CENSURA E VIGILÂNCIA DE JORNALISTAS: UM NEGÓCIO SEM ESCRÚPULOS

REPORTERES SEM FRONTEIRAS
PELA LIBERDADE DA INFORMAÇÃO

RELATÓRIO DA REPÓRTERES SEM FRONTEIRAS
REZA MOINI / BENJAMIN ISMAIL / ELODIE VIALLE

ÍNDICE

Capa : ©FRED TANNEAU / AFP

INTRODUÇÃO

POR OCASIÃO DO DIA MUNDIAL CONTRA A CENSURA CIBERNÉTICA, A REPÓRTERES SEM FRONTEIRAS (RSF) LAMENTA A SUBMISSÃO DE GIGANTES DA WEB QUE NÃO HESITAM EM RESPONDER ÀS INJUNÇÕES DE REGIMES AUTORITÁRIOS EM MATÉRIA DE CENSURA.

ALÉM DISSO, A AUSÊNCIA DE MECANISMOS INTERNACIONAIS DE REGULAÇÃO DAS TECNOLOGIAS DE VIGILÂNCIA PERMITE QUE EMPRESAS VENDAM DISPOSITIVOS DE VIGILÂNCIA ONLINE A REGIMES AUTORITÁRIOS. AO CUSTO DE IGNORAR OS DIREITOS HUMANOS POR ALGUMAS FATIAS DE MERCADO.

1 CENSURA: OS GIGANTES DA WEB

ENTRE SUBMISSÃO E COLABORAÇÃO ATIVA

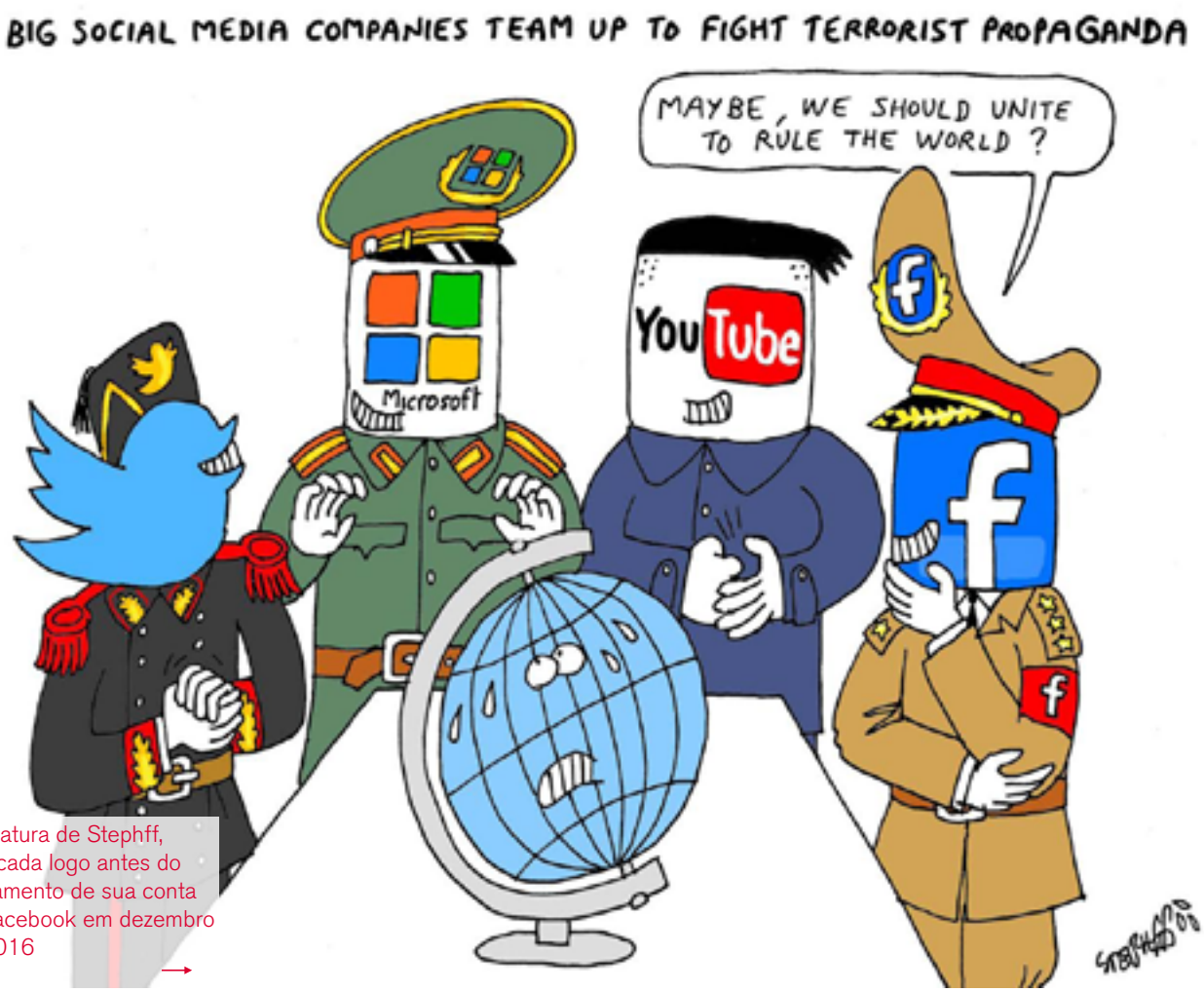
Em novembro de 2016, o New York Times revelou o desenvolvimento pelo Facebook, em total sigilo e com o apoio de seu fundador Mark Zuckerberg, de um software que permite censurar mensagens do fluxo de informação dos usuários, em função de sua localização geográfica. Segundo depoimentos dos funcionários da empresa americana, o Facebook deseja ser capaz de responder às exigências do regime chinês em matéria de censura. Com essa ferramenta, a empresa almejaria retornar ao mercado chinês do qual foi expulsa sete anos atrás, durante as revoltas da minoria uigur em Xinjiang, que usava o Facebook para difundir informações sobre a repressão às manifestações.

A empresa californiana preocupa por conta de sua colaboração ativa com certos Estados, da supressão de conteúdos jornalísticos e de sua política opaca de «moderação» de conteúdos. Como exemplo, a fan page do site de informações ARA News foi bloqueada em dezembro último pelo Facebook durante vários dias, sem que nenhuma explicação fosse apresentada. Essa mídia publica, geralmente, informações sobre Síria, Iraque, Turquia e Oriente Médio, e afirma ser seguida por milhares de visitantes por dia em sua página do Facebook.

