AS POLÍTICAS GLOBAIS DE GOVERNANÇA E REGULAMENTAÇÃO DA PRIVACIDADE NA INTERNET

Rebeca Hennemann Vergara de Souza
Universidade Estadual do Piauí – Brasil

Fabrício Solagna*
Ondina Fachel Leal
Universidade Federal do Rio Grande do Sul – Brasil

Resumo: *Este trabalho tem como pano de fundo o contexto das políticas globais de propriedade intelectual, conjunto de acordos e ordenamentos jurídicos que, em grande medida, entre outras coisas, regulam também o fluxo de informação na internet. Através de uma descrição densa de impasses, disputas e estratégias a respeito da regulamentação da rede, busca-se compreender como se conforma um arcabouço comum às políticas globais de regulação da privacidade e da governança das trocas na internet, as quais impactam diretamente o uso que se faz* nos *e* dos *meios e tecnologias digitais. Neste artigo, partindo-se da descrição do contexto mais geral da produção de políticas globais, foca-se especificamente nos casos norte-americano e brasileiro de regulamentação da internet, com o objetivo de desvendar a racionalidade subjacente a esse sistema de produção de regras que atua sobre aquilo que estamos tomando como uma esfera pública, a internet e/ou as redes sociais digitais.*

Palavras-chave: *internet, políticas globais, propriedade intelectual, tecnologias digitais.*

Abstract: *This paper departs from the context of global intellectual policy, treaties and legal order that regulate, among other things, the flow of information on the internet. By means of a thick description of deadlocks, disputes and strategies regarding the web regulation, we try to understand how the global policy overarching framework*

* Mestrando em Sociologia.

http://dx.doi.org/10.1590/S0104-71832014000100006

that regulates the privacy of internet exchanges and the network governance works. Such a policy framework has direct impact on the uses of *and* within *digital means and technologies. Within the more general context of global policy production, this study focuses specifically on the Brazilian and North American internet regulation, aiming to grasp the underlying rationality of this system of production of rules that affects the internet and/or digital social networks, taken here as a public good.*

Keywords: *global policy, informational technologies, intellectual property, internet.*

> *It has now become of a truism that we are functioning in a world fundamentally characterized by objects in motion. These objects include ideas and ideologies, people and goods, images and messages, technologies and techniques. This is a world of flows. […] They are in what I have called relations of disjuncture.*
>
> Appadurai (2001, p. 5)

Políticas globais e seus mecanismos de *enforcement*

Em consonância com os argumentos de Burawoy (2001), em *Manufacturing the global*, acerca de sua proposta de cânones para o que poderíamos chamar de uma etnografia global, este trabalho parte do contexto das políticas globais de propriedade intelectual, conjunto de acordos e ordenamentos jurídicos que, em grande medida, regulam o fluxo de informação na internet. Para Burawoy (2001, p. 149, tradução nossa), um dos aspectos da globalização é sua característica como uma "força inexorável supranacional que reconfigura, mutila e sobrepõe-se ao local". Nosso cotidiano está perpassado pela invisibilidade dessas "forças" ou processos. Seria tarefa de uma "etnografia global" identificar, desmistificar e desnaturalizar essas forças. O objetivo aqui é fazer uma descrição densa de impasses, disputas e estratégias a respeito da regulamentação da rede, tendo como material empírico de referencia a pesquisa documental a respeito da regulamentação da internet. Na esteira de uma antropologia da política, busca-se colocar em evidência o processo político de produção dessas legislações, regulamentações, normas e estratégias de *enforcement* que acabam por regular o nosso acesso cotidiano, individualizado e localizado à internet. As novas tecnologias de informação

são cada vez mais mediadas por um sistema de regras e mecanismos de *enforcement* adotados como estratégias de controle da informação, passando a regular também o sistema social de trocas na rede, a comunicação entre seus usuários e aquilo que pode ser referido, no sentido de Geertz (1989), como um sistema cultural.

Appadurai (2001), também citado na epígrafe que introduz este texto, chama atenção para o fato de haver uma crescente disjunção entre a globalização do conhecimento e o conhecimento da globalização, convocando os estudiosos da cultura a debruçarem-se sobre esses temas. Nessa perspectiva, neste trabalho, busca-se compreender, pelo menos em parte, como se conforma um arcabouço comum às políticas globais da privacidade e da governança das trocas na rede, as quais impactam diretamente o uso que se faz *nos* e *dos* meios e tecnologias digitais. Partindo-se da descrição do contexto mais geral da produção de políticas globais, foca-se especificamente nos casos norte-americano e brasileiro de regulamentação da internet, para compreender-se a racionalidade subjacente a esse sistema de produção de regras que atua sobre aquilo que está sendo aqui tomado como uma esfera pública, a internet. A internet, as bases de dados interconectadas digitalmente e os fluxos de informação, como aponta Fischer (2011, p. 59), "estão reposicionando e encapsulando os meios culturais mais antigos como a oralidade e a escrita, estão reconfigurando a esfera pública pela mudança das relações de poder […]".

Se um modelo internacional de direitos de propriedade intelectual (DPI), com os contornos do que conhecemos hoje, delineia-se no pós-guerra, no contexto das uniões e da política de diretrizes internacionais de governo, é a partir de 1990, com a finalização da Rodada Uruguai, a criação da Organização Mundial do Comércio (OMC) e a aprovação do acordo relativo aos aspectos do direito à propriedade intelectual relacionados com o comércio (*Trade-Related Aspects of Intellectual Property Rights* – TRIPS), que se pode falar da emergência de um modelo global (supranacional) de regulação de tais direitos. Isso porque o TRIPS não apenas obriga os Estados-Membros da OMC a aderirem a um mesmo conjunto de regras, como também estabelece padrões mínimos a serem implementados. O acordo TRIPS representa a imbricação radical entre direitos de propriedade intelectual e de comércio e, portanto, a sujeição de seus objetos às demandas do mercado, a conversão de todos os objetos (materiais e imateriais) em mercadoria. O advento do TRIPS como um acordo da OMC, com poder de sanção global, marca uma

era sem precedentes de comodificação, mercantilização e globalização no mundo (Leal; Souza, 2012).

A nova tendência de regulação inaugurada pelo TRIPS foi radicalizada nas décadas seguintes à criação da OMC, ao mesmo tempo em que a internet emergiu e consolidou-se como um ambiente potencialmente diverso, baseado em tecnologias e padrões abertos, permitindo fácil compartilhamento e circulação de informação, comunicação e de bens e serviços. Desde o surgimento da internet, como será desenvolvido mais adiante neste trabalho, um dos arranjos técnicos e políticos mais caros a ela é o que se convencionou chamar de neutralidade da rede, ou seja, a não discriminação entre os "tipos" de informações trocados entre os seus diversos usuários, o que garantiria a igualdade de condições para todos os nós da rede sejam igualmente emissores e receptores.

Nosso argumento é que a agenda de escalada de legislações de controle da rede teve início nos Estados Unidos, em 1998, com o *Digital Millennium Copyright Act* (DMCA) (United States, 1998), e expandiu-se, por meio de acordos executivos e iniciativas multilaterais, para os países da zona de influência da OMC. Mais recentemente, o caso Wikileaks marcou a emergência de uma nova onda protetiva, com proposições de novas legislações e acordos que passaram a incidir diretamente sobre os provedores de serviços de internet, encurtando assim caminhos jurídicos tradicionais. Em ambos os casos, DMCA e Wikileaks, observa-se ter havido alterações, em diferentes graus, nas legislações nacionais a fim de atenderem aos parâmetros ditos internacionais de *enforcement*.

A adoção de mecanismos do TRIPS-*plus*, desde o final dos anos 1990, os quais envolvem a ampliação do escopo e/ou do nível de proteção estabelecido no acordo TRIPS, também é preciso ser considerada como uma das principais características das diferentes iniciativas envolvendo direitos de propriedade intelectual, sejam aquelas que demonstram a influência dos interesses corporativos norte-americanos nas agências multilaterais, sejam aquelas vinculadas a acordos bilaterais. Dito de outra forma, "Trips-*plus* são as políticas, estratégias, mecanismos e instrumentos que implicam compromissos que vão além daqueles patamares mínimos exigidos pelo acordo TRIPS, que restringem ou anulam suas flexibilidades ou ainda fixam padrões ou disciplinam questão não abordadas pelo TRIPS" (Basso, 2005, p. 24-25), geralmente impostos por um ator com mais peso político e econômico envolvido na negociação, via de regra, os Estados Unidos.

Por outro lado, também desde o final dos anos 1990, observa-se a emergência de um intenso debate na esfera pública sobre direitos e privacidade na internet, os quais se referem diretamente aos direitos de propriedade intelectual. Esse debate amplia-se, em termos de atores envolvidos e publicidade, na medida em que a internet e as novas tecnologias difundem-se pelo tecido social, deixando de ser assunto restrito a círculos altamente especializados. Um dos primeiros casos de grande repercussão nesse tema ficou conhecido como Caso Napster, envolvendo essa rede de compartilhamento de arquivos, a indústria fonográfica e grandes artistas do *mainstream* da música. Embora com um público relativamente restrito, o Caso Naspter suscitou o primeiro debate sobre o alcance dos DPI na internet, no sentido de designação de autores e autenticidade a bens imateriais em circulação na rede.

