As Quatro Ameaças à Privacidade Na Internet[1]: Os Vírus, As Transações Econômicas, Os Sites e As Redes Sociais[2]

Isadora LIRA[3]
Thiago Soares[4]
Universidade Federal da Paraíba

RESUMO

Em junho de 2013, reportagens do *Washington Post* e do *The Guardian* trouxeram à tona a vulnerabilidade da privacidade mundial na internet. Uma série de documentos comprovavam o monitoramento da rede por parte dos Estados Unidos. Além dos programas de vigilância, detectamos quais seriam as ameaças à privacidade dos usuários na internet: os vírus, que podem desde apagar todos os arquivos de um computador até fazer um avião cair; as transações econômicas, que sendo monitoradas podem cercear a liberdade dos indivíduos; os sites, que estão na mira dos programas de vigilância; e as redes sociais, que servem, principalmente, de bancos de dados gratuito para quem vigia a internet.

PALAVRAS-CHAVE

Privacidade; Internet; Prism; Vigilância; Redes Sociais; Criptografia.

INTRODUÇÃO

Como é estar offline? É uma pergunta que se torna pertinente à medida que cresce o número de máquinas conectadas à internet. "É possível estar offline?" – ainda sim, embora empresas como o Google estejam promovendo ações como o Project Loon, uma forma de fornecer acesso global à internet através de equipamentos instalados em balões estratosféricos – fazendo com que regiões que ainda não estão cobertas com o manto da internet possam acessar a rede.

A convergência dos dispositivos eletrônicos à internet só cresce. E as possibilidades de transformação do cotidiano são diversas. Não só os celulares com

[1] Trabalho apresentado no IJ 08 - Estudos Interdisciplinares da Comunicação do XVI Congresso de Ciências da Comunicação na Região Nordeste realizado de 15 a 17 de maio de 2014.
[2] Este artigo é uma síntese do trabalho de conclusão de curso, de autoria de Isadora Teixeira de Lira, sob orientação do professor doutor Thiago Soares, para obtenção do grau de Bacharelado no curso de Comunicação Social com habilitação em Jornalismo pela UFPB.
[3] Jornalista formada pelo curso de Comunicação Social da Universidade Federal da Paraíba, e-mail: isadoratlira@gmail.com
[4] Orientador do trabalho. Professor Doutor do Departamento de Comunicação - UFPE, e-mail: thikos@gmail.com

GPS registrando passo a passo da sua rotina, mas também geladeiras conectadas à rede – e outros aparelhos. Como se fosse pouco, a Coreia do Sul está construindo uma cidade inteira conectada à internet, com direito a garrafas de refrigerante com sensores wi-fi para computar desconto nos impostos de moradores que jogarem o produto no cesto de reciclagem apropriado. Asfaltos que analisam o tempo de deslocamento de veículos em engarrafamento, sensores nos postes para diminuir a intensidade para quando não houver nenhum transeunte. O nome dessa cidade é Songdo, a 65km de Seul. Tudo isso está sendo feito pela módica quantia de U$80 bilhões.

Essa realidade totalmente conectada não nos interessa – por enquanto. Num nível um pouco inferior, mas mais próximo à cena atual, temos nossa boa vontade em permanecer conectados *full time*, sem que sensores urbanos estejam tão presentes nas atividades corriqueiras: expondo detalhes em redes sociais, preenchendo vários formulários de criação de perfil ou e-mail, instalando diversos aplicativos em celulares, ou seja, alimentando vários bancos de dados. Todas essas ações acabam nos deixando um pouco mais suscetíveis à violação de privacidade. Isso vem sido percebido com escândalos como a venda de arquivos pessoais para empresas de publicidade, ataques a sites, governos espionando uns aos outros (através de monitoramento de rede), ciberguerra, vazamento de informação, suscitam a fragilidade da privacidade de quem acessa a internet – 2,45 bilhões de pessoas no planeta, de acordo com dados divulgados pela União Internacional de Telecomunicações (UIT), em março de 2013.

A capacidade crescente de armazenamento de dados é um fato que preocupa o fundador da WikiLeaks[5], Julian Assange, que explana no livro "Cypherpunks – a liberdade e o futuro na internet" que, a população humana dobra aproximadamente a cada 25 anos, mas a capacidade de vigilância dobra a cada 18 meses.

> Estamos em um estágio no qual é possível comprar apenas US$ 10 milhões uma unidade para armazenar permanentemente os dados interceptados de um país de médio porte. Então me pergunto se não precisaríamos de uma reação equivalente. Essa é uma ameaça enorme e concreta à democracia e à liberdade de todo o planeta, e essa ameaça precisa de uma reação, como a ameaça da guerra atômica precisou de uma reação em massa, para tentar controlá-la enquanto ainda for possível. (ASSANGE, 2013, p.67)

[5] Wikileaks é uma organização transnacional sem fins lucrativos, sediada na Suécia, que publica, em sua página (*site*), postagens (*posts*) de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas.

