Algumas lições importantes que o caso WikiLeaks ensina

*Por **Graciela Selaimen**, editora da poliTICs e coordenadora de comunicação do Instituto Nupef*

Data da publicação:

Dezembro de 2010

O caso WikiLeaks é, sem dúvida nenhuma, um divisor de águas na história recente da Internet (se é que a Internet tem alguma história que não seja recente). A repercussão da divulgação das informações sobre as trocas de mensagens da diplomacia norte-americana, seguida da escandalosa censura ao site do Wikileaks (motivada pelo governo norte-americano e realizada por governos e empresas), somada à perseguição ao criador do site, Julian Assange, e à impressionante resposta da comunidade Internet a favor da liberdade de expressão e em defesa ao Wikileaks evidenciam que a Internet é um campo onde se travam batalhas de porte, muitas delas entre os poderes constituídos e uma multiplicidade de iniciativas que desafiam o status quo. A diferença, neste caso, é que uma das partes que se sentiu atacada – o governo norte-americano - perdeu definitivamente a vergonha de censurar, passando por cima da lei e usando outros braços fortes: empresas como a Amazon, o eBay, a Visa, a Mastercard, a everyDNS.

Antes do vazamento das mensagens dos diplomatas norte-americanos, o site do WikiLeaks estava hospedado em dois provedores de serviços Internet na Suécia: o Bahnhof e o PRQ - provedores comerciais conhecidos por suas políticas razoavelmente progressistas em relação aos conteúdos hospedados em seus servidores. O WikiLeaks também utilizava os serviços de um provedor comercial francês, o Cursys. Assim quedecidiu vazar as informações sobre a diplomacia norte-americana, o WikiLeaks, preocupado com o volume de tráfego que o escândalo gerava em seu website, contratou também os serviços da EC2 cloud - serviço de computação em nuvem da Amazon. A sequência dos eventos muita gente conhece: logo após o escândalo do vazamento das mensagens do governo dos Estados Unidos, os provedores de serviços Internet que hospedavam o wikileaks.org foram alvo de intensos ataques DDoS[1] e tiveram dificuldades para manter o site online. A Amazon rapidamente desconectou o wikileaks.org de seus servidores, argumentando que a natureza dos conteúdos do site infringia os termos do contrato com a empresa - muito embora a imprensa tenha noticiado que o real motivo para a decisão da Amazon tenha sido um telefonema do Senador Joseph Lieberman, que declarou ter “perguntado à Amazon sobre sua relação com o WikiLeaks e inquiriu se a empresa, junto com outros provedores de serviços Internet iria, no futuro, se assegurar que seus serviços não sejam utilizados para distribuir informação secreta roubada”. A pedido do mesmo senador, a Tableau Software, empresa que publica gráficos para visualizações de dados, tirou do ar suas imagens sobre os dados publicados pelo WikiLeaks.

Na madrugada da sexta-feira, dia 3 de dezembro, a everyDNS, (empresa provedora do serviço de DNS[2] ao wikileaks.org) se recusou a fornecer um endereço de IP válido para as solicitações de visita ao site. A empresa, baseada na Califórnia, afirmou que tomou tal iniciativa para prevenir que seus outros 500 mil clientes fossem afetados pelos intensos ciberataques que tinham como alvo o WikiLeaks.

Em resposta, o WikiLeaks transferiu os serviços de hospedagem de seu domínio e de seus arquivos para outros dois blocos de números IP diferentes: um na França, no provedor OVH, e outro na Suécia, no provedor Bahnhof. A hospedagem de seu domínio foi diversificada em diferentes ccTLDs[3] - registrou-se o wikileaks sob o .ch, sob o .nl e outros, contando-se para isso com o apoio de diversos países e provedores DNS locais na luta para manter o site ativo. O domínio wikileaks.org.ch, por exemplo, foi registrado pelo Partido Pirata Suíço.

Além dos já citados provedores de serviços Internet norte-americanos, outras empresas se somaram à empreitada de estrangular o WikiLeaks: nos dias que se seguiram à decisão da Amazon, a PayPal - serviço de pagamentos pela Internet, empresa que pertence ao grupo eBay - suspendeu a transferência de valores doados ao WikiLeaks. Nos dias 6 e 7 de dezembro as redes Mastercard e Visa também cancelaram as doações ao WikiLeaks.