Em um contexto radicalmente diferente daquele em que se deu o Caso Napster,[1] no início de 2012, os Estados Unidos presenciaram a primeira manifestação social de grandes proporções sobre as estratégias de controle da/na rede, o *Blackout-day*, em que diversos *sites* suspenderam, totalmente ou em parte, seus serviços em razão da discussão, no congresso norte-americano, de leis restritivas ao uso da internet. O *Blackout-day* foi parte de uma onda contra-hegemônica, a qual incluiu não apenas ações diretas da sociedade civil. Diversos países têm aprovado legislações que garantem direitos mínimos de governança na internet, principalmente no que se refere ao regramento sobre a trafegabilidade dos dados e a oportunização equânime sobre o acesso a serviços e informações, ou seja, uma gestão que permita a *neutralidade da rede*. Na América Latina, o Chile foi um dos primeiros países a assegurar uma legislação específica nesse sentido, seguido pela Colômbia.

A *neutralidade da rede* é um princípio do *design* técnico da internet, modelo de tráfego entre os serviços e os usuários, que visa assegurar, como instrumento de governabilidade da rede, a equidade da competição entre os

[1] As diferenças de contexto referem-se, em primeiro lugar, à capacidade da articulação social via *web* (tanto na forma de *web* protestos quanto na busca por viabilizar ações fora da rede), a qual era praticamente inexistente à época do Napster e hoje é uma das principais formas de mobilização política; em segundo, à quantidade e à qualidade dos atores envolvidos. Enquanto o Caso Napster ficou restrito aos círculos altamente especializados (advogados de patentes, mídia especializada) e aos envolvidos no processo, o *Blackout-day* mobilizou milhões de pessoas ao redor do mundo, em diferentes níveis de engajamento (a mídia corporativa internacional, as mídias alternativas, grupos de usuários, acadêmicos, atores estatais, etc.). Por fim, enquanto o Caso Napster praticamente ficou restrito aos EUA, o *Blackout-day* tornou-se *viral* e globalizou o debate sobre as liberdades na internet.

diversos *players*, ou usuários, da rede. Como bem argumentou Lessig (2001) ao analisar o disciplinamento jurídico do espaço virtual, a arquitetura original do ciberespaço mudou à medida que governos e os atores corporativos aumentaram sua habilidade de controlar comportamentos no ciberespaço e que tecnologias foram desenvolvidas para limitar a liberdade desse espaço. Lessig (2001, p. 141, tradução nossa) chama atenção sobre a realocação da inovação, de seu lugar em uma internet descentralizada e diversa para instituições que, antes do advento da internet, policiavam a inovação: "[…] o poder que está sendo criado aqui é importantemente artificial – produto de direitos legais criados no ar e defendidos com o rigor das cortes e códigos".

Retomando os argumentos de Lessig, Fischer (2011, p. 61) adverte que:

> É crucial continuar os debates na esfera publica sobre valores culturais que se articulam nos códigos, no mercado e no direito de software para evitar deslocamentos indesejados da propriedade de informação, barreiras de acesso e outras decisões relativas à infraestrutura – e ainda acompanhar as normas culturais em transformação.

A neutralidade da rede é um tema transversal, envolvendo desde interesses corporativos de empresas de telecomunicações sobre o controle dos conteúdos que circulam nos seus cabos e fibras, empresas de mídia, que dependem da infraestrutura de rede para o sucesso de seu negócio, e usuários em geral, na medida em que a neutralidade (ou sua ausência) impacta diretamente a maneira como os serviços de internet são prestados e cobrados.

Cabe questionar, no escopo da presente análise, de que maneira se pode aferir se um país garante um arcabouço jurídico capaz de regulamentar direitos de cidadania e privacidade na internet. Sabendo-se que os arranjos institucionais, a partir do sistema multilateral, são influenciados por sistemas de poder que vão além dos limites do Estado-nação, propõe-se, aqui, apresentar uma cartografia das legislações de DPI relacionadas à internet, bem como iniciativas de controle tocantes ao combate àquilo identificado como "pirataria" digital e os assim chamados *cybercrimes*. Para tanto, a proposta deste trabalho é, no contexto de consolidação de políticas globais que regulam a internet, focar a análise nos casos norte-americano e brasileiro. É preciso apontar ainda que a noção mesma de *enforcement*, de amplo uso no campo do direito, da administração pública e das tecnologias de informação e comunicação em geral, também no Brasil é empregada no original inglês, como sinônimo e execução

de leis, onde "… se associa à ideia de força da lei […] ao esforço que algumas decisões sejam cumpridas […] a sanção e coerção" (Nogueira, 2013).

Como pano de fundo conceitual, é possível remeter aqui a discussões já clássicas na antropologia a respeito de sistemas jurídicos, como aquela que Bourdieu (1990) faz entre regra e estratégia, entre um princípio jurídico, ordenador ideal de condutas sociais e as estratégias, dando lugar a múltiplos arranjos ditados por contingências do "senso prático", do "sentido de jogo dos agentes". Um paralelo entre os planos global e local é inevitável para a discussão aqui apresentada. Na dinâmica de produção de políticas globais, temos o nível prescritivo, o sistema de agências multilaterais, como a OMC e a OMPI (Organização Mundial da Propriedade Intelectual), no qual os Estados-nações são os atores (alguns certamente com posições hegemônicas no modo de produção política desses regimes jurídicos); já no nível *local*, temos os Estados nacionais, que devem criar mecanismos de *enforcement* e estratégias de efetivação dessas políticas. Dupas (2007, p. 21) aponta que:

> Ajudado pelas novas tecnologias da informação, que oferecem a possibilidade de encolher os horizontes temporais e abolir distâncias, o poder do capital se amplia sem enfrentar diretamente as leis nacionais, muitas vezes sem o consentimento explícito de parlamentos ou governos. O agente econômico global, por ser transnacional, estende seu poder explorando sistematicamente as brechas entre diferentes sistemas jurídicos nacionais. Operando nestes interstícios legais, os grandes grupos vão construindo seu próprio arcabouço legal, incluindo os padrões e as normas em relação ao trabalho, aos contratos e aos processos de arbitragem internacional. As antigas soberanias do Estado-nação passam agora a ser compartilhadas entre Estados e atores econômicos. O poder vai deixando de ser público e acaba, de fato, ocupando vazios criados pela lógica global e editando as novas normas do direito internacional.

Direito de autor no contexto digital e o modelo *made in USA*

Como foi dito anteriormente, consideramos a aprovação do DMCA e o caso Wikileaks como marcos fundamentais na produção de um modelo global de políticas públicas de *enforcement* centradas nos DPI.

O *Digital Millennium Copyright Act* é produto de uma agenda em torno dos DPI construída desde os anos 1980, quando, segundo Castells (2000), tais

direitos, considerados como "ativos", passaram a progressivamente ampliar seu peso na balança comercial norte-americana. Aprovado em 1998, no governo Clinton, o DMCA está em vigor desde 2000.[2] Em linhas gerais, a lei criminaliza tanto a infração do direito autoral em si (a exemplo da cópia não autorizada), ampliando consideravelmente a punição às infrações na internet, quanto a produção e distribuição de tecnologia que permita driblar as proteções autorais. Segundo a Eletronic Frontier Foundation (EFF), duas seções do DMCA são especialmente controversas, a 1201 e a 512.

A seção 1201 contempla dispositivos anti-invasão, permitindo a adoção de controles de acesso e medidas técnicas de proteção, como o DRM,[3] e criminalizando tanto o contorno de *bloqueios* quanto a criação de ferramentas que permitam tal contorno. Embora os dispositivos anti-invasão não tenham sido capazes de atingir seu fim explícito ("parar a pirataria na internet"), mostram-se como um importante instrumento de coação dos usos justos dos conteúdos protegidos por direitos autorais, da livre expressão e o desenvolvimento da pesquisa científica ao não diferenciar qualitativamente as cópias. Além disso, argumenta-se, coloca uma barreira à inovação tecnológica ao coibir a produção de tecnologias que, mesmo sem terem sido criadas com tal objetivo, possam ser utilizadas para burlar as travas tecnológicas. Redes de compartilhamento *peer-to-peer* (P2P) são um dos melhores exemplos deste caso. Elas permitem que arquivos sejam compartilhados entre diversos usuários sem um servidor de armazenamento de arquivos central. Um mesmo usuário pode copiar arquivos de terceiros enquanto compartilha outros de seu próprio computador sem necessidade de serviços especializados. Entretanto, as redes P2P são o principal alvo de políticas de *enforcement*, pois seriam o principal canal de compartilhamento conteúdo protegido por direto autoral (músicas, filmes, livros). Muitos provedores de acesso proíbem ou inibem a utilização dessas redes, principalmente em redes públicas universitárias e de acesso público, ainda que não necessariamente a tecnologia tenha qualquer artefato ilegal *per se*.

[2] A produção de instrumentos jurídicos capazes de impactar o aparato tecnológico em si e a produção e circulação de pacotes na rede não está restrita aos EUA. Um exemplo é a diretiva sobre a sociedade da informação da União Europeia, a qual menciona medidas de proteção técnica à propriedade intelectual (União Europeia, 2001).

