e 75 de 2016. Em todo o mundo, governos, com a cooperação de empresas de telecomunicações, cada vez mais recorrem a bloqueios do acesso à internet como uma estratégia para reprimir comunidades, prevenir a mobilização e impedir que informações sobre violações de direitos humanos sejam documentadas e compartilhadas.

“Os bloqueios da internet e as violações aos direitos humanos andam de mãos dadas.”

- Berhan Taye, AccessNow

Os bloqueios podem assumir várias formas, incluindo [a suspensão de plataformas específicas, como aplicativos e sites populares](#), o [desligamento da rede de dados móveis](#), a [limitação da largura de banda](#) ou [cortes totais da internet](#). Todos esses tipos de entraves têm como objetivo interromper a capacidade de comunicar informações e de expor violações em tempo real. Frequentemente, ocorrem durante protestos, eleições e períodos de instabilidade política, e costumam ser acompanhados por repressão estatal intensificada, ofensivas militares e violência. Embora os governos possam tentar justificar os cortes [em nome da “segurança pública” ou de outras razões](#), os bloqueios ocorrem claramente em momentos em que os Estados repressivos têm medo de perder um tênue controle sobre seus povos, sobre informações ou sobre a narrativa política. As paralisações violam os direitos humanos, afetam gravemente as [vidas e os meios de subsistência](#) das pessoas e também têm um [impacto econômico](#) global.

Documentar violações dos direitos humanos é muito importante durante um bloqueio do acesso à internet. Ainda que as informações não possam ser compartilhadas naquele momento, a documentação pode ser uma forma de preservar as vozes que as autoridades estão tentando silenciar e de garantir a existência de evidências de abusos que podem ser usadas para exigir responsabilizações posteriormente. Obviamente, o contexto repressivo e os impedimentos tecnológicos durante um bloqueio da internet tornam a documentação das violações — e a manutenção dessa documentação com segurança — muito mais desafiadora e arriscada. **Como os ativistas podem registrar e proteger seus vídeos durante uma paralisação da internet, e até mesmo compartilhá-los offline, fazendo isso de maneiras mais seguras?**

Esta série

Por meio do nosso trabalho com ativistas que passaram por bloqueios da internet, aprendemos algumas dicas e abordagens úteis para **capturar e preservar documentações em vídeo durante esses momentos**. Esta série foi escrita tendo por base dispositivos Android, mas as dicas podem ser aplicadas também a iPhones. Algumas das estratégias requerem planejamento prévio (e, frequentemente, acesso à internet), portanto, é uma boa ideia revisar as dicas e implementar todas as etapas *antes de* chegar a uma situação em que você não tenha internet e precise documentar. Salve uma cópia dos

tutoriais para que assim possa consultá-los ou compartilhá-los durante o bloqueio. E, finalmente, comece a praticar as técnicas e métodos em seu trabalho diário, para que se tornem algo natural antes de se encontrar em uma situação de crise.

- Preparação
 - [Configurando um telefone para documentar quando não há internet](#)
- Captura
 - [Quais aplicativos devo usar para documentar?](#)
- Armazenamento
 - [Como garantir que sua mídia possa ser verificada por outras pessoas durante um bloqueio da internet](#)
 - [Como fazer backup da mídia do telefone sem internet ou computador](#)
- Compartilhamento
 - [Como compartilhar arquivos e se comunicar durante um bloqueio da internet](#)

Uma observação final: embora essas dicas possam ajudá-lo a continuar a documentar em caso de bloqueios da internet, queremos enfatizar que a solução final deve ser a restauração do acesso à internet e a defesa do [direito de registro](#) e das liberdades de expressão, informação e reunião. Felizmente, há um movimento global liderado por organizações como a [NetBlocks](#), a [AccessNow](#) e muitas outras que ativamente monitoram e compartilham informações sobre bloqueios da internet. Ativistas em todo o mundo estão envolvidos em [litígios estratégicos contra os bloqueios](#). Somos solidários com o seu trabalho de defesa dos direitos humanos.

Configurando um telefone para documentar quando não há internet

Este artigo faz parte de uma série sobre ["Como documentar durante bloqueios da internet"](#)

Última revisão: 31 de janeiro de 2020

Apesar dos bloqueios da internet, as pessoas que estão documentando conseguem capturar importantes evidências em vídeo que podem ser compartilhadas offline ou quando novamente houver acesso à rede.

Aqui estão algumas dicas que aprendemos com ativistas e outros profissionais para configurar um telefone para fazer documentações sem acesso à internet. Observe que algumas das etapas **exigem acesso à internet**, e, portanto, devem ser realizadas antes que ocorra um bloqueio ou durante os períodos em que a conexão for restabelecida. Além disso, não espere até estar em uma situação estressante para executar essas etapas; faça-as agora e dedique um tempo para **treinar o uso do telefone** antes de precisar usá-lo durante uma crise.

Os bloqueios muitas vezes coincidem com medidas de maior controle do fluxo de informações e restrições às liberdades de expressão e reunião. Se você for um documentador, tome precauções extras para proteger a si mesmo e às suas informações durante esses períodos. Se houver o risco de as autoridades confiscarem o seu telefone ou de o obrigarem a desbloqueá-lo e revelar o seu conteúdo (durante um bloqueio ou de outra forma), considere usar um telefone diferente para a documentação, em vez de seu telefone pessoal principal. Isso pode ajudar a reduzir as informações que você carrega consigo e que podem vir a ser comprometidas (por exemplo, seus contatos, contas, mensagens, etc.). Se você não conseguir usar outro dispositivo, ainda poderá seguir este manual para reduzir a quantidade de dados vulneráveis e melhorar a segurança do seu telefone principal.

Se for reutilizar um telefone mais antigo, limpe-o primeiro

Para limpar o telefone, restaure as configurações de fábrica.

Nota: [estudos](#) mostraram que executar uma redefinição para as configurações de fábrica em um telefone não necessariamente limpa todos os dados do aparelho. Na verdade, a única maneira 100% segura de limpar os dados é destruir o telefone, mas esse método não é uma opção se você deseja reutilizar o telefone! [Neste artigo](#), um engenheiro Android sugere criptografar o conteúdo do seu dispositivo antes de restaurar as configurações de fábrica. A criptografia é algo padrão na maioria dos telefones atuais de qualquer maneira, mas caso não seja, vá para Configurações > Segurança> Criptografar Telefone antes de limpar o aparelho e restaurar as configurações de fábrica. Dessa forma, quando você redefinir o telefone para os padrões de fábrica, a chave de criptografia será perdida e todos os dados não apagados ficarão ilegíveis.