Todavia, o esforço para calar o WikiLeaks foi um tiro que saiu pela culatra. Em poucos dias, o conteúdo do WikiLeaks se espalhou pela Web, espelhado[4] em mais de mil de sites publicados por simpatizantes do WikiLeaks e defensores da liberdade de expressão na Internet - tornando assim o WikiLeaks imune a uma única autoridade legal. Para tirar estes sites espelho do ar, seria necessário um concertamento de autoridades de centenas de países, muitos deles nos quais o ordenamento jurídico exigiria o devido processo judicial para o bloqueio de acesso a um site. Mesmo que houvesse tal esforço, é provável que a multiplicação do espelhamento do site do WikiLeaks se intensificasse ainda mais em resposta. O fato é que as ações do senador Lieberman, da Amazon, da everyDNS e de outras empresas envolvidas no boicote tiveram como resultado o aumento da capacidade do WikiLeaks em permanecer ativo na Web.

Este episódio nos presenteia com algumas lições importantes.

Uma delas é a evidência de que a estrutura de governança do ccTLD em cada país (o .br para o Brasil, o .ar para a Argentina ou o .ch, no caso da Suíça) tem um inegável caráter político e que a decisão sobre o que pode ou não ser publicado na Internet ainda é uma decisão tomada no âmbito de um país, uma vez que não há acordos globais que se sobreponham às diferentes jurisdições nacionais, no que diz respeito à publicação de conteúdos na na Internet. Como já dizia há alguns anos o Carlos Afonso, o ccTLD é um bem público, e deve ser defendido como tal - o que inclui uma estrutura de governança transparente, participativa e focada no interesse público. Ter um site registrado sob um domínio .com ou .net significa não estar vinculado a nenhum ccTLD – significa, sim, ter seu site vinculado às regras das empresas norte-americanas que administram estes domínios, e que, por sua vez, estão subordinadas às decisões – muitas delas arbitrárias – de autoridades norte-americanas. Um site nestas condições pode sumir da Internet a qualquer momento, bastando para isso que algum senador ou agência norte-americana decida que há palavras-chave no conteúdo do site que o tornam suspeito, ou que possam significar risco à segurança e aos interesses daquele país.

Todavia, mesmo nos países onde há uma estrutura de gestão da Internet democrática e com participação da sociedade, existem assimetrias em relação ao exercício de direitos na Internet. Grandes provedores de conteúdo podem mudar de jurisdição a qualquer momento – retirando-se de um país onde as leis impliquem limitações ou problemas ao seu negócio, como fez o Google na China. O usuário/a, por sua vez, não pode fazer isso. A Internet é mundial, mas para chegar a ela cada um de nós precisa passar por estruturas físicas locais e por portas de entrada à Internet – como os provedores de acesso e serviços – que respondem a leis locais. Com a intensificação dos discursos que defendem o controle e o vigilantismo na Internet – muitos deles justificados pela luta contra o crime e a proteção de crianças e jovens, mas a grande maioria interessada no bloqueio a trocas de arquivos e downloads de conteúdos, (que ofendem os interesses das grandes corporações de mídia e da indústria da música) -, cresce o número de países que têm aprovado leis que possibilitam a filtragem dos conteúdos que passam pelos provedores de acesso e de serviços Internet. Esta é uma tendência à qual devemos estar atentos, e é importante refletir com mais profundidade sobre o papel dos intermediários na Internet[5] e sobre os possíveis impactos de nossas escolhas ao eleger intermediários para a entrada de nossos serviços e conteúdos na Internet.