[3] O DRM, sigla para *digital rights management*, ou gestão de direitos digitais, em português, consiste na criação de medidas tecnológicas ("travas") para proteger os direitos autorais, impedindo usos não autorizados e, ao mesmo tempo, permitindo o gerenciamento de informações sobre os direitos.

A seção 512 do DMCA, por sua vez, estabelece as chamadas disposições de "porto seguro", limitando as responsabilidades dos prestadores de serviços *online* nos casos de atividades consideradas ilícitas praticadas por seus usuários na rede. Tais disposições protegem os prestadores de terem de indenizar monetariamente terceiros pelos atos ilegais praticados através de seu serviço. Para tanto, os prestadores devem atender a determinadas condições, como adotar procedimentos eficientes de notificação e retirada de matéria (em inglês, *efficient notice and takedown procedures*) protegida por DPI e suspender imediatamente o acesso ao conteúdo quando ocorrer uma denúncia de violação dos direitos por parte do detentor, independentemente do processo judicial. O DMCA também prevê um "porto seguro" ao usuário que, diante de uma notificação de uso de material protegido, alegue que o material não seja de fato ilícito. Seguindo a tendência do acordo TRIPS, ocorre a inversão da lógica da presunção da inocência, conferindo ao acusado responsabilidade de prová-la (Basso, 2005).[4]

O DMCA consolida um modelo convencionado de *notice and takedown*,[5] em que o material, produto ou informação, protegido por direito autoral pode ser retirado e tornado indisponível mediante reclamação do suposto detentor de direitos, com base em suporte jurídico, sem a necessidade de haver processo de escuta de defesa precedente. De fato, percebe-se que a prática tem gerado um imenso volume de pedidos, oriundos de grandes gravadoras e da indústria cinematográfica, enviados diretamente aos buscadores e servidores de hospedagem, que necessitam montar departamentos dedicados ao atendimento a tais solicitações. Como o volume de dados é cada vez maior, sistemas automatizados têm sido utilizados, e a avaliação da legitimidade do pedido fica a cargo somente do reclamante.

[4] Tal princípio estabelece que a regra em relação às acusações penais é a não culpabilidade, implicando o tratamento do acusado como inocente durante o processo, cabendo ao acusador o ônus da prova.

[5] Um exemplo da nova dinâmica de relações na rede mediada pelo DMCA são as Diretrizes da Comunidade, inclusas nos Termos do Serviço do YouTube, com as quais o usuário, ciente ou não, concorda ao utilizar o canal para *upload* de conteúdo. Amparado no DMCA, o detentor de direito autoral (ou seu representante legal) pode notificar o YouTube de suposta infração, por meio de uma notificação ao representante de direitos autorais da plataforma. Mediante a denúncia, o conteúdo pode ser retirado do ar sem que haja qualquer ordem ou processo judicial. Caso o usuário seja qualificado como infrator reincidente, terá seu acesso ao serviço cancelado. O YouTube não deixa claro quem julga o mérito das infrações, uma vez que o acusador não oferece provas.

Segundo dados do *Google transparency report*, somente no mês de julho de 2013, a Recording Industry Association of America (RIAA) somou a solicitação de retirada de 25 milhões de *links* para supostos materiais (músicas, filmes, textos) protegidos do buscador Google. A lista de outros reclamantes não é pequena, demostrando que a tarefa de cumprimento do DMCA é significativa, somando quase 250 milhões de *links* para remoção mensalmente.[6]

Em se tratando de entender como se dá a produção de políticas globais, é preciso apontar para o fato de que a legislação norte-americana tem alcance global, na medida em que grandes serviços de busca e hospedagem estão nos Estados Unidos, como exemplifica o fechamento do *site* MegaUpload, em 2012, pelo FBI. Ainda que o *site* não exercesse controle sobre material hospedado, a suspensão do serviço, apesar de ser regida pela legislação do DMCA, levou milhares de usuários, inclusive não americanos, a perderem seus arquivos, mesmo aqueles não protegidos por direito autoral ou voluntário compartilhados pelos autores/proprietários.

O efeito Wikileaks: justificativa para *enforcement* global

Na esteira do DMCA e da escalada de legislações protetivas, o caso Wikileaks ensejou novas propostas de ampliação do controle na rede e reacendeu a discussão sobre a necessidade de haver parâmetros internacionais de *enforcement*. Em novembro de 2010, o *site* Wikileaks vazou milhares de telegramas secretos da embaixada norte-americana, expondo suas ações militares no Oriente Médio. O *site*, antes visto com bons olhos pelo Pentágono, por revelar documentos secretos de diversos países do mundo, desvelou as estratégias malfadadas das principais guerras em que os Estados Unidos estiveram envolvidos.

De fato, o Wikileaks não estava praticando qualquer ação ilegal, apenas divulgando material recebido por um informante, assim com um veículo de imprensa o poderia fazer amparado pela Lei da Imprensa. Ainda assim, uma série de ações foi deflagrada, baseada não na ilegalidade do *site* ou do conteúdo distribuído, mas no convencimento dos fornecedores de tecnologia e na

[6] Os dados de remoção de *sites* podem ser verificados em tempo real no *Google transparency report* em http://www.google.com/transparencyreport/removals/copyright/.

pressão exercida pelas autoridades sobre eles. A primeira medida adotada foi a suspensão do domínio, obrigando o *site* do Wikileaks a mudar de endereço inúmeras vezes. Logo depois, a empresa Amazon, que disponibilizava os servidores para guarda dos documentos, encerrou o contrato com o *site*. Em seguida, o sistema PayPal e as operadoras Visa e MarterCard fecharam as contas de doações ao *site*, prejudicando ou até mesmo inviabilizando fundos de financiamento do Wikileaks.

Para Benkler (2011), o cenário protetivo mudou radicalmente após as denúncias, principalmente com a proposição das leis *Stop Online Piracy Act* (SOPA) (United States, 2011b) e o *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* (PIPA) (United States, 2011a),[7] que tiveram sua votação suspensa depois de uma onda de protestos e pressão corporativa exercida por diversas empresas do Vale do Silício, notadamente identificadas com uma economia de novo tipo, para além da indústria do entretenimento, com poder de influência política em Washington. Ainda que a disputa tenha seus precedentes, essas empresas conseguiram impor sua agenda, não por questões meramente ideológicas, mas porque seus ganhos provêm de um ecossistema econômico baseado no *commons* da internet (Benkler, 2011). A noção de *commons*, na definição de Benkler (2007, p. 12), é fundamental para se entender a internet, do ponto de vista jurídico, como parte do espaço público:

> *Commons* são um tipo particular de arranjo institucional que governa o uso e a disposição de recursos. Sua principal característica, que os define de forma distinta da propriedade, é que nenhuma pessoa tem o controle exclusivo do uso e da disposição de qualquer recurso particular.

Essas disputas evidenciaram uma conjunção de ações, em parte técnicas, em parte de mobilização política, de amplitude global, que proporcionaram uma capilarização inédita do debate sobre direitos de propriedade. No campo da estratégia política dessas novas legislações, o SOPA e o PIPA remetem a importantes acontecimentos. Benkler (2011) assinala a similaridade entre elas

[7] Essas duas leis foram tratadas em artigo anterior. Ver Souza e Solagna (2012). Para um estudo mais geral sobre regulamentação na internet, não restrito ao caso americano e brasileiro, aqui em análise, ver Solagna, Souza e Leal (2011).

e os esforços, desde o início da década, da indústria do *copyright* na tentativa de produzir legislações capazes de remover completamente *sites* que possam disponibilizar ou distribuir material protegido. O "efeito Wikileaks" propiciou a formulação de uma modelagem mais concisa, que permitiria métodos mais ágeis de *notice and take down*, aliados agora à possibilidade de inviabilização financeira dos "*sites* suspeitos", para usarmos os termos das legislações citadas.

Diferentemente do DMCA, o SOPA e o PIPA focavam três pontos cruciais: a) possibilidade de suspender endereços de internet (domínios ou DNS) dentro dos EUA ou formar *blacklist* de *sites* estrangeiros; b) possibilidade de suspender transferências financeiras por meio de contas de cartão de crédito ou semelhantes; e c) possibilidade de cortar os rendimentos de publicidade *online* proveniente dos *sites* classificados como ilegais. Os pressupostos que nortearam tanto o projeto do PIPA como o SOPA ainda permanecem em debate na nova proposição do chamado *Cyber Intelligence Sharing and Protection Act* (CISPA) (United States, 2012a), aprovado em abril de 2012, aguardando aprovação do senado norte-americano. Seu objetivo é dotar de meios legais o combate à pirataria nas redes de compartilhamento, mediante cooperação entre os provedores de acesso e as agências de inteligência do país. O CISPA foi proposto pelo congressista Michael Rogers e apoiado pela Motion Picture Association of America (MPAA), a Câmara de Comércio norte-americana, o Screen Actor Guild, a Viacon e entidades ligadas à indústria cinematográfica. Assim como ocorreu com o SOPA e o PIPA, o CISPA foi questionado por organizações civis, como a Eletronic Frontier Foundation, o Center for Democracy and Technology, a American Civil Liberties Union e o Human Rights Watch.

