INFORMAÇÃO E PODER NA ARENA DA INTERNET[1]

Rodrigo Moreno Marques[*]
Marta Macedo Pinheiro[**]

RESUMO Informação e conhecimento sempre foram fontes de poder. Atualmente, cada vez mais, as leis que compõe as políticas de informação nacionais assumem importante papel de mediadoras dos interesses conflitantes que surgem na arena da Internet. Esse é o desafio do Marco Civil da Internet no Brasil, projeto de lei em tramitação no Câmara dos Deputados. O objetivo do presente ensaio é apresentar uma análise da origem e do teor desse aparato jurídico, buscando descrever principalmente os embates que envolvem o princípio da neutralidade da rede e a coleta massiva de informação dos usuários. Essas duas temáticas são cruciais para a manutenção ou abolição do caráter livre e isonômico que foi atribuído à *web* quando ela foi concebida. Encerrando a análise, questiona-se o futuro desse projeto de lei, tendo em vista os grandes conflitos que nele residem.

Palavras-chave: Internet. Brasil. Informação e poder. Neutralidade da rede. Política de informação.

[*]Mestre em Ciência da Informação pelo Programa de Pós-graduação em Ciência da Informação da Universidade Federal de Minas Gerais, Brasil. Professor em cursos de graduação e pós-graduação na Universidade FUMEC, Brasil.
E-mail: rodrigomorenomarques@yahoo.com.br

[**] Doutora em Ciência da Informação pela Universidade Federal do Rio de Janeiro, Brasil. Docente permanente no Programa de Pós-graduação em Ciência da Informação da Universidade Federal de Minas Gerais.
E-mail: martakerr@gmail.com.

1 INTRODUÇÃO

Informação e conhecimento sempre foram fontes de poder. Na atualidade empresas e governos empregam a Internet e modernas tecnologias como a inspeção profunda de pacotes (*deeppacketinspection*) para rastrear e sistematicamente coletar informações.

Nesse contexto, cada vez mais as leis e regulamentos que compõe as políticas de informação nacionais ganham importância como mediadoras dos conflituosos interesses que surgem na arena da Internet. Esse é o desafio do Marco Civil da Internet no Brasil, projeto de lei que se encontra atualmente em tramitação na Câmara dos Deputados.

O objetivo do presente ensaio é apresentar uma análise da origem e do teor desse marco regulatório, buscando descrever principalmente os embates que envolvem a chamada neutralidade da rede e a coleta massiva de informação dos usuários. Esses dois temas, que fazem parte do universo das políticas de informação para a Internet, são cruciais para a manutenção ou abolição do caráter livre e isonômico atribuído à *web* quando ela foi concebida. As deliberações da sociedade em relação a essas duas temáticas determinarão o futuro da rede mundial de computadores e o uso que dela fazemos.

Em sintonia com os argumentos de Reis (2002), a abordagem que propomos pressupõe que

1 Esse trabalho foi realizado no âmbito do Programa de Doutorado Sanduíche no Exterior (PDSE) que contou com bolsa da CAPES – Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, Processo No. BEX 0255/12-2.

a legislação é uma estratégia de mediação através da qual os diversos interesses ganham representação e legitimidade. Sob esse ponto de vista, o aparato jurídico representa um espaço onde se efetivam embates ideológicos e políticos em favor de interesses de diferentes atores sociais.

Antes de apresentar a origem do Marco Civil da Internet e a análise do seu teor, serão discutidos os conceitos de política de informação, neutralidade da rede e coleta massiva de informações dos usuários. Ao fim da análise, o futuro desse projeto de lei é questionado, tendo em vista os grandes conflitos que nele residem.

2 POLÍTICA DE INFORMAÇÃO PARA A INTERNET

Braman (2006) define política de informação como as leis e regulamentos que lidam com qualquer estágio da cadeia de produção da informação, onde inclui-se sua criação, processamento (cognitivo e técnico), armazenamento, distribuição, busca, recuperação, uso e destruição. Assim, a autora demarca o domínio das políticas públicas que regulam as dinâmicas da informação, da comunicação e da cultura.

Essa abrangente definição de política de informação abarca diversos temas que ganham relevância com a expansão da Internet como, por exemplo, as temáticas do direito de cópia (*copyright*), direito autoral, liberdade de expressão, transparência governamental, direito de acesso à informação, difusão e compartilhamento de arquivos, controle e restrição de conteúdos, crimes eletrônicos, defesa nacional contra cyberataques, dentre outros.

É importante destacar que cada lei e regulamento voltado para o fluxo de informação e conhecimento na *web* geralmente afeta simultaneamente diferentes temas do rol listado. As políticas de informação serão, portanto, mediadoras de conflitos de interesses que se manifestam em diversas esferas que inter-relacionam-se. Este argumento alinha-se com a percepção de Braman (2006) acerca da crescente pluralidade de atores sociais envolvidos no universo da informação e a diversidade em seus discursos e interesses.

Dado o caráter amplo da categoria política de informação definida pela autora, sua adoção para os fins analíticos exige o estabelecimento de recortes que limitem as temáticas abordadas, sem que esses recortes nos façam perder de vista a totalidade complexa dos fenômenos sociais em análise. Nesse sentido, estabelecemos como focos principais da investigação os aspectos ligados aos temas neutralidade da rede e coleta massiva de informações dos usuários, conceitos esses que serão apresentados e discutidos a seguir.

3 O PRINCÍPIO DA NEUTRALIDADE DA REDE

O princípio da neutralidade da rede, que marcou os primórdios da Internet, estabelece que os responsáveis pela infraestrutura da rede e seus serviços não podem discriminar conteúdos que nela circulam, nem aplicar filtros que discriminem parâmetros como a identificação do usuário, origem e destino da transmissão, conteúdo transmitido, *software* e *hardware* adotados. Em outras palavras, segundo essa concepção que também é chamada de princípio da não discriminação, todos os conteúdos devem ser tratados com isonomia pela infraestrutura da rede e seus usuários devem estar livres de interferência (RILEY; SCOTT, 2009).

Ao defender os princípios que devem guiar a governança e o uso da *web* no Brasil o Comitê Gestor da Internet no Brasil defende que a "Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos , não sendo admissíveis motivos políticos, comerciais, religiosos, culturais; ou qualquer outra forma de discriminação ou favorecimento" (CGI, 2009).

Esse tema ganhou os noticiários em 2007 quando foi divulgado que a Comcast, uma das maiores empresas de telecomunicações dos Estados Unidos, estava praticando o chamado *trafficshapping*, ou seja, estava bloqueando ou retardando a transmissão de alguns tipos de conteúdo. Na ocasião, a empresa alegava que era forçada a adotar tal medida pois os internautas que compartilhavam arquivos em aplicações *peer-to-peer* estavam congestionando a rede (RILEY; SCOTT, 2009; KELLY *et al.*, 2012)[2]. Em 2008, tornou-se público que as maiores empresas de

2 A Federal CommunicationCommission (órgão regulador das telecomunicações nos Estados Unidos) iniciou longa batalha jurídica contra a empresa Comcast. A FCC pretendia acabar com a discriminação e o bloqueio de tráfego por parte da Comcast, enquanto essa companhia questionava a autoridade da FCC para regular a matéria.

telecomunicações do mundo e provedores de acesso também adotavam a mesma prática.[3]

Outro argumento apresentado pelas empresas que defendem o fim da neutralidade da rede é o interesse em criar diferentes classes de serviços para o fornecimento de acesso à Internet. Nesse sentido, a Telebrasil, associação que representa as maiores companhias de telecom que atuam no Brasil, defende a "oferta diversificada de serviços para diferentes perfis de usuários", ou seja, o fornecimento de velocidade de transmissão maior para usuários que podem pagar mais. Segundo o discurso institucional da associação, "não se pode tratar como igual aquilo que é por natureza desigual, já que colocar todos no mesmo patamar pode significar prejuízo de muitos em função do privilégio de alguns" (TELEBRASIL, 2012).

