RESENHA

ASSANGE, Julian ... [et all]. **Cypherpunks:** liberdade e o futuro da internet. Tradução Cristina Yamagami. São Paulo: Boitempo, 2012. ISBN 978-85-7559-307-3

Luiz Fernando Gomes
UNICAMP/UFAL

A liberdade e o futuro da internet estão na pauta do dia, não apenas devido aos escândalos sobre a espionagem mundial praticada, principalmente, pelos países que representam as grandes forças políticas e econômicas, mas também pelas discussões sobre o Marco Civil da Internet, em andamento na Câmara dos Deputados.

As recentes denúncias de que a chefe do governo brasileiro, seus assistentes, a Petrobrás e, muito possivelmente outras pessoas e instituições brasileiras eram monitorados na web por agências de espionagem norte-americanas trouxeram à tona a fragilidade e mesmo a ingenuidade de grande maioria dos usuários da web, quanto ao destino, armazenagem, segurança e privacidade de suas correspondências, postagens e acessos a sites em geral e especialmente, os de relacionamento. As revelações de Edward Snowden, ex-técnico da NSA – Serviço Nacional de Inteligência dos EUA - sobre o esquema de espionagem americano mostraram que esse monitoramento tem escala mundial. Porém, esse tema não é novo: o site WikiLeaks (www.wikileaks.org), fundado pelo ativista Julian Assange em 2006, vem travando uma "guerra invisível" em várias batalhas digitais. O livro **Cypherpunks: liberdade e o futuro da internet** revela, discute e aprofunda grandes questões relacionadas essas batalhas digitais e à "guerra furiosa pelo futuro da sociedade".

A edição do livro Cypherpunks é a primeira a ser lançada na América Latina. O volume foi escrito tendo por base uma conversa entre os autores: Julian Assange, Jacob

Applebaum, Andy Müller-Maghum e Jérémie Zimmermann, mais tarde reelaborada por eles para publicação.

Uma nota introdutória apresenta as credenciais dos *cypherpunks*: eles literalmente "defendem a utilização da criptografia e de métodos similares como meio para provocar mudanças sociais e políticas." Criado no início dos anos 1990, o movimento atingiu seu auge durante as "criptoguerras" e após a censura da internet em 2001, na Primavera Árabe. O termo *cypherpunk*, uma derivação (criptográfica) de *cypher* (escrita cifrada) e *punk* – foi incluído no *Oxford English Dictionary* em 2006 e também dá nome a uma lista de discussões on-line. A bandeira levantada por Assange e seus amigos é pela liberdade na rede mundial de computadores, pois ela, como muitas outras tecnologias, apresenta imensa variedade de usos possíveis e seu rumo vai sendo definido pelo avanço tecnológico e pelo caminhar político. A rede é, pois, um espaço de disputa política.

O livro está dividido em onze capítulos, todos, como dissemos, elaborados a partir de conversas entre os quatro amigos. Além da apresentação contextualizadora da temática do livro, feita por Natália Viana, Julian Assange assina um prefácio para a edição latino-americana, no qual alerta sobre a ameaça da vigilância norte-americana para a América Latina e compara corporações norte-americanas de ampla penetração, como o Facebook, a um "exército ao redor de um poço de petróleo" –, pois a próxima alavanca no jogo geopolítico, diz ele, "serão os dados resultantes da vigilância: a vida privada de milhões de inocentes". O criador da Wikileaks também escreve uma introdução, intitulada: "Um chamado à luta criptográfica" em que alerta sobre o que chama de distopia transnacional da vigilância pós-moderna. Ao afirmar que "os Estados são sistemas através dos quais fluem as forças repressoras" critica nossa ingenuidade pois "como marinheiros a favor do vento, raramente percebemos que, abaixo da superfície visível do nosso mundo, se esconde uma grande escuridão." Essa introdução termina com uma frase que dá o tom extremista, radical e urgente, porém muito fundamentado, inclusive com extensão notas de rodapé explicativas do livro todo: "nossa missão é proteger a autodeterminação onde for possível,

impedir o avanço da distopia onde não for possível e, se tudo falhar, acelerar sua autodestruição."

Cada um dos onze capítulos traz uma visão crítica e bem informada, com análises propositivas, mas nem sempre otimistas. Alguns temas merecem maior atenção e outros são abordados mais ligeiramente. O primeiro capítulo aborda as perseguições sistemáticas e coordenadas que o Wikileaks e pessoas a ele associadas vem sofrendo pelo governo norte-americano desde 2010, após a publicação dos documentos americanos conhecidos como Collateral Murder, War Logs e Cablegate. Tais perseguições envolveram misteriosos problemas nas contas bancárias, desde pequenos detalhes ao fechamento de algumas delas.

O segundo capítulo intitula-se "Maior comunicação, maior vigilância". Nele discute-se não apenas o aumento no volume das comunicações, mas também a proliferação dos tipos de comunicação que antes eram privados e agora são, segundo os autores, interceptados em massa. O mundo já jogou seus detalhes mais secretos na internet. É difícil dissociar vigilância e controle e não se pode organizar protestos usando o Facebook ou o Twitter, pois nem sempre os construtores originais da estrada serão os mesmos que a controlarão; é o panóptico perfeito.