Pensando nesse armazenamento e nas divulgações de programas de vigilância global (será mostrado a seguir), identificamos quatro ameaças claras à privacidade na internet, que são elas: vírus, transações econômicas, sites e redes sociais.

1. Vírus

A primeira referência a vírus de computador foi feita em 1983, pelo pesquisador Fred Cohen, que deu esse nome aos programas de códigos nocivos. No ano seguinte, na *7th Annual Information Security Conference*, o termo vírus foi definido como um programa que infecta outros programas, podendo criar cópias dele mesmo, os vírus passaram por várias transformações. Considerado como o primeiro vírus detectado, o Brain era responsável por danificar o setor de inicialização da máquina. Existem vários tipos e características de vírus, tais como: Boot, que impede a inicialização da máquina; Time bomb, que é programado para atacar em determinada data/horário; Hijacker, que modifica o navegador de internet e pode impossibilitar o download de vírus; Trojan (ou Cavalo de Troia), que invade o computador, rouba envia dados para um terceiro, sem que o computador infectado o detecte. Mas os vírus podem fazer mais estrago do que deletar todos os arquivos de um computador.

Não à toa, a Organização do Tratado do Atlântico Norte (Otan), publicou o Manual Tallin, um livro que serve como uma orientação para que internautas, militares e advogados saibam o que é ou não permitido em ciberguerras e direitos humanos. Por exemplo, no manual se destaca a proibição de ataques cibernéticos contra hospitais, barragens, centrais nucleares e outros locais da natureza civil. Entretanto, não é considerado um documento oficial.

Para treinar pessoas que defendam suas nação de um possível ataque com vírus, foi criado um campeonato chamado Collegiate Cyber Defense, na Bacia do Pacífico. Esse é o maior evento universitário de ciberdefesa dos Estados Unidos. Um dos membros do Chaos Computer Club[6], Jacob Appelbaum, já participou do evento.

> Nós dedicamos um bom tempo competindo num evento de ciberguerra no qual a Spawarr (Space and Naval Warfare Systems Command), um braço civil da Marinha norte-americana que inclui serviços de *pentesting*

[6] O Chaos Computer Club (CCC) é uma associação alemã de hackers. Seus objetivos mais importantes são liberdade de acesso à informação, liberdade de expressão, para mais transparência nos governos e na liberdade da informação.

> envolvendo *hacking* ofensivo e defensivo de computadores, jogou como a Equipe Vermelha. O que eles faziam era atacar todos os outros participantes e cada equipe devia defender seu sistema de computação, recebido no início do evento e do qual não possuía nenhum conhecimento prévio. Você começa sem saber que tipo de sistema precisará defender e nem como será feita a contagem dos pontos, de forma que tenta fazer tudo o que dá pra fazer, esperando um bom resultado. (APPELBAUM, 2013, p.54)

Contudo, os vírus podem afetar outras máquinas também. Em Madri, 2008, mais precisamente no dia 20 de agosto, 154 pessoas morreram carbonizadas na aeronave MD-82 da companhia aérea Spanair por causa de um Cavalo de Troia. O avião não conseguiu decolar do aeroporto Barajas. O comandante percebeu uma falha em um sensor, na segunda tentativa de decolagem, a aeronave saiu da pista, partiu-se ao meio e explodiu. Dezoito pessoas sobreviveram porque foram atiradas para fora do avião. A irregularidade responsável pelo acidente estava no computador central registrava as falhas dos aviões da companhia, e foi impedido de contabilizar o número de problemas nas aeronaves por causa de um Cavalo de Troia. Se o computador estivesse funcionando corretamente, a falha técnica do sensor da aeronave poderia ter sido detectada. Dois erros haviam sido registrados no dia anterior ao acidente. No dia seguinte, quando os mecânicos tentaram inserir no banco de dados um problema detectado pelo comandante, eles não conseguiram por causa dos erros causados pelo código malicioso.

Um vírus também já foi responsável por invadir e queimar 1000 das 8692 centrífugas da usina nuclear Natanz, no Irã. O nome do *malware*[7] é Stuxnet, e ele foi feito para atingir exclusivamente o sistema operacional Scada, da Samsung, que é utilizado apenas em usinas nucleares – por isso não foi detectado em computadores pessoais comuns.

A convergência de rede aponta pra um esgoto de vírus que pode transitar em todos os dispositivos que se conectem. Jérémie Zimmermann, cofundador e porta-voz do grupo La Quadrature Du Net, organização europeia em defesa do anonimato online, argumenta que a complexidade dos dispositivos com acesso à internet é nociva.

> Essa é uma tecnologia que não é feita para ser entendida. É o que acontece com a tecnologia proprietária. (...) Quando um computador é uma máquina genérica, é possível fazer o que se quiser com ela. Você pode processar qualquer informação como um *input* e transformá-la em qualquer *output.* E cada vez mais estamos criando dispositivos que são esses computadores de uso geral, mas restritos a fazer uma coisa só, como só um GPS, ou só um celular ou só um tocador de MP3. Cada vez mais estamos criando máquinas

[7] O termo **malware** é proveniente do inglês ***ma****licious soft****ware***; é um software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não).