Treine práticas básicas de segurança do telefone

Existem práticas gerais de segurança do telefone que são relevantes em todas as situações, esteja você fazendo documentações durante um bloqueio da internet ou não. [Aqui estão alguns recursos úteis de outras organizações](#). Embora nada garanta 100% de segurança, algumas dicas importantes incluem:

- Certifique-se de que seu telefone está criptografado. Os telefones mais novos têm criptografia ativada por padrão. Se você não tiver certeza sobre o seu, verifique as configurações de segurança do aparelho.
- Execute atualizações do sistema operacional (SO) regularmente, pois muitas vezes elas corrigem vulnerabilidades de segurança.
- Atualize regularmente seus aplicativos importantes (como aplicativos de mensagens)
- Defina uma senha forte para o telefone que tenha pelo menos 6 dígitos e não dependa de impressão digital / toque ou identificação facial.
- Configure um bloqueio de tela e um temporizador de bloqueio.
- Desative os serviços de localização se não precisar deles (incluindo serviço de localização de emergência, precisão de localização, histórico de localização e recursos de compartilhamento de localização e opções de verificação de wi-fi e Bluetooth). Verifique também as permissões de localização de aplicativos individuais.

- Desligue o Bluetooth e o wi-fi quando não precisar deles para evitar o rastreamento do dispositivo.
- Desligue o telefone quando não o estiver usando.

Instale aplicativos úteis para a documentação

Para documentações em foto ou vídeo, você pode usar o aplicativo de câmera embutido em seu telefone ou então pode usar um aplicativo de documentação mais especializado, como o [ProofMode](#) ou outros, que permitem uma captura e exportação de metadados mais robusta, identificação e autenticação, criptografia, galerias seguras e outros recursos.

Um aplicativo útil para documentar um *próprio bloqueio* é o [OONI Probe](#), um aplicativo de código aberto que executa testes em seu telefone para avaliar se sites ou plataformas estão sendo bloqueados. O aplicativo pode mostrar como, quando, onde e por quem os sites estão sendo bloqueados. Certifique-se de compreender quais são os [riscos potenciais](#) antes de usar este aplicativo.

Não tem certeza de quais aplicativos usar para documentar? Fornecemos algumas perguntas de orientação em nosso tutorial, [“Devo usar este aplicativo para a documentação?”](#).

Instale alguns aplicativos rotineiros

Ter muito poucos dados e apenas alguns aplicativos especializados em seu telefone pode levantar suspeitas. Para fazer o dispositivo parecer um telefone comum, instale alguns aplicativos rotineiros que são comuns na área onde você está documentando (mas que são baixados de fontes confiáveis) e tire algumas fotos inócuas para a sua galeria.

Para aplicativos de mídia social, você pode desejar criar e fazer login em contas alternativas, mas tenha em mente que contas falsas violam os Termos de Serviço da maioria das plataformas e os requisitos de verificação de identidade de algumas delas podem dificultar a criação de contas falsas. Além disso, você precisará gastar algum tempo criando conteúdo e adicionando amigos ao perfil falso, o que pode ser trabalhoso.

Como instalar aplicativos quando não há internet

Baixar e instalar aplicativos sem acesso à internet é obviamente um desafio. Você precisa baixar os aplicativos com antecedência se considera possível um bloqueio da internet.

Uma estratégia que pode ajudar você e outros mais tarde é baixar o arquivo Android Package (.apk) do aplicativo (**baixado de uma fonte confiável**, como, por exemplo, diretamente do desenvolvedor) e salvá-lo no armazenamento do telefone ou em algum HD.

Ter esses APKs salvos em um dispositivo permitirá que você e outras pessoas compartilhem aplicativos quando não houver internet.

Embora não tenhamos tido a chance de testar, o aplicativo [F-Droid](#) fornece uma interface para trocar esses APKs offline. Aqui está o [tutorial](#) deles.

Mantenha informações pessoais verdadeiras ou privadas / sigilosas fora do dispositivo

Tente reservar o dispositivo para fazer apenas a documentação. Não o use para e-mail, telefonemas ou mensagens com contatos pessoais ou ativistas que possam estar em risco, e não conecte esse dispositivo a nenhuma de suas contas principais verdadeiras.

Use recursos para ocultar conteúdo

Considerando a possibilidade de seu telefone vir a ser vasculhado, pode ser útil tornar suas intenções menos óbvias ou o seu conteúdo mais difícil de encontrar. Para se antecipar a situações em que seu telefone será *examinado apenas superficial e rapidamente*, você pode empregar táticas simples, como:

- Alterar os nomes e ícones dos atalhos do seu aplicativo usando um aplicativo Launcher (como por exemplo, o [Nova Launcher](#), mas há muitas opções), de modo que se torne menos óbvio quais são determinados aplicativos.
- Usar um recurso de privacidade integrado, como o [Modo Privado](#) (Samsung) ou o [Bloqueio de Conteúdo](#) (LG), se o seu telefone suportar essas opções.
- Colocar um arquivo vazio denominado “.nomedia” dentro de qualquer pasta, para assim evitar que a mídia salva em uma pasta apareça em sua galeria. Nota: se a mídia ainda aparecer, pode ser necessário limpar o cache da Galeria. Isso pode não funcionar com consistências em todos os dispositivos.
- Criar pastas ocultas (pastas que começam com “.”) usando um aplicativo gerenciador de arquivos. Você pode mover os arquivos para a pasta oculta manualmente, ou, se usar um aplicativo de câmera como o [Open Camera](#), pode especificar onde a mídia gravada será armazenada. Certifique-se de desativar a opção “mostrar arquivos ocultos” em suas Configurações para que os arquivos ocultos não sejam visíveis.
- Alguns aplicativos de documentação especializados, como o [Tella](#) ou o [Eyewitness to Atrocities](#), armazenam a documentação em galerias criptografadas separadas cujo conteúdo só pode ser acessado de dentro do aplicativo, o que pode tornar o conteúdo menos óbvio para alguém que faz buscas em seu telefone. A documentação nessas galerias seguras requer uma senha de aplicativo separada, por isso permanece criptografada mesmo quando o telefone está desbloqueado.

