

## GOVERNOS, EMPRESAS, WIKILEAKS E GOVERNANÇA DA INTERNET

### Governments, Private Companies, Wikileaks And Internet Governance

GRACIELA B. SELAIMEN \*

#### RESUMO

O caso WikiLeaks é um exemplo concreto e explicitador de como podem ser íntimas as relações entre governos e empresas, num processo que fragiliza a democracia e relativiza a disposição dos governos de agir prioritariamente em função do interesse público. Neste trabalho oferecemos, frente ao episódio do WikiLeaks e a partir de uma perspectiva regulatória e política, um breve resumo sobre as respostas que emergiram em um dos principais espaços globais de discussão sobre a governança da rede mundial de computadores – o IGC, Caucus da Sociedade Civil para a Governança da Internet - em sua tentativa de responder à complexidade desta disputa sobre a vigilância, o controle, a liberdade e a autonomia no ciberespaço.

**PALAVRAS-CHAVE:** Governança da Internet; sociedades de controle; wikileaks; autonomia; regulação e políticas públicas.

#### ABSTRACT

The WikiLeaks case is a concrete example of how close are the relationships between governments and private companies - a process that undermines democracy and questions the willingness of governments to act primarily on behalf of public interest. In this work we offer, analyzing the WikiLeaks episode in the end of 2010 from a regulatory a political perspective, a brief summary of the responses that emerged in one of the main spaces of discussion on the global governance of the Internet - the IGC, the Civil Society Caucus for Internet governance - in its attempt to respond to the complexity of the dispute over surveillance, control, freedom and autonomy in cyberspace.

**KEYWORDS:** Internet Governance; control societies, Wikileaks, autonomy, regulation and public policy.

---

Mestre em Comunicação e Cultura pela ECO/UFRJ, membro do Cibercult. E-mail: [graciela@nupef.org.br](mailto:graciela@nupef.org.br)

Nas redes de comunicação distribuída, o poder e o controle se exercem em vários níveis - sendo que é no nível dos códigos e dos protocolos que este exercício se dá de maneira mais invisível e eficaz. O caso da desconexão do site do WikiLeaks pela Amazon no final de 2010 e posterior perseguição ao seu criador, Julian Assange (fatos que detalharemos mais adiante), deixou claro que as atuais respostas jurídico-discursivas aos desafios impostos pela intensificação e pervasividade dos dispositivos de vigilância e controle nas redes de comunicação distribuída não são suficientes para garantir a construção e manutenção de sistemas sociotécnicos que respeitem a autonomia e os direitos fundamentais de seus usuários. Conforme Palmãs (2011), o diagrama das sociedades de controle nos permite apenas algumas liberdades: nós somos livres, por exemplo, para perambular por entre instituições disciplinares – governos, empresas ou quaisquer outras instituições capazes de impor uma conduta qualquer a uma multiplicidade humana qualquer (DELEUZE, 1988). Neste circuito, os grandes centros de poder contemporâneos são os Estados e as corporações – que, muitas vezes aliados, enfrentam o desafio premente de controlar as redes globais que eles mesmos produzem (BOGARD, 2010) de forma a enfrentar quaisquer possibilidades de resistência e os processos de desconstrução e reconstrução das tecnologias como parte do movimento de luta contra o capital. (DYER-WITHEFORD, 1999).

Não faltam exemplos para ilustrar como esta aliança se dá - dentro do arcabouço da lei e fora dela. No primeiro caso, podemos citar o Patriot Act<sup>1</sup> norte-americano – que, entre outras coisas, permite que o governo dos EUA acesse as bases de dados do Google (AVERY, 2008) e seu gigantesco universo de dados pessoais que abrange indivíduos de quase todos os países do mundo. No segundo caso, quando o governo atropela a lei e explicita a verdadeira natureza de suas relações com algumas grandes corporações (em função da urgência da manutenção do controle e da própria incapacidade da lei em assegurar o exercício do poder governamental e a manutenção do status quo), revela-se a distância entre o discurso de algumas democracias ocidentais e suas práticas.

O caso WikiLeaks é, em nossa opinião, o exemplo mais concreto e explicitador deste hiato: como analisa Mendoza (2011), na narrativa implícita na logo do WikiLeaks, aquela que mostra uma disjunção do mundo, está descrita a luta do poder global, difusamente mantido nas mãos das corporações transnacionais e afirmado pelos governos ao redor do mundo. "Este poder está sendo atacado por um ator relativamente novo que pode ser chamado, por hora, de rede autônoma." (MENDOZA, 2011, s.p. Tradução nossa).<sup>2</sup>

Para Stalder (2010), o surgimento do WikiLeaks mistura pelos menos quatro das grandes tendências que permeiam nossas sociedades. A primeira destas tendências é a transformação na materialidade da comunicação – que se torna cada vez mais extensiva, registrável, e móvel. A segunda tendência é a crise das instituições, particularmente nas democracias ocidentais – onde a retórica moralista e a realidade das práticas diárias se distanciam e divergem mais e mais. Em terceiro lugar vem a ascensão de novos atores, indivíduos "superempoderados"<sup>3</sup>, capazes de intervir nos desenvolvimentos históricos de manei-

ra sistêmica. Finalmente, a quarta tendência é a transformação estrutural da esfera pública (através da consolidação da mídia, de um lado, e da explosão dos meios não-institucionais de outro).

