PRIVACIDADE, NEUTRALIDADE E INIMPUTABILIDADE DA INTERNET NO BRASIL: AVANÇOS E DEFICIÊNCIAS NO PROJETO DO MARCO CIVIL

PRIVACIDAD, NEUTRALIDAD Y INIMPUTABILIDAD DE LA INTERNET BRASILEÑA: AVANCES Y LIMITACIONES EM EL MARCO CIVIL

PRIVACY, NET NEUTRALITY AND NONIMPUTABILITY: STRENGTHS AND WEAKNESSES IN THE BRAZILIAN INTERNET LAW PROJECT

Arthur Coelho BEZERRA

Doutor em sociologia pela UFRJ, com pós-doutorado pela mesma instituição. Pesquisador adjunto do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT). Professor do Programa de Pós-Graduação em Ciência da Informação (PPGCI - IBICT/UFRJ). Pesquisador do Núcleo de Estudos da Cidadania, Criminalidade e Violência Urbana (NECVU- UFRJ)
Email: arthurbezerra@ibict.br

Igor WALTZ

Mestrando do Programa de Pós-Graduação em Comunicação- UFRJ/Brasil
Email: igor.waltz@gmail.com

Revista Eptic Online
Vol.16 n.2 p.161-175
mai-ago 2014
Recebido em 28/02/2014
Aprovado em 20/04/2014

Resumo

O trabalho examina a governança da internet no Brasil, a partir do texto do Marco Civil, sancionado pela Presidente Dilma Rousseff em abril de 2014. A crescente centralidade da rede na vida política e social urge a delimitação de direitos e responsabilidades de usuários, empresas e demais atores envolvidos. Acerca dessa demanda, são analisados os artigos do PLC 21/2014 que dizem respeito à "Privacidade", "Inimputabilidade" e "Neutralidade da Rede", seus avanços e limitações de ordem técnica, econômica e legal.

Palavras-chave

Marco Civil da Internet; Governança; Neutralidade da Rede; Privacidade; Inimputabilidade.

Resumen

Este artículo examina la Gobernanza de Internet en Brasil, desde el Marco Civil sancionado por la presidente Dilma Rousseff en abril de 2014. La creciente centralidad de la red en la vida política y social insta a la delimitación de los derechos y responsabilidades de los usuários, las empresas y otras partes involucradas. Por tanto, se analizan los artículos del proyecto 21/2014 que conciernen a la "Privacidad", "Inimputabilidad" y "Neutralidad de la red", los avances y limitaciones de orden técnico, económico y jurídico.

Palabras clave

Marco Civil de Internet; Gobernanza; Neutralidad de la red; Privacidad; Inimputabilidad.

Abstract

The paper examines the governance of the Internet in Brazil, from the Marco Civil text which is being discussed in the Legislature. The growing centrality of the internet in social and political life urges the delimitation of rights and responsibilities of users, companies and other stakeholders. About this demand, we intend to analize the articles of the law project PL 2.126/2011, focusing on issues such as net neutrality, net privacy and net nonimputability.

Keywords

Internet law, Governance, Net Neutrality, Privacy, Nonimputability.

Introdução

Nas últimas décadas, com a popularização das tecnologias de informação e comunicação (TICs), a internet tem assumido um destacado papel na formatação de uma esfera pública de abrangência global. Com implicações nos campos econômico, político e sociocultural, a rede das redes se tornou um importante palco para o exercício da cidadania e livre expressão. Essa dimensão destaca a governança da internet como uma questão urgente na contemporaneidade.

Ainda que a internet tenha propiciado mais democratização na concessão de vozes por meio de uma proliferação de polos emissores, por ela também espreita uma miríade de ameaças a liberdades democráticas. A defesa da privacidade, em teoria apregoada consensualmente por quase todos os atores envolvidos na rede, é posta em xeque por ações de espionagem e vigilância de governos e grandes empresas. A neutralidade da rede, por sua vez, é ponto de divergência entre os interesses público e de provedoras de internet, no Brasil e ao redor do mundo.

Em vistas de estabelecer uma regulamentação do uso da internet, o Brasil aprovou em abril de 2014 o Marco Civil da Internet, a constituição do país para o setor, que estabelece direitos, deveres e garantias dos usuários. Ainda que a nova lei constitua um passo importante para o estabelecimento de parâmetros legais para a internet, a governança vai muito além de um marco legal e incide também sobre questões econômicas (modelos de negócio) e de infraestrutura (manter compatibilidade de sistemas e dispositivos, mitigar os riscos de fragmentação, etc), entre outras.

Este artigo se propõe a discutir os pontos considerados de maior relevância e controvérsia do Marco Civil da Internet, a saber, a privacidade, a neutralidade da rede e a inimputabilidade da rede, bem como sua eficiência frente a desafios econômicos e infraestruturais.