As justificativas das empresas não revelam, no entanto, algumas controvérsias que elas preferem não divulgar.

Em primeiro lugar, a limitação no tráfego de Internet praticado por elas é um meio para atingir outro objetivo diferente do combate ao congestionamento. Trata-se da corrida para cumprimento das metas de retorno financeiro que disparam gatilhos de fartos bônus trimestrais para diretores e acionistas das companhias. A prática do *trafficshapping* permite a expansão da lucratividade das empresas no curto prazo pois posterga dispendiosos investimentos necessários para a ampliação na capacidade das suas sobrecarregadas redes, induzindo à queda da qualidade do serviço e ao congestionamento.[4]

Adicionalmente, sem o princípio da neutralidade da rede surge a possibilidade de discriminação de tráfego em favor de acordos comerciais estabelecidos entre as operadoras de telecomunicações e os produtores/provedores de conteúdo. Esse tipo de pacto permite que uma operadora de telecom priorize a oferta de alguns conteúdos específicos, bloqueando ou reduzindo a velocidade dos demais. Dessa maneira, elimina-se o princípio da livre circulação de informação e conhecimento estabelecido nos primórdios da Internet e coloca-se em risco tanto a liberdade de escolha do usuário, quanto à isonomia no direito de difundir idéias, sufocando a diversidade cultural e a inovação criativa.

Também é preciso contestar os valores que norteiam a criação de classes de serviço para atender cada perfil de usuário e seu respectivo poder aquisitivo. Alguns defensores dessa idéia o fazem comparando-a com as ruas e vias públicas de uma cidade, onde existem veículos com diferentes capacidades e velocidades (LEVY, 2012)[5].

No entanto, esta mesma metáfora das ruas e do trânsito de automóveis também pode ser estendida para revelar a perversidade dessa lógica quando aplicada à Internet. Se houvesse diferentes classes de serviço para os carros privados que usam as vias públicas de uma cidade, elas deixariam de ser bem comum. Assim como em uma Internet com classes de serviço, no caso do trânsito urbano poderia haver um espaço exclusivo para a circulação dos mais abastados, assim como prioridade nos congestionamentos para motoristas de maior poder aquisitivo. Levando-se essa concepção ao extremo, os defensores da lógica mercantil poderiam considerar legítimo que o destino de um veículo ou a rentabilidade associada ao destino – seja ele um *shopping center* ou uma escola pública, por exemplo – influenciasse na determinação da prioridade daquele automóvel em nosso caótico trânsito. Na esfera da rede mundial de computadores, isso equivale à defesa da priorização, por parte das empresas de telecom, do tráfego de certos conteúdos que tenham sido objeto de acordos comerciais com seu produtor ou provedor, seja ele, por exemplo, a Time Warner, o UOL - Universo Online ou as Organizações Globo.

Portanto, a essência do debate sobre a neutralidade da rede é o confronto entre dois pontos de vista antagônicos que podem ser resumidos nas seguintes indagações. A Internet

3 O documento *FirstResultsfromVuze Network Monitoring Tool*, divulgado em 18 de abril de 2008, revelou o percentual de interrupções das conexões de internautas que se prontificaram a participar de um monitoramento *online* feito com o aplicativo Vuze Plug-In. Constam no relatório como praticantes de *trafficshapping* todas as maiores operadoras de telecomunicações nacionais e internacionais. Naquela ocasião, o índice de interrupção de tráfego em algumas delas era maior do que 20%. O relatório está disponível em <http://download.ebooks6.com/First-Results-from-Vuze-Network-Monitoring-Tool-Released-April-download-w29748.pdf>. Acesso em: 15 jan. 2013.

4 Tendo em vista os notórios problemas apresentados nos últimos anos pelas redes de telecomunicações no Brasil, bem como a baixa qualidade e falta de transparência na prestação do serviço de acesso à Internet no país, a ANATEL - Agência Nacional de Telecomunicações publicou a Resolução nº 574, de 28 de outubro de 2011, que aprovou o Regulamento de Gestão da Qualidade do Serviço de Comunicação Multimídia. Ele entrou em vigor em outubro de 2012 (ANATEL, 2011).

5 Esse autor representa o Sinditelebrasil - Sindicato das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal.

representa um bem comum, direito universal de todos que dela precisam para tomar parte ativa na sociedade da informação? Ou estamos diante de uma rede de caráter privado cuja evolução e expansão deve ser pautada exclusivamente pela lógica do mercado e do lucro?

Essa peleja evidencia as contradições da sociedade da informação quando ela é assaltada por grandes interesses econômicos que têm tido forte influência nos processos de construção de políticas públicas.

Passemos ao segundo eixo temático proposto. A questão da coleta massiva de informação dos usuários também envolve interesses econômicos, mas nesse caso surgem também outros argumentos ligados ao combate ao crime e à defesa nacional.

4 COLETA MASSIVA DE INFORMAÇÃO DOS USUÁRIOS: a avidez do mercado

Uma tecnologia que ganhou o noticiário no Brasil em outubro de 2012 chamava de coleta massiva de dados uma idéia que preferimos designar coleta massiva de informações dos usuários.

Naquela ocasião, a empresa Vivo, pertencente à espanhola Telefónica, recebeu notificação o Ministério da Justiça brasileiro por meio do Departamento de Proteção e Defesa do Consumidor para que prestasse esclarecimentos sobre o produto SmartSteps que estava em fase de testes e prestes a ser ofertado nos mercados do Brasil, Alemanha e Reino Unido (BORBA, 2012; REUTERS, 2012).

Trata-se da proposta de comercialização de informações dos usuários de telefonia móvel coletados por um sistema capaz de registrar deslocamentos em tempo real, dentre outros aspectos do perfil pessoal dos clientes como sexo, idade e alguns dos seus hábitos. O produto SmartSteps é o primeiro da Telefonica Dynamics Insights, subsidiária responsável por explorar comercialmente a coleta massiva de informações dos clientes da operadora.[6]

Esse não é um caso isolado. No mercado de bens intangíveis, grandes bases de dados dinâmicas de comportamento pessoal são um tipo valioso de mercadoria que está em franca expansão. Esse tipo de iniciativa acompanha o avanço e a sofisticação dos mecanismos de publicidade dirigida[7], que passam a explorar cada vez mais a convergência digital, a evolução tecnológica das redes móveis e a ubiquidade da Internet.