Ao longo de sua história, o WikiLeaks publicou informações sobre a existência de esquadrões da morte no Quênia, relatórios sobre o despejo de lixo tóxico na costa africana, manuais da Igreja da Cientologia, documentos sobre procedimentos das forças armadas norte-americanas em Guantanamo e relatórios internos de instituições financeiras como os bancos Kaupthing e Julius Baer. Em 2010, o WikiLeaks ocupou seguidamente espaços na mídia internacional: após a publicação de um vídeo mostrando o ataque de um helicóptero estadunidense matando civis no Iraque em abril; com a publicação de documentos confidenciais sobre as ações americanas no Afeganistão e Iraque em julho; e novamente em novembro, ao publicar o conteúdo de 251.287 telegramas de embaixadas americanas pelo mundo.

A divulgação destes documentos foi feita, num primeiro momento, exclusivamente para os jornais The New York Times, The Guardian, Der Spiegel, Le Monde, e El País – que se puseram a analisar, selecionar e formatar as informações que julgavam mais relevantes, para em seguida publicá-las. Foi assim que, três anos após sua criação, o WikiLeaks passou a ser considerado uma das 'histórias definidoras da Internet', (STALDER, 2010) o que significa, também, uma das histórias que melhor retratam o tempo em que vivemos. Este último episódio gerou uma campanha massiva anti-WikiLeaks nos Estados Unidos. A repercussão da divulgação das informações sobre as trocas de mensagens da diplomacia norte-americana seguiu-se da censura ao site do WikiLeaks (motivada pelo governo dos EUA e realizada por governos e empresas), somada à perseguição ao criador do site, Julian Assange.

A sequência dos eventos muita gente conhece: após um telefonema do Senador Joseph Lieberman, a Amazon e a everyDNS, empresas norte-americanas que faziam provimento de serviços Internet ao WikiLeaks suspenderam unilateralmente seus contratos, tirando temporariamente o site WikiLeaks do ar. Outras empresas seguiram os mesmos passos, suspendendo a prestação de serviços ao 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 através de seus serviços. Nos dias 6 e 7 de dezembro as redes Mastercard e Visa também cancelaram as transferências de doações ao WikiLeaks feitas por cartões de crédito destas bandeiras.

## **1. ANÔNIMOS, ESPELHOS E A REPERCUSSÃO NA REDE**

Este conjunto de ações contra o WikiLeaks foi um tiro que saiu pela culatra. Em poucos dias, o conteúdo do WikiLeaks se espalhou pela Web, espelhado<sup>4</sup> em mais de mil sites mantidos 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 acordo entre autoridades de centenas de países, muitos deles nos quais o ordenamento jurídico exigiria o devido processo legal 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, com a publicação de cópias fiéis de seu site sediadas em centenas de servidores, em diversos países.

O jornal The Guardian publicou uma lista sequencial de atores estatais e empresas do setor privado que, sob pressão, suspenderam ou negaram serviços ao WikiLeaks, muitas vezes fazendo argumentações sobre violações a termos de serviço, embora não embasadas em fatos. (Conforme Eddan Katz, da EFF, escreveu: "Liberdade de expressão: não tem preço; para tudo o mais, existe o Mastercard."). (KATZ apud MUELLER, 2011).

Assim que o conjunto de documentos do WikiLeaks foi colocado a salvo na rede de sites- espelho e em múltiplos sites e redes de compartilhamento de arquivos, um grupo de hackers<sup>5</sup> partiu em apoio ao WikiLeaks atacando<sup>6</sup> os serviços Internet do PayPal e em seguida os do PostFinance, banco suíço que congelou a conta de Julian Assange, criador do WikiLeaks. Começou assim o levante do grupo autodenominado 'Anonymous', que se coordenou para atacar serviços Internet de instituições governamentais e corporações que empreendessem qualquer tentativa de represália ao WikiLeaks – o que passou a ser chamado de Operação Payback. Na lista de empresas cujos sites sofreram ataques estão a MasterCard, a PayPal, a Visa, entre outras. De acordo com o Tim Hwang (2010), ex-pesquisador do Berkman Center for Internet and Society da Universidade de Harvard, o grupo à frente destas ações faz parte de uma longa tradição de 'expansionistas da Internet', que defendem que a Web deve remodelar o resto do mundo à sua imagem.

Um dos consultores do governo norte-americano na área de cibersegurança, Charles Dodd, chamou o episódio capitaneado pelo Anonymous de cyber guerrilla warfare: "Eles atacam das sombras e não temem retaliação." <sup>7</sup>.

Para Nicolás Mendoza, estes episódios mostram que é tarde demais para desarmar o que é hoje a coexistência cada vez mais contenciosa entre dois mundos – tal qual está representada na logomarca do WikiLeaks. Um destes mundos é a "sociedade capitalista pré-apocalíptica do individualismo, do lucro e do controle"; o outro é a "comunidade pós-apocalíptica de sobreviventes colaborativos que se auto-regulam" (MENDOZA, 2010, s.p.). O conflito nasce de um paradoxo essencial: porque a web existe, ambos os mundos dependem dela – um para prevalecer sobre o outro:

O Anonymous é uma das incontáveis iterações de uma vibrante periferia digital, uma fonte sem precedentes da produção cultural situada fora das condutas normais: aquelas reguladas pelo governo e exploradas por empresas, a fim de padronizar identidades e estimular o consumo. O que é sem precedentes não é

apenas o método, mas também o tema da produção. O método e o assunto são um: a comunidade colaborativa deslocalizada. Anonymous é uma provocação aberta a partir da episteme marginal da comunidade colaborativa. Esta é não apenas incompreensível para a episteme corporativa, mas, mais importante, é reprimida, excluída e policiada; manual de procedimentos sobre como lidar com a produção cultural que não pode ser absorvida pela imagética corporativa. (MENDOZA, 2010, s.p. Tradução nossa)<sup>8</sup>

Neste cenário, diante da impotência em calar e penalizar o WikiLeaks, o governo norte-americano partiu para o ataque ao seu criador, Julian Assange – que foi tachado de “terrorista”<sup>9</sup>. O discurso construído pelo governo e sustentado pela mídia estadunidense baseou-se no argumento que o WikiLeaks estaria ‘em guerra’ com os Estados Unidos. O mundo inteiro teria que polarizar em torno desta questão: “ou vocês estão do nosso lado, ou estão do lado do WikiLeaks. Assange deveria ser condenado à morte ou assassinado. As forças armadas norte-americanas deveriam empreender uma ciberguerra em larga escala contra o WikiLeaks e qualquer sítio Web que os apoiasse”. (MUELLER, 2011).