A questão da governança da internet

A rede mundial de computadores tem suas raízes nos laboratórios militares de pesquisa tecnológica dos Estados Unidos durante a Guerra Fria. Uma das redes pioneiras foi a *Advanced Research Projects Agency Network* (ARPANet), idealizada pelo Departamento de Defesa estadunidense nos anos 1960, como um modelo descentralizado de transmissão de dados por computadores interligados, com o intuito de proteger o fluxo de informações militares de um possível ataque soviético. Na década seguinte, com o desenvolvimento dos protocolos TCP/IP, foi possível que diferentes redes de distintos países e continentes se comunicassem entre si, o que lançou as bases para uma rede em escala global.

A formatação de uma grande rede de redes sem um nó central, somada à popularização dos computadores pessoais, *smartphones* e serviços de comunicação nas décadas seguintes, fizeram da internet um fenômeno com implicações políticas, econômicas e socioculturais. Segundo MacKinnon (2012), a rede se consolidou como uma nova esfera política internacional, uma vez que plataformas e serviços oferecidos na internet atribuíram mais poder aos cidadãos, permitindo-os desafiar o governo de seus países e governos estrangeiros que de alguma forma os afetam.

A ausência de uma centralidade da rede, no entanto, não configura uma dispersão equivalente dos fluxos. Quase a totalidade do trânsito de dados da América Latina passa pelos Estados Unidos, que concentra grande parte da infraestrutura global de telecomunicações. Apenas em 2013 foi inaugurado o primeiro caminho digital binacional entre Brasil e Uruguai, considerado o primeiro passo para a implantação de um anel óptico sulamericano, que conectará os países do continente entre si e com a Europa e a África[1].

1 - MINISTÉRIO DAS COMUNICAÇÕES. "Começa de fato a implantação do anel óptico sul-americano". Disponível em http://www.mc.gov.br/telecomunicacoes/noticias-telecomunicacoes/27200-comeca-de-fato-a-implantacao-do-anel-optico-sul-americano. Acesso em 30 de abril de 2014

O debate em torno do tema ganhou força no país após a divulgação de ações espionagem da Agência Nacional de Segurança dos EUA (NSA, na sigla em inglês), por meio da quebra da criptografia de mensagens que circulam pela internet e armazenamento de metadados (e possivelmente de dados) dessas comunicações. Não apenas países considerados como integrantes do Eixo do Mal, como China, Rússia e Irã, foram alvos de espionagem, mas também Brasil, México, Alemanha e França. Segundo o jornalista Luciano Martins Costa, "esse tipo de informação privilegiada coloca em xeque o mito da liberdade comercial e, teoricamente, quebra o princípio da igualdade de condições que supostamente governa o capitalismo globalizado"[2].

2-Disponível em: http://www.observatoriodaimprensa.com.br/radios/view/gt_gt_o_big_brother_desmascarado_lt_br_gt_gt_gt_soberania_e_privacidade) Acesso em 30 de abril de 2014

Como exemplos, Costa cita o risco de uma empresa norte-americana de petróleo conseguir mapear a estratégia de investimentos da Petrobras, ou dos benefícios que o setor agrícola dos Estados Unidos teria a partir do rastreamento de informações do agronegócio brasileiro; "se a espionagem americana no Irã e no Paquistão é motivada por questões de segurança, o monitoramento das comunicações na China e no Brasil deve ter outras razões, uma vez que esses dois países estão fora do mapa principal do terrorismo internacional"[3].

O abuso de poder de vigilância do governo norte-americano veio à tona por meio de denúncias do jornal *The Guardian,* com base em informações vazadas por Edward Snowden, ex-analista de segurança da NSA. O programa de vigilância Prism, usado pela agência, coletaria dados de provedores online, como e-mail, chats, vídeos, fotos e toda a sorte de dados armazenados na internet, com o envolvimento de gigantes da internet, como Google e Facebook (BEZERRA; SCHNEIDER; SALDANHA, 2013).

Após as revelações, a governança da internet para uma nova arquitetura que permita uma governança global da rede foi reconduzida ao protagonismo dos debates internacionais. O tema já vinha sendo debatido no âmbito dos órgãos de direito internacional desde 2004, época da realização do primeiro fórum global sobre o assunto. Em 2014, São Paulo sediou a Conferência Multissetorial Global sobre o Futuro da Internet (NETMundial), com a presença de representantes de 95 países, tendo como um dos principais temas de debate

a transferência de parte do controle de Washington sobre a internet do mundo para organismos multilaterais, como a Organização das Nações Unidas (ONU), por meio da União Internacional de Telecomunicações (UIT).