Observação importante sobre como ocultar o seu conteúdo

É importante observar que as técnicas acima podem ser o suficiente para afastar alguém que está apenas rapidamente passando os olhos pelo seu telefone, mas **não esconderão efetivamente o seu conteúdo de alguém que está realmente investigando você.**

Lembre-se também de que alguns países podem ter leis que restringem ou criminalizam o uso de aplicativos de segurança que criptografam ou apagam seus dados. Usá-los para impedir que as autoridades acessem seus dados pode ser visto como destruição de provas ou obstrução de uma investigação e pode ser punível como crime. Este [mapa](#) (abrangente, mas de 2017) fornece um bom ponto de partida se você tiver dúvidas sobre as leis em seu país.

Configure o compartilhamento offline

Em uma situação em que você não tenha internet depois de capturar o conteúdo, você ainda pode querer retirar a documentação do seu telefone por motivos de segurança, para liberar espaço ou compartilhar com outras pessoas. Descarregar com frequência a documentação de seu telefone também ajudará a minimizar quais informações serão comprometidas caso o seu telefone seja confiscado e desbloqueado.

Mesmo se você não conseguir se conectar à internet, ainda pode se conectar a dispositivos habilitados para wi-fi ou Bluetooth localmente, como outro telefone ou um drive USB wi-fi. Normalmente, o telefone deve vir com um aplicativo / interface para você conectar e transferir o conteúdo. Se o seu telefone for compatível, você também pode conectar um drive ou um conector USB On-The-Go (OTG) para descarregar a documentação para o drive OTG ou outro dispositivo.

Esses métodos são discutidos em mais detalhes em nosso tutorial sobre [compartilhamento de arquivos e comunicação durante um bloqueio da internet](#) e em nossa planilha de dicas [Video como Evidência: Ferramentas Tecnológicas - Transferindo Arquivos](#).

Treine antes que você esteja em uma situação de crise

Configure o telefone agora se e enquanto você tiver acesso à internet. Comece a praticar o uso dos aplicativos em situações cotidianas (nas quais não há problemas de segurança) para que assim você se familiarize e se sinta à vontade para usá-los. Faça da boa segurança básica do telefone a sua prática padrão. Dessa forma, os métodos serão algo natural quando você estiver em uma situação de crise, com outras coisas com que se preocupar.

Confira a próxima publicação desta série, [“Quais aplicativos devo usar para documentar?”](#)

Quais aplicativos devo usar para documentar?

Última revisão: 31 de janeiro de 2020

Existem muitos aplicativos que os documentadores podem usar para capturar imagens em vídeo, desde o [aplicativo de câmera original](#) do seu telefone até aplicativos de documentação mais especializados, como o [ProofMode](#), o [Tella](#), e o [Eyewitness to Atrocities](#). Alguns aplicativos têm recursos que dependem de conexões online, portanto, lembre-se de que esses recursos podem não estar disponíveis caso haja um bloqueio à internet.

Não podemos dizer qual aplicativo específico é o mais adequado para você, pois isso depende da sua situação, das suas necessidades e dos riscos que enfrenta (confira esta publicação do blog para mais informações sobre [como avaliar quais são os seus riscos e ameaças](#)). Com sua avaliação de risco em mãos, as perguntas de orientação abaixo podem ajudar você a avaliar qual aplicativo de documentação de vídeo pode funcionar melhor para a sua situação.

Quem fez o aplicativo, e eu confio nessas pessoas?

Você deve sempre levar em consideração quem são os criadores de qualquer aplicativo que você baixa e instala em seu dispositivo, e se você pode ou não confiar neles para não o colocarem em uma situação de risco, intencional ou não.

Algumas questões a serem levadas em consideração:

- O desenvolvedor do aplicativo é confiável? O que as pessoas de sua comunidade e de sua rede mais ampla estão dizendo sobre esses desenvolvedores e suas ferramentas?
- O desenvolvedor do aplicativo está vulnerável? Considere o contexto do desenvolvedor, e a probabilidade de eles serem obrigados a entregar seus dados ou a criar uma backdoor (porta dos fundos) no aplicativo para fornecer acesso às autoridades; saiba também se já fizeram isso no passado. Em que país os dados são armazenados, e quais são as leis relativas às ordens judiciais nessa jurisdição?
- O desenvolvedor do aplicativo mantém o aplicativo atualizado? Ferramentas sem manutenção são suscetíveis a hackers, que exploram vulnerabilidades descobertas. Verifique o site do desenvolvedor ou a página do aplicativo no Google Play para saber a data da “última atualização”.
- O desenvolvedor do aplicativo está estabelecido e parece que ele será capaz de cuidar e fazer a manutenção do aplicativo ao longo do tempo?

- O aplicativo é de código aberto? Os aplicativos que estão abertos para análise são mais propensos a terem seus problemas de segurança resolvidos ou pelo menos identificados. O desenvolvedor está sendo transparente sobre a eficácia e a segurança do aplicativo?
- Que motivações ou incentivos impulsionam o trabalho do desenvolvedor de aplicativos e como isso pode influenciar o seu nível de confiança? Por exemplo, eles são motivados por uma missão? Tem fins lucrativos? São patrocinados por um determinado financiador?
- Embora não seja um indicador direto de confiabilidade, o preço do aplicativo pode ser um fator importante a se considerar. Alguns aplicativos têm um alto custo de assinatura mensal ou têm uma taxa por vídeo.

Confira o guia de autodefesa contra a vigilância da [EFF](#) para obter mais informações sobre como [escolher aplicativos](#).

De onde o aplicativo pode ser baixado?

Você deve sempre baixar e instalar aplicativos apenas de lojas de aplicativos ou de sites confiáveis. Mesmo que você tenha feito uma pesquisa completa para determinar a confiabilidade de um aplicativo, lojas de aplicativos inseguras podem adulterar seus produtos e fazer com que você baixe um aplicativo impostor e ilegítimo, criado com objetivos nefastos. Por exemplo, no ano passado, a organização de direitos digitais [SMEX](#) emitiu [um alerta](#) sobre vários sites que faziam propaganda de um aplicativo chamado "WhatsApp Plus" (para ser claro, esse não é um produto do WhatsApp!), que poderia salvar e vender dados de usuários, ou possibilitar que telefones que o instalavam fossem hackeados.