> com um controle integrado, para proibir o usuário de fazer certas coisas. (ZIMMERMANN, 2013, p.49)

Appelbaum (2013) coloca que todas as máquinas se tornaram computadores. Não temos mais carros, aparelhos auditivos ou aviões, mas computador com quatro rodas, computadores com asas, computadores que nos ajudam a escutar.

> E parte disso não é se eles são computadores de finalidade única ou não, é se podemos ou não verificar que eles realmente fazem o que dizem que fazem. (...) Quando não temos controle algum sobre a nossa tecnologia, essas pessoas a usam para seus próprios fins – mais especificamente, para a guerra. (APPELBAUM, 2013, p.50)

A convergência dessas tecnologias é uma ameaça latente à privacidade à medida que estamos integralmente conectados numa rede vulnerável.

2. Transações econômicas

A praticidade de realizar transferências online trouxe mais do que conforto na hora de realizar pagamentos, mas também permitiu que as transações se tornassem mais facilmente rastreáveis. Por exemplo: todas as compras efetuadas em cartão de crédito ou débito ficam registradas nos bancos de dados dessas empresas – e onde ficam as sedes delas? Andy Müller-Maguhn, membro do Chaos Computer Club, ressalta o problema desse método centralizador de registro das transações econômicas.

> Duas companhias de crédito, ambas com uma infraestrutura eletrônica de autorização centralizada nos Estados Unidos – o que implica acesso aos dados na jurisdição norte-americana –, controlam a maioria dos pagamentos em cartão de crédito do planeta. Empresas como o Paypal, que também atuam sob a jurisdição norte-americana, aplicam as políticas do país, seja bloqueando a venda de charutos cubanos por parte de varejistas on-line alemães ou os pagamentos ao WikiLeaks em jurisdições não norte-americanas. Isso significa que o governo dos Estados Unidos tem acesso aos dados, além da opção de impor controles aos pagamentos internacionais. (MÜLLER-MAGUHN, 2013, p. 105)

E, já que as transações podem ser rastreadas, é possível que elas sejam censuradas. Quando o governo dos Estados Unidos iniciou sua ação contra o WikiLeaks, uma das primeiras medidas adotadas foi pressionar a Visa, MasterCard, Paypal e Bank of America a negar a prestação de serviços financeiros ao WikiLeaks. E desde dezembro de 2010 as transferências bancárias e doações realizadas com cartão de crédito foram bloqueadas. Quadro que só reverteu na Islândia no dia 25 de abril de 2013, quando o Supremo Tribunal islandês condenou a subsidiária da Visa, a Valitor, a

parar com o bloqueio econômico. Foi decidido que a Valitor teria que repor as transferências aos apoiantes da WikiLeaks num prazo de 15 dias ou a pagar uma multa de € 5350 por dia.

> É de extrema importância criar uma moeda eletrônica justamente porque o controle dos meios de pagamento constitui um dos três ingredientes do Estado (controle sobre as forças armadas em determinada região, controle sobre uma infraestrutura de comunicações e controle sobre uma infraestrutura financeira) (...). Se retirarmos o monopólio estatal dos meios de interação econômica, removeremos um dos três principais ingredientes do Estado. No modelo do Estado como uma máfia, no qual o Estado não passa de um esquema de extorsão, ele tira o dinheiro das pessoas de todas as maneiras possíveis. É importante para o Estado poder controlar os fluxos monetários, possibilitando assim a arrecadação de dinheiro, mas também para simplesmente controlar o que as pessoas fazem – dando incentivos aqui, removendo acolá, banindo completamente determinadas atividades, organizações ou interações entre certas organizações. (ASSANGE, 2013, p. 104 e 105)

Mas íntima ligação entre privacidade, informação e economia pode ser resumida no seguinte trecho:

> Todos nós falamos sobre a privacidade das comunicações e o direito de divulgar informações. É fácil entender isso – a questão tem uma longa história (...). Mas, se compararmos esse valor com o valor da privacidade e da liberdade de interação econômica, a cada vez que a CIA vê uma interação econômica, eles sabem que ela está sendo feita entre tal e tal pessoa ou empresa, desse local para aquele, e também sabem o valor e a importância da interação. Então, será que a liberdade de interação econômica, ou a privacidade nessas interações, não é mais importante que a liberdade de expressão, já que são as interações econômicas que de fato fundamentam toda a estrutura da sociedade? (ASSANGE, 2013, p.111)

A alternativa possível que Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn e Jérémie Zimmermann apontam é a utilização de uma criptomoeda[8], no caso,

[8] **Criptomoeda** é um conceito descrito originalmente em 1998 por Wei Dai na lista de discussões Cypherpunk. É um termo usado para moedas digitais passíveis de criptografia, que utiliza um algoritmo próprio.

a bitcoin. Criada em 2009, a moeda é utilizada na rede *peer-to-peer* (P2P)[9] para registrar as transações. A moeda não depende da confiança em nenhum emissor centralizado como um servidor de um banco. As transações são públicas, mas os usuários são privados.