De maneira geral, a controvérsia estabelecida circunscreveu-se à garantia de direitos de privacidade, anonimato e segurança em detrimento de mais controle da circulação de bens imateriais nas redes digitais. Recentemente, o tema voltou a ocupar as manchetes quando Edward Snowden, ex-funcionário da Agência Nacional de Segurança dos Estados Unidos (NSA), revelou uma série de mecanismos de vigilância praticada pelas agências de inteligência norte-americanas e as maiores empresas na área de internet. Esse é um caso singular, pois desvelou que as práticas de monitoramento e cooperação institucional e corporativa vão além das regras públicas estabelecidas. Como pano de fundo, está em jogo a propriedade dos dados e artefatos digitais como bens imateriais. Entre licenças e "termos de uso", há uma clara disputa para se definir se o prestador de serviço também é dono da produção dos utilizadores. Pode-se

arbitrariamente usar, vender ou ceder essas informações? E, em última instância, quem deve ser responsabilizado pelos possíveis ilícitos dentro da rede?

O princípio da neutralidade da rede e a privacidade regulada

Um dos arranjos mais centrais à rede, mobilizado com mais ênfase nesses últimos anos, é o que se convencionou chamar de *neutralidade da rede*. O termo tem sua origem na legislação de telégrafos de 1860 e, em relação à internet, foi consagrado por Tim Wu (2003, 2004). Em suma, essa neutralidade consiste na capacidade de os pacotes da rede terem iguais condições de tratamento nos diversos pontos da rede que perpassam. O arranjo técnico projeta uma não discriminação de tipos de pacotes de dados, o que garantiria a igualdade de condições de toda a informação da rede circular sem barreiras preestabelecidas. Pacotes de dados, na linguagem dos usuários *experts*, é a forma como as informações são agrupadas e transmitidas na rede. A metáfora liberal clássica a partir desse condicionamento é imediata, "todos os pacotes são iguais perante a rede", e fornece a estética da rede diante da governabilidade da rede.

Para Benkler (2007, p. 18), a liberdade e a inovação tornadas possíveis pela economia em rede dependem diretamente da construção de uma infraestrutura básica de espaços de comunicação de uso comum (*digital commons*), de acesso público, que seja paralela à estrutura proprietária, isto é, de acesso privado, sendo que ao menos uma parte de cada camada deve "poder ser utilizada por todos sem a necessidade de ter qualquer permissão". A arquitetura da internet, diferentemente de outros meios de comunicação, permitiu que diversas camadas da rede pudessem ser usadas sem que fossem necessários intermediários.

> Esta infraestrutura de *commons* deve se estender desde a camada física do ambiente da informação até as camadas lógicas e de conteúdo. Ela deve ser estendida para que toda pessoa tenha certo conjunto de recursos primeiros e últimos que lhe permita fazer e comunicar a informação, o conhecimento e a cultura para todos os demais. (Benkler, 2007, p. 18).

Na prática, o arranjo técnico e institucional da rede proporcionou que houvesse uma separação entre os provedores de acesso (ISPs) e os provedores de conteúdo, como fornecedores independentes. A neutralidade da rede corresponde à separação unívoca dessas duas camadas, para que

(pretensamente) não haja arbítrio nem vigilância do conteúdo que esteja circulando na infraestrutura.

Desde 1990, o debate sobre as regras de governabilidade da rede tem se tornado mais frequente, principalmente devido ao englobamento dos ISPs pelas empresas de telecomunicação. Benkler (2007) chama atenção para dois efeitos da comunicação de massa fundamentais para se compreender o processo de *cercamento* técnico e judicial da internet. O primeiro, conhecido como o efeito Berlusconi, é definido como "o poder político desproporcional que a propriedade dos meios de comunicação em massa dá aos seus proprietários ou aqueles que podem pagar por eles" (Benkler, 2007, p. 16), a exemplo das estratégias de inclusão de temas privados nas agendas públicas e no ordenamento jurídico, como os *lobbies*, grupos de pressão e o mecanismo de "portas giratórias".[8] O segundo efeito refere-se a "a substituição sistemática do discurso público pela distribuição de produtos de entretenimento vendidos como mercadorias" (Benkler, 2007, p. 16). Esse mecanismo permite analisar a progressiva mercantilização da produção cultural, científica e artística em níveis inéditos por meio dos direitos de propriedade intelectual como principal estratégia de produção do valor de troca. Ambos os efeitos radicalizam a ideia de que o acesso a bens e serviços deve ser restrito aos que possam por eles pagar, independentemente da função social, do bem-estar coletivo e dos direitos individuais e coletivos. É nesse sentido que, contra a neutralidade da rede, os porta-vozes das corporações, geralmente da área de telecomunicações, argumentam que serviços de vídeo e voz deveriam ser priorizados porque dependem de alto consumo de banda e qualidade de entrega para sua efetividade.

O argumento dos defensores da neutralidade é o de que a rede deve ser tratada como espaço público, como um *bem comum* (*common resource*), e que serviços não devem ser diferenciados ou priorizados. Diversas iniciativas legislativas nos Estados Unidos têm tentado regulamentar esses princípios, sendo que, entre as mais significativas, estão o *Network Neutrality Act* (United States, 2006), e o *Internet Freedom Preservation Act* (United States, 2008).

A neutralidade de rede também remete a uma leitura do funcionamento da rede a partir da sociedade civil - seus ativistas, entusiastas, *hackers* e

[8] Do inglês *revolving doors*, refere-se, no contexto norte-americano, ao movimento de alternância das mesmas pessoas em cargos públicos, na estrutura legislativa e nas agências reguladoras do Estado e cargos nas indústrias afetadas por regulações oriundas do Estado.

técnicos - que conformam um movimento social específico. Os primeiros manifestos sobre uma "governabilidade da rede" surgiram em meados da década de 1990. Os dois mais significativos foram *A rape in cyberspace*, de Julian Dibbell (1998) e *Declaration of the independence of cyberspace*, de John Perry Barlow (1996). Estes atores não eram "nativos" da rede e não tinham nenhum vínculo com os técnicos fundadores da internet; entretanto, foram fundamentais para traduzir o que seria um "novo espaço" para um público não técnico, além de arregimentar uma militância "libertarianista", defendendo uma desvinculação de governos sobre a rede (Goldsmith; Wu, 2006). Esse caráter libertário de uma geração ligada aos primórdios da internet é bastante abordado por Barbrook e Cameron (1996) no que classificaram de uma fusão da cultura libertária dos anos 1960 com uma cultura empresarial de alto risco dos anos 1980 que "promiscuamente combina o espírito desgarrado dos hippies e o zelo empreendedor dos yuppies". Coleman (2005), em sua etnografia sobre a constituição da comunidade Debian, grupo de ativistas técnicos ligados ao movimento de *software* livre e código aberto, detalha essa influência política nas comunidades *hackers* e como os ideais de um liberalismo radical orientam as práticas de compartilhamento de *software*. Pode-se afirmar que os embates em torno da neutralidade de rede, entre o *enforcement* de legislações protetivas e o ativismo na rede traduz, em grande medida, o embate entre modelos políticos da rede, interpretados a partir de modos de organização política e novas formas de movimentos sociais na contemporaneidade.

Desde o advento do TRIPS como um regime global de propriedade intelectual, atores importantes da assim chamada sociedade civil global têm chamado a atenção para o processo de *cercamento* (*enclosure*) que ocorre ao domínio público, ou *intellectual commons*. Fazendo um paralelo histórico com o processo de cercamento de terras ocorrido na Inglaterra entre os séculos XV e XIX, terras até então de domínio público, e a transferência de direitos de propriedade para os nobres, tornando essas áreas propriedade privada, ambos os termos, *commons* e *cercamento*, passam a fazer parte do discurso a respeito da legislação de propriedade intelectual, em geral, sob uma perspectiva analítica crítica.[9]

[9] Ver, entre outros: Benkler (2006, 2007); Boyle (2003); Lessig (2001).

Os anos de 2006 a 2008 constituíram um período de intensa disputa pela neutralidade da rede, tendo sido de extrema importância o posicionamento da Comissão Federal de Comunicações dos Estados Unidos (FCC), no emblemático caso da Comcast. Em 2006, o provedor teria começado a discriminar pacotes de dados de origem de redes *peer-to-peer*, (entre eles, por exemplo, o BitTorrent), protocolo usado para compartilhamento de arquivos entre usuários. O argumento era que a enorme quantidade de dados utilizados era, na sua grande maioria, oriundos de pirataria e que, portanto, não deveria degradar "o bom uso da rede". Em resposta às queixas encaminhadas à FCC pelo Public Knowledge e pelo Free Press, ambos grupos de defesa do consumidor, e pela distribuidora de vídeo online Vuze, a comissão manifestou-se contrária à discriminação dos pacotes. No ano anterior, a FCC publicara uma declaração de política da internet (United States, 2005), a qual estabelecia quatro princípios que buscavam defender direitos dos usuários e, por consequência, acabavam apoiando a neutralidade. São esses direitos: acessar conteúdo legal na internet; rodar aplicativos e usar os serviços de sua preferência; rodar aparelhos de sua preferência, desde que não prejudiquem a rede; e beneficiar-se da competição entre operadoras e provedores de conteúdo e de aplicação. Entretanto, cabe destacar que, em 2009, a Corte de Apelações do Distrito de Colúmbia, Estados Unidos, declarou que a FCC não tinha autoridade estatutária para impor princípios de neutralidade na rede.