Como afirmam Bezerra, Schneider e Saldanha (2013), a pregnância mundial e a natureza descentralizada da internet trazem um considerável potencial democratizante, possibilitando uma maior autonomia para produção, reprodução e distribuição de bens culturais e informacionais do que aquela alcançada no século anterior. No entanto, ao mesmo tempo em que as redes empoderam usuários com mais voz e capacidade de mobilização social, elas abrem uma importante lacuna à vigilância de governos e grandes corporações, possibilitando maior controle estatal sobre a vida dos cidadãos, violação da privacidade de indivíduos e de segredos empresariais, espionagem internacional e outros expedientes. De acordo com MacKinnon, ao redor do mundo, "**todos** os governos, de ditaduras a democracias, estão aprendendo rapidamente como usar a tecnologia para defender seus interesses" (MacKINNON, 2012, p. 5. Grifo da autora. Tradução nossa).

No Brasil, o debate em torno da legislação específica para regulamentar os direitos e as garantias dos usuários da internet tomou corpo depois da revelação da espionagem norte-americana à Presidente Dilma Rousseff e outras autoridades. O PLC 21/2014, aprovado em 22 de abril de 2014, foi redigido para dar maior peso à questão da privacidade e foi uma das prioridades do governo brasileiro no ano de 2013. Com a instituição da nova lei, o Brasil passou a compor, junto com Países Baixos e Chile, um seleto grupo de nações que promulgaram legislações específicas para regular a rede.

Apesar de ter sido aprovado em tempo recorde pelo Senado Federal, e sancionado pela Presidente Dilma Rousseff no dia seguinte, durante a abertura do NETMundial, o projeto do Marco Civil permaneceu quase três anos emperrado na Câmara dos Deputados, principalmente por conta do *lobby* das grandes empresas de telefonia contra a chamada neutralidade da rede, isto é, a não-discriminação no trânsito da rede dos pacotes de dados em relação a seu conteúdo ou origem.

Assim como nos debates que tomam corpo em todo o mundo, as discussões que prenderam o projeto na Câmara giraram em torno de duas correntes: os defensores da neutralidade como uma garantia à liberdade de expressão, e os "desreguladores", que apregoam que qualquer tipo de intervenção no setor poderia desincentivar investimentos e inovações dos provedores de serviços na rede.

Ramos (2005) lembra que o discurso do livre-mercado e da desregulação dos serviços públicos tornou-se hegemônico na América Latina a partir dos anos 1980, com a consolidação da doutrina neoliberal. Nas palavras do autor, durante a onda de privatizações, o Estado passou a se distanciar do papel de "definidor da políticas" para a área de telecomunicações e adotou a postura de "fiscalizador", por meio de agências reguladoras. Não obstante, é possível afirmarmos que a postura mais atuante do governo em relação a um marco regulatório para a internet a partir de 2013 ganhou impulso especial por motivações de segurança e especificidades da rede.

Como explica Califano (2013), a internet representa novos desafios regulatórios em relação aos modelos tradicionais de telecomunicações, pelo volume de dados que se transporta. E por esse mesmo motivo, é preciso que haja intervenção dos governos por meio de leis específicas para assegurar os direitos de quem acessa a rede. "A gestão do tráfico da internet requer regulação específica, com intuito de equilibrar os interesses dos usuários, dos provedores de serviço de conectividade e dos provedores de conteúdos e aplicações". (CALIFANO, 2013, p. 33)

O texto da nova lei foi elaborado com base no documento "Princípios para a governança e o uso da internet", do Comitê Gestor da Internet no Brasil (CGI.br), organismo multissetorial responsável por integrar iniciativas de uso e desenvolvimento da internet brasileira. O documento é resultado de uma consulta pública, promovida entre 2009 e 2010, na qual foram arroladas mais de 800 contribuições de diferentes representantes da sociedade civil. Entre os principais eixos temáticos tratados pelo texto, e adotados pelo Marco Civil da Internet, estão a **privacidade**, a **neutralidade da rede** e a **inimputabilidade da rede**. Tais princípios garantiriam os direitos e liberdades democráticas de internautas frente a ações abusivas de governos (nacionais e estrangeiros) e empresas prestadoras de serviços. Trataremos mais a fundo a efetividade de cada um desses eixos a seguir.

Privacidade e Segurança contra Espionagem

A privacidade e a intimidade são direitos fundamentais presentes na Declaração Universal dos Direitos Humanos e na Constituição da República de 1988. A privacidade refere-se a tudo o que o indivíduo não pretende que seja de conhecimento público, reservado apenas aos integrantes de seu círculo de convivência particular, enquanto a intimidade diz respeito única e exclusivamente ao indivíduo. Esses direitos se estendem ao domicílio, à correspondência, às comunicações e aos dados pessoais.