EMPRESAS E NUVENS CINZA CHUMBO

Outra lição importante que o caso WikiLeaks traz é a evidência sobre a verdadeira natureza da Internet de hoje. Como aponta o pesquisador Ethan Zuckerman, do Berkman Center for Internet and Society da Universidade de Harvard, *A verdade é que a Web é, em sua maior parte, de propriedade privada. Então o que acontece aqui é que nós temos normativas que entendem que deve-se tratar a Internet como um espaço público - no qual você deve ter o direito de se expressar livremente e ninguém deve restringir seus direitos - mas em seguida você descobre que, basicamente, você está organizando uma passeata política num shopping center. Este é um espaço de discurso comercial, controlado por regras comerciais. Minha sensação é que as empresas tentam, com muito empenho, não deixar tão evidentes seus imperativos comerciais, nem dizer claramente: "nós vamos, silenciar vozes", porque isso deixa as pessoas realmente desconfortáveis.*[6]

O caso Wikileaks ilustra bem este fato. Ao comentar sobre o comportamento da Amazon neste episódio, a pesquisadora Rebecca MacKinnon alertou sobre o quanto a atitude da empresa impacta a democracia. Em artigo recente, Rebecca diz: "Uma parte substancial, se não fundamental, de nosso discurso político migrou para o universo digital. Este universo é em sua maior parte feito de espaços virtuais que são criados, possuídos e operados pelo setor privado.(...) Embora a Amazon tenha agido dentro de seus direitos legais, a companhia, a despeito de qualquer coisa, mandou um recado claro para seus usuários: se você se envolver em discursos controversos que desagradem algum membro do governo norte-americano... a Amazon vai descartar você ao primeiro sinal de problema."

Vale sempre lembrar, então, que não são apenas os governos que impõem medidas de controle e censura sobre os usuários de Internet. Em inúmeros países onde as leis são razoavelmente orientadas a proteger a defesa do cidadão/consumidor/usuário de Internet, são as empresas que fazem a filtragem, a censura, os bloqueios sutis e a gestão tendenciosa do tráfego Internet de seus usuários, muitas vezes sob as barbas dos governos.

DIGA-ME COM QUEM - E ONDE - ANDAS…

Os motivos para descartar um usuário ou usuária podem ser muitos. Todavia, em muitas das vezes em que este tipo de atitude é tomada, há uma justificativa tecnológica para a decisão da empresa. Aqui no Brasil já houve casos de grandes provedores de serviços Internet recusarem-se a continuar hospedando o site de uma entidade do movimento negro por conta dos frequentes ataques que o site sofria por parte de grupos racistas e xenófobos. Na argumentação do provedor, esta era uma questão técnica e não havia capacidade instalada na empresa para lidar com a necessidade de um monitoramento constante para a defesa do site. Todavia, o mesmo site já havia sido hospedado antes em um provedor de serviços Internet não-comercial - e ali o compromisso com a defesa do site era permanente, a despeito do alto custo que a operação envolvia. No provedor comercial, a relação entre o custo da defesa aos ataques e o valor pago pela organização tornava aquele cliente desinteressante – e fácil de ser descartado.

Esta constatação é especialmente importante para indivíduos, organizações e empresas que têm sob sua responsabilidade conteúdos “sensíveis”: aqueles que tornam-se mais facilmente alvo de censura, controle e, eventualmente, ataques. Uma pesquisa7 realizada pelo Berkman Center for Internet and Society da Universidade de Harvard mostra que, de agosto de 2009 a setembro de 2010, pelo menos 280 sites de organizações que defendem direitos humanos e espaços de mídia progressistas que apoiam campanhas de direitos humanos foram alvo de ataques DDoS. Os pesquisadores crêem que os ataques contra entidades e ativistas sociais devem aumentar nos próximos anos, e orientam as organizações de direitos humanos e a mídia independente a aumentarem sua capacidade de defesa contra este tipo de ação que tenta silenciar ativistas e vozes dissidentes.

Segundo o relatório da pesquisa, os ataques DDoS são apenas a parte mais visível de ofensivas muito mais amplas - que incluem filtragem de conteúdos, invasões a sistemas para roubo de senhas, entre outras ações. O pesquisador Ethan Zuckerman afirmou recentemente, em entrevista à BBC[8], que “se você é uma organização de direitos humanos ou um veículo de media independente, você provavelmente deve ter uma conta num provedor de serviços Internet pela qual paga £20 por mês, e é muito difícil, neste padrão de serviço de hospedagem, que você consiga se defender de ataques DDoS”. Conforme Zuckerman, os ataques não precisam ser prolongados: “Basta que eles durem o suficiente para incomodar seu provedor de serviços Internet - até que ele mande sua organização embora você tenha que encontrar outro lugar para hospedar seus serviços”.