Casos parecidos foram replicados em diversos outros países. No Brasil, vários estudos apontaram a técnica de *traffic shapping* em provedores como a NET e Brasil Telecom (Evangelista, 2006). Para além da priorização de serviços específicos e do bloqueio de outros "indesejados", o princípio da neutralidade delimita a privacidade dos conteúdos que circulam na rede. Se um serviço é mais priorizado que outro, é necessário que o "dono do cabo" saiba o que o usuário está transmitindo, mediante técnicas convencionadas de *deep package inspection*. Esse é o argumento utilizado, também, para um "exame" mais acurado de materiais ilícitos na rede, tendo sido implementado como legislação em diversos países, como forma juridicamente aceita para o combate às cópias ilegais.

Para uma política mais eficiente de controle, uma agenda que dissolva essas camadas está sendo paulatinamente consolidada, a partir da responsabilização dos ISPs pela vigilância sobre possíveis delitos cometidos pelos usuários da rede. Essa agenda é conhecida como "resposta gradual" ou *three*

strikes. Em termos gerais, uma comissão específica julga casos relatados pelos ISPs ou reclamantes sobre possíveis infrações de propriedade intelectual. Os usuários são notificados por duas vezes, até serem desconectados e processados na última notificação reincidente. Como exemplos de resposta gradual, pode-se citar o mecanismo de *enforcement* da Hadopi, lei francesa aprovada em 2009 (France, 2009), e o caso sul-coreano. O primeiro gerou mais de 500 mil primeiras notificações em 2011 e, atualmente, há cerca de 60 casos de usuários em fase de desconexão e processo. Já na Coreia do Sul, a resposta gradual foi implementada em 2009, a partir de uma revisão da lei de direito autoral, ampliando o poder desse ordenamento jurídico para se controlar a circulação de conteúdo *online* mediante um sistema de inspeção profunda dos *pacotes* (cf. Tong-Hyung, 2009).

Como mencionado anteriormente, considerando-se os embates verificados em torno da neutralidade da rede, cabe questionar de que maneira pode-se mensurar se um país garante um arcabouço jurídico capaz de regulamentar direitos de cidadania e privacidade na internet. Nossa análise busca evidenciar as diferenças existentes entre os sistemas regulatórios, em uma perspectiva comparativa. Para tanto, consideramos os seguintes aspectos: a) existência de legislação nacional específica sobre internet; b) necessidade de haver ordem judicial para retirada de conteúdo protegido por *copyright*; c) existência de legislação ou mecanismo legal de bloqueio de serviço de conexão; e d) legislação nacional específica sobre privacidade digital.

Um dos estudos comparativos comumente utilizados é o relatório *Freedom on the Net*, elaborado pela Freedom House, instituição independente sediada nos Estados Unidos que produz relatórios anuais monitorando a liberdade de expressão e imprensa. Essa organização se dedicou nos últimos dois anos a produzir um relatório específico sobre a liberdade na internet, abrangendo mais de 50 países.[10] A metodologia empregada no estudo concentra-se na análise de três grandes eixos: obstáculos de acesso, no qual são analisadas as dificuldades econômicas e de infraestrutura; controle de conteúdo, referindo-se à existência de filtros e bloqueios de *sites* e outras formas de censura; e violação de direitos de usuários, relacionando formas de limitação de privacidade, vigilância na rede e restrição de atividades habituais nas redes digitais.

[10] Para esses dados ver também Kelly, Cook e Troung, (2012).

Os três eixos são desdobrados em 21 questões metodológicas, que avaliam as condições de liberdade da internet nos países que compõem a amostra, numa pontuação que varia entre 0 e 100, entre os países com maior ou menor liberdade, respectivamente.

Segundo esse ranking, Brasil e Estados Unidos estariam na faixa de países "livres", com uma pontuação abaixo de 33 pontos; porém, o relatório público, nossa referência para este artigo, não permite acesso aos dados brutos, mas somente ao resultado agregado. Nesse sentido, os Estados Unidos aparecem com pontuação positiva para "violação de direitos de usuários" (somando somente cinco pontos), também não havendo registros de "evidências de vigilância, regulação ou restrição de anonimato". O Brasil é apontado como um dos melhores países no *ranking* da América Latina, apesar de, segundo o relatório, carecer de uma lei mais específica sobre regulamentação de direitos autorais de bens imateriais.

Em nosso exercício, propomos aqui analisar três eixos transversais ao relatório da Freedom House, envolvendo especificamente neutralidade da rede, regulamentação quanto à retirada de conteúdo e mecanismos de inspeção do tráfego de conteúdo. A partir disso, é nosso objetivo traçar uma cartografia do cenário, nos Estados Unidos e no Brasil, de iniciativas legislativas, de regulações e pressões multilaterais, sempre no contexto da produção de políticas globais, com base em casos emblemáticos balizadores no campo da regulação de direitos na internet. Destacamos a tensão continuada que há entre o domínio público e o ordenamento jurídico da propriedade intelectual sobre os bens intangíveis. Reiteramos que não se trata apenas de decisões legais e econômicas relativas a domínios na rede e governança de fluxos de informação, comunicação e dados, "mas escolhas, valores e pontos de inflexão culturais que fazem uma certa diferença nas direções que a vida cultural pode tomar […]" (Fischer, 2011 p. 62).

A escolha dos dois países como casos em nossa análise se justifica na medida em que os EUA têm sido o protagonista de legislações de *enforcement* na área de propriedade intelectual e internet, bem como um ator subjacente com poder de influência de políticas domésticas de diversos países. O Brasil, por protagonizar uma das primeiras experiências de discussão e construção de lei específica para governança da internet de forma aberta e colaborativa, através de um *website* específico, promovido pelo governo federal. A plataforma do Marco Civil da internet, como ficou conhecido, foi lançado em 2009 e

o projeto de lei resultante ainda tramitava no Congresso Nacional quando da escrita deste artigo.

Estados Unidos da América

Práticas consideradas censoras da internet adotadas por diferentes países, como China, Coreia do Norte, Arábia Saudita e Irã, que violam o princípio da neutralidade da rede, nem sempre se basearam em lei(s) específica(s) sobre e para a regulação da internet. Os Estados Unidos foi o primeiro país a estabelecer um arcabouço jurídico para regulação da rede, tanto mediante decisões judiciais pontuais, quanto por meio de legislações específicas. As primeiras dessas legislações foram relativas ao setor de telecomunicações, a exemplo do *Communications Deceny Act* (United States, 1996), o qual estava incluso na lei de telecomunicações, regulando a vinculação de material pornográfico na rede.

No que se refere à legislação específica para a internet, os Estados Unidos constituíram um modelo conformado por interesses corporativos transnacionais e por pressões multilaterais, cabendo avaliar, em cada caso, a maior ou menor capacidade dos atores pautarem a agenda a partir desses interesses. A confluência de interesses da indústria do entretenimento e das telecomunicações com o discurso antiterror pós-11 de Setembro tem constituído um solo fértil para a produção de legislações reguladoras da internet, a ponto de o deputado Darrell Issa, em 2012, ter proposto um bloqueio, por dois anos, de qualquer tentativa de regulamentação da rede, diante do debate público e especializado do SOPA, PIPA e CISPA.

Como abordado anteriormente, o DMCA (2000) foi a primeira experiência de regulação de direitos de propriedade intelectual no contexto da internet, congregando em uma única legislação: a) tratamento de propriedade intelectual para bens digitais; b) gestão de direitos digitais (DRM); c) criminalização da prática de reversão técnica de dispositivos controladores de gestão de direitos digitais; e d) normalização de pedidos de retirada de conteúdo sem ordem judicial (*notice and takedown*). Esse modelo tem sido exportado especialmente por meio do relatório *Special 301*, elaborado anualmente pelo Escritório do Representante do Comércio dos EUA (USTR), que trata de barreiras comercias colocadas às empresas norte-americanas pelas legislações de propriedade

intelectual. Conforme revelado pelos telegramas *vazados* pelo Wikileaks, o relatório é utilizado para forçar governos a alinhar suas legislações com uma proteção "adequada e eficaz" aos parâmetros norte-americanos.[11]

Especificamente quanto à retirada de conteúdo protegido por *copyright*, o DMCA provê instrumentos legais e técnicos para tanto, aplicados diretamente aos provedores de acesso e provedores de serviço, sem que haja necessidade de os reclamantes apresentarem ordem judicial. Em todos os grandes serviços de internet, é possível verificar as cláusulas do DMCA quanto ao conteúdo. De serviços de hospedagem de fotos e vídeos a redes sociais, o DMCA, assim como o acordo TRIPS, inverte a presunção da inocência, imputando ao acusado a responsabilidade de provar que não cometeu um crime. Os pedidos de retirada de conteúdo têm aumentado na mesma medida que têm se ampliado os canais de distribuição de conteúdos (lícitos ou ilícitos). No que tange a grandes repositórios e *sites* de busca, os pedidos têm sido feitos de modo automatizado, a partir de algoritmos que rasteiam conteúdo que possivelmente infrinja direitos autorais.