O advento das tecnologias digitais foi acompanhado por uma gradual restrição à proteção desses direitos. Silva aponta que, a respeito de uma ameaça que atente contra a privacidade, a expectativa culturalmente firmada é a de que "o trânsito facilitado de informação não evada a dimensão pessoal, de coisas que os indivíduos têm o direito e/ou o dever de guardar para si" (SILVA, 2013, p. 396). Mas o fluxo e o armazenamento de comunicações e informações pessoais na rede abrem brechas à vigilância estatal indevida, uso impróprio de dados de clientes por empresas, ataque de *hackers* a *data centers* e a dispositivos pessoais, vazamento de informações sigilosas por pessoas mal-intencionadas a fim de denegrir a imagem de terceiros, entre outros.

A necessidade de se estabelecer regras claras e específicas para a proteção da privacidade e da intimidade parece ter sido o motor para a tentativa do governo de acelerar a votação do Marco Civil no Congresso Nacional. O artigo 7º reconhece a importância da internet para a cidadania e reitera a inviolabilidade da vida privada e das comunicações em fluxo

e armazenadas, salvo ordem judicial. O artigo 8º, por sua vez, estabelece a liberdade de expressão e da privacidade como condições para o pleno exercício de direito da internet.

Além de salvaguardar garantias já previstas pela Constituição, a aprovação de uma legislação nacional que regule o uso da rede colocaria o Brasil em posição de destaque no debate internacional. A governança global da internet parece ter entrado na agenda das relações exteriores do país, e a inviolabilidade das comunicações, inclusive, foi a tônica do discurso da Presidente Dilma Rousseff durante a abertura da 68ª Assembleia da Organização das Nações Unidas. Tal fato se explica pela própria líder ter sido alvo de espionagem pelo governo dos EUA, algo que considerou uma ameaça à soberania nacional.

Como afirmam Assange, Müller-Maguhn, Appelbaum e Zimmermann (2013), em nome do combate ao que chamam de "Cavaleiros do Infoapocalipse" – pornografia infantil, terrorismo, lavagem de dinheiro e tráfico internacional de drogas – erigiu-se um sistema de vigilância de alcance global, sem grande resistência da opinião pública. Mas os autores denunciam que todo esse aparato é utilizado para fins outros que o combate ao crime internacional.

O armazenamento em massa das informações transmitidas por serviços de telecomunicações, aponta Assange, seria uma das estratégias em curso de um processo de militarização do ciberespaço. Se antes havia uma seleção dos indivíduos dos quais se queria interceptar, a estratégia hoje é a de interceptação e armazenamento geral de dados, ou o que Müller-Maguhn chama de "armazenamento em massa – o armazenamento de todas as telecomunicações, todas as chamadas de voz, todo o tráfego de dados, todas as maneiras pelas quais se consomem serviços de mensagem de texto (SMS), bem como conexões à internet" (ASSANGE *et al.*, 2013, p. 56). Segundo Appelbaum, trata-se de "uma questão de controle por meio da vigilância. Em certos aspectos, é o panóptico perfeito" (idem, p. 39).

Appelbaum refere-se à ideia do jurista inglês Jeremy Bentham, analisada na década de 1970 pelo filosofo francês Michel Foucault (2000), de uma arquitetura de poder, conhecida como *panopticon*, em que a possibilidade de uma vigilância se faz interiorizada na forma de disciplina pelos sujeitos. É na ideia de "panóptico perfeito", ou seja, da vigilância perpétua real, e não apenas presumível, que reside o grande paradoxo da rede: na mesma medida em que permite a proliferação de uma infinidade de novas formas de comunicação mais livres de censura, aumenta também a vigilância sobre essas novas formas. É por esse imperativo ao *oversharing* e à tecnointeração que se exercem as novas formas de controle, como a infovigilância e o datacontrole, listados por Sodré (2012).

Apesar do tom pessimista de denúncia que permeia a obra de Assange *et al.*, os autores apontam duas saídas para o problema da infovigilância. De um lado, pelas leis da física, que possibilitariam o desenvolvimento de dispositivos que impedissem a interceptação, e do outro, pelas "leis dos homens", por meio de controles democráticos e prestação de contas em termos legislativos, sob o slogan *cypherpunk* "privacidade para os fracos, transparência para os poderosos".

Mas até que ponto interessa aos governos proteger a privacidade de seus cidadãos? Estariam comprometidos com a questão da transparência a despeito de interesses próprios? Como coibir abusos do próprio Estado que, teoricamente, nas democracias, legisla em nome dos cidadãos? Essas questões se fazem pertinentes, uma vez que, enquanto brada em órgãos internacionais contra a espionagem, o governo brasileiro adota medidas similares por meio da Agência Nacional de Telecomunicações (Anatel). Segundo Ronaldo Lemos, o sistema criado pela citada agência permite acessar os registros de todas as ligações telefônicas feitas no País. Soma-se a isso a proposição da Anatel, também lembrada por Lemos, de "obrigar empresas de telefonia a revelar à polícia a localização exata de qualquer usuário de celular, imediatamente e por mera solicitação, sem o controle do Judiciário" (*apud* BEZERRA; SCHNEIDER; SALDANHA, 2013).