Não foram apenas Julian Assange e o WikiLeaks que se tornaram alvo de tentativas de censura e vigilância. Em 14 de dezembro, o Departamento de Justiça norte-americano emitiu um mandado ordenando que a rede social Twitter entregasse dados relativos às contas de cinco pessoas ligadas ao WikiLeaks – antigos e atuais colaboradores voluntários. Os dados exigidos incluíam todos os endereços de e-mail e informação das contas dos usuários, todas as suas conexões, detalhando-se tempo de duração e horário de cada conexão, todos os endereços IP usados por estas pessoas para acessar o Twitter, assim como meios e pagamentos de eventuais serviços, com registros bancários e de cartões de crédito. O conjunto de dados deveria abranger o período de 01 de novembro de 2009 até aquela data. A determinação judicial exigia que o Twitter mantivesse segredo sobre a requisição dos dados, inclusive para as pessoas que eram alvo da coleta de dados. O Twitter entrou com uma apelação reclamando seu direito de informar os usuários e em 5 de janeiro de 2001 outra ordem foi expedida, permitindo que as pessoas investigadas fossem informadas sobre a ação e dando a elas o prazo de dez dias para apresentar qualquer objeção.

Notemos que esta lista de ‘apoiadores’ do WikiLeaks foi formulada pelo governo dos EUA e alcançava muitas pessoas fora da jurisdição do governo americano. Um exemplo é a congressista da Islândia, Birgitta Jonsdottir. Em consequência da inclusão do nome dela na lista, o governo da Islândia convocou imediatamente o embaixador norte-americano no país para explicações e o caso tornou-se (mais) um mal-estar diplomático. Uma das questões que ficam sem resposta neste episódio é: será que o Departamento de Justiça dos EUA emitiu mandados apenas contra o Twitter, ou outras redes sociais foram alvo das mesmas ações invasivas? Em caso positivo, será que outras empresas simplesmente se calaram e acataram as determinações do Departamento de Justiça, ainda que estas pudessem ser facilmente

questionadas pelas vias legais? É possível que nunca surjam respostas a estas perguntas, mas um fato é incontestável: a aliança que se criou entre governo e empresas no caso do WikiLeaks se colocou acima da lei máxima dos Estados Unidos e estendeu seus braços para muito além da jurisdição do governo deste país, escancarando o fato que a máquina imperial colocou em prática seus poderes de intervenção sem qualquer ocultamento de seus mecanismos de gerenciamento industrial e dos usos políticos da tecnologia. (HARDT e NEGRI, 2001).

O WikiLeaks representa, para muitos, o primeiro confronto sustentado entre a velha ordem estabelecida e a cultura da Internet – a intolerância da antiga ordem foi exposta, exibida em praça pública e todo o discurso contraditório que se seguiu a esta exposição tornou ainda mais evidente a dimensão da incompetência, corrupção e hipocrisia das elites políticas de algumas democracias ocidentais. Já não é apenas para as ditaduras orientais que a Internet pode ser uma pedra no sapato: o gênio saiu, definitivamente, da garrafa.

## 2. IMPÉRIO

Hardt e Negri já afirmavam em 2001 que no Império e seu regime de biopoder, produção econômica e constituição política tendem, cada vez mais, a coincidir. Conforme estes autores,

A forma primária de poder que realmente nos confronta hoje [...] é bastante terrena e mundana. [...]. A forma predominante de soberania contemporânea - se ainda quisermos chamá-la assim - é completamente inserida e apoiada por sistemas jurídicos e instituições de governança, uma forma republicana caracterizada não apenas pela regra da lei, mas também igualmente pela regra de propriedade. Dito de outra forma, a política não é um domínio autônomo, mas um domínio completamente imerso nas estruturas econômicas e legais. Não há nada de extraordinário ou excepcional sobre esta forma de poder. Sua pretensão de naturalidade, na verdade seu funcionamento silencioso e invisível, diariamente, torna extremamente difícil reconhecê-la, analisá-la e desafiá-la. Nossa primeira tarefa, então, será trazer à luz as relações íntimas entre a soberania, a lei, e o capital. (HARDT e NEGRI, 2005, p. 5. Tradução nossa)<sup>10</sup>

No episódio do WikiLeaks o nublamento das fronteiras entre público e privado recebeu o foco de luz mencionado por Hardt e Negri. Neste caso específico, as 'relações íntimas' explicitadas expulsaram da alcova a lei, uma vez que, se tivesse sido levado a cabo o devido processo legal, o exercício de poder por parte do senador Lieberman e seus colegas dificilmente se concretizaria na expulsão de um serviço de informação da infraestrutura técnica que o hospedava, ou a suspensão do acesso da organização responsável pelos serviços de informação a serviços financeiros contratados. As barreiras legais seriam gigantescas no país que reza no altar da Primeira Emenda. Entretanto, como apontou Yochai Benkler, "a aliança implícita,

uma parceria público-privada entre as firmas que operam a infraestrutura e o governo que as encoraja a ajudá-lo na guerra ao terror [...] foi capaz de alcançar de maneira extra-legal muito mais do que a lei teria permitido ao próprio Estado” (BENKLER, 2011, p.p. 23, 24. Tradução nossa).<sup>11</sup>