Na Tailândia, o caricaturista Stephff, conhecido por seus desenhos incisivos, também constatou a supressão de sua conta logo após ter publicado nela uma caricatura das redes sociais, incluindo o Facebook. Em junho do mesmo ano, a conta de David Thompson, jornalista da RFI especializado em jihadismo, viu o mesmo acontecer com sua conta, por causa de uma foto que deixava entrever a bandeira do grupo Estado Islâmico. A conta do jornalista Kevin Sessums ou a foto da pequena vietnamita queimada por napalm encontram-se também entre os numerosos casos de censura arbitrária que, a cada vez, terminam com o restabelecimento do conteúdo ou da conta, o cancelamento da proibição de publicar e a mesma mensagem de desculpas «Lamentamos por este erro. A mensagem foi removida por engano e restaurada assim que pudemos verificar. Nossa equipe processa milhões de relatórios todas as semanas e, às vezes, cometemos erros.»

> “ÀS VEZES, COMETEMOS ERROS”

A icônica fota da menina vietnaminta queimada por napalm é um dos casos de censura arbitrária do Facebook
©www.presse-citron.net



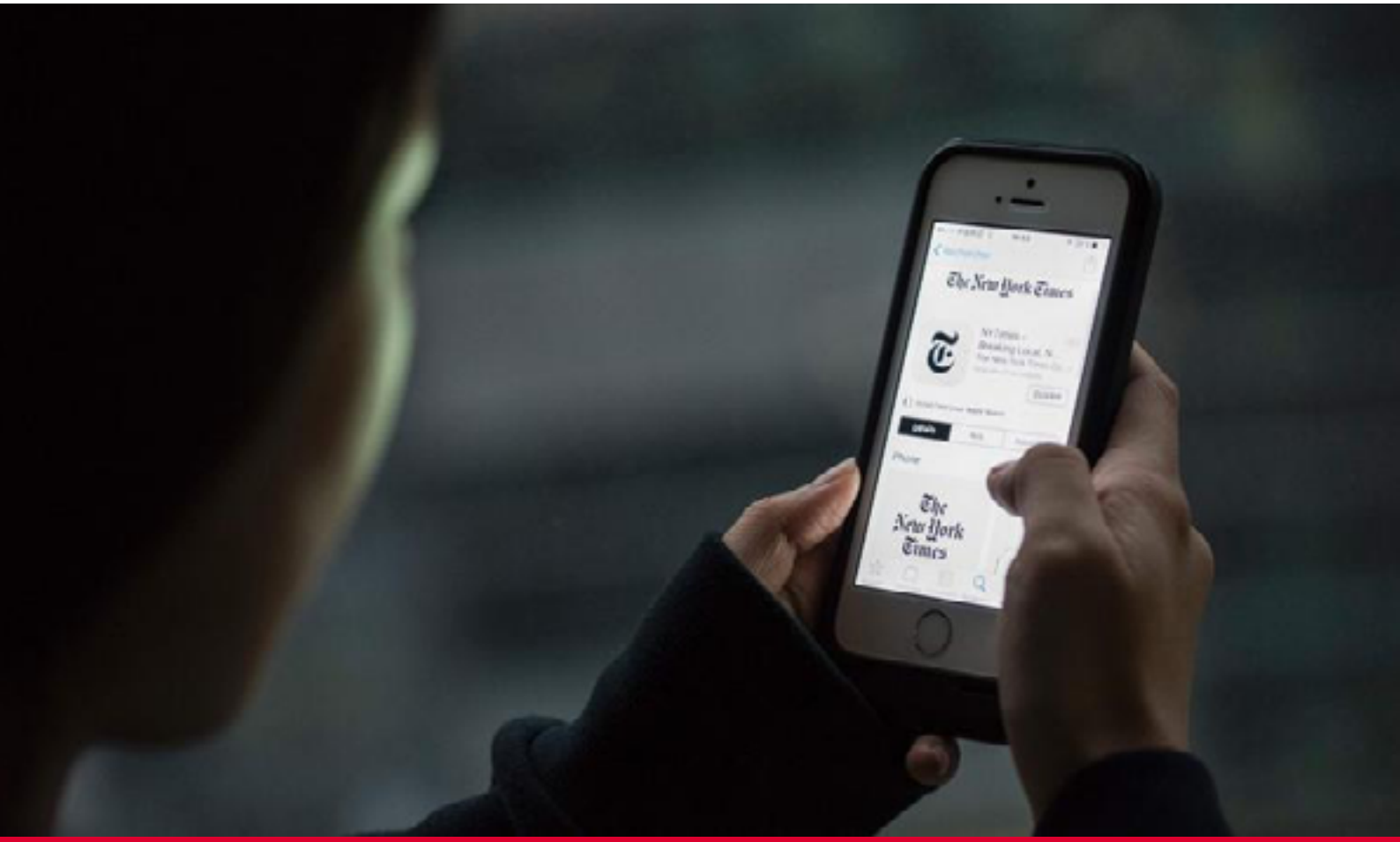
Caricatura de Stephff, publicada logo antes do fechamento de sua conta no Facebook em dezembro de 2016

Os outros gigantes da Web não fazem por menos. O Twitter foi, por várias vezes, acusado de censura de jornalistas em 2016. Foi também na Turquia que o Twitter usou, em 2014, sua ferramenta de gestão local dos conteúdos, proibindo o acesso a uma conta ou a um tweet a partir de uma conexão turca. Na Turquia, a rede social, que afirma em seu site só levar em consideração as injunções «válidas e corretamente definidas» foi rápida na aplicação do decreto publicado apenas alguns dias depois da tentativa de golpe de estado de 15 de julho passado, censurando nada menos de que cerca de vinte contas de jornalistas e de veículos de mídia. A maioria das contas censuradas foi de antigos repórteres e editores do diário Zaman Amerika. A lista inclui ainda um jornalista curdo, @AmedDicleeT, que tem 186.000 seguidores, o diário curdo Özgür Gündem (@ozgurgundemWeb1) e até mesmo a conta oficial da agência de notícias curda, DIHA (@DicleHaberAjans).

Mais recentemente, em janeiro de 2017, a empresa Apple também esteve no centro de uma polêmica quando o New York Times anunciou que as versões inglesa e chinesa de seu aplicativo haviam sido removidas da loja iTunes a pedidos da Administração do Ciberespaço da China (CAC), o órgão oficial de controle da Internet do Partido Comunista Chinês. A autocensura da loja iTunes já havia sido constatada pouco tempo após a implantação de sua primeira loja física na China, em 2008. Desde então, inúmeros aplicativos, como aqueles sobre o Dalai Lama e temas tabu no país, foram bloqueados pela Apple. No fim de 2015, um empresário americano constatou o bloqueio do aplicativo «News» quando viajava para a China continental a partir de Hong Kong. A política da Apple não diz respeito somente à China. Em setembro de 2015, a empresa bloqueou o aplicativo de Josh Begley, jornalista do The Intercept, que fazia um levantamento de todos os ataques de drones lançados pelos Estados Unidos, assim como um outro sobre a matança ocorrida em Ferguson, no estado do Missouri.