> A observância da honestidade no sistema 'bancário do bitcoin está imbuída em sua própria arquitetura. A computação se traduz em custos de eletricidade para cada agência do banco Bitcoin, de forma que é possível atribuir o custo de cometer uma fraude em termos de preços de energia elétrica. O trabalho necessário para cometer uma fraude é configurado para ser maior em termos de custos de eletricidade do que o benefício econômico resultante dessa fraude. (ASSANGE, 2013, p. 108)

No dia 19 de agosto de 2013, o site PC World publicou uma declaração do Ministério Federal das Finanças alemão que diz que, embora a Bitcoin não seja uma moeda de pleno direito, é permitido utilizá-la em operações privadas no país. Mas as empresas que queiram utilizá-la precisam da autorização da Autoridade de Supervisão Financeira Federal (BaFin).

A bitcoin, embora apontada como uma alternativa, possui alguns pormenores. As transações são lentas, levam cerca de dez minutos de processamento computacional entre a entrega da moeda e aquele que a recebeu. A segurança do dinheiro também é de responsabilidade do usuário – e como é uma criptomoeda, exige domínio de criptografia. Zimmermann (2013) também aponta outra falha: por ter uma natureza deflacionária, o dinheiro tende a sumir. Não é vantagem utilizar essa moeda como poupança. Mas é útil para transações imediatas. Ao menos por enquanto.

3. Sites

Já que podemos falar dessa convergência em rede, não se pode cometer a imprudência de ignorar o monopólio que existe na World Wide Web: o Google. A empresa, criada em 1996 por Larry Page e Sergey Brin, hoje pode ser considerada a muletas da internet. O Google oferece diversos tipos de serviços que vão, pouco a pouco, se tornando indispensáveis pra quem utiliza a rede. Ao criar um login no Google, o usuário tem acesso ao Gmail, Blogger, Youtube, Google+, GoogleGroups – dentre tantos outros serviços que não necessariamente exigem a criação de uma conta, mas que, caso você a possua, facilitará o seu trânsito na rede.

[9] **Peer-to-peer** é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

O Chrome, navegador mais utilizado no mundo desde maio de 2012, de acordo com o site de métricas de navegadores StatCounter, sendo 750 milhões de usuários ativos mensais[10]. E ainda existem os usuários de Android, o sistema operacional do Google para dispositivos móveis.

Mas existem outras dezenas de serviços oferecidos pela empresa – e a tendência é aumentar. Eric Schimidt, chefe-executivo do Google, disse em 2007, em entrevista ao Financial Times: "O objetivo é permitir que usuários do Google sejam capazes de fazer perguntas como 'O que vou fazer amanhã?' e 'Em qual trabalho devo me ocupar?'". E voltou a reafirmar isso em 2010, em entrevista ao Wall Street Journal: "Eu realmente acho que a maioria das pessoas não querem o Google para responder suas perguntas, elas querem Google para dizer-lhes o que fazer em seguida". Essa onisciência e onipresença da empresa confere uma aura divina a essa tecnologia que nos cerca.

> A máquina e a ciência, que o homem comum ainda olha com desconfiança, estão progressiva, mas irreversivelmente convertendo-se no destino espiritual da humanidade tecnificada. (FELINTO, 2005, p. 32)

Todo esse poder que cabe à internet levanta algumas questões quanto à nossa privacidade e o quanto estamos vulneráveis a esse controle. Em junho de 2013, os jornais The Guardian e Washington Post publicaram matérias divulgando o esquema de vigilância global de internet da Agência de Segurança Nacional americana (NSA). Os dados foram concedidos por Edward Snowden, um estadunidense de Elizabeth City, Carolina do Norte, que já trabalhou como engenheiro de sistema, administrador de sistema, assessor sênior da Agência Central de Inteligência (CIA), consultor de soluções e oficial do sistema de telecomunicações e, até junho de 2013, era funcionário no setor de defesa da empresa Booz Allen Hamilton, que prestava um trabalho para a NSA.

O programa de vigilância eletrônica se chama Prism[11]. Snowden apresentou detalhes do programa através de slides no PowerPoint (figuras 1, 2 e 3). Perguntado sobre as razões de ter denunciado o programa, Edward falou, em entrevista à Glenn

[10] Dados divulgados no Google I/O 2013, evento realizado do dia 15 ao dia 17 de maio de 2013.
[11] O Prism nasceu em 2007, sob o governo de George W. Bush, com autorização concedida por um tribunal sigiloso, a Corte de Vigilância de Inteligência Estrangeira (dia 20 de julho de 2013 essa autorização foi renovada). A administração do programa é de responsabilidade da Agência de Segurança Nacional dos Estados Unidos, a NSA, que faz parte do Departamento de Defesa dos Estados Unidos e é responsável por espionar comunicações de outros países, decifrar códigos governamentais e desenvolver sistemas de criptografia para o governo, embora suas pesquisas não sejam divulgadas. A NSA tem 35,2 mil funcionários, segundo os documentos fornecidos por Snowden.