Por outro lado, uma outra polaridade foi explicitada: a da Internet livre versus poder estatal. O pesquisador norte-americano Milton Mueller afirma que “a histeria gerada pelos gaviões da política externa polariza o mundo em torno da Internet e de suas possibilidades e mostra que, muito frequentemente, aqueles que alegam serem defensores da liberdade na verdade são seus piores inimigos” (MUELLER, 2011, p. 14). Mueller diz que a razão pela qual os poderes estadunidenses estão de tal forma aborrecidos é que eles acreditam profundamente no tipo de poder executivo sem limites que está associado à emergência de um estado nacional de segurança globalmente estendido. “Assange revelou esta profunda contradição entre, de um lado, os valores liberal-democráticos relativos ao governo transparente e responsável, e de outro, a existência de um império norte-americano. Revelar esta contradição mina seriamente a prática dos negócios da maneira como costuma ser na política externa dos EUA. É isso que é tão imperdoável”. (MUELLER, 2011, p. 14).

Para Benkler (2011), essa incongruência entre um discurso que afirma a liberdade na Internet e a agilidade ao censurar, perseguir, vigiar e violar direitos estabelecidos expõe o governo estadunidense ao ridículo. Em 21 de janeiro, a secretária de estado Hillary Clinton fez um discurso em Washington reafirmando o compromisso com a liberdade na Internet e apontando um dedo acusador para a China, ao relatar como o presidente Barack Obama, em visita àquele país, “defendeu o direito das pessoas de acessar livremente a informação, dizendo que quanto mais livremente a informação flui, mais fortes as sociedades se tornam”(NAUGHTON, 2011, s.p. Tradução nossa).<sup>12</sup>

Portanto cabe agora, mais do que nunca, a reflexão crítica sobre a possibilidade de liberdade de informação e comunicação num “espaço público” composto de redes informacionais que, em sua maioria absoluta, são propriedade privada de grandes corporações, prontas a atender a determinações de governos, quando lhes convém.

### **3. GOVERNANÇA DA INTERNET**

Partimos do pressuposto que a governança, a regulação e a distribuição de poder nas sociedades conectadas em redes de comunicação distribuída são exercidas em múltiplos níveis, que vão da construção da arquitetura das redes e dos softwares aos processos de discussão de legislações e políticas públicas em âmbito nacional e global. O episódio WikiLeaks para nós é um exemplo importante de como as atuais respostas jurídico-discursivas aos desafios impostos pelas dinâmicas de poder e controle contemporâneas nas redes de comunicação distribuída não são suficientes para garantir a construção e manutenção de sistemas sociotécnicos que respeitem a autonomia e os direitos fundamentais de seus usuários, como a liberdade de expressão e a privacidade.

Hoje, os mecanismos formais de governança global da Internet incluem acordos negociados pelos governos, pelo setor privado e pela sociedade civil em espaços de discussão, formulação de políticas e tomadas de decisão – em nível global, as entidades e instâncias de maior relevância neste campo têm sido a IETF (Internet Engineering Task Force), a ICANN (International Corporation for Assigned Names and Numbers), o WSIS (World Summit on Information Society) e o IGF (Internet Governance Forum). Todavia, na prática o que prevalece de fato são modalidades de governança impostas por poucos e poderosos governos, bem como por um punhado de empresas que possuem poder de monopólio ou oligopólio nos mercados globais. O fato é que temos visto uma proliferação do número e das modalidades de mecanismos de governança – formais e informais -, bem como uma profunda mudança nas tendências de regulação das redes de telecomunicações e de comunicação digital – cada vez mais focadas em promover mercados globalizados, fortalecer o setor privado e consolidar mecanismos de controle e vigilância, em nome da segurança.

Ao observarmos de perto<sup>13</sup> a repercussão da “caçada ao WikiLeaks” num dos principais espaços dedicados à discussão sobre governança da Internet nos dias de hoje – o IGF (Internet Governance Forum) - constatamos que a capacidade de resposta e formulação de posições por parte dos principais atores envolvidos neste fórum da ONU foi pequena - e que o impacto das poucas manifestações públicas em relação ao caso foi pífio, se comparado à repercussão que o episódio do WikiLeaks teve na mídia e nas redes sociais – vocalizada principalmente por ativistas, blogueiros, acadêmicos e pesquisadores do campo da comunicação e dos direitos humanos, fora do âmbito do IGF.

Os fatos que se seguiram à divulgação dos Cablegates levaram ao reconhecimento por parte de alguns atores-chave neste Fórum sobre o vácuo regulatório e no campo de políticas públicas que permanece, apesar dos cinco anos de existência e atuação do IGF. Para o coordenador do Internet Governance Caucus (IGC)<sup>14</sup>, Jeremy Malcom, há um vácuo que devemos enfrentar. Para Malcom (2010), não existem princípios universais ou um marco conceitual e político para orientar resoluções sobre disputas em jurisdição transfronteiras, o que pode envolver hospedagem de conteúdos, propriedade de conteúdos, publicação de conteúdos, registro de domínios, hospedagem de domínios, e as responsabilidades de cada um destes atores em seus respectivos países.