Alguns desenvolvedores preocupados com a segurança até fornecem chaves criptográficas que permitem verificar a sua autenticidade. Eles geralmente fornecem uma explicação sobre como verificar essas identificações.

Onde os dados serão armazenados?

Alguns aplicativos de documentação apenas armazenam os seus dados e a sua documentação localmente em seu dispositivo, enquanto outros enviam e armazenam seus dados em outro lugar. Em muitos casos, essa função é inerente ao design e à finalidade do aplicativo, como no caso do app Eyewitness to Atrocities, que envia uma cópia inalterada de sua documentação para uma instalação de armazenamento Lexis Nexis, de modo que a Eyewitness possa se assegurar da proteção e da integridade do material. Você só pode exportar os seus registros para fora da galeria criptografada do aplicativo Eyewitness *depois que* eles tiverem sido enviados para proteção.

Cabe a você determinar se é necessário que a sua documentação permaneça em seu dispositivo apenas, se é preciso que ela seja enviada e armazenada em um local remoto que você controla (como é uma opção com o [Tella](#)), ou se você precisa enviá-la para uma organização ou plataforma externa à qual você concede acesso e direito de uso de sua documentação. Tenha em mente que, durante um bloqueio da internet, você não poderá

transmitir a sua documentação pela internet de modo imediato, então precisará de um aplicativo que permita armazenar (e, idealmente, fazer backup) a sua documentação localmente pelo menos de modo provisório (Confira [Como fazer backup da mídia do telefone sem internet ou computador](#)).

Se seus dados forem enviados para um local remoto, saiba em quais países os dados ficarão armazenados. Quão vulneráveis estão os dados nesses países, quais são as chances de serem expostos, seja por ordens judiciais ou outros meios? Quais riscos você corre ao ter seus dados lá guardados expostos?

O aplicativo criptografa a documentação que produz?

Alguns aplicativos, como o Tella e o Eyewitness to Atrocities, oferecem criptografia de arquivos e / ou armazenamento criptografado para a sua documentação, de modo separado da galeria principal de seu telefone e da criptografia de seu telefone para que sua mídia e metadados nunca sejam descriptografados em seu dispositivo, exceto se acessados por meio do aplicativo com uma senha. Isso significa que, mesmo se o telefone estiver desbloqueado, a documentação permanecerá criptografada. Isso pode fornecer um nível extra de proteção para a sua documentação.

Se o aplicativo enviar e armazenar a sua mídia em um local remoto após a restauração da internet, verifique também se você precisa que os seus arquivos estejam criptografados enquanto estiverem sendo enviados e guardados no local remoto, algo que o aplicativo EyeWitness, por exemplo, faz.

Lembre-se de que, embora a criptografia seja legal na maioria dos lugares, alguns países podem ter leis que restringem ou criminalizam o seu uso. Este [mapa](#) (abrangente, mas de 2017) fornece um bom ponto de partida se você tiver dúvidas sobre as leis em seu país.

O aplicativo captura metadados importantes (sem internet)?

[Metadados](#) são dados que descrevem seu vídeo ou foto, como a hora e a data ou o local do registro. Essas informações são valiosas para se identificar, entender, autenticar e verificar o seu vídeo ou foto como sendo a documentação de um evento específico. No contexto de um bloqueio da internet, a capacidade de um aplicativo de coletar automaticamente determinados metadados e / ou permitir que você insira facilmente informações descritivas úteis é especialmente valiosa, pois pode demorar um longo período antes que você possa compartilhar a documentação com outra pessoa (e, durante esse período, os detalhes podem ser esquecidos, as circunstâncias podem mudar, etc, etc).

A maioria dos aplicativos de documentação especializados, como o ProofMode, têm recursos de metadados aprimorados e reúnem mais metadados do que os aplicativos de câmera integrados convencionais. Os metadados aprimorados podem incluir vários dados do sensor, sinais de wi-fi ou bluetooth próximos, dados do dispositivo, função hash criptográfica e informações fornecidas pelo usuário. Todos esses itens podem facilitar a autenticação e verificação da mídia posteriormente.

Lembre-se de que, durante o bloqueio da internet, você precisará de um aplicativo que não dependa da transmissão de dados para gerar ou registrar os metadados. Alguns aplicativos podem depender da internet, em vez dos sensores de hardware, para coletar certos metadados. Por exemplo, se os dados de localização forem capturados a partir de pesquisas no dispositivo, os metadados podem refletir a última localização quando o dispositivo teve conexão de dados, em vez da posição real do aparelho. Idealmente, o aplicativo também deve permitir que você armazene os metadados localmente, sem internet, incluindo o salvamento de todos os formulários que estiver preenchendo (como, por exemplo, o “modo offline” do aplicativo Tella).

Posso exportar dados do aplicativo?

Dependendo das suas intenções para a documentação, pode ser crucial ser capaz de exportar a documentação em vídeo e os seus metadados do aplicativo, em um formato que não seja de propriedade daquele aplicativo. Ou seja, pode ser importante para você ser capaz de abrir, visualizar e usar a mídia e os metadados fora do aplicativo. A capacidade de exportar significa que você e outras pessoas não vão depender de um único aplicativo ou de um provedor de serviços para acessar a sua documentação. Isso dá a você mais margem de manobra para trabalhar com o conteúdo no futuro. Lembre-se de que alguns metadados podem não ser compreensíveis se você não tiver acesso a determinados bancos de dados ou gráficos de conversão para interpretar os números (por exemplo, no caso de IDs de torre de celular ou de redes Wi-Fi).

Observe que alguns aplicativos podem ter uma cadeia de custódia deliberadamente fechada e não permitir que os usuários exportem seus dados, enquanto alguns aplicativos podem simplesmente não ser projetados tendo a exportação em mente. Esteja ciente também de que alguns aplicativos, como o Eyewitness to Atrocities, podem não permitir que você exporte os dados até ter carregado a mídia para um servidor remoto (algo que exige conexão à internet). Alguns aplicativos podem permitir que você exporte a mídia, mas não os metadados (exceto quaisquer metadados que estejam no próprio arquivo).