Greenwald, que ao se deparar com todos aqueles dados, todas aquelas informações, ele se sentiu obrigado a tornar o fato público. De acordo com o documento obtido pelo Guardian, a primeira empresa a fazer parte do Prism foi a Microsoft, logo no início da existência do programa. Em seguida vieram Yahoo (2008); Google, Facebook e PalTalk (2009); Skype e AOL (2011); Apple (2012). Todas as empresas envolvidas negaram.

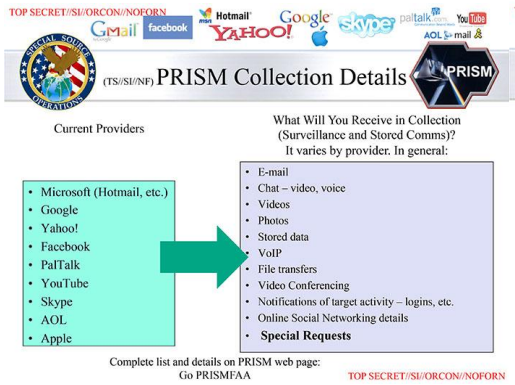

Figura 1: empresas colaboradoras

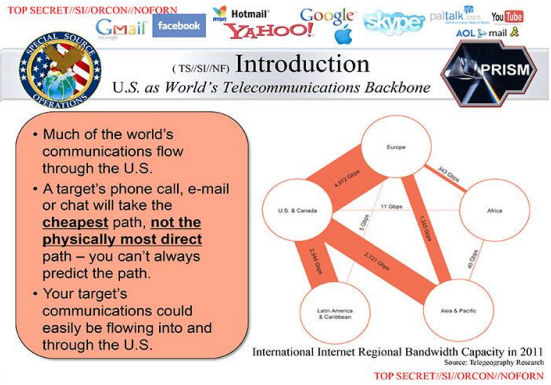

Figura 2: tráfego de informações pelo Prism

Os documentos apresentados mostraram que a NSA possui muita informação sobre cidadãos de vários países - além do programa de vigilância de internet, existe o XKeyscore, que monitora as ligações telefônicas -, mas tais informações só seriam averiguadas em caso de "atividades suspeitas", já que é impossível analisar todos os dados de cada cidadão. Pra isso serve essa capacidade gigantesca de armazenamento.

> Eu gostaria de explorar um pouco mais essa analogia da vigilância em massa como uma arma de destruição em massa. Foi constatado pela física que seria possível construir uma bomba atômica, e, quando ela foi construída, toda a geopolítica mudou, e a vida de muitas pessoas mudou. (...)Então me pergunto se não precisaríamos de uma reação equivalente. Essa é uma ameaça enorme e concreta à democracia e à liberdade de todo o planeta, e essa ameaça precisa de uma reação, como a ameaça da guerra atômica precisou de uma reação em massa, para tentar controlá-la enquanto ainda for possível. (ASSANGE, 2013, p. 67)

No livro "Cypherpunks", a solução apresentada é a criptografia. Apropriação dessa tecnologia pela massa e privacidade para os fracos e transparência para os fortes. Afinal, qual o preço a ser pago por essa "segurança" que o monitoramento da internet oferece? Vamos tomar como exemplo o caso da jornalista Michele Catalano. No primeiro dia de agosto de 2013, ainda pela manhã, seu marido estava sentado na sala de estar com seus dois cachorros, quando ouviu barulhos de carros parando em sua calçada. Ao olhar pela janela, identificou três SVUs pretos e seis homens vestidos casualmente se espalhando pelo jardim. O marido de Michele abriu a porta para os homens, que vasculharam superficialmente a casa e perguntaram se eles possuíam

bombas[12]. Por que a casa de Michele foi revistada? Porque a jornalista havia pesquisado por panelas de pressão no Google, o marido buscou por mochilas, e seu filho de 20 anos havia lido sobre como era realizada a confecção de bombas com panela de pressão. E já que isso tudo aconteceu poucos meses após os atentados de Boston, pareceu pertinente ao governo estadunidense averiguar de perto o que estava acontecendo. Foi uma medida de segurança nacional e insegurança pessoal. Vale a pena?