Pesquisas de marketing e rastreamento em tempo real são apenas algumas das aplicações para esse tipo de tecnologia já bastante difundida em diversos segmentos como o de cartão de crédito, bancos, supermercados, telecomunicações, sistemas operacionais, serviços de e-mail, mecanismos de busca, redes sociais, dentre outros.

Algumas tecnologias que executam a coleta massiva de informações alertam previamente seus usuários sobre a prática, deixando para eles a opção de não usar a ferramenta caso não concordem com a invasão da sua privacidade. No entanto, muitas vezes a vigilância eletrônica é feita de maneira oculta ou sem deixar alternativas para aqueles que encontraram esse tipo de mecanismo embarcado em algum produto recém adquirido. Dois exemplos de práticas desse tipo são emblemáticos.

Em julho de 2012 o órgão Federal Trade Commission (FTC) do governo dos Estados Unidos estabeleceu a multa com valor recorde de 22,5 milhões de dólares a ser paga pela empresa Google[8]. A empresa foi multada por ter, durante vários meses entre 2011 e 2012, rastreado os internautas por meio do navegador Safari adotado em produtos Apple como iPhones, iPads e computadores Mac. Os usuários do *web browser*eram informados que as ferramentas de rastreamento (*cookies*) estavam bloqueados na configuraçãoinicial do navegador. No entanto, o código criado pela Google abria as portas do programa, sem que o usuário percebesse, permitindo a instalação do *cookie*DoubleClick

6 A apresentação comercial do produto SmartSteps e dos seus recursos está disponível em: <http://dynamicinsights.telefonica.com/what-is-smart-steps>. Acesso em:15 jan. 2013.

7 Segundo Turow (2008, p.180), os conceitos de *targetedadvertising* (publicidade dirigida), *targetedtracking*(rastreamento dirigido), *personalizedadvertising* (publicidade personalizada) ou *behaviouraladvertising* (publicidade comportamental) referem-se as práticas das empresas de marketing ou mídia que registram as atividades dos clientes ou potenciais clientes para capturar seus interesses pessoais e apoiar a tomada de decisão acerca dos produtos a serem ofertados à eles.

8 O valor aparentemente alto da multa aplicada revela-se insignificante quando comparado com a receita trimestral da empresa naquela ocasião, que era de 12,21 bilhões de dólares (KRAVETS, 2012). No período de janeiro a junho de 2012 a companhia faturou com publicidade 21 bilhões de dólares, o que representa mais que toda mídia impressa dos Estados Unidos (RICHTER, 2012).

ID, a principal ferramenta de rastreamento da Google (ANGWIN e VALENTINO-DEVRIES, 2012; KRAVETS, 2012).

Em outra artimanha tecnológica, com o lançamento do iPhone5, a empresa Apple embarcou em seus dispositivos um novo mecanismo de rastreamento de informações e hábitos dos internautas. Chamado de identificador para anunciantes (*identifier for advertisers*), o novo recurso aprimorou a tecnologia de rastreamento que já existia na linha Apple. O identificador para anunciantes é mais sofisticado que seu antecessor e guarda vários obstáculos para aqueles que não desejam ser rastreados: (i) o rastreamento vem habilitado como opção de fábrica e muitos usuários não estão cientes da sua existência; (ii) caso o usuário deseje desabilitá-lo, ele terá dificuldade de encontrar essa opção pois ela não foi inserida no menu *Privacy* como se esperaria, mas sim em um tortuoso caminho que passa pelos menus *Settings*, *General*, *About* e *Advertising*; (iii) o controle de rastreamento foi designado *Limit Ad Tracking* e precisa ser colocado na posição *on* (ligado), o que pode gerar confusão pois o termo 'ligado' nesse caso significa rastreamento desligado; (iv) e o que é pior, se seguir todos esses passos anteriores, o internauta continuará a ter as suas informações pessoais remetidas para os anunciantes, com a diferença que elas carregarão um aviso que registra o seu desejo de não ser rastreado, cabendo ao anunciante acatar ou não essa decisão (EDWARDS, 2012; STAMPLER, 2012).

Esses exemplos ilustram a avidez do mercado em capturar sistematicamente informações e hábitos pessoais, ignorando o princípio do direito à privacidade. Mas esse tipo de prática não é empregado apenas para fins econômicos. Sua adoção é defendida por instituições governamentais que alegam a necessidade de combater o crime e promover a defesa nacional.

5 AVANÇA O CONTROLE DO ESTADO

No final do século XVIII, Bentham (1791) concebeu o Panopticon, um modelo de edificação a ser empregado quando os ocupantes precisavam ser mantidos sob constante vigilância. Na ausência das tecnologias de informação e comunicação disponíveis hoje, naquela ocasião a inspeção permanente seria obtida por meio de uma solução arquitetônica. Em um edifício circular, os apartamentos ou celas ocupariam a sua circunferência e o alojamento da equipe de vigilância seria posicionado no centro do edifício. Todos os detalhes daquela arquitetura foram meticulosamente pensados para permitir que os vigiados não enxergassem os vigilantes. Segundo o autor, o modelo era particularmente útil para presídios, indústrias e fábricas em geral, abrigos para pobres, hospitais, lazaretos, sanatórios e escolas.

Diferentemente do objetivo financeiro que move hoje o rastreamento voltado para a publicidade dirigida, o Panopticon nascido nos primórdios do capitalismo destinava-se ao controle dos indivíduos. Conforme explica o seu criador, tratava-se de "um novo modo de se obter poder da mente sobre a mente, em uma dimensão até então inédita" (BENTHAM, 1843, p.39).

Assim, a idéia de Bentham representa um curioso prelúdio para a nova forma de coleta massiva de informações que o Estado implementa atualmente com as mais avançadas tecnologias disponíveis.

Para Braman (2006), no estado informacional o controle social, antes arquitetado no modelo panopticon de vigilância, evolui para o panspectron, pois o controle sobre o intangível não determina o local, nem o tempo e se realiza sem previsão de sua ação, pois não se sabe onde e quando vão se manifestar. No modelo panspectroné que são pensados e exercidos os dispositivos jurídicos e maquínicos do estado informacional, como o do Echelon, do sistema bancário, das identidades não somente numéricas, mas signaléticas e distintivas através dos robôs de busca.

> O panspectron corresponde ao controle contínuo, digital e ondulatório [...]. O panspectron age em todos os sentidos, abarcando desde as intenções mais utilitárias e "benéficas" ao indivíduo, como as tecnologias de rastreamento dos sites de comércio eletrônico que detectam os interesses do comprador, até propósitos governamentais de privação de direitos individuais (SILVA; PINHEIRO, 2012, p.84).

As políticas de informação para a *web* da China e dos Estados Unidos ilustram o avanço do controle informacional estatal.

Segundo o artigo 35 da constituição chinesa, seus cidadãos "gozam de liberdade de expressão, de imprensa, de reunião, de associação, de desfile e de manifestação" (REPÚBLICA POPULAR DA CHINA, 2004).

No entanto, esses direitos subordinam-se ao poder do Partido Comunista Chinês, conforme explica o relatório em que Kelly *et al.* (2012) apresentam alguns aspectos das políticas de informação para a Internet de diferentes países. A respeito da China, os autores apontam diversas práticas contrárias ao princípio da neutralidade da rede e descrevem as técnicas de coleta massiva de informações adotadas pelo Estado chinês em nome da defesa nacional e do combate ao crime.