Se você precisar exportar, idealmente seu aplicativo deve permitir que você exporte uma cópia da mídia sem quaisquer alterações ou transformações, e uma cópia dos metadados em um formato de texto legível padronizado. Os metadados do Tella, por exemplo, são armazenados criptografados na galeria do aplicativo, mas podem ser exportados como CSV. Além disso, durante um bloqueio da internet é necessário ter opções para exportar os dados para aplicativos offline ou serviços não dependentes da rede. A maioria dos aplicativos que permitem a exportação tem algum tipo de botão “Compartilhar”, que aciona um menu de compartilhamento, e então o Android oferece uma lista de aplicativos em seu telefone que são capazes de lidar com esse tipo de conteúdo. Infelizmente, os desenvolvedores de aplicativos podem personalizar seus menus de compartilhamento e não há padrões consistentes entre os aplicativos.

Para uma quantidade maior de arquivos, pode ser mais eficiente acessar os arquivos armazenados por meio de um aplicativo gerenciador de arquivos e copiar os arquivos de lá,

embora você não consiga acessar os metadados armazenados no banco de dados de um aplicativo dessa forma. Essa opção também não está disponível para aplicativos que fornecem suas próprias galerias seguras, pois os arquivos estarão criptografados ao serem armazenados. Para esses aplicativos, é necessário ter uma função de compartilhamento dentro do aplicativo.

Confira nosso gráfico de comparação de aplicativos de documentação e a próxima postagem desta série, "[Como garantir que sua mídia possa ser verificada por outras pessoas durante um bloqueio da internet](#)"

Como garantir que a sua mídia possa ser verificada por outras pessoas durante um bloqueio da internet

Esta publicação faz parte de uma série sobre "[Como documentar durante bloqueios da Internet](#)"

Última revisão: 31 de janeiro de 2020

[Defensores de direitos humanos](#), [investigadores](#), [pesquisadores](#) e [jornalistas](#) com frequência dependem de documentação de primeira mão filmada por testemunhas para monitorar, relatar e se referir a violações de direitos humanos. Para garantir que estão agindo com base em informações corretas, esses usuários tomam medidas para autenticar e verificar a documentação que recebem, um processo que pode ser trabalhoso e demorado.

Se estiver documentando, existem passos simples que você pode fazer para facilitar a verificação para outras pessoas e corroborar sua documentação para que ela possa ser usada de maneira oportuna e eficaz. Essas poucas etapas extras são ainda mais valiosas durante um bloqueio da internet, considerando que:

- Se você não puder enviar imediatamente seu material, a data de publicação e as informações de localização fornecidas por mídias sociais não são tão úteis para mostrar que o seu vídeo foi registrado em uma determinada data ou em um determinado local.
- Se outras pessoas também não conseguirem enviar seus dados, pode haver menos documentação disponível que possa ser usada para corroborar o seu vídeo.
- Se você precisar passar seu vídeo por muitas mãos offline até chegar ao seu destino, pode ser mais difícil para outras pessoas rastrearem a origem do arquivo.
- Se você precisar excluir o vídeo original do seu telefone por motivos de segurança ou devido à capacidade de armazenamento limitada sem backup na nuvem, ou se você tiver que se livrar do telefone, pode ser mais difícil confirmar a autenticidade do arquivo.

- Se você esquecer os detalhes sobre um determinado vídeo e o aplicativo que está usando não capturar ou gravar metadados sem acesso à internet, outras pessoas podem não ser capazes de identificá-lo mais tarde.

As dicas a seguir podem ajudá-lo a proteger seu vídeo durante um bloqueio da internet e a otimizar a sua capacidade de verificação e de utilização como documentação posterior.

Filme ou forneça detalhes de identificação no vídeo

Tente incluir detalhes em seu vídeo que tornem mais fácil para um investigador ou jornalista identificar posteriormente a hora e o lugar, como pontos de referência únicos, o horizonte, placas de rua, vitrines, placas de veículos, bandeiras, relógios, primeiras páginas de jornais, etc. Você também pode narrar informações básicas, como seu nome e informações de contato (se for seguro fazer isso), a hora, data e localização, coordenadas de GPS (ou anote esses dados em um pedaço de papel e filme o papel). Quanto mais detalhes você incluir, mais fácil será para outra pessoa pesquisar e verificar o vídeo mais tarde, mesmo que não conheça você ou de onde veio o vídeo. Confira nossas dicas sobre [práticas básicas para captura, armazenamento e compartilhamento](#) para obter mais informações.

Adicionar descrição / metadados

Aproveite um dos muitos aplicativos de documentação especializados que extraem metadados aprimorados ou informações técnicas de seu telefone e permitem que você adicione manualmente outras informações descritivas. Lembre-se de que, durante um bloqueio da internet, você precisa de um aplicativo que não dependa de acesso à internet para gravar ou armazenar esses metadados. Confira [“Devo usar este aplicativo de documentação?”](#) para saber mais sobre como escolher um aplicativo apropriado.

Mesmo se você não estiver usando um aplicativo de documentação especializado, ainda assim pode criar informações complementares na forma de notas, mapas ou fotos em seu telefone. Você pode organizar seu vídeo com essas informações adicionais usando o seu aplicativo gerenciador de arquivos favorito. As principais informações complementares a serem incluídas são hora, data e localização do incidente registrado, bem como a fonte da gravação (ou seja, seu nome e informações de contato), se for seguro incluir esses dados. Exporte os metadados e insira-os no vídeo (você pode colocar tudo em uma pasta e compactar) ao compartilhá-lo.

Guarde um backup

Faça backup da mídia de seu telefone regularmente, de preferência em 2 dispositivos de armazenamento separados. Você pode, por exemplo, conectar um dispositivo *On-the-Go* (OTG) ou pen drives sem fio ao telefone, mesmo sem um computador. Confira nossas dicas em [“Como fazer backup da mídia do telefone sem internet ou computador”](#) para obter mais detalhes. O backup irá garantir que você guarde uma cópia do seu vídeo para caso perca ou quebre seu telefone, ou se precisar excluir vídeos de seu aparelho. Ter uma cópia segura de seu vídeo original também permitirá que um investigador ou jornalista que vê o seu vídeo por algum outro meio obtenha o vídeo diretamente de você mais tarde (contanto que possam rastrear os registros até você), criando uma cadeia de verificação completa.