Esta visão é corroborada por Parminder Jeet Singh, membro do IGC e coordenador da ONG indiana IT for Change, que afirma haver inúmeras questões transfronteiras urgentes na área da governança da Internet e das políticas públicas de Internet que requerem soluções urgentes, mas que não são abordadas nos mecanismos existentes de governança da rede mundial. Parminder defende a ideia de que é urgente examinar que mecanismos institucionais serão capazes de enfrentar estas importantes questões relativas a políticas públicas de Internet de uma forma global, democrática, inclusiva. Para ele, o caso WikiLeaks é, de fato, um divisor de águas na Governança da Internet, por conta da maneira como o governo estadunidense exercitou autoridade extra-legal, fazendo uso de seu poder político e

econômico de uma forma bastante clara, para controlar os fluxos globais de tráfego na Internet. Na opinião do ativista, isso evidencia diretamente o porquê da necessidade urgente de um devido processo legal global, informado por marcos políticos claros – incluindo aqueles relativos aos direitos humanos. (SINGH, 2010).

Ian Peter, ex-coordenador do IGC, concorda que a ausência de um regime de políticas e de princípios universalmente aceitos é uma das questões da governança da Internet sobre as quais o IGF deveria se debruçar. “Na ausência de qualquer regime de políticas públicas que abranja tais questões relativas ao uso da Internet, as corporações estão se curvando a pressões de governos e/ou agindo unilateralmente para preservar os segredos do governo e a maneira como as coisas costumavam ser antes da era digital”. (PETER, 2010. Tradução nossa.)<sup>15</sup>

Para Michael Gurstein, diretor executivo do Centre for Community Informatics Research, Development and Training e membro do IGC,

O fato é que hoje há uma forte percepção por parte dos ‘poderes constituídos’ de que as coisas estão ‘fora de controle’ (vejamos, por exemplo, os vários tipos de reações ao que são, evidentemente, ataques triviais feitos pelo ‘Anonymous’) e presumidamente, o próximo discurso [dos governos] será do tipo ‘algo precisa ser feito!’. A questão então é o que será feito, por quem, e sob que autoridade? Eu acho que o argumento aqui é que devemos chegar logo a algum tipo de abordagem para um amplo marco de governança, porque os ‘poderes constituídos’ estarão fervorosamente trabalhando no seu modelo – e um novo panorama de governança vai surgir muito rapidamente e muito assertivamente. (GURSTEIN, 2011, s.p. Tradução nossa.)<sup>16</sup>

Visão semelhante é sustentada por Avri Doria, ex-consultora do Secretariado do IGF, que considera que o episódio do WikiLeaks é apenas um passo de um caminho muito longo que temos adiante, no qual os poderes constituídos suprimirão qualquer conteúdo dos quais eles não estejam a favor. Doria acredita que governos como o dos EUA e da Suécia estavam temerosos que a China e outros governos estivessem deixando-os para trás no que diz respeito à regulação de conteúdos, e precisavam de um motivo para avançar no sentido da censura (DORIA, 2010).

Nesta discussão, algumas vozes mais críticas se levantaram: o pesquisador norte-americano Milton Mueller, por exemplo, questionou o clamor generalizado por políticas públicas globais, com o seguinte contraponto: “quando vocês falam de ‘políticas públicas’, de que ‘público’ vocês estão falando? Na Internet global, há mais de 200 públicos nacionais, muitos outros públicos subnacionais e diversos públicos transnacionais envolvidos. Sendo assim, o que dá a um ‘público nacional’, representado por seu gover-

no, o direito de legislar de maneira que afeta outros 20 ou 30 públicos sobre os quais este governo não tem nenhuma autoridade legítima?”. (MUELLER, 2010. Tradução nossa)<sup>17</sup>

Totalitários ou democráticos, governos querem manter sua soberania. Indiferentes ao que se passa nas discussões do IGF, alguns governos tomaram medidas imediatamente após o início da perseguição ao WikiLeaks pelo governo estadunidense. Uma das primeiras reações veio do governo da Rússia, que em janeiro de 2011 oficializou a decisão de começar a usar software livre como estratégia para diminuir sua dependência da Microsoft e de outros softwares proprietários produzidos por empresas norte-americanas. Outros governos se movimentam no sentido de assumir maior controle sobre seus recursos da Internet:

Os fundamentos da política da Internet foram seriamente abalados. As fissuras que não apareceram durante os testes de estresse anteriores, incluindo Iraque e Afeganistão, manifestaram-se em questão de dias, durante o episódio WikiLeaks.[...] Alguns governos da União Européia (UE) já estão em dúvida sobre as enormes quantidades de dados e documentos que pertencem ao seus cidadãos que estão flutuando nas nuvens, nuvens que são principalmente pertencentes ou administradas por empresas dos EUA. A principal preocupação da União Européia é sobre o regime flexível de proteção de dados usado por empresas de internet dos EUA. O Google também está sob séria investigação por anti-truste pelas autoridades da UE. [...] Muitos governos queixaram-se do papel primus inter pares dos EUA e do setor privado norte-americano. Em 2011, podemos esperar que muitos governos nacionais adotarão uma política de duas vias. Por um lado, eles vão continuar recuperando o controle de seus e-espacos nacionais, com o risco de fragmentação da Internet global. Por outro lado, eles vão acelerar a pressão sobre os EUA para a internacionalização completa da governança da Internet e, em particular, da ICANN.(KURBALIJA, 2011. Tradução nossa.)<sup>18</sup>

Há, portanto, poucos sinais de que modelos e mecanismos de uma governança efetivamente democrática da Internet emergem dos atuais fóruns e espaços de debates formais sobre o tema da Governança da Internet. Para nós ficou claro, no episódio do WikiLeaks, que os governos – em aliança com empresas ou não – estão dispostos a ‘puxar o fio da tomada’, a interferir diretamente nos gargalos das estruturas físicas e lógicas da Internet, onde o controle pode ser imposto de maneira imediata e muito concreta, sempre em nome da soberania e da segurança nacional.