4. Redes sociais

Se a privacidade já está ameaçada só com a ação de fazer pesquisas corriqueiras nos sites de busca, o que dizer da utilização de redes sociais? Primeiramente é pertinente colocar o que caracteriza uma rede social, de acordo com a definição de Raquel Recuero:

> Sites de redes sociais propriamente ditos são aqueles que compreendem a categoria dos sistemas focados em expor e publicar as redes sociais dos atores. São sites cujo foco principal está na exposição pública das redes conectadas aos atores, ou seja, cuja finalidade está relacionada à publicização dessas redes. É o caso do Orkut, do Facebook, do Linkedin e vários outros. São sistemas onde há perfis e há espaços específicos para a publicização das conexões com os indivíduos. Em geral, esses sites são focados em ampliar e complexificar essas redes, mas apenas nisso. O uso do site está voltado para esses elementos, e o surgimento dessas redes é consequência direta desse uso. No Orkut, por exemplo, é preciso construir um perfil para interagir com outras pessoas. E é só a partir desta construção que é possível anexar outros perfis à sua rede social e interagir com eles. Toda a interação está, portanto, focada na publicização dessas redes. (RECUERO, 2009, p.102)

Mas foi com o Facebook, criado em 2004 por Mark Zuckerberg, que se pôde perceber a força catalisadora de dados pessoais de uma rede social. Com mais de 1 bilhão de usuários no mundo inteiro[13], sendo 67 milhões no Brasil, a empresa concentra informações pessoais de, pelo menos, 14% da população mundial.

O primeiro escândalo em relação à venda de dados do Facebook ocorreu em outubro de 2010. Ao utilizar determinados aplicativos dentro da rede social (que são programados por outras empresas), os usuários concor dam que os programas tenham acesso aos seus

[12] O relato completo sobre o incidente pode ser lido no https://medium.com/something-like-falling/2e7d13e54724, na postagem da própria Michele.
[13] Informação divulgada pelo Facebook no dia 14 de setembro de 2012.

dados. Na época o Facebook emitiu um texto no blog dos Desenvolvedores dizendo que é totalmente intolerante com os *brokers* (corretores de dados), uma vez que eles "põem em risco o que os usuários esperam do Facebook". E ainda acrescentou: "Essa violação da nossa política é algo que levamos a sério".

Entretanto nem todo mundo se sente totalmente confortável com essa ideia de armazenamento de dados do Facebook. Em 2011, Max Schrems, então estudante de Direito, evocou as leis europeias de proteção à privacidade e pediu cópias de todas as informações que a rede social guardava sobre ele. Recebeu como resposta um dossiê com 1.222 páginas, incluindo lista de locais onde ele acessou o site e comentários que ele havia apagado, além do que ele compartilhava com os amigos. Isso inspirou Max a fundar o grupo Europa Contra o Facebook, que cobra respeito às regras de privacidade dos usuários. A entidade, ao pressionar o Facebook para entregar os dados armazenados a respeito delas (sob os termos da Legislação Europeia de proteção de dados), descobriu que o menor volume de dados foi 350 MB e o maior de aproximadamente 800 MB[7]. E também foi revelado como é a estrutura de dados da rede social. Cada vez que você faz o login com o número IP, cada clique, cada horário, número de vezes que você acessou uma determinada página é registrado.

Max Schrems concedeu uma entrevista à Folha de S. Paulo, publicada no dia 15 de julho de 2013. Apontou que a saída não é excluir as contas nas redes sociais – até porque é muito difícil utilizar a internet sem fornecer algum dado que seja ao Google, à Apple, à Microsoft, Amazon, ou ao Facebook. Max acredita que o que deve ser feito é pressionar as empresas para que as mesmas respeitem a nossa privacidade:

> A maior ameaça à privacidade é que nós não temos nenhum controle sobre o que eles fazem com esses dados em seus servidores dos Estados Unidos. As empresas têm criado suas próprias políticas de privacidade na internet, mas normalmente elas são tão vagas que permitem que se faça qualquer coisa com as suas informações pessoais. (...)Se você sair individualmente do Facebook, possivelmente vai tentar levar seus amigos para outra rede social. A única solução real seriam redes sociais abertas, em que você pudesse interagir com pessoas que estão em outras redes. Da mesma maneira que pode mandar um email de um provedor para outro ou ligar para um telefone de outra operadora. (SCHREMS, 2013, p.1)

Não é só utilizando a rede social de forma recreativa que a sua privacidade está ameaçada. As pessoas envolvidas o protesto organizado por meio do Facebook em 2008, no Cairo, foram devidamente rastreadas. A manifestação foi realizada em 6 de

abril de 2008, em defesa da greve coibida dos trabalhadores da indústria têxtil de Mahalla al-Kobra. Foi criado um grupo no Facebook para o April 6 Youth Movement (Movimento dos Jovens de 6 de Abril), para encorajar os egípcios a realizar manifestações no Cairo e em outras cidades para coincidir com a ação da indústria têxtil em Mahalla. Os protestos não foram realizados e os administradores do grupo no Facebook, Esraa Abdel Fattah Ahamed Rashid e Ahmed Maher -, foram presos, o último foi torturado até revelar a sua senha da rede social. Na Revolução Egípcia, em 2011, o manual *Como protestar de forma inteligente,* recomendava que não fossem usados nem Twitter nem Facebook.