A tecnologia, enquanto campo de luta entre governos e cidadãos por hegemonia, aparece com mais evidência após as ondas de protestos que tomaram as ruas de diversos países do mundo, inclusive do Brasil. Tal fenômeno chama a atenção especialmente por aparecer sem grandes constrangimentos em regimes democráticos ocidentais. Na Espanha, a recente *Ley de Seguridad Ciudadana* estabelece como "infração muito grave", sujeita a multa de 3 mil a 6 mil euros, a convocação de "manifestações com finalidade coativa". Nos EUA, o FBI coletou nos sistemas das Universidades, com a conivência das reitorias, informações sobre alunos participantes do movimento *Occupy Wall Street,* em 2012.

No Rio de Janeiro, houve uma tentativa de se criar, via decreto, uma Comissão Especial de Investigação de Atos de Vandalismo em Manifestações Públicas (CEIV), que conferiria ao governo do estado poderes para a quebra de sigilo telefônico e de internet. "O governador Sérgio Cabral, ao propor tal medida, parece se alinhar ao discurso de Barack Obama para justificar as denúncias de Snowden: você não pode ter 100% de segurança, e então 100% de privacidade e zero de inconveniência" (BEZERRA; SCHNEIDER; SALDANHA, 2013).

O Papel das Empresas

Uma vez que a efetividade da proteção à privacidade aludida pelo Marco Civil pode ser limitada por medidas governamentais de caráter antidemocrático, o que dizer de abusos externos a esse direito constitucional? Como dito anteriormente, grande parte dos fluxos de dados da América Latina são transportados e armazenados por empresas sediadas em solo estadunidense. O governo brasileiro defendeu que poderia contornar o problema ao obrigar grandes provedores estrangeiros de serviços de internet, tais como Google e Facebook, a implantarem *data centers* em território nacional. Contudo, o artigo do Marco Civil que previa tal norma não foi aprovado na Câmara dos Deputados, em parte graças à ação de *lobby* das empresas citadas.

O grande problema em relação à eficácia da instalação de tais bancos, porém, diz respeito à arquitetura da rede. Mesmo que os dados sejam armazenados no Brasil, eles trafegam

em infovias que passam por outros países – especialmente os EUA. Ou seja, ainda permaneceriam vulneráveis à interceptação e vigilância.

O fato é que os produtos e serviços fornecidos pelos provedores de conexão e aplicativos de internet são os meios pelos quais os cidadãos interagem e exercem sua cidadania na rede. Cada vez mais, empresas privadas tomam para si um papel fundamental de mediação do debate público ao redor do mundo. E isso não se daria sem perdas à democracia, ideologicamente pautada pelo confronto entre diferentes vozes.

Um exemplo: o algoritmo do Facebook faz com que um determinado usuário veja com mais frequência atualizações de pessoas mais próximas, com base em interações prévias. Ele deduz o que e quem são mais prováveis ao interesse do usuário. O restante geralmente tende a se perder na saturação de mensagens, imagens e vídeos do site de rede social. A formação desses feudos informativos por meio do excesso de personalização, que caracteriza aquilo que Pariser (2011) chama de bolha filtro (*filter bubble*), seria a arma silenciosa das empresas de internet para fortalecer suas estratégias comerciais.

> Assim como o sistema de produção da fábrica que produz e fornece nosso alimento molda o que comemos, a dinâmica da mídia modela que informação consumimos. (...) Os filtros de personalização funcionam como uma espécie de autopropaganda invisível, doutrinando-nos com nossas próprias ideias, ampliando nosso desejo por coisas que nos são familiares e deixando-nos alheios aos perigos à espreita no escuro território do desconhecido. (PARISER, 2011, p. 9. Tradução nossa)

MacKinnon (2012) vai além e propõe que a habilidade de organizar nossa fala está sendo moldada pelos provedores de serviços de internet. Se haveria uma velada manipulação das nossas comunicações, nossa competência para entender como o poder está agindo sobre nós e nossa capacidade de tomar esse poder de volta começariam a ser erodidas de uma maneira insidiosa, imperceptível. Para a autora, companhias de internet como Google e Facebook ganharam muito poder sobre a vida dos cidadãos, com muito pouca transparência ou prestação de contas (*accountability*) ao público.