Ficou claro também, que os gargalos neste caso não são absolutos: a Internet é rede, não é ampulheta. Em resposta a iniciativas de controle, censura e supressão de liberdades na rede, indivíduos e grupos independentes se articulam rapidamente para produzir novas correlações de força alternativas aos ensaios de respostas baseadas na concepção jurídico-discursiva do poder, sobre a qual se fundamentam o

sistema das Nações Unidas. As disputas em jogo são muito mais complexas, e os EUA deveriam saber disso. Foi para isso que a Internet foi criada – para resistir.

#### 4. RUPTURAS

No início da década de 90 Arquilla e Ronfeld (1996) escreviam sobre as implicações das redes em uma guerra cibernética como uma forma assustadora de conflito militar, e consagraram o conceito de netwar – guerra em rede – “ao pensar o conflito da era da informação na ponta menos militar, e mais social do espectro” (ARQUILLA e RONFELD, 1996). Com este conceito, os dois pesquisadores buscavam se referir a uma forma emergente de conflito protagonizado por organizações dispersas, descentralizadas e formadas por pequenos núcleos articulados através da Internet, que se tornariam, segundo eles, num dos principais fenômenos das décadas futuras. Arquilla e Ronfeld apontavam, então, que os governos tendem a ser tão restringidos pelos hábitos hierárquicos e interesses institucionais que podem sofrer derrotas agudas – para enfrentar a guerra em rede, seria necessária —uma renascença estratégica, um renascimento conceitual que nos levaria a todos para longe dos velhos paradigmas [...]: a arte da persuasão terá que ser experimentada cada vez mais, vaticinavam os pesquisadores. (ARQUILLA E RONFELD, 2001)

As propostas apresentadas por estes pesquisadores se mostram atuais. Se por um lado ficou claro que uma ação autoritária e hierárquica, viabilizada pela combinação de interesses governamentais e empresariais pode se constituir em uma ameaça considerável à liberdade nas redes de comunicação, também ficou claro que a robustez e resiliência das redes distribuídas é capaz de fazer frente a um ataque sistemático por parte de uma das nações e por algumas das empresas mais poderosas do planeta.

O fato é que o WikiLeaks está online – sediado em múltiplos servidores, espelhado, distribuído, amparado por uma ecologia emergente de atores anônimos e autônomos. O episódio WikiLeaks é, ao nosso ver, um exemplo do que Galloway e Thacker chamam de ‘ruptura’<sup>19</sup> – um evento, dentro de uma rede, que destrói o poder da própria rede. No livro *The Exploit: A Theory of Networks* (GALLOWAY e THACKER, 2007), estes autores mostram que redes descentralizadas não necessariamente estão isentas de controle, mas sim que elas têm suas próprias lógicas de controle que podem eventualmente ser subvertidas por uma “ruptura” que irrompe da própria rede. Os ataques a sites que aconteceram no episódio do WikiLeaks – partindo tanto de seus oponentes quanto de seus apoiadores – são exemplos deste fenômeno de ruptura, que tem como objetivo minar as funções de controle de uma rede.

Conforme estes autores, “para serem eficazes, os futuros movimentos políticos devem descobrir uma nova ruptura. Toda uma nova topologia de resistência deve ser inventada, que seja tão assimétrica em relação às redes quanto a rede foi, em relação aos galopes do poder”. (GALLOWAY E THACKER, 2007, p. 22. Tradução nossa.)<sup>20</sup>

Qual seria a energia mobilizadora destas rupturas? Como se estrutura, como se multiplica, como se fortalece a biopolítica na rede – entendida como “um conjunto de atos de resistência e de contra insurgência de vidas que não se deixam capturar pelo controle” (ANTOON e MALINI, 2010, p.6)? Que modelos de regulação estão sendo postos em prática e como estender a democracia para além de suas fronteiras tradicionais, adentrando os domínios da vida social tecnicamente mediada? Na busca por novas energias de mobilização, ao fazer frente a gargalos estrangulados e infraestruturas dominadas pelo capital, qual o papel dos dispositivos tecnológicos que atuam na camada dos códigos, protocolos e das arquiteturas de sistemas computacionais?

Não temos a ambição de oferecer respostas para todas estas perguntas, mas consideramos que é urgente aprofundar a reflexão sobre possíveis caminhos para a exploração de fissuras nas fronteiras entre o controle e a autonomia, explorando possibilidades de resistência ao biopoder através da construção e uso de sistemas sociotécnicos emancipadores, livres e voltados ao fortalecimento da autonomia nos sujeitos contemporâneos.

## REFERÊNCIAS

ANTOUN, H; MALINI, F. Ontologia da Liberdade na Rede - as multi-mídias e os dilemas da narrativa coletiva dos acontecimentos. In: Anais do XIX Encontro Anual da Associação Nacional dos Programas de Pós-Graduação em Comunicação, 2010, Rio de Janeiro. Rio de Janeiro: COMPÓS/PUC-Rio.

ARQUILLA, John e RONFELDT, David. The Advent of Netwar. Santa Monica: Rand Corporations, 1996.

\_\_\_\_\_. Networks, netwars and the fight for the future. In: First-Monday, University of Illinois, ano 6, n. 10. Chicago: 2001

AVERY, S. Patrioct Act haunts Google service. The Globe and Mail, 24 de março de 2008. Disponível em: <<http://www.theglobeandmail.com/news/technology/article675014.ece>>. Acessado em 24 de fevereiro de 2011.

BENKLER, Yochai. A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate. Massachussets: Harvard Civil Rights-Civil Liberties Law Review, 2011.