Desde 2009 aplicações como Youtube, Facebook e Twitter têm permanecido bloqueadas na maior parte do tempo em território chinês. Insurreições e protestos são considerados pelo Estado motivos razoáveis para desligamento de sistemas de comunicações, *sites* e *blogs*. O acesso anônimo à Internet tem sido combatido, sendo substituído pela exigência de registro de nomes reais.

Ainda segundo o relatório, para levar a cabo um amplo programa de rastreamento invasivo, as conexões internacionais da rede chinesa possuem controle centralizado. Avançados sistemas automatizados implementam filtros de palavras chaves que vasculham conteúdo de *sites*, mensagens em trânsito na Internet, e-mails, redes sociais, telefonia celular e dispositivos móveis em geral.[9]

Curioso notar que, devido à criatividade dos usuários para driblar os sofisticados filtros das ferramentas de rastreamento, dezenas de milhares de pessoas são empregadas pelo governo chinês para inspecionar o conteúdo que escapa desses modernos sistemas automatizados de busca (KELLY *et al*., 2012).

Lemon (2002), Goldsmith e Wu (2006) e Kelly *et al.*(2012) destacam que, para atuar no mercado de Internet da China, as empresas privadas também precisam tomar parte ativa na inspeção de conteúdo com equipes e *softwares* próprios, caso queiram manter suas licenças. A exigência é imposta a pequenos estabelecimentos como cafés e hotéis e também à grandes empresas, como a Yahoo, que são obrigadas a aderir aos termos do "Compromisso público sobre auto-disciplina para a indústria chinesa de internet" (*PublicPledgeon Self-Discipline for The Chinese Internet Industry*). O documento estabelece, por exemplo, que

> Provedores de serviço de acesso à Internet devem inspecionar e monitorar de informações em sites domésticos e internacionais e bloquear acesso aos sites que disseminam informações nocivas para proteger os usuários da Internet na China de influências adversas e informações nocivas (LEMON, 2002).

A comparação das políticas de informação adotadas na China com as iniciativas em curso nos Estados Unidos revela diferente abordagem em relação à censura, porém mostra similaridades no campo da captura massiva de informações pelo Estado.

Nos Estados Unidos, em relação à censura de conteúdos que tenham cunho político ou ideológico, a Internet pode ser considerada relativamente livre. As cortes têm mantido o entendimento que o princípio constitucional da liberdade de expressão aplica-se também à *web*, não havendo restrição legal à publicação anônima. Adicionalmente, a legislação vigente estimula o pleno funcionamento de provedores de serviços e conteúdo ao impedir que eles sejam responsabilizados legalmente por infrações cometidas por usuários. Os internautas, em geral, não são processados pelo governo, exceto nos casos de pornografia infantil e violação de propriedade intelectual. A censura de conteúdos *online* tem se intensificado principalmente com vistas a coibir a violação de direitos de cópia e direitos autorais, bem como para combater divulgação de pornografia infantil, conteúdo indecente e prejudicial, assédio ou comentários difamatórios, informação confidencial, jogos de apostas eletrônicas e crime financeiro[10]. Essas

9 Os mais novos sistemas voltados para vasculhar o conteúdo que circula na Internet implementam técnicas que têm sido chamadas inspeção profunda de pacotes (*deeppacketinspection*). Esses produtos são fornecidos por empresas que formam um mercado pouco transparente, não regulado efetivamente, onde estão incluídas grandes conglomerados empresariais como HP, Nokia, Siemmens e Alcatel. O documento *ImplicationsofDeepPacketInspection (DPI) Internet Surveillance for Society* (FUCHS, 2012) apresenta os recursos destas tecnologias e seu alcance, a partir de um estudo feito com 20 empresas européias e suas soluções, que são fornecidas para governos e instituições privadas. Outra boa fonte de informações sobre o alcance da inspeção profunda de pacotes e das empresas desse segmento é o relatório *The Spyfiles* divulgado recentemente pela organização WikiLeaks (WIKILEAKS, 2012).

10 O Google TransparencyReport apresenta algumas estatísticas sobre os pedidos de remoção de conteúdo por parte de órgãos governamentais e tribunais. Segundo esse relatório, as principais motivações dos pedidos nos Estados Unidos tem sido difamação, privacidade e sergurança, direito autoral/copyright e marca registrada. Disponível em: <http://www.google.com/transparencyreport/removals>. Acesso em: 15 jan. 2013.

questões têm motivado forte ímpeto para criação e implementação de agressiva legislação (KELLY *et al*., 2012).

Em 2011 dois projetos de lei - *Stop Online PiracyAct* (SOPA) e *Preventing Real Online Threatsto Economic Creativityand TheftofIntellectual PropertyAct (Protect IP Act* ou PIPA*)* - foram encaminhados ao congresso norte-americano, com o apoio bipartidário de democratas e republicanos, visando combater infrações de propriedade intelectual por parte de sites hospedados dentro e fora dos Estados Unidos. Na lista das punições estabelecidas por essas propostas de lei, estava o bloqueio do acesso aos *sites* infratores,bloqueio de transações financeiras destinadas aos mesmos, bem como a proibição de exibição dos seus endereços por parte dos mecanismos de busca como Google. Ambos os projetos acabaram não avançando no congresso depois que defensores da liberdade de expressão e da privacidade na Internet manifestaram suas críticas, que encontraram o respaldo dos provedores de conteúdo insatisfeitos com a ideia de serem responsabilizados ecriminalizados por atos dos usuários.

No campo do rastreamento intensivo de informações executado pelo governo norte-americano, é possível afirmar que avança o recrudescido das leis e das práticas institucionais[11]. Em defesa dessas medidas argumenta-se, como na China, a necessidade de combater o crime e promover a defesa nacional. O argumento do combate ao terrorismo tem sido especialmente enfatizado nos Estados Unidos desde o ataque de 11 de setembro de 2001.

O *Patriot Act,* ato do Congresso norte-americano sancionado em 2001, em nome da segurança nacional, permitiu às agências de inteligência governamental ter acesso ilimitado à comunicações entre indivíduos e instituições (via telefone, e-mail ou outros meios), vasculhar informações particulares (financeiras, médicas, dentre outras), sem que fosse necessário ordem jurídica prévia, consentimento ou conhecimento do investigado. Atualmente disposições chave do *Patriot Act* continuam vigentes, tendo elas sido renovadas por mais quatro anos a partir de maio de 2011.[12]

Além do SOPA e do PIPA, um terceiro projeto de lei do campo da política de informação para Internet foi concebido nos Estados Unidos em 2011. Conhecido como *Cyber IntelligenceShari ngandProtectionAct*(CISPA), seus propositores não o justificam com base na proteção da propriedade intelectual, mas sim na necessidade de segurança da Internet, dos seus serviços e usuários. O projeto pretende promover o intercâmbio mais ágil entre empresas e governo das informações que supostamente representam ameaças à segurança. Se nos primeiros projetos de lei citados os provedores de serviço e conteúdo podiam ser responsabilizados legalmente pela infração de *copyright* e direitos autorais, o CISPA tenta transformá-los em agentes a serviço da vigilância governamental e propõe ampla imunidade para as empresas contra responsabilização civil e criminal em casos de monitoramento digital. Adicionalmente, admite-se o rastreamento de comunicações privadas sem supervisão judicial e a motivação para tal prática é definida de maneira tão abrangente que acaba por incluir atividades rotineiras dos internautas (SALVES, 2012; TIMM, 2012)

No âmbito da infraestrutura física para coleta massiva de informações, a lei de 1994 designada *Communications Assistance for Law EnforcementAct* exige que companhias telefônicas e provedores de banda larga projetem seus sistemas de modo a facilitar a interceptação quando agências governamentais tenham autorização para esta prática (KELLY *et al*., 2012).