Contrariando a expectativa do poder organizacional das massas através das redes sociais, o jornalista bielorruso Evgeny Morozov[14], em entrevista concedida à revista Época e publicada no dia 26 de fevereiro de 2011, se mantém cético quanto à utilização dessas redes:

> Mas há muitas outras coisas que o Google e o Twitter poderiam ter feito – especialmente em termos de fazer seus serviços mais amigáveis aos ativistas – e não fizeram. Nós devemos nos manter céticos sobre o compromisso das empresas de tecnologia com a liberdade de expressão e os direitos humanos, e não celebrá-las como campeões dessas causas. (...) Quando há empresas americana e europeias vendendo toda a tecnologia que os ditadores agora usam para monitorar os dissidentes, acho difícil de acreditar que os dissidentes consigam vencer um dia. Além disso, precisamos distinguir entre ativistas 'profissionais' e 'ocasionais'. Claro que aqueles que praticam a dissidência no dia a dia estão mais cientes dos riscos que correm e sabem os pontos fracos das mídias sociais. Mas não tenho certeza se o mesmo acontece com os "ativistas ocasionais" – aqueles que se juntam a um grupo no Facebook porque seus amigos estão lá ou que repassam uma messagem no Twitter. A promessa inicial da mídia social era que os dissidentes profissionais conseguiriam ter contato com os dissidentes ocasionais – mas as capacidades de vigilância cancelaram algumas dessas promessas. (MOROZOV, 2011, p.1)

Para Zimmerman, o Facebook e o Google se tornaram extensões das agências de inteligência dos Estados Unidos. As redes sociais acabam servindo como serviço de espionagem privada, visto que armazenam todos os dados e registram todas as conversas de seus usuários. Jacob Appelbaum alegou já ter seus dados solicitados pelo Governo:

[14] **Evgeny Morozov** é pesquisador-visitante da Universidade Stanford e analista da New America Foundation. É autor de "The Net Delusion: The Dark Side of Internet Freedom" (a ilusão da rede: o lado sombrio da liberdade na internet).

> Segundo o *Wall Street Journal*, o Twitter, o Google e a Sonic.net, três serviços que utilizo ou utilizei no passado, receberam uma citação 2703(d), uma forma incomum de intimação secreta (...) Sob o Stored Communications Acts, basicamente, o *Wall Street Journal* diz que esses serviços afirmaram que o governo queria os metadados, alegando ter o direito de acesso a eles sem a necessidade de apresentar um mandado. Atualmente está em discussão no judiciário o direito do governo de manter suas táticas em sigilo, não só do público, mas dos autos judiciais. (...) Se você constrói um sistema que registra tudo sobre uma pessoa e sabe que está em um país que possui leis que o forçarão a revelar essas informações ao governo, então talvez você não devesse construir esse tipo de sistema (...) Seria absolutamente negligente da parte de uma empresa tentar vigiar as pessoas sabendo que está em um país que explicitamente faz isso, seria absolutamente negligente se uma empresa como o Facebook instalasse servidores na Líbia de Gaddafi ou na Síria de Assad."(APPELBAUM, 2013, p. 73-76)

A questão que fica é: como seria possível utilizar as redes sociais sem que nossa privacidade esteja ameaçada? Não é uma questão de "está na chuva é para se molhar", e mais de apropriação desse espaço como um ambiente livre, o cenário utópico da internet.

CONSIDERAÇÕES FINAIS

Todos os pontos abordados nesse artigo estiveram focados nas ameaças para quem utiliza a *surface web*, o conjunto de conteúdos indexado aos mecanismos de busca padrão. Não foi mencionado como isso se daria com a utilização da *deep web*[15], uma alternativa para quem quisesse utilizar a rede sem tamanha vigilância, utilizando serviços como o Tor, um software livre e uma rede aberta para quem pretende preservar a privacidade na internet. Isso é possível pela forma que a conexão é realizada[16]. Mas essa é uma experiência que merece um espaço próprio.

[15] **Deep web** é o conjunto de sites e/ou comunidades, os quais não são identificados pelos mecanismos de busca, como o *Google*. Estes endereços eletrônicos somente são detectados através de sistemas avançados de busca e utilizando códigos específicos e técnicos. Uma das características deste tipo de site é a ausência do formato HTML, justamente para não ser identificado facilmente.