A Apple havia retirado da iTunes Store o aplicativo do jornal The New York Times na China ↓

©FRED DUFOUR / AFP



2 O COMÉRCIO DUVIDOSO, MAS LUCRATIVO, DA VIGILÂNCIA

A vigilância da Web e das telecomunicações é antes de tudo o apanágio dos «Inimigos da Internet» - os países mais repressivos do mundo em matéria de liberdade de informação na Web - em nome dos assim chamados «interesses vitais da Nação». À frente do pelotão, estão regimes autoritários como a China, o Irã, a Síria, ou o Uzbequistão, que adquiriram, e continuam a comprar, tecnologias que lhes permitem rastrear os menores fatos e gestos dos jornalistas, blogueiros e internautas que lhes são críticos.

Nos países ditos democráticos, como a França, o Reino Unido, os Estados Unidos, a Austrália, ou ainda o México (ver abaixo), que recorrem à vigilância em nome de imperativos de segurança, coloca-se a questão da proteção das fontes jornalísticas.

Seria possível uma entrada ética de empresas de telecomunicação no mercado iraniano?

O Irã é um dos melhores exemplos de país repressivo em matéria de controle de internautas. Uma polícia cibernética vigia permanentemente as atividades online dos iranianos. Nos últimos três anos, mais de uma centena de internautas, entre os quais inúmeros jornalistas e jornalistas cidadãos, foram arbitrariamente convocados e detidos, e alguns deles foram condenados a penas pesadas em diferentes cidades do país. A maioria desses jornalistas, profissionais ou não, é vítima de vigilância e de rastreamento, realizados por meio de tecnologias ditas de «vigilância lícita» (Lawful Interception Management System, LIMS). Mesmo sob o regime dos Guardiães da Revolução, as tecnologias cobertas por esta sigla são usadas de maneira ilegal.

Desde o acordo nuclear histórico de janeiro de 2015, um número crescente de empresas de telecomunicações (Vodafone, Telecom Itália, AT&T e Nokia) desejam investir no país. A empresa francesa Orange iniciou discussões para obter uma participação no capital da MCI, líder iraniana de telefonia móvel que está nas mãos dos Guardiães da Revolução, deixando vagas as suas intenções: «Assim como outras operadoras internacionais, o grupo estuda as oportunidades que se apresentam no mercado iraniano», responde a empresa. Segundo Richard Marry, um dos responsáveis pela Vivaction, outra empresa francesa também em «fase de redescoberta do mercado», faz «mais de doze meses que vamos todos os meses a Teerã para encontrar o ecossistema das Telecomunicações».

«Com uma taxa média de penetração dos telefones celulares muito superior a 100% e sabendo que cerca de um domicilio a cada dois possui uma assinatura de Internet fixa, não somente é legítimo perguntar-se sobre a maneira como as empresas estrangeiras desejam se implantar no país, mas é também fundamental que essas empresas deem mostras de transparência com relação aos acordos que assinaram ou se preparam para assinar com o regime, declara Reza Moïni, encarregado do escritório Irã-Afeganistão da Repórteres sem Fronteiras. «*Acima de tudo, não queremos mais outros casos Nokia-Siemens e Ericsson.*»

De fato, em setembro de 2011, a Repórteres sem Fronteiras denunciou para que sanções internacionais fossem aplicadas contra essas empresas, tão logo fosse comprovado que as tecnologias ou infraestruturas que elas instalavam no país permitiam ao regime vigiar e reprimir sua população.

Hacking team e NSO: empresas na sombra dos Inimigos da Internet

Em março de 2013, a Repórteres sem Fronteiras publicou um relatório especial sobre vigilância trazendo pela primeira vez à luz uma lista de cinco empresas «mercenárias da era digital», - baseadas no Reino Unido, Alemanha, Itália, França e Estados Unidos - cujos produtos eram usados por países repressivos para cometer violações dos direitos humanos e da liberdade de informação. Nessa lista, uma empresa de Milão, Hacking Team, havia sido questionada devido à venda de tecnologias «ofensivas» de vigilância ao Marrocos e aos Emirados Árabes Unidos, usadas por esses regimes para espionar sites de informação e de militantes dos direitos humanos.

Em julho de 2015, a empresa foi novamente assunto de notícias após a piratagem de centenas de gigas de seus dados, incluindo especialmente inúmeras informações sobre seus clientes e as tecnologias a eles vendidas. Entre eles, o México seria o primeiro cliente da Hacking Team, com cerca de seis milhões de euros em compras. A lista de clientes mexicanos inclui o Ministério do Interior, a Polícia Federal, o exército, a marinha, a agência interna de informações, o escritório do procurador geral, governos regionais e até a empresa estatal de petróleo, a PEMEX.

Diante dessa insidiosa generalização da vigilância online pelas autoridades, em março de 2016, a organização de defesa dos direitos digitais Red en Defensa de los Derechos Digitales (R3D) defendeu publicamente sua posição, em nome de um grupo de jornalistas, ativistas de direitos humanos e estudantes mexicanos. Em 11 de maio de 2016, a 2a câmara da Corte Suprema do México recusou colocar em questão o dispositivo da lei federal sobre as telecomunicações (Federal Telecommunications Act), autorizando a retenção maciça de dados digitais (meta-dados), sem recurso a um juiz. Ainda que a coalizão R3D tenha apelado dessa decisão junto à Corte Interamericana de Direitos Humanos, jornalistas, blogueiros e ativistas cibernéticos continuam hoje vulneráveis aos abusos do governo, cujas relações comerciais com a Hacking Team ilustram claramente uma vontade de vigilância maciça da Internet e das telecomunicações.

©Captura de tela do site da Hacking Team ↓

Poderiam me dizer, se interrogados sobre esse tema, que essas pessoas se defendem afirmando a necessidade de se lutar contra o terrorismo e lembrando que elas respondem às leis dos países nos quais estão implantadas, como o fez o Hacking Team na Itália. «*Isso não basta, pois suas tecnologias continuam sendo usadas por regimes autoritários, inimigos da internet, para vigiar e prender jornalistas*", explicou Christophe Deloire.

"Ao constatar as relações de um sem número de órgãos governamentais mexicanos com um dos principais exportadores de tecnologia de vigilância, somos obrigados a nos perguntar sobre a capacidade dos jornalistas de investigar de forma independente e de proteger suas fontes», declarou Emmanuel Colombié, diretor do escritório regional para a América Latina da RSF. *"A opacidade das autoridades sobre o uso previsto dessas tecnologias adquiridas reforça essa preocupação. Devem ser oferecidas garantias para proibir o uso sistemático de tais tecnologias contra todos os agentes da informação, profissionais de mídias, blogueiros e defensores de direitos.»*

O MALWARE PODIA TER ACESSO A TODAS SUAS INFORMAÇÕES PESSOAIS, VER SUAS FOTOS, ARQUIVOS, LER SUAS MENSAGENS DE SMS, E-MAILS, CONVERSAS POR WHATSAPP, SKYPE E ATÉ DO TELEGRAM.