Conforme denuncia Lannier (2013), para tornarem-se rentáveis e desenvolver anúncios relevantes, as companhias precisam conhecer profundamente os usuários, seguindo seus rastros e informações que disponibilizam na rede. O conteúdo produzido gratuita e voluntariamente pelos indivíduos, que inclui seus hábitos de consumo, *cybermovimentos* e outras informações relevantes, é armazenado e convertido em estratégia comercial por meio de potentes servidores, batizados por ele de "servidores-sereia" (*siren servers*), acessíveis apenas a grandes conglomerados do setor. Para o autor, a saída – um tanto quanto utópica – seria a instituição de micropagamentos a cada vez que os dados individuais são utilizados para a tomada de decisão.

> Suponhamos que qualquer servidor em nuvem, seja uma rede social, um esquema de Wall Street ou mesmo uma agência governamental, fosse obrigado a pagar-lhe por dados úteis derivados de você. (...) Você teria direitos comerciais intrínsecos, inalienáveis aos dados que não existiriam sem você. Isso significaria, por exemplo, que o Facebook lhe enviaria pequenos pagamentos quando dados obtidos automaticamente a partir de você tenham ajudado algum anunciante a vender algo para um amigo seu. Se o seu rosto aparece em um anúncio, você é pago. Se você é rastreado enquanto anda pela cidade, e ajuda ao governo tornar-se ciente de que a segurança de pedestres pode ser melhorada com uma melhor sinalização, você deveria obter um micropagamento por ter contribuído dados valiosos. (LANIER, 2013, p. 673-674. Tradução nossa)

A proposição do autor dificilmente será levada a cabo pelo modelo concentrador desenvolvido pelos grandes do Vale do Silício, mas atenta os usuários sobre usos de informações geradas por eles sem que tenham sequer consciência disso. Os artigos 10, 11 e 12 do Marco Civil da Internet tratam da proteção aos registros dos usuários, mas em nenhum momento regulam os usos desses registros.

O Art. 10 estabelece que a guarda e a disponibilização de registros de conexão e acesso a aplicações na internet deve ocorrer de forma a preservar a intimidade, a vida privada, a honra e a imagem das partes direta ou indiretamente envolvidas, determinando que o responsável pela guarda somente será obrigado a disponibilizar informações que levem à identificação do usuário mediante solicitação judicial. Após o parecer do relator do projeto de lei, foram incluídos dados pessoais e conteúdo de comunicações privadas no escopo do artigo. Mas embora a lei proteja o usuário da divulgação imprópria de informações de caráter pessoal, não contempla o fato de que o uso comercial dessas informações em poder das empresas também poderia ser considerado uma violação de privacidade e da intimidade dos indivíduos.

Em suas obras, MacKinnon, Lanier e Pariser apontam o grande empoderamento das grandes empresas da internet nas relações políticas e econômicas atuais. Mas haveria alguma forma de regular ou limitar tal poder de gerenciamento do fluxo da rede, em torno da qual cada vez mais se organiza a sociedade contemporânea? Essa questão permanece aberta a futuras considerações.

Neutralidade da Rede

Um dos principais empecilhos que atrasaram a votação do Marco Civil foi a falta de consenso ao redor do tópico "neutralidade da rede". Prevista no Artigo 9º, a neutralidade estabelece que todos os dados que trafegam na rede devem receber o mesmo tratamento

das empresas provedoras de acesso, sem distinção de origem, destino, serviço, conteúdo ou dispositivo (computador ou aparelho móvel).

O conceito de neutralidade da rede alinha-se à resolução da Organização das Nações Unidas que aponta o acesso à internet como um Direito Humano. O Pacto Internacional Sobre Direitos Civis e Políticos, adotado pelo Brasil em 1992, estabelece no 2º parágrafo do Art. 19 que "toda pessoa terá direito à liberdade de expressão; esse direito incluirá a liberdade de procurar, receber e difundir informações e ideias de qualquer natureza, independentemente de considerações de fronteiras, verbalmente ou por escrito". A ONU entende que qualquer restrição ou bloqueio à internet constitui uma violação do artigo 19, mesmo por conta de infrações de direitos autorais, como acontece em países como Reino Unido e França.

As empresas de telecomunicações alegam que neutralidade acarreta um prejuízo ao modelo de negócios baseado em vendas de planos específicos de tráfego, como os de acesso exclusivo a redes sociais, jogos ou vídeos. Esses planos bloqueariam ou reduziriam a velocidade para acesso a outros serviços ou páginas da internet. Outro argumento das companhias é o de que aplicativos gratuitos de mensagens instantâneas para dispositivos móveis, como *WeChat* e *WhatsApp*, estariam sobrecarregando a rede e reduzindo o uso de serviços pagos de SMS.