O Google é dos *sites* que tem anunciado a origem e o número de pedidos de retirada de conteúdo da rede. Em julho de 2013, por exemplo, somente o Google recebeu quase cinco milhões de pedidos de remoção.[12] Entre os dez primeiros colocados na lista de demandantes, estão entidades antipirataria, geralmente firmas de tecnologia e escritórios de advocacia especializados em casos de disputa sobre DPI. Também é possível perceber a presença de gravadoras e da indústria cinematográfica, cujos pedidos somam mais da metade do total.

No caso dos Estados Unidos, não há legislação para bloqueio de serviço de conexão por infração de propriedade intelectual, como ocorre na França e Espanha, por exemplo, que incluíram, no ordenamento jurídico, uma metodologia de resposta gradual (*three-strikes*) ao procedimento legal doméstico. Como descrito anteriormente, a estratégia disciplinadora da *resposta gradual* consiste em monitorar a conexão dos usuários por meio do provedor de acesso que, suspeitando de *download* de material protegido por direito autoral, envia

[11] O caso da Espanha é significativo nesse sentido, revelado pelo Wikileaks; ver Anderson (2010).

[12] Nos dados do *Transparency report* do Google, veem-se a origem e o número de pedidos de retiradas de conteúdo, bem como se constata a impressionante escalada de pedidos e as principais empresas ou organizações envolvidas. Para esses dados, ver: http://www.google.com/transparencyreport/.

notificações (que podem ocorrer via *e-mail* ou carta registrada, a depender do sistema) a fim de alertar o usuário sobre possíveis penas. Se o usuário continuar fazendo cópias e não apresentar defesa, pode ser multado ou ter sua conexão suspensa.

Nos Estados Unidos, o modelo implantado consiste no Copyright Alert System (CAS), implantado em julho de 2011, que não é um dispositivo legal, mas um sistema privado de alerta que congrega os maiores provedores de internet dos Estados Unidos – AT&T, Cablevision, Time Warner, Verizon e Comcast –, escritórios de representação da indústria fonográfica e cinematográfica – RIAA e MPAA – e alianças menores, como Independent Film and Television Alliance (IFTA) e American Association of Independent Music (A2IM). Os esforços de monitoramento são coordenados por uma entidade privada, sem fins lucrativos, chamada Center for Copyright Information, a qual provê a infraestrutura logística para a realização do monitoramento e dos envios dos alertas. O foco do sistema "educacional" são as redes públicas P2P e BitTorrent, ou seja, redes abertas de compartilhamento de arquivos. Segundo os dados divulgados no *site* da instituição, o procedimento não é realizado por meio de *deep package inspection*, mas pela comparação de semelhança de *downloads* realizados pelos usuários com arquivos que notadamente possuam proteção autoral para circulação na rede, ou seja, há algum tipo de monitoramento do conteúdo consumido pelo usuário para estabelecer a "presunção da culpa".

Também conhecida como *six strikes* ou *resposta gradual*, essa metodologia dita "educacional" consiste em, primeiramente, avisar o usuário que possivelmente esteja copiando algum material protegido por *e-mail*, alertando-o sobre questões legais. No segundo momento, um novo *e-mail* ou uma mensagem de voz do provedor é enviada a fim de que o usuário confirme ter conhecimento sobre as consequências de sua conduta. Na terceira e quarta fase, é enviado um vídeo educativo contendo questões sobre propriedade intelectual. O quinto e sexto passo, caso não haja qualquer manifestação por parte do usuário, interferem diretamente na conexão. O limite de banda é reduzido ao mínimo, e, a cada intervalo de tempo de navegação, uma página de alerta é apresentada. A estratégia de *enforcement* da assim chamada resposta gradual pretende ser pedagógica e objetiva o disciplinamento do usuário, neste caso, incidindo nos usuários norte-americanos.

Apesar de o monitoramento e recolhimento desses registros não ter força legal de denúncia, entidades de defesa de direitos digitais advogam que eles podem significar um valioso trunfo de chantagem. Nos Estados Unidos, é usual o envio de cartas de conciliação prévia, a partir das grandes associações de gravadoras, por exemplo, em que multas já são estipuladas, a fim de que o processo por infração de direito autoral não seja levado aos tribunais. A Eletronic Frontier Foundation chegou a abrir um processo chamado *RIAA versus the people*[13] em 2008, denunciando o método jurídico conhecido como *John Doe*. Reticentes quanto a levar a cabo grandes processos de defesa, de altos custos judiciais, os usuários preferem o pagamento da multa. Além disso, a interferência e redução da velocidade da conexão por meio de avisos intermitentes constituem ingerência sobre a neutralidade da rede. Apesar de não figurar uma priorização ou depreciação de um tipo de serviço em relação a outro, a metodologia ataca diretamente as redes de compartilhamento de arquivos, em particular, as redes BitTorrent. Em sentido estratégico, essa é uma forma de se desestimular a troca de arquivos, se intervindo tecnicamente em serviços de troca de arquivos, numa aliança entre provedores e detentores de DPI. Nesses termos, as regras de tratamento isonômico dos dados trafegados na rede entram em choque com a campanha "educacional", já que esta tem impacto direto nas tecnologias e protocolos disponíveis para uso na rede. Além disso, o uso da rede, suas tecnologias e protocolos são julgados independentemente de qualquer processo judicial, tendo os provedores de acesso e detentores de direitos o arbítrio sobre os casos.

Quanto à privacidade digital, nos Estados Unidos, os aspectos relativos ao tratamento de dados pessoais, mais especificamente, relativos a dados pessoais trafegados em meio eletrônico, são contemplados de maneira ampla pelo *Privacy Act*, de 1974 (cf. United States, 2012b), modificado pelo *Computer Matching and Privacy Protection Act*, de 1988 (cf. United States, 2013) e pelo *Computer Matching and Privacy Protection Ammendment*, de 1990 (cf. United States, 1991). Uma das leis mais significativas sobre e para a privacidade digital é o *USA Patriot Act*, aprovado em 2001, como resposta aos ataques terroristas ocorridos em território norte-americano (United States, 2001). A lei, que autoriza uma série de procedimentos com o intuito de "combater o

[13] Ver RIAA v. the people (2008).

terrorismo", é alvo de crítica no que tange à privacidade digital, por autorizar escutas telefônicas em massa.

Em março de 2011, o presidente Barack Obama assinou uma reedição do *Patriot Act*, o *Foreign Intelligence Surveillance Act* (cf. Liu, 2011). Em 2013, um extenso programa de vigilância e interceptação de dados da internet foi revelado pelo ex-funcionário da NSA, Edward Snowden. Os programas PRISM, XKeyscore e Tempora estariam sendo usados para inspecionar grandes volumes de dados, oriundos principalmente de provedores de serviço de *e-mail* e redes sociais, como Google, Facebook, Microsoft e Skype. Tal inspeção dispensaria ordem judicial, requerendo, do funcionário responsável, apenas o preenchimento de formulários de justificativa para a obtenção de dados pessoais de qualquer usuário dessas redes. Apesar de negar a inspeção massiva, o presidente Obama admitiu publicamente que pelo menos 1,6% dos dados trafegados nos Estados Unidos seria interceptado pela NSA.

Brasil

No Brasil, não existe legislação específica sobre a internet. No entanto, após longo debate acerca de uma lei sobre crimes digitais e diversas tentativas de se aprovar o projeto de lei nº 84/1999, de autoria do Deputado Eduardo Azeredo, um projeto específico sobre crimes ou delitos informáticos foi aprovado no final de 2012, entrando em vigor em 2013 (Brasil, 2012a).

O projeto de lei nº 84/1999, conhecido como AI-5 Digital, fez emergir uma das maiores mobilizações de especialistas e militantes em defesa de direitos de privacidade no contexto da internet no cenário doméstico. Nesse sentido, destacam-se duas delas, que funcionaram como principais iniciativas de contraposições de cunho técnico e político: a consulta pública digital para a criação de um marco civil para a internet, pautada pelo Ministério da Justiça, em 2009, e a consulta pública digital acerca da reforma na Lei do Direito Autoral, realizada pelo Ministério da Cultura, em 2010. Ambas as propostas tiveram o papel de conformar um ambiente de mediação, deslocando o caráter da discussão do campo da criminalização e do *enforcement* para o das responsabilidades e direitos (Solagna, 2012). A lei nº 12.737/2012 (Brasil, 2012b), também conhecida como Lei Carolina Dieckmann, foi proposta e aprovada celeremente após a divulgação de fotos pessoais da atriz homônima na internet, obtidas de seu computador após ela ter passado seus dados pessoais

respondendo a um *e-mail* contendo técnicas de *phishing*.[14] Cabe destacar que, neste artigo, essa não é considerada uma legislação específica, na medida em que está vinculada a uma alteração do Código Civil, não constituindo um conjunto autônomo de dispositivos legais. A lei foi proposta pelo deputado Paulo Teixeira e tipifica três tipos de crimes cibernéticos: a) invasão de computador a fim de obter, adulterar ou destruir dados ou informações, sem autorização expressa ou tácita do titular do dispositivo, ou instalar vulnerabilidades para obter vantagem ilícita; b) interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública; e c) falsificação de documento ou cartão bancário.