As recentes revelações envolvendo a empresa israelense NSO e o jornalista investigativo mexicano Rafael Cabrera poderiam servir para trazer à luz um abuso de vigilância pelas autoridades mexicanas. Em agosto de 2016, a Citizen Lab e a Look out revelaram a existência de um software espião que permitiria tomar o controle total dos iPhones aproveitando-se de várias falhas de segurança (já corrigidas). «Pegasus», que seria o nome do malware, se instalaria no telefone da vítima depois que esta clicasse num link de hipertexto enviado por SMS. O malware poderia assim recolher contatos, detalhes e conteúdo das chamadas, SMSs, e-mails, conversas de WhatsApp, Skype e até mesmo Telegram, cuja reputação é de ser seguro. Também podem acionar remotamente a máquina fotográfica do iPhone, seu microfone, e saber a qualquer momento onde está seu usuário.

O jornalista Rafael Cabrera, que trabalha principalmente para o site de informações Aristeguinoticias.com, foi vítima do malware Pegasus em agosto de 2016, depois de ter participado da investigação que revelou um escândalo de corrupção envolvendo a família do presidente Peña Nieto. O jornalista tinha recebido inúmeras mensagens suspeitas convidando-o a ir até a rede UNO TV e «informando-o» que a presidência estava pensando em processá-lo por difamação e prender os jornalistas envolvidos na investigação sobre a «Casa Branca» mexicana.

Rafael Cabrera, jornalista do site Aristegui Notícias, foi vítima do malware Pegasus →

Segundo o NYT, o governo mexicano teria pago 15 milhões de dólares à NSO para lançar três projetos indefinidos. A NSO se defendeu afirmando que os softwares que vendiam eram unicamente utilizados para vigilância legal. Contudo, no momento em que essas revelações eram feitas, a Citizen Lab expunha uma tentativa semelhante de vigilância do blogueiro emiradense, administrador do fórum de debate democrático Al-Hewa, Ahmed Mansoor. Nos dias 10 e 11 de agosto de 2016, o blogueiro recebeu duas vezes o mesmo SMS em seu iPhone 6 incitando-o a clicar em um link para conhecer mais sobre os abusos cometidos pelo regime dos Emirados. Analisado pela Citizen Lab, esse SMS permitiu que a ação fosse rastreada até a NSO e seu software Pegasus.

Contactada pela RSF, a NSO respondeu que: «A NSO contribui para transformar o mundo num lugar mais seguro, forneçendo aos organismos governamentais autorizados, tecnologias que os ajudam a combater o terrorismo e a criminalidade. Os clientes podem utilizar nossos produtos exclusivamente para a investigação e a prevenção do crime e do terror. A utilização ética e legal dos nossos produtos por nossos clientes é de grande importância para a empresa. Em casos de suspeita de violação do contrato, a empresa tomará as medidas apropriadas para com o cliente em questão», afirmações que a RSF não esteve em medida de verificar.

3 REGULAMENTAÇÕES INTERNACIONAIS EM PANE OU BLOQUEADAS POR LOBBIES

A resolução sobre «a promoção, a proteção e o exercício dos direitos humanos na Internet» adotada pelo Conselho de Direitos Humanos das Nações Unidas em sua 32a sessão, de 13 de junho a 1o de julho de 2016, afirma novamente que «os mesmos direitos dos quais dispõem as pessoas quando estão desconectadas também devem ser protegidos online, especialmente a liberdade de expressão, que se aplica independentemente de fronteiras e quaisquer que sejam os meios que escolhamos, em conformidade com o artigo 19 da Declaração Universal dos Direitos Humanos e do Pacto Internacional sobre Direitos Civis e Políticos». Além disso, a resolução apela para que «todos os Estados abordem as preocupações de segurança na Internet em conformidade com suas obrigações internacionais sobre os direitos humanos para garantir a proteção da liberdade de expressão, da liberdade de associação, do direito à vida privada e de outros direitos humanos online, por meio, especialmente, de instituições nacionais democráticas e transparentes, fundadas sobre os princípios do direito, de maneira que garanta a liberdade e a segurança na Internet».

AS RESOLUÇÕES DO CONSELHO DE DIREITOS HUMANOS NÃO SÃO VINCULANTES E PORTANTO EFICAZES QUANDO SE TRATA DE IMPEDIR OS ESTADOS MAIS REPRESSIVOS EM MATÉRIA DE LIBERDADES INDIVIDUAIS ONLINE

Uma outra resolução do Conselho, adotada em setembro de 2016, enfatiza «*que na era do digital, os jornalistas devem poder dispor de ferramentas de criptografia e de proteção do anonimato para serem capazes de praticar livremente sua profissão e de exercer seus direitos humanos, especialmente seus direitos à liberdade de expressão e à vida privada, sobretudo, tornando seguras as suas comunicações e protegendo o sigilo de suas fontes, e pede aos Estados que não cometam ingerência na utilização de tais tecnologias com a imposição de restrições, cumprindo assim suas obrigações relacionadas ao direito internacional dos direitos humanos*». Contudo, as resoluções do Conselho de Direitos Humanos são ainda textos não vinculantes e ineficazes quando se trata de impedir os Estados mais repressivos em matéria de liberdades individuais online.

Desde as revelações de Edward Snowden e do fim da hegemonia norte-americana na governança da Internet, os Inimigos da Internet fazem pressão para obter um papel crescente na regulação das redes, em particular por meio das agências da ONU, como a União Internacional das Telecomunicações (UIT), a UNESCO e a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (CNUCED), que fizeram todas inúmeras declarações em defesa das liberdades fundamentais online e sobre a governança da Internet. Após a Declaração de princípios que resultou da cúpula de Genebra em 2003, a Cúpula Mundial sobre a Sociedade de Informação (SMSI), constitui uma das principais plataformas multilaterais da governança da Internet, dentro da qual nenhum texto vinculante surge para impedir os regimes autoritários de censurar e vigiar maciçamente suas populações.