A militarização do ciberespaço é abordada no capítulo três. Nele os autores mostram que os custos para a produção de armamentos bélicos são cada vez maiores, mas que os custos da vigilância, dos *ciberguerreiros* (sic) e do armazenamento dos dados ficam cada vez mais baratos. Os governos de quase todos os países utilizam o que se chama de vigilância estratégica: por *default*, simplesmente gravam tudo e esmiúçam depois, por meio de sistemas analíticos. Seria impossível, pelo volume de dados, fazer uma triagem e somente então conseguir mandado judicial. Empresas como a francesa Amesys e a alemã Siemens já vêm comercializando plataformas de vigilância capazes de "ouvir" todas as comunicações de determinado povo ou país e de desencadear reações automáticas, com base na interceptação de palavras-chave.

O capítulo quatro discute em que ponto traçar os limites para a supervisão judicial e para o controle dos cidadãos. Estados democráticos europeus, alertam os autores, estão construindo máquinas que lhes permitem agir fora da lei no que se refere à interceptação, já que intercepta *todo mundo*(grifo original), independente de serem inocentes ou culpados. Os sistemas de vigilância internacional não são regulamentados, já que todas as nações têm interesse na vigilância e no controle de seus cidadãos e umas das outras. As tecnologias móveis implicam ausência de privacidade no que diz respeito a localização e conteúdo. O celular é um dispositivo de monitoramento que também faz ligações. Os dados são a nova moeda.

A espionagem pelo setor privado é o tema do capitulo cinco, que nos mostra que a espionagem não é apenas estatal, política, mas também se ocupa diretamente do indivíduo. O Google sabe com quem você se comunica, quem você conhece, o que está pesquisando e, possivelmente, sua preferência sexual, sua religião e suas crenças filosóficas, e também sabe quando voe está on-line e quando não está. O Facebook ganha dinheiro reduzindo a distinção da linha entre privacidade, amigos e publicidade. Google e Facebook são como extensões das agências de espionagem estatais. Na verdade, afirmam os autores, o usuário do Facebook é o produto e os verdadeiros clientes são as empresas anunciantes.

O argumento de que é necessário que as pessoas tenham medo para que compreendam o problema e comecem a se preocupar com formas de combater a vigilância é defendido acanhadamente no capítulo seis. Já no capítulo sete, os autores discutem sobre a internet ser um antídoto contra as narrativas políticas. Se a internet divulga, ela também é obrigada, por Lei dos Direitos Autorias do Milênio Digital (DMCA, em inglês) a retirar todo conteúdo publicado, quando solicitado por carta, pela pessoa que se sentir lesada e se "a prensa tipográfica ensinou as pessoas a ler, a internet ensino-as a escrever" e a compartilhar suas ideias.

No capítulo oito, sobre as relações da internet com a economia, os autores criticam principalmente as companhias de

crédito e operadoras como a PayPal, que controlam a maioria dos pagamentos em cartão de crédito do planeta e estão centralizadas nos Estados Unidos e lá guardam todos os nossos dados. "Fazer pela internet" acaba sendo quase sempre mais cômodo e mais barato, então, perguntam os autores, "será que a privacidade nas interações econômicas não seria mais importante que a liberdade de expressão, já que são as interações econômicas que de fato fundamentam toda a estrutura da sociedade?"

Sem pretender resumir o livro todo, que é denso e merece uma leitura atenta e anotada, não é possível finalizar essa resenha sem comentar sobre a censura na internet, abordada no capítulo nove, e a citação de Orwell, na página 127, feia por Assange: "Quem controla o presente, controla o passado, e quem controla o passado controla o futuro." Segundo os autores, a história está sendo apagada, na censura pré e pós-publicação e a censura ao WikiLeaks é um exemplo emblemático em meio a milhares de outros.

O capítulo dez traz, no título, o mote do livro todo: privacidade para os fracos e transparência para os poderosos. Se você tiver acesso aos seus registros do Facebook, diz Assenge, verá que eles têm 800 MB de informações sobre sua vida. Precisa dizer mais?

O livro termina com o capítulo intitulado Ratos na Ópera. Os ratos que estragam "a festa" seriam uma internet livre, aberta e universal, pois ela é, segundo os autores, provavelmente, a ferramenta mais importante para resolver os problemas globais e defendê-la é uma das tarefas fundamentais da nossa geração. Podemos, coletivamente, elevar o custo político do controle da informação e precisamos continuar a aprimorar nossas táticas, criar ferramentas para capacitar os cidadãos a criar suas próprias infraestruturas criptografadas e descentralizadas. O que os autores defendem, em última instância, é "software livre para um mundo livre e (precisamos de) um hardware livre e aberto."

Cypherpunks é uma leitura de arregalar os olhos de espanto diante das revelações sobre a guerra virtual que vem sendo travada pelo poder na rede; depois uma leitura de abrir os

olhos para o que se tem feito com nossa privacidade e nossos dados e, finalmente, uma leitura para nos fazer navegar mantendo os olhos bem abertos.