Temendo que a legislação atrapalhasse seus interesses comerciais, empresas de telecomunicações, por meio de um eficiente *lobby*, entraram em um acordo diretamente com o Poder Executivo para que a venda de pacotes diferenciados fosse permitida, o que gerou tensão no Congresso Nacional. De acordo com o Marco Civil, a degradação do sinal só poderia ocorrer por conta da ausência de requisitos técnicos necessários ao bom funcionamento ou para a priorização de serviços de emergência, mas, mesmo nesses casos, as empresas responsáveis deveriam "abster-se de causar danos aos usuários" e "agir com proporcionalidade, transparência e isonomia".

No Artigo 9º, o 3º parágrafo veda expressamente o bloqueio, monitoramento, filtro ou análise dos pacotes de dados, sendo excluída a proibição de "fiscalizar", presente na redação original do projeto. Livres para "fiscalizar", as empresas não seriam impedidas de acessar os cabeçalhos dos pacotes de dados, que argumentam ser essencial para a boa gestão da rede e evitar congestionamentos.

Califano (2013) aponta que novas tecnologias permitem identificar o conteúdo de um pacote de dados ao transmití-lo, o que permite aos provedores saber se ele precisa ser transportado em uma largura de banda maior ou menor. Da mesma forma que essas tecnologias podem ser utilizadas com propósito de identificar a que velocidade ele deve ser transmitido, podem usá-lo para sobretaxar esse envio. Silveira (2009) afirma que esse controle do fluxo de pacotes pode conferir às operadoras de telefonia e de conexão um papel de controladores de acesso (*gatekeepers*) da internet.

Dessa forma, é observado mais uma vez um foco de tensão entre modelos comerciais de exploração da rede e interesses sociais inerentes a ela. A internet foi concebida a

partir da necessidade de um fluxo de comunicação livre da ameaça de interferências e sem distinção de origem e destino. A neutralidade garante que conteúdos e usuários sejam tratados de maneira equivalente. Se a cidadania é cada vez mais exercida por meio da rede, o modelo das provedoras de telecomunicação garante melhor acesso àqueles que podem pagar mais por isso.

Inimputabilidade da Rede

A inimputabilidade da rede – ou a exclusão de culpabilidade – alude à delimitação das responsabilidades de diversos atores envolvidos na disponibilização e no uso da internet, com vistas a impedir a censura e promover a liberdade de expressão. De acordo com o Artigo 18 do Marco Civil, "o provedor de acesso à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros". Ou seja, companhias provedoras de conexão, de hospedagem de sites ou de *search engines* responderiam apenas em caso de desobediência de ordem judicial para exclusão de determinados conteúdos.

Exemplos de penalização de provedores da internet se proliferam no Judiciário brasileiro. Em setembro de 2012, Fábio Coelho, diretor-presidente do Google Brasil, foi detido pela Polícia Federal após a empresa negar a responsabilidade de vídeos publicados no YouTube que acusavam um candidato a prefeito de Campo Grande, Mato Grosso do Sul, de cometer crimes como lesão corporal e enriquecimento ilícito.

Com a aprovação do Marco Civil, situações como essa não devem se repetir. A adequada responsabilidade limitaria ações indiscriminadas de censura e coerção. Mas há na lei uma importante restrição: ela não se aplica a direitos do autor nem a direitos , que dependerá de uma legislação específica futura. Tal mudança foi incluída pelo relator do projeto graças à pressão de emissoras de televisão, especialmente pela Rede Globo.

Apesar de o Marco Civil ser baseado em um documento que expressa demandas da sociedade por meio de consultas públicas, a demora de sua votação provém da tentativa de ajuste do projeto aos interesses comerciais de grandes empresas. Tanto as teles como as emissoras fazem parte do grupo que Silveira (2009; 2011) classifica como "indústrias de intermediação", cujos negócios se baseiam na venda de suportes materiais, controle dos canais de exibição e transmissão de bens imateriais. Com a desintermediação, ou seja, a libertação desses bens de seus suportes por meio da rede, grupos de radiodifusão e de telecomunicações estão iniciando uma verdadeira cruzada para a criação de dispositivos legais possam bloquear a libertação da criação e distribuição na internet.

Considerações finais

Por delimitar direitos e responsabilidades de usuários, a partir das demandas da sociedade enviadas por meio de consultas públicas, o Marco Civil da Internet representa um importante avanço na governança da rede no país. Todavia, exatamente por conta do caráter global da rede, medidas legais de segurança perdem efetividade se não forem acompanhadas de devidos avanços de infraestrutura.

O Marco Civil constitui talvez uma das pedras fundamentais para a promoção da liberdade de expressão, combate à censura e promoção de direitos constitucionais da internet, mas não encerra o debate, uma vez que é preciso avançar em termos técnicos, políticos, legais e sociais. A efetividade de uma legislação para a rede depende que o governo produza, em curto prazo, uma série de regulamentações que instituirão os detalhes de como serão tratados temas centrais do novo arcabouço jurídico, como liberdade de expressão, segurança de dados e, especialmente, direitos de autor e *copyright*, que dependerão de leis ainda a serem criadas. Somente dessa forma será possível caminhar para que os avanços propostos pelo marco se tornem efetivos e as suas deficiências sejam superadas.