«A luta ao redor da questão estratégica da governança da Web ameaça cada vez mais de culminar na oficialização de uma Internet fragmentada e censurada, declara Benjamin Ismaïl, responsável pelo escritório Ásia da RSF. *Se cada país decidir reclamar sua soberania na Internet, teremos que lidar com um sistema no qual os regimes autoritários terão total legitimidade para restringir a liberdade de expressão e o direito a informar online. Para evitar isso, é vital que mecanismos internacionais vinculantes sejam instaurados para garantir a existência de uma Internet livre e mundial. Essa garantia depende, hoje mais do que nunca, de um controle rigoroso das empresas da Web e das empresas exportadoras de tecnologias de vigilância em massa».*

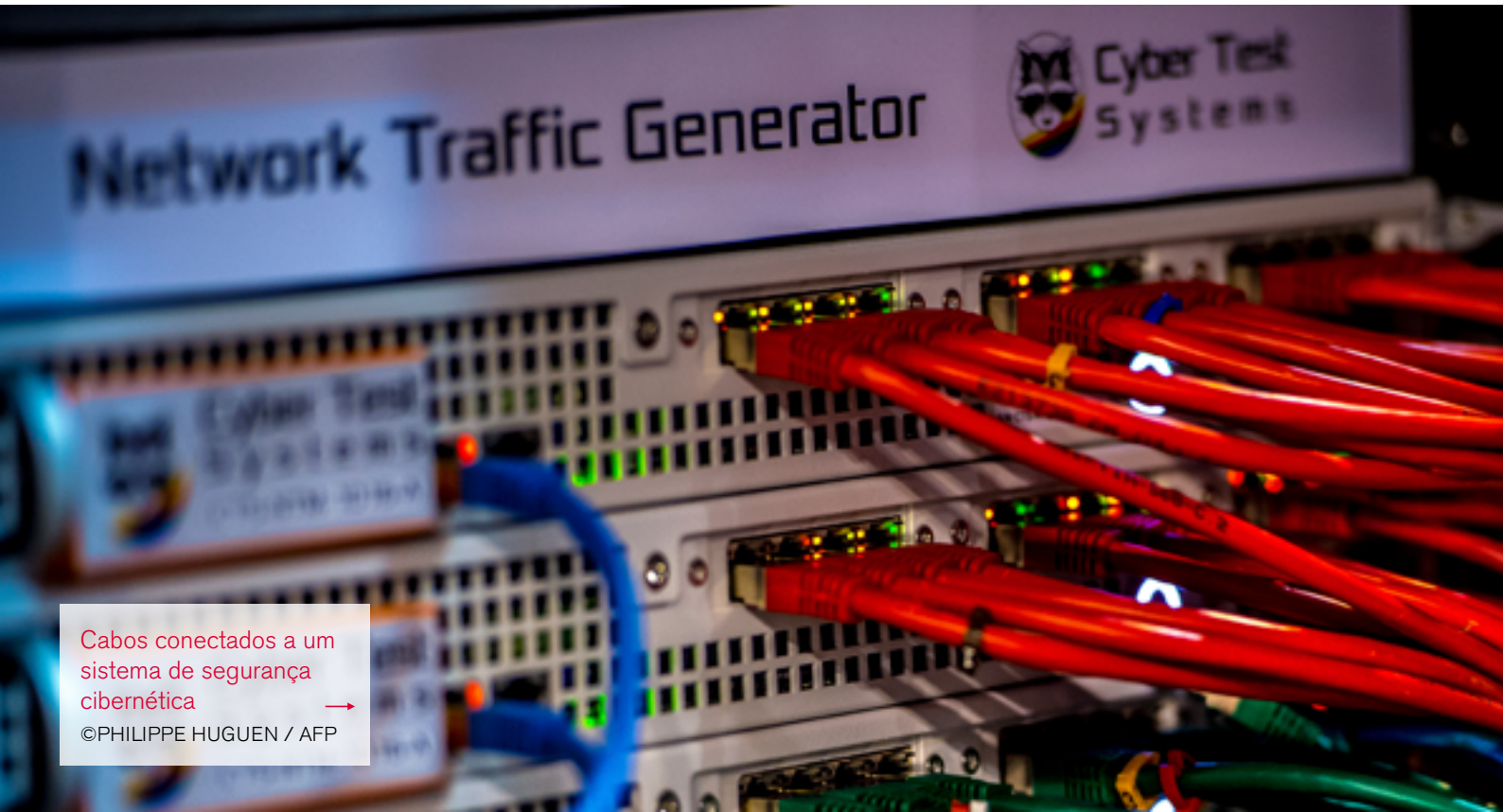
Ex analista de segurança da NSA que denunciou abusos cometidos pela agência, Edward Snowden.
©FREDERICK FLORIN / AFP ↓

Desde 2014, a RSF pede ao Conselho de Direitos Humanos a criação de uma convenção internacional sobre a responsabilidade das empresas em matéria de direitos humanos para impor aos Estados a aplicação de um controle rigoroso da exportação de tecnologias de vigilância e a instauração de recurso para indivíduos vítimas de vigilância e das consequências que dela podem resultar (detenções, prisões, violências físicas, torturas).

Alguns meses mais tarde, em 28 de novembro de 2014, a RSF, a Privacy International, a Digitale Gesellshaft, a FIDH e a Human Rights Watch saudaram o «primeiro passo da Europa a favor de um maior controle das tecnologias de vigilância», pela inclusão de tecnologias de vigilância online na lista das tecnologias de uso duplo (dual use technology). Em 2 de dezembro de 2014, os membros da coalizão CAUSE (Coalition Against Unlawful Surveillance Exports), RSF, Anistia Internacional, Difgitalle Gesellschaft, FIDH, Human Rights Watch, Open Technology Institute e Privacy International endereçaram uma carta aberta aos Estados participantes da Assembleia plenária do Acordo de Wassenaar sobre os Controles à Exportação de Armas Convencionais e Bens e Tecnologias de Dupla Utilização - um tratado que reúne 41 países, sendo a maioria da União Europeia - para pedir-lhes que tomem medidas contra a proliferação alarmante das tecnologias de vigilância acessíveis aos países repressivos conhecidos por perpetrar violações sistemáticas dos direitos humanos.

CERCA DE TRÊS ANOS APÓS ESSES APELOS A FAVOR DE UM CONTROLE EFICAZ DAS EMPRESAS PRIVADAS, A UNIÃO EUROPEIA PARECE TER DADO MARCHA RÉ

Cerca de três anos após esses apelos a favor de um controle eficaz das empresas privadas, a União Europeia parece ter dado marcha ré. Sob a pressão do lobby da indústria das tecnologias digitais, a regulação das exportações de tecnologias de vigilância está em ponto morto. O lobby, representado especialmente pela associação DigitalEurope cuja instância diretora inclui diretores de empresas como Nokia, Siemens, AMETIC, IBM, ANITEC, Cisco e Microsoft, com o apoio de um grupo de diplomatas de nove países (Áustria, Finlândia, França, Alemanha, Polônia, Eslovênia, Espanha, Suécia e Reino Unido) conseguiu que fossem feitas alterações na proposta de «regulação do Parlamento Europeu e do Conselho», para amputar a lista inicial de tecnologias que deveriam ser controladas, como certos materiais de interceptação das telecomunicações, os softwares de invasão, os centros de vigilância e os sistemas de conservação de dados.