Desenha-se assim uma infraestrutura de vigilância onipresente cujo núcleo é formado pelos três poderes que compõe o Estado, que expande seu alcance empregando como tentáculos as empresas que atuam no universo da Internet, a exemplo das companhias de telecomunicações, provedores de acesso, provedores de conteúdo, mecanismos de busca e redes sociais.

No caso dos Estados Unidos, o ponto central desta estrutura orwelliana será o Utah Datacenter, cuja inauguração está prevista para 2013. Localizado em Bluffdale, no estado de

11 De acordo com o Google TransparencyReport, os Estados Unidos é líder isolado do ranking de solicitação de dados de usuários por parte de governos e tribunais. O relatório está disponível em: <http://www.google.com/transparencyreport/userdatarequests>. Acesso em: 15 jan. 2013.

12 Outra lei federal, conhecida como *Electronic Communications PrivacyAct*, tem sido interpretada no sentido de permitir que governo norte-americano tenha acesso à *e-mails* e outros documentos privativos por meio de intimações, ainda que não haja aprovação judicial (CDT, 2012).

Utah, esse será um complexo de instalações computacionais capaz de capturar, armazenar e analisar grandes volumes das comunicações que atravessam as redes domésticas e estrangeiras. Com um custo estimado de 2 bilhões de dólares e capacidade de armazenamento da ordem de yottabytes[13], esse está sendo considerado o maior projeto de rastreamento de informações do mundo.[14]

Em direção contrária às tendências observadas nas políticas de informação da China e dos Estados Unidos, quando o Marco Civil da Internet no Brasil foi inicialmente concebido, o princípio da neutralidade da rede foi tomado como basilar e foram criados mecanismos para pôr limites à coleta irrestrita das informações dos usuários.

6 MARCO CIVIL DA INTERNET NO BRASIL: em defesa do bem comum

O artigo 5º da Constituição Federal brasileira garante a liberdade de "manifestação do pensamento" e de "expressão da atividade intelectual, artística, científica e de comunicação, independente de censura ou licença".[15]

Porém, algumas leis limitam essas liberdades e o aparato constitucional forma um quadro complexo para lidar com o discurso *online*. Apesar do governo não empregar técnicas de filtros para bloqueio de publicações na Internet, observa-se um alto número de pedidos de remoção de conteúdo. As maiores restrições à liberdade de expressão na rede decorrem de processos de difamação movidos pelo Estado e por agentes privados contra provedores de conteúdo e de acesso, reivindicando o bloqueio de *sites* e de redes sociais.[16] Os tribunais no Brasil estão divididos em relação à responsabilidade legal dos provedores. Enquanto em alguns processos eles são responsabilizados pelas postagens dos internautas, em outros a responsabilidade tem sido imputada a eles somente caso recebam e não cumpram ordem judicial para a remoção do conteúdo (KELLY *et al.*, 2012).

A respeito das atividades de vigilância na Internet, podemos afirmar que essas não representam um grande problema no Brasil, embora a coleta de informações dos usuários pelo governo tenha aumentado nos últimos anos (KELLY *et al.*, 2012).[17]

Sobre esse tema, o artigo 5º da Constituição Federal estabelece que o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas é inviolável, salvo por ordem judicial em casos de crime e processo penal. Adicionalmente, determina que a intimidade, a vida privada, a honra e a imagem das pessoas também são invioláveis.

Até o final do ano 2012 o Brasil não tinha lei específica para tratar dos crimes relacionados ao universo da Internet. Foi com essa justificativa que o Projeto de Lei 84 foi apresentado ao Congresso em 1999. No entanto, o teor do texto proposto ia muito além do combate aos crimes digitais. Logo após a sua criação, ele passou a ser chamado de AI-5 Digital, apelido que refletia as críticas que passou a receber[18]. Segundo Varella (2011), a aprovação do marco legal da forma originalmente concebida instituiria um cenário de vigilância e monitoramento constante na rede brasileira, colocaria em risco a privacidade dos internautas, limitaria sensivelmente seus direitos e liberdades, e criminalizaria condutas de usuários consideradas cotidianas. No campo cultural, ficariam limitadas as possibilidades de trocas simbólicas, de compartilhamento, de liberdade de acesso a informações e conteúdos.

Se por um lado esse projeto de lei trouxe grande rejeição por parte da sociedade civil, por outro lado ele acabou estimulando um efeito positivo. O polêmico projeto fomentou o início de amplos debates que deram origem ao Marco Civil

13 Um yottabyte equivale a 10^{24} bytes, ou seja, 1.000.000.000.000.000.000.000.000 bytes.

14 Bamford (2012) apresenta uma descrição rica em detalhes do Utah Datacenter. Disponível em: <http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all>. Acesso em: 15 jan. 2013.

15 Ao contrário da legislação dos Estados Unidos, o art. 5º da Constituição brasileira veda o anonimato: "é livre a manifestação do pensamento, sendo vedado o anonimato".

16 Segundo o Google TransparencyReport, as principais motivações dos pedidos de remoção de conteúdo por parte de órgãos governamentais e tribunais no Brasil têm sido difamação, falsificação de identidade, privacidade e segurança, lei eleitoral. Disponível em: <http://www.google.com/transparencyreport/removals>. Acesso em: 15 jan. 2013.

17 De acordo com o Google TransparencyReport, em 2011 o Brasil ocupou o sexto lugar na comparação dos países com mais requisições de informações dos usuários por parte do governo e tribunais (2.318 requisições), enquanto os Estados Unidos (líder do *ranking*) apresentou 12.271 requisições. O relatório está disponível em: <http://www.google.com/transparencyreport/userdatarequests>. Acesso em:15 jan. 2013.

18 AI-5 (Ato Institucional nº 5) foi o quinto decreto emitido pelo governo militar brasileiro (1964-1985) e foi considerado o maior golpe à democracia pelos poderes absolutos concedidos ao regime militar.

da Internet no Brasil, Projeto de Lei 2126/2011, encaminhado à Câmara dos Deputados em agosto de 2011. Atualmente designado Projeto de Lei 5403/2001, ele não foi concebido como marco jurídico dos crimes digitais, que foram objeto das Leis Nº 12.735 e Nº12.737 sancionadas em 30 de novembro de 2012. Em outra direção, o Marco Civil da Internet visa estabelecer os princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determinar as diretrizes para atuação do governo em relação à matéria.[19]

Sua elaboração se deu a partir de um processo de construção coletiva que contou com diversos seminários e audiências públicas em várias capitais do país, além de consultas públicas *online*. Segundo Varella (2012a), esse foi "um processo inédito de participação social na elaboração de uma lei". Concordando com o autor, o documento *Brazilian Civil Rights Framework for the Internet* afirma que esse é "um exemplo da importância e do grande potencial do envolvimento multiparticipativo na elaboração de políticas públicas" (ARTICLE19, 2012, p.5).