BOGARD, William. Digital Resisto(e)rs. Code Drift: Essays in Critical Digital Studies. Abril de 2010. Disponível em <<http://www.ctheory.net/articles.aspx?id=636>> . Acessado em 15 de julho de 2010.

DELEUZE, Gilles. Foucault. São Paulo: Brasiliense, 1988.

DORIA, Avri. RE: [governance] Re: Draft IGC statement on Wikileaks. Mensagem pessoal recebida por Graciela B. Selaimen na lista de discussão do Internet Governance Caucus em 11 de dezembro de 2010.

DYER-WITHEFORD, Nick. Cyber-Marx: Cycles and Circuits of Struggle in High Technology Capitalism. Champaign: University of Illinois Press, 1999.

GALLOWAY, Alexander. Protocol. How Control Exists After Decentralization. London: MIT Press, 2004.

\_\_\_\_\_, THACKER, Eugene. The Exploit. A Theory of Networks. Minneapolis: University of Minnesota Press, 2007.

GURSTEIN, Michael. RE: [governance] Re: Draft IGC statement on Wikileaks. Mensagem pessoal recebida por Graciela B. Selaimen na lista de discussão do Internet Governance Caucus em 12 de dezembro de 2010.

HARDT, M; NEGRI, A. Império. Rio de Janeiro: Record, 2001.

KURBALIJA, Jovan; After the deluge: Internet governance in the aftermath of WikiLeaks. Reflections on Diplomacy, 2011. Disponível em <<http://deepdip.wordpress.com/2011/01/14/after-the-deluge-internet-governance-in-the-aftermath-of-wikileaks/>>. Acessado em 8 de março de 2011.

HWANG, Tim. WikiLeaks and the Internet's Long War. Washington: The Washington Post, 12 de dezembro de 2010. Disponível em: <<http://www.washingtonpost.com/wpdyn/content/article/2010/12/10/AR2010121007133.html>>. Acessado em 22 de dezembro de 2010.

MALCOLM, Jeremy. Re: [governance] FW: [IP] Fwd: Wikileaks Domain Revoked? Mensagem pessoal recebida por Graciela B. Selaimen na lista de discussão do Internet Governance Caucus em 5 de dezembro de 2010.

MENDOZA, Nicolás. A tale of two worlds. Apocalypse, 4Chan, WikiLeaks and the silent protocol wars. In: Radical Philosophy, número 166, março/abril de 2011. Disponível em: <[http://www.radicalphilosophy.com/default.asp?channel\\_id=2187&editorial\\_id=29462](http://www.radicalphilosophy.com/default.asp?channel_id=2187&editorial_id=29462)>. Acessado em 2 de março de 2011.

MUELLER, Milton. Re: [governance] Re: [ciresearchers] Guardian Online: Live with the WikiLeaks world or shut down the net. It's your choice. Mensagem pessoal recebida por Graciela B. Selaimen na lista de discussão do Internet Governance Caucus em 9 de dezembro de 2010.

MUELLER, Milton. Por que o Wikileaks polariza a política de Internet norte-americana? Revista poliTICs, no. 8, março de 2011. Rio de Janeiro, 2011.

PALMÅS, Karl. Predicting what you'll do tomorrow: Panspectric surveillance and the contemporary corporation. In: Surveillance and Society 8 (3): 338-354, 2011.

PETER, Ian. Re: [governance] FW: [IP] Fwd: Wikileaks Domain Revoked? Mensagem pessoal recebida por Graciela B. Selaimen na lista de discussão do Internet Governance Caucus em 4 de dezembro de 2010.

SINGH, Parminder Jeet. Re: [governance] FW: [IP] Fwd: Wikileaks Domain Revoked? Mensagem pessoal recebida por Graciela B. Selaimen na lista de discussão do Internet Governance Caucus em 5 de dezembro de 2010.

STALDER, Felix. Leaks, Whistle-Blowers and the Networked News Ecology. Notes and Nodes, 2010. Disponível em <<http://felix.openflows.com/node/149>>. Acessado em 25 de novembro de 2010.

## NOTAS

<sup>1</sup>Lei estadunidense promulgada em outubro de 2001 visando deter e punir atos de terrorismo nos EUA e ao redor do mundo, fortalecer ferramentas investigativas para o cumprimento da lei e outros propósitos. Ver em <http://epic.org/privacy/terrorism/hr3162.html> Cf. a Wikipedia, o nome US Patriot Act é acrônimo de “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001” (algo como Ato de Unir e Fortalecer a América Providenciando Ferramentas Apropriadas Necessárias para Interceptar e Obstruir o Terrorismo, de 2001).

<sup>2</sup>This power is under attack by a relatively new actor that can be called, for now, the autonomous network.

<sup>3</sup>De acordo com Stalder, os estrategistas militares vêm construindo um discurso sobre os indivíduos superempoderados, que eles compreendem como alguém que é capaz de criar um evento em cascata de maneira autônoma: “[...] a ‘system perturbation’; a disruption of system function and invalidation of existing rule sets to at least the national but more likely the global scale. The key requirements to become ‘superempowered’ are comprehension of a complex system’s connectivity and operation; access to critical network hubs; possession of a force that can be leveraged against the structure of the system and a willingness to use it”. Ver em ‘The Super Empowered Individual’, Zenpundit, 28 October 2006.

<sup>4</sup>O espelhamento de um site é a publicação na Internet de uma cópia fiel de seu conteúdo, porém se-diado em outro servidor e muitas vezes publicado sob um outro domínio.