[16] Na internet convencional, o computador é conectado a um determinado servidor, por isso você acessa é passível de rastreamento. Utilizando o Tor, a conexão passa por vários outros computadores, criando IPs falsos, até chegar ao servidor. O caminho completo não é revelado individualmente aos elos que formam essa corrente, sendo cada etapa criptografada e os circuitos completos têm vida útil de 10 minutos, depois são gerados outros. Cada servidor na cadeia recebe o pacote e passa adiante, registrando apenas a máquina anterior e a posterior. Mais informações: http://www.torproject.org/

Não existe um mapa da internet. Por que ela é controlada? Como? Por quem? Temos pistas bem consistentes em relação a essas perguntas. Resta aos usuários a apropriação desse território. Hakim Bey, um libertário e pesquisador da organização dos Piratas, escreveu uma espécie de manifesto chamado: "TAZ – Zona Autônoma Temporária" em 1985. Embora ele não engesse um conceito do que seria uma TAZ, ficam evidentes alguns princípios anarquistas, de total ausência de hierarquias opressivas. Mas esses espaços "livres" poderiam estar inseridos numa sociedade controladora e opressora. A questão é: apropriar-se do funcionamento de rede acaba sendo uma questão primordial para que se escape do controle que ela oferece; a rede pode, e deve, resgatar o espírito de zona autônoma, não apenas num sentido romântico ou político, mas como uma extensão de liberdade humana. E pra chegar lá, vai ser preciso muita criptografia e pressão nas empresas de internet.

No Brasil, a discussão sobre privacidade na internet aumentou com a aprovação do Marco Civil na Câmara dos deputados no dia 25 de março de 2014. O texto aprovado garante: a neutralidade de rede, as empresas de internet não podem alterar o preço do pacote de acordo com a frequência que o usuário acesse a internet; armazenamento de dados, os registros de conexão dos usuários devem ser guardados pelos provedores de acesso pelo período de um ano, são informações sobre IP, data e hora inicial e final da conexão; retirada de conteúdo e responsabilidades, um conteúdo só pode ser retirado do ar sob ordem judicial[17]. O Marco Civil foi

A iminência da vida completamente conectada só traz à tona a necessidade de privacidade dos cidadãos. E é importante saber como isso será feito: através da pressão nas empresas de internet ou apropriação de tecnologia.

REFERÊNCIAS

ASSANGE, Julian et al. **Cypherpunks - liberdade e o futuro da internet**. São Paulo: Boitempo, 2013.

TRIVINHO, Eugênio. **Bunker glocal: configuração majoritária sutil do imaginário mediático contemporâneo e militarização imperceptível da vida cotidiana**. Comunicação, mídia e consumo. São Paulo, v.5, n. 12, mar. 2008, p. 11-34.

[17] O texto prevê exceções. Por exemplo: um conteúdo pode ser retirado do ar sem ordem judicial desde que infrinja alguma matéria penal como pedofilia, racismo ou violência.

FELINTO, Erick. **A religião das máquinas: ensaios sobre o imaginário da cibercultura.** Porto Alegre: Sulina, 2005.

ROSA, Natalie. **Otan determina regras contra os ataques virtuais**. Disponível em: http://tecmundo.com.br/seguranca-de-dados/38191-otan-determina-regras-contra-os-ataques-virtuais.html. Acesso em: 05 de abril de 2013.

RECUERO, Raquel. **Redes sociais na internet**. Porto Alegre: Sulina, 2009.

COSTA, Renata. **O que é um vírus de computador?** Disponível em: http://revistaescola.abril.com.br/ciencias/fundamentos/virus-computador-internet-491683.shtml. Acesso em: 07 de julho de 2013.

HAMMERSCHMIDT, Roberto. **Chrome finalmente bate o Internet Explorer e se torna o rei dos navegadores**. Disponível em: http://www.tecmundo.com.br/google-chrome/23858-chrome-finalmente-bate-o-internet-explorer-e-se-torna-o-rei-dos-navegadores.html. Acesso em: 22 de julho de 2013.

Google testa balões para prover acesso à internet.
Disponível em: http://oglobo.globo.com/tecnologia/google-testa-baloes-para-prover-acesso-internet-8701861. Acesso em: 22 de julho de 2013.

SORG, Letícia. Evgeny Morozov: **"Graças à internet, regimes fracos vão morrer mais rápido".** Disponível em:
http://revistaepoca.globo.com/Revista/Epoca/0,,EMI214594-15227,00-EVGENY+MOROZOV+GRACAS+A+INTERNET+REGIMES+FRACOS+VAO+MORRER+MAIS+RAPIDO.html. Acesso em: 25 de julho de 2013.

O que é bitcoin? Disponível em: http://www.bitcoinbrasil.com.br/?page_id=2 Acesso em: 31 de julho de 2013.

CATALANO, Michelle. **Pressure cookers, backpacks and quinoa, oh my!**
Disponível em: https://medium.com/something-like-falling/2e7d13e54724 Acesso em: 06 de agosto de 2013.

MOROZOV, Evgeny. **O Facebook está contra a alegria**. Disponível em: http://www1.folha.uol.com.br/colunas/evgenymorozov/1010856-o-facebook-esta-contra-a-alegria.shtml. Acesso em: 20 de agosto de 2013.

BEY, Hakim. **Taz: Zona Autônama Temporária**. Disponível em: http://www.slideshare.net/binopaz/hakim-bey-taz-zona-autonoma-temporaria. Acesso em: 28 de agosto de 2013.

O que muda na sua vida. Disponível em: http://tecnologia.terra.com.br/marco-civil/ Acesso em: 03 de abril de 2014.