Cabos conectados a um sistema de segurança cibernética →
©PHILIPPE HUGUEN / AFP

A proposta mais recente não inclui mais os controles inicialmente previstos sobre os equipamentos biométricos, os sistemas de geolocalização ou as tecnologias ditas de «deep packet inspection» (inspeção profunda de pacotes) que permitem interceptar e inspecionar os pacotes de dados que trafegam na Internet. Em um contexto de vigilância, o uso do DPI pode permitir que se acesse o conteúdo de e-mails, de conversas instantâneas e de trocas por VoIP e descobrir se uma comunicação está criptografada ou não. A proposta não menciona a obrigação dos Estados de informar o público sobre as empresas que eles autorizam a exportar tecnologia.

Nas Nações Unidas, assim como na União Europeia e na maioria das legislações nacionais, o arcabouço jurídico relativo à vigilância na Internet, à proteção dos dados e a exportação de material de vigilância informática permanece, até hoje, incompleto e insuficiente com relação às normas e padrões internacionais de proteção dos direitos humanos. Desde já, a adoção de um arcabouço jurídico protetor das liberdades na Internet é primordial, tanto pela questão geral da vigilância na Internet, quanto pelo problema específico das empresas exportadoras de material de vigilância.

4 AS RECOMENDAÇÕES DA RSF PARA LUTAR CONTRA A CENSURA CIBERNÉTICA

Por ocasião do dia internacional de luta contra a censura cibernética, a RSF pede:

Às empresas:

- Que sistematizem e melhorem os relatórios de transparência e publiquem as ordens judiciais dos governos que peçam para retirar do ar conteúdos ou contas de usuários.
- Que respeitem a Declaração Universal dos Direitos Humanos e as convenções das Nações Unidas sobre os Direitos Humanos
- Que respeitem os Princípios Orientadores sobre Empresas e Direitos Humanos das Nações Unidas e formulem compromissos precisos quanto à sua aplicação
- Que adotem cartas éticas e de mecanismos eficazes de «rastreabilidade» das tecnologias que exportam
- Que se proíba a exportação de tecnologias de vigilância a países não democráticos e repressivos, e que se exerça um dever de vigilância para identificar os riscos e prevenir as violações graves dos direitos humanos, das liberdades fundamentais e da segurança das pessoas
- Que apliquem os princípios de «contratos responsáveis» elaborados pelo Representante Especial do Secretário Geral encarregado da questão dos direitos humanos e das empresas transnacionais e outras empresas, John Ruggie, tornando-as, em parte, responsáveis pelas violações dos direitos humanos a que possam levar suas tecnologias.

Aos Estados :

- Que incluam o livre acesso à Internet e a garantia das liberdades digitais nos direitos fundamentais

- Que adotem leis que garantam as liberdades digitais, especialmente a proteção da vida privada e dos dados pessoais diante da invasão das forças da lei ou dos serviços de informação, e que coloquem em prática mecanismos de recurso apropriados.

- Que se assegurem que a medidas de vigilância das comunicações respeitem estritamente os princípios de legalidade, de necessidade e de proporcionalidade, em conformidade com o artigo 19 do Pacto Internacional sobre Direitos Civis e Políticos

- Que favoreçam uma maior transparência quanto às demandas de vigilância que façam às empresas, seu número, suas bases legais e seus objetivos.

- Que alinhem suas políticas àquelas dos Estados que melhor controlem a exportação de tecnologias e que apliquem sanções às empresas que tenham colaborado com regimes autoritários.

À União Européia

- Que incluam o livre acesso à Internet e a garantia das liberdades digitais na Carta dos Direitos Fundamentais da UE

- Que considerem, nas relações entre membros da UE e com Estados terceiros, assim como nas instâncias internacionais, especialmente a OMC, os mecanismos de vigilância da Internet como mecanismos protecionistas e barreiras às trocas, e que os combatam como tais.

- Que se assegurem da harmonização e uniformização dos procedimentos e sanções relativos à vigilância e do controle das tecnologias de vigilância.

Às Nações Unidas:

- Que reforcem o mandato do Grupo de Trabalho das Nações Unidas «Direitos Humanos e Empresas Transnacionais», sobretudo, habilitando-o para receber reclamações individuais e a investigar casos individuais de violações dos direitos humanos ligados às empresas;

- Que reflitam sobre a elaboração se uma convenção internacional sobre a exportação de tecnologias de vigilância na Internet que permita, principalmente, controlar e proibir o fornecimento de tecnologias sempre que existir um risco substancial de que esses materiais sirvam para cometer ou facilitar violações dos direitos humanos.

5 JORNALISTAS, PROTEJAM SEUS DADOS E SUAS COMUNICAÇÕES

Para lutar com eficácia contra a vigilância e a censura, os jornalistas, profissionais ou não, podem recorrer aos softwares desenvolvidos por organizações da sociedade civil e aplicar medidas concretas graças aos guias de segurança cibernética disponíveis online. A RSF, por sua vez, atualizou em 2015 o seu Guia Prático de Segurança, incluindo nele inúmeros conselhos práticos com relação ao ciberespaço.

Os conselhos resumidos abaixo, válidos tanto para o seu computador quanto para o seu smartphone, não pretendem ser exaustivos. A Repórteres sem Fronteiras organiza, regularmente, sessões de formação em segurança cibernética e propõe tutoriais gratuitos

Atenção: Sempre pesquise sobre as ferramentas que você pretende utilizar e sobre as técnicas que você vai aplicar. As tecnologias evoluem rapidamente e os conselhos oferecidos hoje estão sempre suscetíveis de não o serem mais amanhã.

Jornalistas acompanham o congresso do partido comunista chinês
©AFP PHOTO / Greg BAKER

→

Comportamento geral online:

Antes mesmo de pensar em tornar seu computador mais seguro ou instalar softwares que permitam criptografar suas comunicações ou dados, convém adotar uma boa higiene digital, respeitando alguns conselhos de bom senso que evitarão que você veja a sua conta de e-mail ou o seu computador pirateados.