A análise do teor do Marco Civil da Internet revela que as questões da neutralidade da rede e da coleta massiva de informações dos usuários são pontos centrais da sua concepção.

O tema neutralidade da rede está presente desde os princípios norteadores da lei, que incluem, conforme artigo 3º, a garantia da liberdade de expressão, comunicação e manifestação de pensamento; a preservação e garantia da neutralidade da rede; e a preservação na natureza participativa da rede.

O artigo 9º detalha esses princípios. Determina que as operadoras de telecomunicações e provedores de acesso têm "o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicativo". Segundo o parágrafo 1º, é admitida a ocorrência de discriminação e degradação de tráfego apenas para priorização de serviços de emergência e se houver necessidade técnica indispensável à fruição adequada dos serviços e aplicações. A regulamentação dessas exceções seria objeto de Decreto, depois de ouvidas as recomendações do Comitê Gestor da Internet no Brasil (CGI.br). O parágrafo 3º veda expressamente o bloqueio e a filtragem de conteúdo por parte dos provedores de conexão (empresas de telecomunicações e provedores de acesso à Internet), ressalvadas as hipóteses da lei citadas no parágrafo 1º.

Visando assegurar a liberdade de expressão e evitar a censura, o projeto de lei estabelece que provedores somente poderão ser responsabilizados civilmente por danos decorrentes de conteúdo publicado por terceiros se, após ordem judicial devidamente justificada, não tomarem as providências cabíveis para tornar indisponível o conteúdo apontado como infrator. Ao usuário acusado, há previsão do direito ao contraditório e ampla defesa em juízo (artigos 15º, 16ºe 17º).

A questão da coleta massiva de informações está contemplada em diversos artigos da lei, a começar pelos princípios estabelecidos no artigo 3º, que incluem também a proteção da privacidade e dos dados pessoais.

Nesse sentido, o texto legal estabelece em seu artigo 7º que são direitos assegurados ao usuário a inviolabilidade da intimidade e da vida privada; a inviolabilidade e o sigilo de suas comunicações pela Internet, salvo por ordem judicial nos casos de investigação criminal ou processo penal; o não fornecimento a terceiros de registros de conexões e de aplicações de Internet, exceto se houver consentimento livre, expresso e informado do usuário ou nas hipóteses anteriormente citadas; o acesso à informações contratuais claras e completas sobre a prestação dos serviços, com previsão expressa de proteção dos registros de conexão e das aplicações de Internet; a exclusão definitiva, quando requerida pelo usuário, dos seus dados pessoais que tenham sido coletados durante sua navegação da Internet.

O parágrafo 3º do artigo 9º também aborda a coleta de informações dos usuários. Segundo ele, aos provedores de conexão (empresas de telecomunicações e provedores de acesso à Internet) é vedado monitorar, filtrar, analisar ou fiscalizar o conteúdo que circula na *web*, ressalvadas as hipóteses anteriormente citadas.

O texto determina que a guarda e a disponibilização dessas informações devem atender a preservação da intimidade, vida privada, honra e imagem das partes direta ou

19 A análise aqui apresentada baseia-se no texto do substitutivo oferecido pelo relator do projeto de lei em 11/07/2012. O texto da lei, o parecer do relator e o substitutivo apresentado por ele estão disponíveis em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1012195&filename=Tramitacao-PL+5403/2001>. Acesso em: 15 jan. 2013.

indiretamente envolvidas. Acrescenta que a possibilidade de identificação do usuário ou seu equipamento por meio das suas informações coletadas só deve ocorrer mediante ordem judicial (artigo 10º).

O artigo 11º acrescenta que os registros de conexão devem ser mantidos sob sigilo em ambiente controlado e de segurança. A responsabilidade pela manutenção desses registros não pode ser transferida a terceiros.

Percebe-se, portanto, que a proposta do Marco Civil da Internet no Brasil tem como objetivos principais assegurar a garantia do pleno direito de acesso à Internet, a salvaguarda da liberdade de expressão e comunicação, a proteção da privacidade e das informações pessoais, e a preservação da neutralidade da rede.

Os interesses divergentes que esse aparato jurídico media ficam evidentes quando se observa o embate entre os seus defensores e os que nele percebem o risco da perda de renda e poder, conforme argumentamos a seguir.

7 CONTRA-ATAQUES DAS EMPRESAS DE TELECOMUNICAÇÕES E DA INDÚSTRIA CULTURAL

Diversas organizações civis têm apoiado o projeto do Marco Civil da Internet nos termos apresentados pelo seu relator, como a SBPC - Sociedade Brasileira para o Progresso da Ciência, a RNP - Rede Nacional de Ensino e Pesquisa, o CTS/FGV - Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, o CGI. br - Comitê Gestor da Internet no Brasil, o IDEC - Instituto Brasileiro de Defesa do Consumidor, a PROTESTE - Associação Brasileira de Defesa do Consumidor, dentre outros.

No segmento empresarial, a proposta legislativa ganhou apoio das empresas cuja atividade relaciona-se diretamente com a oferta de conteúdo, como Facebook, Google e MercadoLivre, que divulgaram em setembro de 2012 uma carta de apoio ao Marco Civil da Internet.[20]

Em direção oposta, manifestações contrárias ao projeto de lei revelam aqueles que viram ameaçados os seus interesses econômicos e os seus instrumentos de poder. Três pontos do texto proposto pelo relator geraram o contra-ataque de representantes das empresas de telecomunicações e da indústria cultural.

Um dos aspectos do projeto de lei que tem gerado discordâncias é o fato que foi atribuído ao Poder Executivo o dever de regulamentar por decreto as exceções à regra da neutralidade da rede, aplicáveis em caso de priorização de serviços de emergência e caso haja necessidade técnica indispensável à fruição de serviços e aplicações.

O *lobby* das operadoras de telecomunicações entende que essa questão crucial deve ser regulada pela Anatel (Agência Nacional de Telecomunicações) e não pelo Governo Federal. Questiona também a exigência de que o Comitê Gestor da Internet no Brasil seja consultado antes da regulamentação (VARELLA, 2012b).

Podemos afirmar que se pleito do mercado de telecom fosse atendido, a visibilidade da regulamentação da rede ficaria ofuscada e o controle público do tema seria obstruído, dada a própria natureza e composição desses órgãos.

No âmbito da Anatel, segundo sua própria ouvidoria, a autarquia requer uma reestruturação pois "o organograma da Agência concentra a competência regulatória no Conselho Diretor, o que induz, estruturalmente, a alguma dificuldade em termos de controle social" (ANATEL, 2003, p. 42). A agência reguladora é deficiente em relação à representatividade da sociedade em suas instâncias e carece de um "aprofundamento mais atento das formas de operacionalização do controle social diante do poder regulado" (ANATEL, 2003, p.51).