A Lei Carolina Dieckmann foi considerada uma forma de se neutralizar o projeto mais amplo de tipificação de crimes apresentado pelo deputado Eduardo Azeredo, embora a avaliação quanto a seu impacto não seja consensual entre os ativistas. A principal crítica refere-se à aprovação de uma lei criminal antes de ter sido colocado em prática o Marco Civil da internet. A existência dessa tipificação isolada, num contexto de demanda por regulação do ambiente digital, pode acarretar o alargamento de sua interpretação, na ausência de uma regulação mais abrangente, a qual seria fornecida pelo Marco Civil.

Para a retirada de conteúdo *online*, é necessário haver ordem judicial emitida ao provedor da hospedagem, porém há alguns casos clássicos de má interpretação jurídica da estrutura de funcionamento da internet no que se refere a bloqueio de material em provedores de conteúdos não hospedados em território nacional. Cabe destacar que muitos *sites* são hospedados nos Estados Unidos, razão pela qual o usuário brasileiro vincula-se ao DMCA, mesmo sem saber. Um exemplo nesse sentido foi o bloqueio ao *site* YouTube, em 2007, devido a uma ação judicial iniciada por Tato Malzoni, então namorado da apresentadora de TV Daniela Cicarelli, expedido contra o *site* por conta de um vídeo que exibia cenas íntimas do casal. Durante cerca de 24 horas, o YouTube ficou bloqueado por todos os provedores de acesso no Brasil. Também cabe destacar a ocorrência de reiteradas denúncias de censura na internet, sem que tenha havido qualquer ordem judicial para tanto.

[14] Termo oriundo do inglês (*fishing*), que quer dizer pescaria, configura um modo de fraude eletrônica, caracterizada por tentativas de se adquirirem dados pessoais de diversos tipos, senhas, dados financeiros como número de cartões de crédito e outros dados pessoais. O ato ocorre quando um fraudador se faz passar por uma pessoa ou empresa confiável, enviando uma comunicação eletrônica "oficial".

Por exemplo, durante os protestos ocorridos ao longo do Brasil, em julho de 2013, abundaram denúncias de retirada de *posts* no Facebook relacionados às manifestações, bem como ausência de sinal de celular nas áreas dos protestos, impedindo o acesso à internet. O projeto Rede Livre, criado nesse contexto por pesquisadores da Fundação Getúlio Vargas, congrega denúncias de ataque à liberdade de expressão na internet.

Diferentemente dos países do Norte, o Brasil não possui qualquer mecanismo de bloqueio da conexão por infração de direito autoral, a exemplo do método de "resposta gradual" implementado pelos EUA, França, Espanha e Austrália. O país tem sido alvo da pressão exercida pela *Special 301*, que, por várias vezes, indicou a necessidade de haver aumento do *enforcement* no que tange à pirataria digital. Como o projeto de lei do deputado Eduardo Azeredo esteve em discussão por diversos anos, sendo inclusive citado no relatório, o foco da discussão foi direcionado para leis de tipificação de crimes cibernéticos.

Igualmente, não há uma legislação nacional específica para garantir a privacidade digital. O Marco Civil da internet é, atualmente, o projeto com melhor desenvolvimento na área, já que pontua expressamente a responsabilidade dos provedores de acesso e, principalmente, inibe a prática de rastreamento de serviços web por parte dos provedores de conexão. Trata com exclusividade da neutralidade de rede, ponto polêmico que tem travado a votação do projeto na Câmara dos Deputados, principalmente pela atuação das empresas de telecomunicação, através do SindiTelebrasil. Mesmo tramitando em regime de urgência no final de 2013, a pedido do Executivo, o projeto não obteve consenso e a votação foi adiada para 2014.

Considerações finais

Os elementos propostos para avaliação do grau de liberdade na internet não podem ser tomados de forma absoluta, razão pela qual o levantamento aqui descrito constitui a primeira etapa de uma análise a ser aprofundada posteriormente. A existência de uma legislação específica sobre internet ou sobre privacidade digital, por exemplo, é pouco informativa, caso não se considerem o conteúdo e as possibilidades interpretativas da lei. Ao passo que, no caso norte-americano, o DMCA configura um indicador da existência de restrições à liberdade na rede, no Brasil, a ausência de legislação semelhante tem funcionado como garantia da liberdade e neutralidade, em que pesem as

recorrentes críticas e pressões bilaterais (notadamente, dos Estados Unidos mediante a *Special 301*) e dos proprietários de DPI ao clima de insegurança jurídica provocado pela ausência de tal legislação. Já a necessidade de haver ordem judicial para retirada de conteúdo apresenta-se como um indicador de segurança jurídica para o usuário e uma forma de coibir práticas abusivas e arbitrárias na gestão do conteúdo na rede por parte de governos, provedores e corporações. A existência de mecanismos de bloqueio ataca diretamente o princípio da neutralidade da rede, na medida em que impõe o controle do tráfego de serviços e informação e a discriminação dos pacotes de informação.

A construção de indicadores de liberdade e privacidade na rede apenas em termos formais pode implicar o reforço do argumento segundo o qual, apesar dos *lobbies* e pressões corporativas e governamentais, os países ocidentais mantêm a internet livre, restringindo-se a ideia de censura apenas aos países asiáticos e árabes nos quais a rede esteja a cargo dos aparelhos de Estado locais. O entendimento reiteradamente apresentado por ativistas ligados não apenas aos direitos da internet, mas também aos direitos civis e do consumidor, é o de que a *internet está sob ataque*, porque se observa haver um amplo movimento técnico-jurídico para que as camadas da rede fundam-se sob um mesmo controle, ou seja, para que as empresas que controlam a infraestrutura controlem também o fluxo da informação. Essa fusão ataca direta e violentamente o princípio da neutralidade, garantido exatamente pela separação do controle das camadas – ou, dito de outra forma, pela garantia do não controle.

Neste trabalho, comparando-se o caso norte-americano e o caso brasileiro de sistemas de legislação e controle da internet, a análise desloca-se dos aspectos mais formais das dificuldades de acesso e/ou barreiras técnicas para a dinâmica de trocas de informações na rede, como no caso do relatório da Freedom House, para se compreender o arcabouço de políticas globais e multilaterais em que estão inseridas as normativas jurídicas específicas e ações locais de *enforcement* dessas políticas. Nesse sentido, cabe questionar e relativizar a posição dos Estados Unidos como uma das nações melhor colocadas no *ranking* de países com mais garantias de acesso livre à rede, principalmente após o governo admitir que mantém monitoramento expressivo, sem haver ordem judicial, dos principais serviços de comunicação na rede. Esse é um caso claro no qual mais regulação significa menos direitos.

Por sua vez, há um extenso número de países que aprovaram legislações que garantem juridicamente a manutenção da neutralidade da rede, como

Chile, Colômbia, Equador, México, Peru, Holanda e Bélgica, entre outros. Nada obstante, essas prerrogativas estarão garantidas somente na medida em que os grandes provedores de serviço, a maioria notadamente hospedada nos Estados Unidos, passem a atender às legislações locais. Nesse cenário, a disputa entre o global e local assume contornos multilaterais em que as pressões corporativas ditam as principais regras da rede.

Para concluir, retomemos o argumento de Bourdieu (1989), ao apontar com veemência que as práticas e os discursos jurídicos são produto do funcionamento de um campo cuja lógica está determinada pelas relações de força específicas que lhe conferem estrutura e orientam os conflitos de competência. E, ainda em termos da análise bourdiana, poder-se-ia dizer que a constituição do campo jurídico de regulação de direitos na internet seria o princípio mesmo de constituição da própria rede, compreendida não apenas como uma infraestrutura técnica, mas como, no sentido dado ao termo por Geertz (1989), um sistema cultural, no qual estão implicadas certas formas de pensar e significar o mundo no qual estamos inseridos, seja este "real" ou "virtual".

Referências

ANDERSON, N. How Wikileaks killed Spain's anti-P2P law. *Ars Technica*, 22 Dec. 2010. Disponível em: < http://arstechnica.com/tech-policy/2010/12/how-wikileaks-killed-spains-anti-p2p-law/>. Acesso em: 30 ago. 2013.

APPADURAI, A. *Globalization*. Durham: Duke University Press, 2001.

BARBROOK, R.; CAMERON, A. *A ideologia californiana*. 1996. Disponível em: <http://pt.scribd.com/doc/149089294/A-Ideologia-Californiana-1>. Acesso em: 24 abr. 2013.

BARLOW, J. P. *Declaration of the independence of cyberspace*. 1996. Disponível em: <https://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration>. Acesso em: 26 jun. 2013.

BASSO, M. *Propriedade intelectual na era pós-OMC*. Porto Alegre: Livraria do Advogado, 2005.

BENKLER, Y. *The wealth of networks*: how social production transforms markets and freedom. New Haven: Yale University Press, 2006.

BENKLER, Y. A economia política dos *commons*. In: GINDRE, G. et al. (Org.). *Comunicação digital e a construção dos commons*. São Paulo: Perseu Abramo, 2007. p. 11-20.