Evite os olhares indiscretos:

- Evite trabalhar de costas para uma janela
- Ao viajar, no trem ou no avião, coloque um filtro de confidencialidade sobre a sua tela. O filtro de confidencialidade é uma folha transparente que, quando colocada sobre a sua tela, restringe a visão lateral. Assim, somente a pessoa à frente da tela (você) é capaz de enxergá-la.
- Durante deslocamentos, sempre que possível, evite se separar do seu equipamento. Isso permite evitar que um indivíduo mal-intencionado retire arquivos do seu computador ou introduza nele um cavalo de Troia.
- Todos os sistemas operacionais (Windows, Mac OS e Linux) permitem que você proteja a sua sessão com uma senha. Você deve utilizar esta funcionalidade.
- Não baixe arquivos ou clique em links que tenham sejam enviados por desconhecidos. Verifique cuidadosamente o endereço de e-mail ou a conta de Twitter daqueles que compartilharem um link com você. Em caso de dúvida, verifique a identidade do remetente com outros contatos, ou por meio de um motor de busca.
- Se um arquivo e o remetente parecerem suspeitos, entre em contato com especialistas que possam ajudá-lo. O Citizen Lab é um órgão que analisa os vírus enviados por dissidentes ou ativistas, ajudando-os a se proteger melhor.

Além dessas medidas, instale os softwares seguintes e ative as funções de proteção integradas ao seu equipamento:

- Use um antivírus E um anti-malware (como Malwarebytes)
- Ative o seu firewall
- Mantenha o seu sistema operacional (Windows, Mac OSX, etc.) atualizado
- Criptografe o seu disco rígido (função nativa a ativar no OsX)

Rastros digitais:

Se você trabalhar em um cybercafé ou com um computador que não seja o seu, cuide para não deixar rastros quando terminar o trabalho:

- Se você consultou a sua caixa de e-mails, sua conta no Facebook ou no Twitter, lembre-se de se desconectar.
- Apague o seu histórico de navegação. Ele contém inúmeras informações que podem também permitir que alguém com o necessário conhecimento acesse algumas de suas contas online.
- Em um computador público, nunca salve a sua senha no navegador. Se você o fez por distração, lembre-se de apagá-las da memória do navegador ao terminar o trabalho
- Apague os campos de formulário
- Elimine os cookies

A limpeza desses dados é feita de forma diferente em cada navegador. Uma boa maneira de evitar erros é utilizar o modo «navegação privada» do Firefox ou do Chrome.

Serviços de mensagens e acesso aos serviços online:

A maioria dos serviços online (Twitter, Facebook, WordPress, Tumblr, Skype, etc.) permitem recuperar uma senha perdida pelo envio de uma senha à sua caixa de e-mail. Portanto, é fundamental proteger o melhor possível a sua caixa de e-mails. Quando for é comprometida, com muita frequência, toda a sua identidade digital também será.

O serviço de e-mail do Google, o Gmail, permite instaurar uma segurança adicional: a «validação em duas etapas». Esse serviço permite que a sua conta de e-mail seja protegida com:

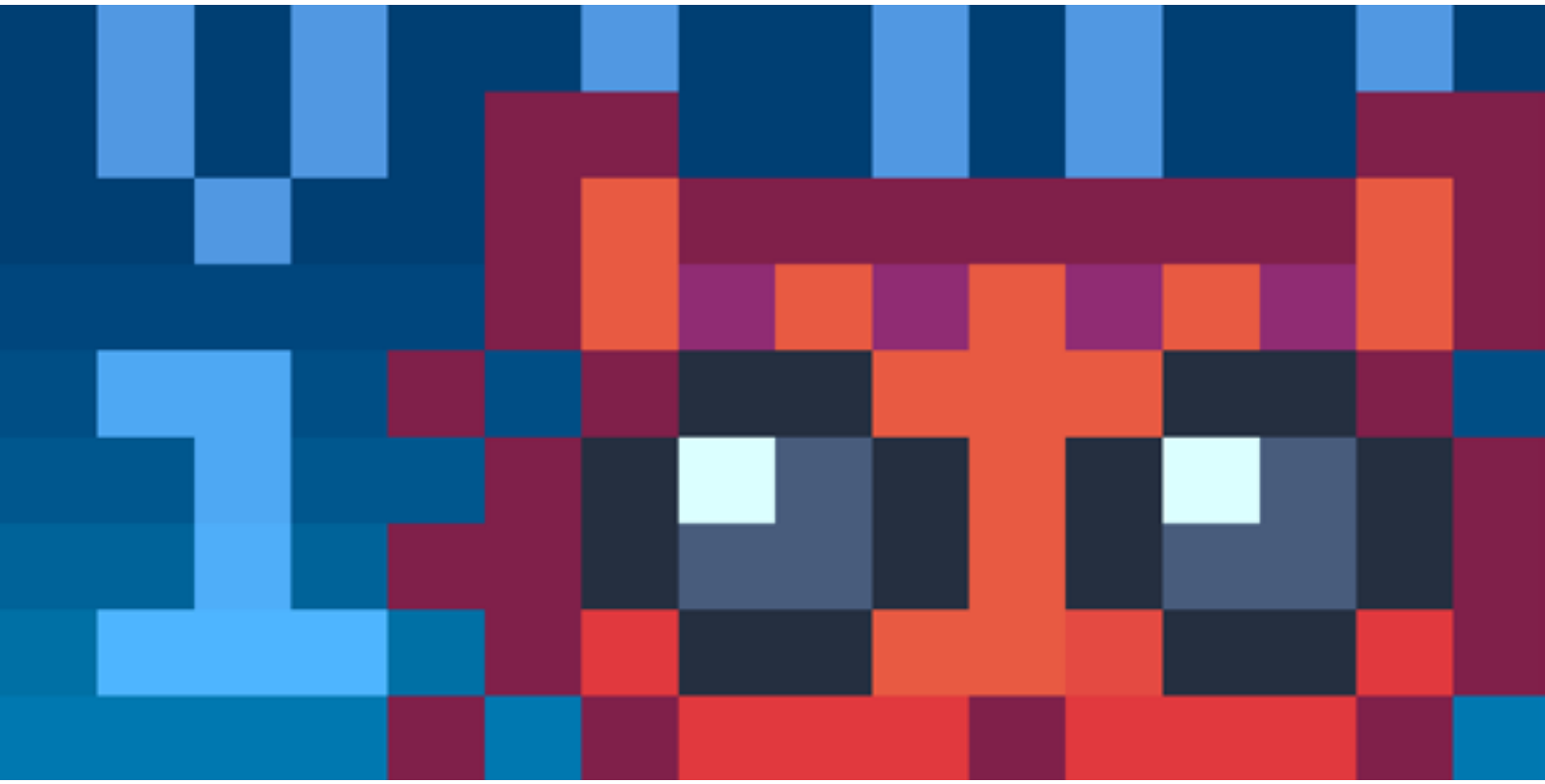
1. um nome de usuário
2. uma senha
3. um código que você receberá pelo telefone celular cada vez que se conectar à sua caixa de entrada.

Assim, sem o seu celular, é impossível acessar os seus e-mails.