Confira a próxima postagem desta série, [“Como fazer backup da mídia do telefone sem internet ou computador”](#)

Como fazer backup da mídia do telefone sem internet ou computador

Esta publicação faz parte de uma série sobre [“Como documentar durante bloqueios da internet”](#)

Última revisão: 31 de janeiro de 2020

Um [backup](#) é algo crucial para garantir que seus dados e sua documentação não serão acidentalmente excluídos, corrompidos ou perdidos se o seu dispositivo for confiscado. Durante um bloqueio total ou parcial da internet, você pode não ser capaz de executar um backup comum na nuvem ou então de enviar a documentação para um local externo seguro. Descarregar os dados para um desktop ou laptop é uma forma de fazer backup, mas como as pessoas geralmente não têm acesso a um computador, aqui estão algumas opções e dicas para fazer backups dos arquivos de seu telefone durante um bloqueio da internet utilizando outros métodos.

Use um drive OTG ou um drive sem fio

Dispositivos OTG, ou *On-the-Go* (em movimento), são um tipo de drive conectável por USB compatível com muitos (mas não todos) Androids. Você pode conectar um pen drive OTG diretamente em seu telefone ou usar um adaptador para USB para conectar seu telefone a um disco rígido USB normal. Com o OTG, seu telefone fornece energia para o drive. Marcas populares de dispositivos OTG incluem SanDisk, Kingston e Samsung, embora existam muitas outras. Em dólares, normalmente custam entre US\$ 8 e US\$ 25, dependendo da capacidade de armazenamento.

Os pen drives e drives sem fio são semelhantes aos discos rígidos normais, exceto que eles não exigem cabos. Isso permite que você conecte a eles dispositivos que normalmente não se conectam a discos rígidos, como o telefone. Uma vantagem de um drive sem fio em relação a um drive OTG é que você pode conectar vários usuários ao mesmo drive sem fio ao mesmo tempo. Isso pode ser útil, por exemplo, em uma situação de protesto quando você está filmando como uma equipe — as filmagens de todos podem ser copiadas para um disco rígido que outro membro da equipe esteja portando. Observe que, como não estão consumindo energia de um dispositivo, os discos rígidos sem fio dependem de bateria e precisam ser carregados.

A SanDisk é provavelmente a marca mais popular de pen drives sem fio, embora existam outras. Os pen drives sem fio são geralmente mais caros do que os drives OTG e seus preços variam de cerca de US\$ 25 a US\$ 100, dependendo da capacidade de armazenamento. Discos rígidos externos sem fio maiores custam em torno de US\$ 150, dependendo da capacidade de armazenamento.

Alternativa: Use um telefone antigo que não é mais utilizado

Se você não tem um drive OTG ou um disco rígido sem fio, mas tem um telefone antigo que ainda funciona e não usa mais, você também pode reutilizá-lo para fazer backup. Contanto que os dois telefones estejam próximos, você pode conectar e copiar mídia de um para o outro usando Bluetooth, Wi-Fi Direct ou Near Field Communication (NFC) / Android Beam.

O Bluetooth e Wi-Fi Direct são tecnologias sem fio que permitem “emparelhar” dois dispositivos sem outro roteador ou ponto de acesso entre eles. O Wi-Fi Direct oferece um alcance mais amplo e transferência de dados mais rápida do que o Bluetooth, mas consome muito mais energia. Enquanto isso, o NFC tem um alcance muito menor (de aproximadamente 4 cm) e velocidades de transferência muito mais lentas do que o Bluetooth ou Wi-Fi Direct, mas se conecta mais rápido e usa menos energia, então pode ser útil para pequenas transferências rápidas quando você tem os dois dispositivos em mãos.

Seu telefone provavelmente possui aplicativos / recursos Bluetooth, Wi-Fi Direct ou NFC integrados que permitem que você escolha dispositivos próximos com os quais compartilhar arquivos. Se os dois telefones tiverem o app Files do Google instalado, você também poderá compartilhar arquivos offline usando essas tecnologias no aplicativo.

Importante: a desvantagem da facilidade de conexão oferecida por esses serviços é que eles não são seguros. Beacons e scanners de bluetooth e wi-fi podem ser usados para rastrear sua localização ou sondar seu dispositivo para obter informações. Infiltradores podem tentar se emparelhar com o seu dispositivo, enviar arquivos indesejados ou até mesmo obter o controle do seu dispositivo se ele estiver vulnerável. **Para ficar mais seguro, desative esses serviços quando não os estiver usando e só os ative quando estiver em locais seguros, limite as permissões do aplicativo para apenas aquilo e para as pessoas que você precisa que tenham acesso e acostume-se a realizar práticas de segurança do telefone, como executar atualizações e ter uma senha forte.**

Ao fazer a cópia, inclua qualquer descrição e metadados separados

Ao copiar seus registros para um drive OTG, para um drive sem fio ou para um telefone antigo, é útil incluir qualquer informação descritiva ou os metadados que possam estar separados da mídia em si. Muitos [aplicativos de documentação](#), por exemplo, geram

documentos de texto CSV ou JSON que incluem metadados extraídos do dispositivo (como, por exemplo, a geolocalização, a hora e a data do registro) e também qualquer descrição inserida manualmente pelo usuário. Certifique-se de exportar e incluir esses documentos de metadados em seus backups.

Proteja o drive com uma senha

Muitos discos rígidos sem fio podem ser protegidos por senha com um dispositivo móvel que vem junto com a unidade. Observe que a proteção por senha não é a mesma coisa que a criptografia (veja abaixo). A maioria dos discos rígidos sem fio ou drives OTG não possibilita a criptografia de disco completo usando apenas um telefone celular, mas permitem que o disco inteiro seja criptografado usando um computador.

Considere criptografar os arquivos

Se você precisa armazenar seus arquivos com mais segurança, considere criptografar seus backups. Embora não seja possível criptografar a maioria dos discos rígidos sem fio ou drives OTG com um telefone celular, você pode criptografar os próprios arquivos antes de movê-los para o drive. Alguns aplicativos que permitem criptografar arquivos no Android incluem o [ZArchiver](#) e o [RAR](#). Esteja ciente de que você vai precisar lembrar as suas senhas de criptografia. Não há como recuperar arquivos criptografados se você perder a senha.