BENKLER, Y. WikiLeaks and the PROTECT-IP Act: a new public-private threat to the internet commons. *Daedalus*, v, 140, n. 4, p. 154-164, Fall 2011. Disponível em: <http://www.mitpressjournals.org/doi/abs/10.1162/DAED_a_00121>. Acesso em: 1 set. 2012.

BOURDIEU, P. A força do direito: elementos para uma sociologia do campo jurídico. In: BOURDIEU, P. *O poder simbólico*. Rio de Janeiro: Bertrand Brasil, 1989. p. 209-254.

BOURDIEU, P. Da regra às estratégias. In: BOURDIEU, P. *Coisas ditas*. São Paulo: Brasiliense, 1990. p. 77-95.

BOYLE, J. The second enclosure movement and the construction of the public domain. *Law and Contemporary Problems*, v. 66, n. 33, p. 33-74, Winter/Spring 2003.

BRASIL. *Lei nº 12.735, de 30 de novembro de 2012*. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, 2012a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 10 ago. 2013.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Brasília, 2012b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 10 ago. 2013.

BURAWOY, M. Manufacturing the global. *Ethnography*, London: Sage, v. 2, n. 2, p. 147-159, 2001.

CASTELLS, M. *A era da informação*: economia, sociedade e cultura. São Paulo: Paz e Terra, 2000.

COLEMAN, E. G. The political agnosticism of free and open source software and the inadvertent politics of contrast. *Anthropological Quarterly*, v. 77, n. 3, p. 507-519, 2005.

DIBBELL, J. *A rape in cyberspace*. 1998. Disponível em: <http://www.juliandibbell.com/articles/a-rape-in-cyberspace/>. Acesso em: 26 jun. 2013.

DUPAS, G. Propriedade intelectual: tensões entre a lógica do capital e os interesses sociais. In: VILLARES, F. *Propriedade intelectual*: tensões entre o capital e a sociedade. Rio de Janeiro: Paz e Terra, 2007. p. 15-24.

EVANGELISTA, R. Os donos dos cabos querem controlar a rede. *Dicas-L*. Zona de Combate. 10 out. 2006. Disponível em: <http://www.dicas-l.com.br/zonadecombate/zonadecombate_20061010.php#.UgfKdG2mVVe>. Acesso em: 10 ago. 2013.

FISCHER, M. *Futuros antropológicos*: redefinindo a cultura na era tecnológica. Rio de Janeiro: Zahar, 2011.

FRANCE. *LOI n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet*. Paris, 12 jun. 2009. Disponível em: <http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432>. Acesso em: 26 jun. 2013.

GEERTZ, C. *A interpretação das culturas*. Rio de Janeiro: LTC, 1989.

GOLDSMITH, J.; WU, T. *Who controls the internet*: illusions of a borderless world. New York: Oxford University Press, 2006.

KELLY, S.; COOK, S.; TROUNG, M. (Ed.). *Freedom on the net 2012*: a global assessment of internet and digital media. Washington: Freedom House, 2012. Disponível em: <http://www.freedomhouse.org/sites/default/files/resources/FOTN – Full Report_0.pdf>. Acesso em: 8 mar. 2013.

LEAL, O. F.; SOUZA, R. H. V. Ciência, tecnologia e patentes: o regime global de propriedade intelectual. In: FONSECA, C. ROHDEN, F.; MACHADO, P. S. *Ciências na vida*: antropologia da ciência em perspectiva. São Paulo: Terceiro Nome, 2012. p. 277-302.

LESSIG, L. *The future of ideas*: the fate of commons in a connected world. New York: Randon House, 2001.

LIU, E. C. *Amendments to the Foreign Intelligence Surveillance Act (FISA) extended until June 1, 2015*. Washington: Congressional Research Service, 2011. Disponível em: <http://www.fas.org/sgp/crs/intel/R40138.pdf>. Acesso em: 26 jun. 2013.

NOGUEIRA, M. A. Enforcement. In: DI GIOVANNI, G.; NOGUEIRA, M. A. (Org.). *Dicionário de políticas públicas*. São Paulo: FUNDAP, 2013. Disponível em: <http://dicionario.fundap.sp.gov.br/Verbete/92>. Acesso em: 20 ago. 2013.

RIAA V. THE PEOPLE: five years later. Eletronic Frontier Foundation, 2008. Disponível em: <https://www.eff.org/wp/riaa-v-people-five-years-later>. Acesso em: 30 ago. 2013.

SOLAGNA, F. *Internet, software livre e propriedade intelectual*: estratégias de *enforcement* e as mobilizações de contestação no cenário brasileiro. Trabalho de conclusão de curso (Bacharelado Ciências Sociais)–Instituto de Filosofia e Ciências Humanas, Universidade Federal do Rio Grande do Sul, Porto Alegre 2012. Disponível em: <http://hdl.handle.net/10183/66989>. Acesso em: 20 ago. 2013.

SOLAGNA, F.; SOUZA, R.; LEAL, O. F. Regime de propriedade intelectual: controle, liberdade e conflitos na gestão de bens intangíveis no contexto digital. In: WACHOWICZ, M. (Org.). *Propriedade intelectual e internet*. Curitiba: Juruá, 2011. v. 2., p. 59-90.

SOUZA, R. H. V.; SOLAGNA, F. *Tomando a* sopa *e derrubando a* pipa: propriedade intelectual e mobilização transnacional. Trabalho apresentado no 3º Encontro Internacional de Ciências Sociais, Universidade Federal de Pelotas, Pelotas, 2012.

TONG-HYUNG, K. New online copyright law baffles users. *Korea Times*, 21 jul. de 2009. Disponível em: <http://www.koreatimes.co.kr/www/news/biz/2009/07/123_48856.html>. Acesso em: 26 jun. 2013.

UNIÃO EUROPEIA. Directiva 2001/29/CE do parlamento europeu e do conselho de 22 de maio de 2001 relativa à harmonização de certos aspectos do direito de autor e dos direitos conexos na sociedade da informação. *Jornal Oficial das Comunidades Europeias*, ano 44, L 167, p. 10-19, 22 jun. 2001. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32001L0029&from=ES>. Acesso em: 26 jun. 2013.

UNITED STATES. The Computer Matching and Privacy Protection Ammendment of 1990 and the Privacy Act of 1974. *Federal Register*, v. 56, n. 78, p. 18599-18601, 23 abr. 1991. Disponível em: <http://www.whitehouse.gov/sites/default/files/omb/inforeg/computer_amendments1991.pdf>. Acesso em: 26 jun 2013.

UNITED STATES. *Telecommunications Act of 1996*. Washington, 8 fev. 1996. Disponível em: <http://www.fs.fed.us/specialuses/commsites/documents/pl-104-104.pdf>. Acesso em: 26 jun. 2013.

UNITED STATES. *Digital Millennium Copyright Act*. Washington, 28 out. 1998. Disponível em: <http://beta.congress.gov/105/plaws/publ304/PLAW-105publ304.pdf>. Acesso em: 26 jun. 2013.

UNITES STATES. *USA Patriot Act*. Washington, 16 out. 2001. Disponível em: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm>. Acesso em: 26 jun. 2013.

UNITED STATES. Federal Communications Commision. *Policy state*. Washington, 23 set. 2005. Disponível em: <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf>. Acesso em: 26 jun. 2013.

UNITED STATES. *Network Neutrality Act of 2006*. Washington, 2 maio 2006. Disponível em: <http://beta.congress.gov/109/bills/hr5273/BILLS-109hr5273ih.pdf>. Acesso em: 26 jun. 2013.

UNITED STATES. *Internet Freedom Preservation Act of 2008*. Washington, 12 fev. 2008. Disponível em: <http://beta.congress.gov/110/bills/hr5353/BILLS-110hr5353ih.pdf>. Acesso em: 26 jun. 2013.

UNITED STATES. *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011*. Washington, 26 maio 2011a. Disponível em: <http://beta.congress.gov/112/bills/s968/BILLS-112s968rs.pdf>. Acesso em: 26 jun. 2013.

UNITED STATES. *Stop Online Piracy Act*. Washington, 26 out. 2011b. Disponível em: <http://beta.congress.gov/112/bills/hr3261/BILLS-112hr3261ih.pdf>. Acesso em: 26 jun. 2013.

UNITED STATES. *Cyber Intelligence Sharing and Protection Act*. Washington, 7 maio 2012a. Disponível em: <http://beta.congress.gov/112/bills/hr3523/BILLS-112hr3523rfs.pdf>. Acesso em: 26 jun. 2013.

UNITED STATES. Department of Justice. *Overview of the Privacy Act of 1974*. 2012b. Disponível em: <http://www.justice.gov/opcl/1974privacyact-2012.pdf>. Acesso em: 26 jun. 2013.

UNITED STATES. Department of Treasury. Internal Revenue Service. *Internal revenue manual. Disclosure of official information. Computer Matching and Privacy Protection Act.* 17 set. 2013. Disponível em: <http://www.irs.gov/irm/part11/irm_11-003-039.html>. Acesso em: 20 ago. 2013.

WU, T. Network neutrality, broadband discrimination. *Journal on Telecommunication & High Tech Law*, v. 2, p. 141-170, 2003.

WU, T. Copyrights communications policy. *Michigan Law Review*, v. 103, p. 278-366, 2004.

Recebido em: 26/08/2013
Aprovado em: 20/12/2013