Sejamos realistas: poucos provedores de serviços Internet fariam frente ao governo de seu país (este não é um pecado exclusivo da Amazon) ou se dariam ao trabalho de manter pessoas monitorando sites que são prioritariamente alvos de ataques DDoS sem serem muito bem pagos por isso.

O caso WikiLeaks serve, também, para nos tirar da zona de conforto e romper definitivamente com antigas utopias sobre a Internet. Nas palavras de Parminder Jeet Singh, coordenador da organização indiana ItforChange, sobre o caso WikiLeaks,

“...é hora de percebermos que a Internet é, de fato, um universo que tem sido governado através do exercício ilegítimo do poder de governos e empresas. Há dois problemas claros com a abordagem de usar táticas de governança de bastidores. O primeiro é o fato de haver sempre uma grande possibilidade de que estas táticas sejam de algum modo abusivas - e no nosso ponto de vista, no caso do WikiLeaks o abuso foi enorme. O segundo é que, em eventuais situações em que seja legitimamente necessário fazer uso de algum sistema de resposta global a possíveis problemas e ameaças (ou mesmo a oportunidades), (...) este poder de bastidores exercitado por potências políticas e comerciais - como fazem alguns governos e seus comparsas corporativos nesta situação do WikiLeaks -, não está disponível para atores políticos ou países menos poderosos. Esta situação evidencia um déficit democrático e uma necessidade por princípios democráticos globais e arcabouços institucionais na área da governança da Internet”.

É fato que no nível global precisamos urgentemente de princípios democráticos globais e arcabouços institucionais na área da governança da Internet - e no nível local precisamos, além de marcos regulatórios que priorizem os direitos humanos fundamentais, também de espaços de confiança - projetos e serviços intermediários, de

provimento de acesso e de serviços Internet - focados na promoção da cidadania, da democracia, na defesa dos direitos humanos e no fortalecimento de uma Internet verdadeiramente livre. O Alternex foi pioneiro nesta abordagem do provimento de serviços Internet no Brasil – um trabalho árduo, nem sempre reconhecido, mas resiliente, que hoje continua ativo através do projeto Tiwa, exclusivamente por uma questão de princípios e de certeza sobre a necessidade cada vez mais premente de espaços de confiança e de defesa de direitos na Internet.

Se o WikiLeaks estivesse hospedado no Tiwa, a sequência de fatos após o vazamento de informações “secretas” teria sido bem diferente.

---
1. Um ataque DDoS – sigla para Distributed Denial of Service – tem como objetivo fazer com que websites fiquem inacessíveis: através de um número imenso de requisições simultâneas (visitas) ao site, aqueles que promovem os ataques fazem com que os visitantes realmente interessados não consigam acessar o site atacado. As visitas massivas se parecem muito com o tráfego web usual, por isso são difíceis de ser identificadas para a defesa do site. Geralmente estes ataques têm como objetivo sites muito visados – tais como sites governamentais, de organizações políticas e de instituições financeiras.

2. O DNS (Domain Name System) é um dos elementos fundamentais da Internet, responsável por “traduzir” os números de endereços IP para palavras – nomes – mais fácil de serem lembrados. Assim, quando o DNS falha, um site não é encontrado quando digitamos sua URL [por exemplo, http://www.politics.org.br] na barra de navegação do browser – ele só é “encontrável” se soubermos o número IP ao qual aquela URL se remete.

3. ccTLD é o Country Code Top Level Domain – ou nome de domínio de primeiro nível de código de país – como o .br, o .ar, o .uk, etc.

4. O espelhamento de um sítio web é a cópia fiel de seu conteúdo, porém sediado em outro servidor e muitas vezes publicado sob um outro domínio.

5. São intermediários na Internet as organizações ou empresas que provêem acesso, hospedam, transmitem e indexam conteúdos gerados por terceiros ou provêem serviços baseados na Internet a terceiros.

6. Em The News Frontier - http://www.cjr.org/the_news_frontier/

7. Em http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_DDoS...

8. Em http://www.bbc.co.uk/news/technology-12054774

Categoria:

- poliTICs 8