Ao defender que a regulamentação da neutralidade de rede deve ficar a cargo da poder executivo, Lemos (2012a) argumenta que nesse caso "há a possibilidade de fiscalização política, permeável à sociedade. Se for a Anatel, a sociedade sai de cena. A questão torna-se "técnica", desacoplada de contrapesos".

A respeito do Comitê Gestor da Internet, Molon (2012) destaca que a composição do órgão inclui representantes do Governo Federal, do setor empresarial, do terceiro setor, da comunidade científica e tecnológica, além de um pesquisador de notório saber em assuntos de Internet. Segundo o autor, essa estrutura é mais

20 A carta de apoio está disponível no *site*: <ttps://docs.google.com/a/oglobo.com.br/document/d/1shVfcpJC7x0XOkBuslx9MyJgl8Kh23Dxsm9JhYsp7wI/edit?pli=1>. Acesso em: 15 jan. 2013.

favorável a uma visão balanceada, que reflita posições maduras e que representem a vontade geral.

Outro aspecto da proposta de lei que tem gerado discórdia é a proibição do monitoramento de usuários por parte dos provedores de conexão. Em relação a esse ponto, as empresas de telecomunicações e provedores de acesso advogam o princípio da isonomia ao solicitar que tenham a mesma prerrogativa atribuída às empresas do ramo de conteúdo, como Facebook e Google.

Contra esse argumento, é preciso esclarecer que a restrição expressamente imposta aos provedores de conexão justifica-se, pois eles têm acesso à todas as informações de navegação dos seus clientes, ao contrário dos *sites* de conteúdo e serviços, capazes de rastrear as informações dos usuários apenas quando seus sistemas são acessados. Objetiva-se, portanto, evitar a concentração de um poder praticamente ilimitado nas empresas de telecomunicações e provedores de acesso. Nesse sentido, Lemos (2012b) argumenta que "se um site faz monitoramento, cabe ao usuário decidir se quer acessá-lo ou não. Mas, se o monitoramento é feito na raiz, pelos provedores [de acesso], a única maneira efetiva de evitar ser monitorado será não acessar a internet ou mudar de país".

Um terceiro embate surgido durante a tramitação do projeto de lei também tem exposto outra controvérsia. Uma recente sugestão de modificação do artigo 15º propõe o acréscimo de um novo parágrafo que abre precedente para que seja eliminada a necessidade de ordem judicial para remoção de conteúdo da *web* nos casos de materiais que firam o direito autoral e seus direitos conexos.

Nota-se que, se acatada essa sugestão, a liberdade de expressão na Internet ficaria cerceada em benefício de interesses privados que podem carecer de autenticidade e legitimidade. Caso fosse eliminada a necessidade de ordem judicial conforme sugerido, haveria o risco de censura por parte dos provedores, que passariam a ser os responsáveis por julgar a pertinência das acusações de infração de direitos autorais.

Varella (2012b) alega que esse é um pleito da indústria cultural, ou seja, da indústria do *copyright*, composta por instituições como a ABDR (Associação Brasileira de Direitos Reprográficos), a ABPD (Associação Brasileira de Produtores de Discos), a MPAA (Motion Picture Association of America) representante do segmento cinematográfico norte-americano, as organizações Globo, dentre outros grandes produtores de conteúdo. Esse segmento empresarial tenta, portanto, introduzir no Marco Civil da Internet a questão do direito autoral, que havia sido excluída do escopo da lei durante os debates que antecederam a sua proposição, uma vez que essa matéria já é objeto da reforma da Lei 9.610 de 1998 (Lei de direitos autorais) que está sendo conduzida de maneira pública e aberta pelo Ministério da Cultura desde 2007.

8 CONCLUSÃO

Os conflitos que emergem com a proposição do Marco Civil da Internet revelam grandes interesses contraditórios que tornam improvável a aprovação da lei nos termos do substitutivo apresentado pelo seu relator. Entre os meses de julho e novembro de 2012, a votação da lei foi adiada várias vezes no Congresso devido aos impasses surgidos e às pressões dos influentes *lobbies* envolvidos, colocando em dúvida o futuro do projeto e das idéias que ele representa.

No Brasil, assim como no resto do mundo, estamos diante de embates que determinarão o futuro da Internet. A manutenção do caráter aberto, livre e igualitário da rede está em jogo.

Sem o princípio da neutralidade, a *web* perderá uma diretriz que norteou-a desde a sua origem. Nesse cenário, coloca-se em risco o direito de disseminar informação e conhecimento sem discriminações e filtros. Novos instrumentos de poder ganham força na sociedade da informação, tanto na esfera do mercado, quanto do Estado.

Paradoxalmente, é a plena liberdade na Internet que permite o monitoramento dos internautas por empresas e por governos. Portanto, é preciso que a luta por uma rede aberta, livre e igualitária seja também acompanhada pela reivindicação do controle social da coleta massiva de informações.

Sem uma política de informação para Internet direcionada por esses valores, corremos o risco de nos tornarmos reféns de interesses privados e governamentais que cada vez mais tornam a rede mundial uma infraestrutura panspectra.

INFORMATION AND POWER IN THE INTERNET ARENA

ABSTRACT *Information and knowledge have always been source of power. Nowadays, increasingly the laws that constitute the national information policies play an important role in mediating the conflicts that belong to the Internet arena. This is the challenge of the Civil Rights Framework for the Internet, a bill proposed at the Brazilian Chamber of Deputies. This essay aims to present an analysis of the origin and the content of this legislation, focusing on the conflicts of net neutrality and mass surveillance of user information. These two themes are crucial to preserve or to abolish the freedom and the isonomy originally attributed to the web. Concluding the analysis, the future of the proposed law is questioned, given the huge conflicts that it brings.*

Key-words: *Internet, Brazil, Information and power, Net neutrality, Information policy.*

Artigo recebido em 15/02/2013 e aceito para publicação em 16/06/2013

REFERÊNCIAS

ANATEL. *Relatório semestral ouvidoria*. Brasília, DF, 2003.

_____. Resolução nº 574 de 28 de outubro de 2011. Brasília, DF, 2011.

ANGWIN, J.; VALENTINO-DEVRIES, J. Google'siPhoneTracking. *Wall Street Jornal*. Disponível em: <http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html>. Acesso em: 15 jan. 2013.

ARTICLE19. *Brazil Civil Rights Framework for the Internet*. London: Article19. Disponível em: < http://www.article19.org/data/files/medialibrary/3389/12-07-26-LA-brazil.pdf>. Acesso em: 15 jan. 2013.

BAMFORD, J. *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say). Wired.* Disponível em: <http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all>. Acesso em: 15 jan. 2013.

BENTHAM, J. *Panopticon or the inspection house*.London: T Pane, 1791. Disponível em: <http://books.google.com.br/books/about/Panopticon_Or_the_Inspection_House.html?id=NM4TAAAAQAAJ&redir_esc=y>. Acessoem 15 jan. 2013.

_____. *The works of Jeremy Bentham*. London: Simpkin, Marshall & Co, 1843. 4 v. Disponível em: <http://books.google.com.br/books/about/The_works_of_Jeremy_Bentham.html?id=QdEQAAAAYAAJ&redir_esc=y>. Acesso em: 15 jan.2013.