Quando você se conectar à sua caixa do Gmail, lembre-se de clicar no link «detalhes», embaixo da página. Ele abre uma janela que exibe todas as conexões recentes à sua caixa. Você poderá, assim, detectar qualquer atividade suspeita

Você também deve criptografar os seus e-mails. Existem ferramentas de criptografia muito simples de usar. Você pode incentivar a suas fontes a usá-las, para conversar com elas de maneira criptografada:

- Cryptocat, uma extensão que se instala simplesmente em um computador, criptografa as conversas instantâneas de ponta a ponta e as destrói em seguida.
- Privnote e Zerobin são sites que permitem criar URLs para mensagens criptografadas que podem se autodestruir após a leitura.
- Você quer telefonar para suas fontes via internet? Sem problemas, mas use o Jitsu Meet, o «Skype livre».



Logo do « Cryptocat », uma extensão que se instala simplesmente em um computadore criptografa as conversas instantâneas ↑
©Cryptocat

Passphrases, senhas longas:

O tamanho de uma senha é o principal fator de sua solidez. Daí não se falar mais em «passwords» (palavras passe), que devem ser banidas, mas em «passphrases» (frases passe), único método capaz de resistir a um «ataque por força bruta». Cada vez que você criar uma senha longa (passphrase):

- Crie uma frase na qual inclua números, letras minúsculas e maiúsculas para obter uma cadeia de caracteres relativamente complexa, mas ao mesmo tempo, mas fácil de memorizar do que uma senha curta, porém abstrata (números + caracteres especiais).
- Use uma senha longa diferente para cada serviço online.
- Use um gerenciador de senhas longas. Por exemplo, LastPass é um gerenciador de senhas disponível em formato de extensão para Firefox, Chrome e Safari. Ele permite gravar todas as suas senhas longas

Pegada nas redes sociais:

Facebook e Twitter são ferramentas muito eficazes para se comunicar. Contudo, você deve cuidar para controlar as informações que torna visíveis ao público. Esses tutoriais e serviços online o ajudarão a controlar melhor a sua presença online:

- Verifique a sua presença na Internet com o «namechecker»
- Torne sua conta Twitter segura
- Administre as suas informações privadas no Facebook quando um conteúdo é compartilhado

Torne sua navegação segura:

Acrescente as funcionalidades seguintes ao Firefox e Chrome, pela utilização de plug-ins:

- Https Everywhere: para verificar para cada site se uma versão https (criptografada) existe e evitar, especialmente, certas iscas
- No script: para controlar os scripts javascript lançados nos sites visitados
- Privacy Badger: para bloquear os rastreadores usados pelos sites
- Certificate Patrol: para verificar os certificados apresentados pelos sites em “https”
- Instale um VPN pago para criptografar as suas conexões na Internet
- Instale o navegador «Top Browser» que permite navegar de forma anônima

Telefonia móvel:

- Crie e utilize um sistema codificado para se comunicar com as suas fontes e outros contatos. «Bipe» os seus contatos para se comunicar (deixe o telefone do seu correspondente tocar uma vez ou duas e desligue em seguida para indicar que você chegou a um local determinado, ou que tudo está bem, por exemplo).

- Não use os nomes verdadeiros dos seus contatos em suas agendas telefônicas. Atribua a eles números ou pseudônimos. Assim, se algum dia as forças de segurança confiscarem o seu telefone ou cartão SIM, não terão acesso a toda a sua rede.

- Leve cartões SIM extras para manifestações se você achar que há risco de serem confiscadas. É muito importante que você tenha com você um celular que funcione. Se por acaso você precisar descartar o seu cartão SIM, tente destruí-lo fisicamente.

- Se o seu telefone permitir, proteja-o com uma senha. Todo cartão SIM dispõe de um código PIN por padrão. Mude-o e bloqueie o seu cartão SIM com esse código PIN. Uma senha (o seu código PIN) será pedida cada vez que você usar o telefone.

- Se você achar que uma manifestação vai acabar em forte repressão pelas forças de segurança, ative o modo avião do seu telefone. Você não será mais capaz de enviar ou receber chamadas, mas poderá tirar fotos ou gravar vídeos e carregá-los para sites da Internet mais tarde. Essa tática também é útil se você achar que as forças de segurança vão focar prioritariamente naqueles que dispõem de um celular durante a manifestação. Mais tarde, o governo poderá exigir as gravações de chamadas, de SMS ou de dados telefônicos de todos que se encontravam em um local específico, num momento específico, para executar prisões em massa.

- Desative as funções de geolocalização dos seus aplicativos, a menos que você só use essa função para fins de militância, marcando com um tag algumas mídias durante um acontecimento. Se você usar o seu celular para difundir vídeo em streaming ao vivo, desative as funções de GPS e de geolocalização.

- Se o seu telefone funciona com o sistema operacional Android, você pode usar inúmeras ferramentas para criptografar a navegação na Internet, os seus chats, SMSs e mensagens de voz por meio dos aplicativos criados pelo Guardian Project e Whispersys. Quando você usar o celular para acessar a Web, use o HTTPS sempre que possível.

Lute contra a censura:

Algumas ferramentas apresentadas acima permitem contornar a censura imposta pelas autoridades (anonimização da conexão, VPN, etc.). Para saber mais:

- Consulte o site «Collateral Freedom» da Repórteres sem Fronteiras: Para contornar a censura tecnológica instaurada por Estados que não respeitam os Direitos Humanos, a RSF usou um dispositivo original baseado na técnica de mirroring, que consiste em duplicar os sites censurados e hospedar as copias em servidores gigantes da Web, como Amazon, Microsoft ou Google.

- Visite o site "Circumvention Central", lançado pela GreatFire (organização na origem da iniciativa "Collateral Freedom") para saber mais sobre VPN

- Consulte o site "Security in-a-box" da Tactical Tech e os artigos da Electronic Frontier Foundation para driblar melhor a censura online e permanecer anônimo.

Lançado em 2011, o projeto «Collateral Freedom» tonar acessíveis sites que foram censurados. →

©RSF

A REPÓRTERES SEM FRONTEIRAS promove e defende a liberdade de informar e de ser informado em todo o mundo. A organização com sede em Paris possui dez escritórios internacionais (Berlin, Genebra, Madrid, New York, Estocolmo, Turin, Viena, Washington DC, Rio de Janeiro), assim como uma rede de 130 correspondentes espalhados poelos cinco continentes.

Secretário Geral: CHRISTOPHE DELOIRE
Editora Chefe da RSF: VIRGINIE DANGLES

SECRETARIA INTERNATIONAL
CS 90247
75083 Paris Cedex 02
Tel. +33 1 44 83 84 84
Web : www.rsf.org

REPORTERES SEM FRONTEIRAS
PELA LIBERDADE DA INFORMAÇÃO