Lembre-se de que alguns países podem ter leis que limitam ou criminalizam o uso de criptografia. Usar criptografia para impedir que as autoridades acessem seus dados pode ser visto como destruição de provas ou obstrução de uma investigação e pode ser uma ação punível como crime. Este [mapa de 2017](#) pode estar desatualizado, mas fornece um bom ponto de partida se você tiver dúvidas sobre quais são as leis em seu país.

Guarde dois backups em locais separados

Um único backup nem sempre é confiável. Por exemplo, você pode perder o drive do backup, danificá-lo ou ele pode simplesmente falhar. Os especialistas em TI geralmente aconselham as pessoas a terem 2 backups (ou seja, 3 cópias no total), em dispositivos independentes mantidos em locais separados. Isso ajuda a reduzir os riscos de todas as cópias.

Confira a publicação final desta série, [“Como compartilhar arquivos e se comunicar durante um bloqueio da internet”](#)

Como compartilhar arquivos e se comunicar durante um bloqueio da internet

Esta postagem faz parte de uma série sobre ["Como documentar durante bloqueios da internet"](#)

Última revisão: 31 de janeiro de 2020

O bloqueio e a repressão da internet impostos em 2019 na Caxemira, o mais longo bloqueio da internet já posto em vigor em uma democracia, teve um [impacto catastrófico](#) nas vidas das pessoas na região. Para piorar a situação, em dezembro de 2019, as [contas no WhatsApp da Caxemira começaram a ser canceladas](#) em função dos 120 dias de inatividade dos usuários, de acordo com as políticas do WhatsApp.

No momento em que este artigo foi escrito, em janeiro de 2020, a Suprema Corte da Índia decidiu que a suspensão da internet por tempo indeterminado na Caxemira era [ilegal e um abuso de poder](#). A banda larga limitada e a internet móvel foram restauradas em algumas áreas, mas apenas para sites selecionados de uma "lista de permissões".

Os bloqueios da internet são projetados para impedir as pessoas de compartilharem informações e se comunicarem (e também para forçar o uso de formas menos seguras de comunicação, como o telefone celular e o SMS, que são mais fáceis de interceptação e monitoramento pelas autoridades). Nem sempre há boas soluções alternativas durante os bloqueios totais. Em um dos períodos mais duros da suspensão da internet na Caxemira, por exemplo, as pessoas utilizaram [bilhetes escritos à mão e mensageiros](#) para enviar recados a seus entes queridos.

Não há maneiras infalíveis de contornar todos os bloqueios, mas por meio de conversas com ativistas e colegas, aprendemos alguns métodos e abordagens de compartilhamento de arquivos e comunicação offline que podem funcionar para você, dependendo das circunstâncias. Observe que algumas dessas opções precisam de internet para serem configuradas (por exemplo, para baixar aplicativos, etc).

Compartilhe arquivos diretamente por Bluetooth, Wi-Fi Direct ou NFC

Você não precisa ter uma conexão com a internet para conectar seu telefone a outro dispositivo próximo via Bluetooth, Wi-Fi Direct ou Near Field Communication (NFC) (método às vezes chamado de Android Beam em dispositivos mais antigos). O Bluetooth e o Wi-Fi Direct são tecnologias sem fio que permitem "emparelhar" dois dispositivos sem outro roteador ou ponto de acesso entre eles. O Wi-Fi Direct oferece um alcance mais amplo e transferência de dados mais rápida do que o Bluetooth, mas consome muito mais energia. Enquanto isso, o NFC tem um alcance muito mais curto (de cerca de 4 cm) e velocidades de transferência muito mais lentas do que o Bluetooth ou Wi-Fi Direct, mas se

conecta mais rápido e usa menos energia, e por isso pode ser útil para pequenas transferências quando os dois dispositivos estiverem em suas mãos.

Provavelmente, você dispõe de recursos Bluetooth, Wi-Fi Direct e NFC integrados ao seu telefone, que aparecem em suas opções de compartilhamento. Além disso, aplicativos com recursos de compartilhamento de arquivos, como o [Files do Google](#), também integram essas tecnologias.

Uma observação importante: a desvantagem da facilidade de conexão oferecida por esses serviços é que eles não são seguros. O Bluetooth e os wi-fi beacons/scanners podem ser usados para rastrear a sua localização ou sondar seu dispositivo para obter informações. Invasores podem tentar se emparelhar com o seu dispositivo, enviar arquivos indesejados ou até mesmo obter o controle do aparelho se ele estiver vulnerável. **Para ficar mais seguro, desative esses serviços quando não os estiver usando e só ative-os quando estiver em locais seguros. Também limite as permissões do aplicativo para apenas aquilo e para as pessoas que você precisa que tenham acesso, e pratique hábitos que assegurem a segurança do telefone, como executar atualizações e ter uma senha forte.**

Compartilhe arquivos com um drive wi-fi ou através de uma rede local sem fio (WLAN)

Um disco rígido sem fio ou um flash drive podem ser usados para compartilhar arquivos entre uma equipe ou várias pessoas ao mesmo tempo. O drive wi-fi normalmente vem com instruções e / ou um aplicativo para conectar seu telefone à unidade e é relativamente fácil de usar. Lembre-se de definir uma senha no drive para ter mais segurança.

Se você não tiver um disco rígido sem fio, também pode compartilhar arquivos por meio de um drive USB normal, conectando-o a um roteador sem fio. Um roteador portátil de viagem com uma porta USB, por exemplo, é relativamente barato e muito fácil de transportar. Os usuários podem se conectar ao drive USB por meio de uma rede local (sem necessidade de internet). Para acessar arquivos no drive USB conectado ao seu telefone, você precisará usar um aplicativo gerenciador de arquivos que possa se conectar ao armazenamento em rede, como o [Solid Explorer](#). O endereço de IP do seu roteador geralmente pode ser encontrado nas configurações de wi-fi avançadas do seu telefone.

Enquanto isso, outra opção é o [PirateBox](#), um projeto do tipo "faça você mesmo" que fornece software licenciado gratuitamente. Os usuários podem compartilhar arquivos das maneiras descritas acima, mas o Piratebox permite que eles façam isso anonimamente e também inclui recursos de bate-papo e mensagens. Configurar um Piratebox exige que se faça download de alguns softwares, e que eles sejam instalados e configurados. [As instruções de como fazer isso](#) estão no site do Piratebox.