Bibliografia

ASSANGE, Julian; APPELBAUM, Jacob; MÜLLER-MAGUHN, Andy; ZIMMERMANN, Jéremie. **Cypherpunks: liberdade e o futuro da internet.** São Paulo: Boitempo, 2013.

BRASIL. **Constituição Federal de 1988**. Brasília: Senado Federal.

_____. **Redação final do Projeto de Lei da Câmara 21/2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília: Congresso Nacional.

_____. **Decreto nº 592, de 6 de julho de 1992**. Promulgação do Pacto Internacional sobre Direitos Civis e Políticos. Atos Internacionais. Brasília: Presidência da República/Casa Civil.

BEZERRA, Arthur Coelho; SCHNEIDER, Marco; SALDANHA, Gustavo Silva. "Ascensão e

queda da utopia tecnoliberal: a dialética da liberdade sociotécnica". Encontro Nacional de Pesquisa em Ciência da Informação – Enancib, 14, 2013. **Anais Eletrônicos.** Florianópolis: UFSC, 2013. Disponível em http://enancib.sites.ufsc.br/index.php/enancib2013/ XIVenancib/paper/viewFile/364/358. Acesso em 10 de nov. 2013.

CALIFANO, Bernadette. "Políticas de Internet: la neutralidad de la red y los desafíos para su regulación". Em: **Eptic – Revista de Economía Política de las Tecnologías de la Información y Comunicación**. Vol.15, n.3, p.19-37, set.-dez 2013. Disponível em http://www.seer.ufs.br/index.php/eptic/article/viewFile/1353/1351. Acesso em 7 de julho 2013.

CASTELLS, Manuel. **A Sociedade em Rede.** São Paulo: Paz&Terra, 2000, 2ª edição.

COMITÊ GESTOR DA INTERNET NO BRASIL. **O CGI.br e o Marco Civil da Internet.** São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em http://cgi.br/publicacoes/documentacao/CGI-e-o-Marco-Civil.pdf. Acesso em 9 de dez. de 2013.

FOUCAULT, Michel. **Vigiar e Punir: nascimento da prisão.** Rio de Janeiro: Ed. Vozes, 2000.

GRAZIANO, Diólia de Carvalho. "Governança da Internet: vulnerabilidades, ameaças e desafios para a manutenção da liberdade de expressão e não discriminação na rede telemática conectada". Encontro Nacional de Pesquisadores em Jornalismo, 10, 2012. **Anais eletrônicos.** Curitiba: PUC-PR, 2012. Disponível em http://soac.bce.unb.br/index.php/ENPJor/XENPJOR/schedConf/presentations. Acesso em 1º de dez. de 2013.

LANIER, Jaron. **Who Owns the Future?** New York: Simon & Schuster, 2013.

MacKINNON, Rebecca. **Consent of the Networked: the worldwide struggle for internet freedom**. New York: Basic Books, 2012.

PARISER, Eli. **The Filter Bubble: What the internet is hiding from you.** New York: The Penguin Press, 2011.

RAMOS, Murilo César. "Agências reguladoras: a reconciliação com a política". Em: **Eptic – Revista de Economía Política de las Tecnologías de la Información y Comunicación.**

V.7, n. 5, mai-ago 2005. Disponível em http://www2.eptic.com.br/arquivos/Revistas/VII,n.2,2005/MuriloCesarRamos.pdf. Acesso em 20 de jan. 2014.

SILVA, Rodrigo Marques de Miranda. **Internet: Sociologia de suas ameaças**. Tese (Doutorado em Sociologia e Antropologia). Instituto de Filosofia e Ciências Sociais, Universidade Federal do Rio de Janeiro (IFCS/UFRJ), Rio de Janeiro. 2013.

SILVEIRA, Sérgio Amadeu da. "Arquiteturas em disputa: ativistas P2P e a indústria da intermediação". Em: **Revista de Economía Política de las Tecnologías de la Información y Comunicación – EPTIC**. Vol. XI, n. 1, janeiro – abril 2009.

_____. "Ambivalência e confrontos no cenário informacional: O avanço do commons". Em: MACIEL, Maria Lúcia; ALBAGLI, Sarita (orgs.). I**nformação, conhecimento e poder: mudança tecnológica e inovação social**. Rio de Janeiro: Garamond, 2011.

SODRÉ, Muniz. **Antropológica do Espelho**. Petrópolis: Vozes, 2012. 7ª edição.