<sup>5</sup>É importante assinalar que há controvérsias sobre a referência ao Anonymous como grupo hacker, embora esta tenha seja a maneira como o grupo se apresenta, e repercute na mídia. A 2600 Magazine, tradicional publicação da comunidade hacker editada desde 1984, se posicionou contra as reportagens a artigos que afirmavam que os ataques promovidos pelo Anonymous tenham sido uma ação de hacktivism.

<sup>6</sup>Um ataque DDoS – sigla para Distributed Denial of Service – tem como objetivo fazer com que websites fiquem inacessíveis por conta de um número imenso de requisições simultâneas (visitas) ao site. 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. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga. Os ataques de negação de serviço são feitos geralmente de duas formas: forçando o sistema vítima a reinicializar ou consumir todos os recursos (como memória ou processamento por exemplo) de forma que ele não pode mais fornecer seu serviço ou obstruindo a mídia de comunicação entre os utilizadores e o sistema vítima de forma a não comunicarem-se adequadamente.

<sup>7</sup>They attack from the shadows and they have no fear of retaliation. There are no rules of engagement in this kind of emerging warfare. Em artigo de Bernd Debusmann na Reuters: <http://www.reuters.com/article/2010/12/10/us-column-usa-leaks-idUSTRE6B934D20101210>

<sup>8</sup>Anonymous is one of countless iterations of a vibrant digital fringe, an unprecedented source of cultural production situated outside of the regular conducts: those regulated by governments and exploited by corporations in order to standardize identity and stimulate consumption. What is unprecedented is not only the method but also the subject of production. The method and subject are one: the de-localized collaborating community. Anonymous is an open provocation from the rogue episteme of the collaborating community. Not only incomprehensible to the corporate episteme, more importantly it is repressed, excluded and policed; handbook procedure on how to deal with cultural production that cannot be absorbed into corporate imagery.

<sup>9</sup>Uma semana após a divulgação dos Cables, a Senadora do Partido Democrata e Presidente do Comitê de Inteligência do Senado, Diane Feinstein, pediu a perseguição de Assange conforme determina o Espionage Act, de 1917, uma das ferramentas legais mais repressivas no arcabouço legal dos Estados Unidos.

<sup>10</sup> The primary form of power that really confronts us today [...] is rather earthly and mundane. [...]. The predominant contemporary form of sovereignty – if we still want to call it like that – is completely embedded within and supported by legal systems and institutions of governance, a republican form characterized not only by the rule of law but also equally by the rule of property. Said differently, the political is not an autonomous domain, but one completely immersed in economic and legal structures. There is nothing extraordinary or exceptional about this form of power. Its claim to naturalness, in fact its silent and invisible daily functioning, makes it extremely difficult to recognize, analyze and challenge. Our first task, then, will be to bring to light the intimate relations between sovereignty, law, and capital.

<sup>11</sup>However, the implicit alliance, a public-private partnership between the firms that operate the infrastructure and the government that encourages them to help in its war on terror [...] was able to achieve extra-legally much more than law would have allowed the state to do it by itself.

<sup>12</sup>[...] defended the right of people to freely access information, and said that the more freely information flows the stronger societies become.

<sup>13</sup>A autora é membro do Multistakeholder Advisory Group do Internet Governance Forum e membro do Internet Governance Caucus.

<sup>14</sup>Principal espaço de discussões da Sociedade Civil sobre os temas de Governança da Internet, conta atualmente com 91 membros e é reconhecido como ator político relevante pelas Nações Unidas, no processo do IGF. Ver <http://www.igcaucus.org/>

<sup>15</sup>In the absence of any policy regime covering such internet usage issues, corporations are bowing to government pressure and/or acting unilaterally to preserve government secrecy and the way things used to be before the digital age.

<sup>16</sup>The fact is that there is now a strong perception on the part of “the powers that be” that “things are out of control” (see as an example the various types of reactions to what are evidently quite technically trivial attacks by Anonymous) and presumably the follow-on of “something needs to be done”! So the question is what will be done, by whom, and under what authority? I think the argument here is that we should get in soon with some sort of suggested approach to a broad governance framework because the “powers that be” will be feverishly working on their approach and it will emerge very quickly and very forcefully.

<sup>17</sup>When you talk about “public policy” what “public” are you talking about? On the global internet, there are 200+ national publics, many more subnational publics, and several transnational or regional publics involved. If so, what gives a “national” public in the form of one government the right to legislate in ways that affect 20 or 30 other publics over which they have no legitimate authority?

<sup>18</sup>The foundations of Internet politics have been seriously shaken. The fissures that did not appear during previous stress tests including Iraq and Afghanistan, manifested themselves in a matter of days during the WikiLeaks episode.[...] Already some governments in the EU are uneasy about the huge amounts of data and documents belonging to their citizens that are floating around in the clouds, clouds which are principally owned or run by US companies. The EU's main concern is about the relaxed regime of data protection used by US Internet companies. Google is also under serious investigation by the EU's anti-trust authorities. [...] Many governments have complained about the primus inter pares role of the USA and the US-heavy private sector. In 2011, we can expect that many national governments will adopt a two-track policy. On the one hand, they will continue reclaiming control of their national e-spaces, with the risk of fragmentation of the global Internet. On the other hand, they will accelerate pressure on the USA towards complete internationalization of Internet governance and, in particular, of ICANN.

<sup>19</sup>Os autores falam em “Exploit” - ou exploração, na tradução literal do termo. Optamos, todavia, adotar o conceito de ruptura.

<sup>20</sup> [...] to be effective, future political movements must discover a new exploit. A whole new topology of resistance must be invented that is as asymmetrical in relationship to networks as the network was in relation to power canthers.

---

**Artigo recebido em:** 02 de junho de 2011.

**Aprovado em:** 28 de julho de 2011.

**ISSN:** 18099386