Atualização: o projeto PirateBox está [fechando](#) aos poucos. O site e o repositório github ainda estão online, mas o principal desenvolvedor do projeto não está mais cuidando de sua manutenção de maneira ativa.

Comunique-se por aplicativos de chat peer-to-peer (P2P)

Há dois novos aplicativos de mensagens ponto-a-ponto (peer-to-peer, P2P) que conhecemos por meio de redes de ativistas: o [Briar](#) e o [Bridgefy](#). Ainda não os experimentamos, mas conhecemos outros que os estão testando.

O [Briar](#) é um aplicativo de mensagens criptografadas de código-fonte aberto que não depende de um servidor central. Em vez disso, ele sincroniza mensagens entre os dispositivos dos usuários, para que o conteúdo fique no dispositivo de cada usuário. Ele pode sincronizar os dispositivos mesmo quando não há internet usando Bluetooth ou wi-fi (quando há internet, o aplicativo sincroniza os dispositivos pela rede [Tor](#)). O Briar também oferece grupos privados, fóruns públicos e blogs. Quando usado offline, o seu alcance é limitado pelo alcance do Bluetooth ou do wi-fi (o máximo é de cerca 100 metros).

Enquanto isso, o [Bridgefy](#) é um aplicativo de mensagens criptografado de ponta a ponta (exceto ao usar o recurso de “transmissão”) que usa o Bluetooth para enviar mensagens. Ao contrário do Briar, as mensagens podem viajar por distâncias maiores, pulando ao longo de uma rede mesh de outros usuários do Bridgefy (mas apenas o destinatário pretendido pode ler a mensagem). O Bridgefy não dispõe de grupos privados, fóruns e recursos de blog de Briar, mas tem um modo de transmissão em que você pode enviar uma mensagem para até sete usuários do Bridgefy que estejam dentro do seu raio de alcance, que não precisam ser seus contatos (as mensagens de transmissão não são necessariamente criptografadas).

Comunique-se via SMS criptografado

As mensagens de texto SMS são enviadas por meio de redes de celular e não dependem da internet, e, portanto, ainda podem funcionar durante um bloqueio da internet. No entanto, o SMS é considerado muito inseguro. Ao contrário de aplicativos que dependem da internet, como o WhatsApp ou o Signal, o SMS não dispõe de criptografia de ponta a ponta. Isso significa que as mensagens de texto (e seus metadados) podem ser lidas por governos e operadoras de celular ou interceptadas por hackers. O SMS também pode ser “falsificado”, o que significa que um remetente pode corromper as informações de endereço para se passar por outro usuário.

Se você precisar usar o SMS, o [Silence](#) é um aplicativo que criptografa mensagens SMS de ponta a ponta. O aplicativo é de código aberto e usa o protocolo de criptografia do Signal. Embora não tenhamos experimentado, conhecemos a experiência de outras pessoas que o usaram. Tanto o remetente quanto o destinatário precisam instalá-lo e trocar as chaves entre si. Como as mensagens SMS passam obrigatoriamente pelos servidores da sua operadora de telecomunicações, mesmo com o Silence, o fato de você estar enviando uma mensagem criptografada e os metadados da sua mensagem ficarão acessíveis para a operadora de telecomunicações.

Bloqueios parciais: como contornar sites bloqueados

Um “bloqueio da internet” muitas vezes não corresponde a um corte total da internet, mas sim ao bloqueio ao acesso de sites específicos ou de plataformas de mídias sociais. Os governos, por meio de provedores de serviços de internet (ISPs), podem bloquear sites com base em endereços IP, em seu conteúdo ou por meio de pesquisas DNS. Se você não tiver certeza se um site está sendo bloqueado, organizações como o [Open Observatory of Network Interference](#) e o [Netblocks](#) monitoram e medem as suspensões e a censura da internet em todo o mundo.

Felizmente, contanto que você tenha acesso à internet, existem algumas maneiras de tentar contornar os bloqueios parciais. Assim como acontece com a criptografia, lembre-se de que burlar sites bloqueados pode ser uma atividade criminalizada em seu país.

VPN

Uma maneira de contornar um bloqueio baseado em IPs e em conteúdo é usar uma rede privada virtual (VPN, *Virtual Private Network*), como o [ProtonVPN](#) ou o [TunnelBear](#). Quando você se conecta por meio de uma VPN, seu tráfego de internet é criptografado e roteado por um servidor VPN em outro local, como em outro país, ocultando assim o verdadeiro destino e o conteúdo do seu tráfego para o seu provedor.

Lembre-se de que alguns governos proíbem o uso de VPNs ou podem tentar detectar e bloquear conexões por VPNs. Também é importante usar um provedor de VPN confiável, de preferência um que não armazene dados ou guarde logs, pois esse provedor poderá ver sua atividade na internet. Esteja ciente do país em que o provedor de VPN está baseado e a quais processos legais ele pode estar sujeito com base em sua jurisdição. Considere também que as VPNs aprovadas pelo governo podem, na verdade, autorizar a vigilância e a inspeção de seus dados.

Servidores DNS

O servidores DNS (“sistema de nomes de domínio”, “domain name systems”) funcionam traduzindo os nomes de domínio ou URLs que um usuário digita em um navegador em endereços IP numéricos que a internet usa para identificar páginas da web. Um provedor de acesso à internet pode modificar os servidores DNS que controla para bloquear certas consultas ou retornar uma página incorreta informando que o site não existe. Em 2014, o primeiro-ministro turco Recep Tayyip Erdoğan [tentou bloquear o Twitter](#) durante as eleições turcas usando essa técnica. A proibição foi [rapidamente frustrada](#) por ativistas que compartilharam dicas passo a passo sobre como usar VPNs e mudar servidores DNS.

Você pode alterar o servidor DNS padrão nas configurações de rede ou wi-fi do seu telefone. Em vez do servidor DNS padrão, você pode usar servidores DNS alternativos, como o [Google Public DNS](#) para contornar os bloqueios baseados em DNS.

Essas são apenas duas maneiras de contornar as técnicas de bloqueio mais comuns. Confira os guias úteis da [Internet Society](#), da [Access Now](#), da [Security-in-a-Box](#) e da [EFF](#) para obter informações mais detalhadas.