BORBA, J. Ministério notifica Vivo por venda de dados sobre comportamento de clientes. *Folha de São Paulo*. Disponível em: <http://m.folha.uol.com.br/mercado/1171498-ministerio-notifica-vivo-por-venda-de-dados-sobre-comportamento-de-clientes.html>. Acesso em: 15 jan. 2013.

BRAMAN, S. *Change of State: information, policy and power*. London: MIT Press, 2006.

CDT (Center for Democracy & Technology). *A Brief History of Surveillance Law.* Disponível em <https://www.cdt.org/issue/wiretap-ecpa>. Acesso em: 15 jan. 2013.

BRASIL. Projeto de Lei 5403/2001. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=34462>. Acesso em: 15 jan. 2013.

CGI (Comitê Gestor da Internet no Brasil). *Princípios da governança e uso daiInternet no Brasil*. Disponível em: <http://www.cgi.br/regulamentacao/resolucao2009-003.htm>. Acesso em: 15 jan. 2013.

EDWARDS, J. Apple Has Quietly Started Tracking iPhone Users Again, and It's Tricky To Opt Out. *Business Insider*. Disponível em: <http://www.businessinsider.com/ifa-apples-

iphone-tracking-in-ios-6-2012-10>. Acesso em: 15 jan. 2013.

FUCHS, C. *Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society.*Uppsala: Uppsala University. 2012. Disponível em: <http://www.projectpact.eu/documents-1/%231_Privacy_and_Security_Research_Paper_Series.pdf>. Acesso em: 15 jan. 2013.

GOLDSMITH J. ; WU, T.*Who Control the Internet? Illusions of a Borderless World.* New York: Oxford, 2006.

KELLY, S.; COOK, S.; TRUONG, M. (Org.) *Freedom on the Net 2012*.Washington: Freedom House. Disponível em: <http://www.freedomhouse.org/report/freedom-net/freedom-net-2012>. Acesso em: 15 jan. 2013.

RAVETS, D. FTC Dings Google $22.5M in Safari Cookie Flap. *Wired*. Disponível em: <http://www.wired.com/threatlevel/2012/08/ftc-google-cookie>. Acesso em: 15 jan. 2013.

LEMON, S. Yahoo Criticized for Curtailing Freedom Online. *PC World*. Disponível em: <http://www.pcworld.com/article/103865/article.html>. Acesso em: 15 jan. 2013.

_____. Votação do Marco Civil é decisiva para o país na área de tecnologia. *Folha de São Paulo.* 2012a. Disponível em: <http://www1.folha.uol.com.br/poder/1184644-analise-votacao-do-marco-civil-e-decisiva-para-o-pais-na-area-de-tecnologia.shtml>. Acesso em: 15 jan. 2013.

_____. Ao adiar votação do Marco Civil, Brasil deixa de exercer soberania sobre a rede. *Folha de São Paulo.* 26 nov. 2012b. Disponível em: <http://www1.folha.uol.com.br/tec/1190433-opiniao-ao-adiar-votacao-do-marco-civil-brasil-deixa-de-exercer-soberania-sobre-a-rede.shtml>. Acesso em: 15 jan. 2013.

LEVY, E. O lado econômico da neutralidade na internet. *Convergência Digital*. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=32357&sid=15> Acesso em: 15 jan. 2013.

MOLON, A. Parecer da comissão especial destinada a proferir parecer ao PL 5403/2001. Câmara dos Deputados, Brasília, 2012. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1012195&filename=Tramitacao-PL+5403/2001>. Acesso em: 15 jan. 2013.

REIS, A. S. *Educação a distância no Brasil no contexto da Lei 9394/96*: uma leitura sob o prisma da razão jurídica. Tese (Doutorado em Educação) – Faculdade de Educação/UFMG. Belo Horizonte, 2002.

REPÚBLICA POPULAR DA CHINA, *Constitution of The People's Republic of China*, Beijin: National People's Congress, 2004.

REUTERS. Telefonica targets retailers with street smart data. *Reuters*. Disponível em: <http://www.reuters.com/article/2012/10/08/telefonica-big-data-idUSL6E8L8L5A20121008>. Acesso em: 15 jan. 2013.

RICHTER, F. *Google Rakes In More Ad Dollars Than U.S. Print Media*. 12 nov. 2012. Disponível em <http://www.statista.com/topics/1001/google/chart/709/google-s-ad-revenue-since-2004>. Acesso em: 15 jan. 2013.

RILEY, M. C. ; SCOTT, B. *Deep packet inspection. The end of the Internet as we know it?* Florence: Free Press, 2009. Disponívelem<http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf>. Acesso em: 15 jan. 2013.

SALVES, D. *Novo Sopa recebe apoio do Facebook e rejeição da Casa Branca*. Disponível em: <http://tecnologia.terra.com.br/internet/novo-sopa-recebe-apoio-do-facebook-e-rejeicao-da-casa-branca,a789e194c2bda310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 15 jan. 2013.

SILVA, T. E.; PINHEIRO, M. M. K. Configurações contemporâneas da Política de Informação: poder, política e regime de informação. In: TOMAÈL, Maria Inês (Org.) *Compartilhamento da Informação*. Londrina: Eduel, 2012.

STAMPLER, L. Here's Everything We Know About IFA, The iPhone Tracking Technology In Apple's iOS 6. *Business Insider*. Disponível em:

<http://www.businessinsider.com/everything-we-know-about-ifa-and-tracking-in-apples-ios-6-2012-10>. Acesso em: 15 jan. 2013.

TELEBRASIL (Associação Brasileira de Telecomunicações). *Carta de Brasília*. In: 56º Painel Telebrasil. Disponível em: <http://www.telebrasil.org.br/56-edicao>. Acesso em: 15 jan. 2013.

TIMM, T. The Disturbing Privacy Dangers in CISPA and How To Stop It. *Electronic Frontier Foudation*.15 abr. 2012. Disponível em: <https://www.eff.org/deeplinks/2012/04/cybersecurity-bill-faq-disturbing-privacy-dangers-cispa-and-how-you-stop-it>. Acesso em: 15 jan. 2013.

TUROW, J. *Niche envy: marketing discrimination in the digital age*. Cambridge: MIT Press, 2008.

VARELLA, G. A contramão dos direitos e liberdades na Internet. *Carta Capital*. Disponível em: <http://www.cartacapital.com.br/sociedade/a-contramao-dos-direitos-e-da-liberdades-na-internet/>. Acesso em: 15 jan. 2013.

_____. *Marco Civil Já!* 2012a. Disponível em: <http://www.idec.org.br/email_mkt/marcocivil/alerta-06-08-12.html>. Acesso em: 15 jan. 2013.

_____. *Marco Civil da Internet*: entre o lobby e a liberdade. 2012b. Disponível em: <http://www.idec.org.br/em-acao/artigo/marco-civil-da-internet-entre-o-lobby-e-a-liberdade>. Acesso em: 15 jan 2013.

WIKILEAKS. *The Spy Files*. Disponível em: <http://wikileaks.org/the-spyfiles.html>. Acesso em: 15 jan. 2013.