REVISTA ECO PÓS | ISSN 2175-8689 | AS FORMAS DO ARTÍFICIO | V. 18 | N. 3 | 2015 | PERSPECTIVAS

Privacidade e Regulamentação do Marco Civil da Internet: registros e preocupações

Privacy and Regulation of Internet's Marco Civil: Records and concerns

Esta é uma versão ampliada de "Cuestiones de Privacidade después del Marco Civil de Internet", comunicação apresentada na 3ª International Conference On Media Ethics, em Sevilha, Espanha. Foram incorporadas sugestões e atualizadas as informações sobre o processo de regulamentação da matéria. Este texto é resultado da pesquisa "Deontologia e Tecnologia: dilemas éticos contemporâneos no jornalismo", financiado pelo CNPq.

Rogério Christofoletti
Professor e pesquisador do Departamento e do Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina (UFSC). Bolsista de produtividade do CNPq e um dos líderes do Observatório da Ética Jornalística (objETHOS).
E-mail: rogerio.christofoletti@uol.com.br.

SUBMETIDO EM: 10/10/2015
ACEITO EM: 28/10/2015

PERSPECTIVAS

RESUMO
Este artigo apresenta preocupações sobre a manutenção da privacidade de usuários e jornalistas depois da aprovação do Marco Civil da Internet, em abril de 2014. Esta lei garante a privacidade dos dados de navegação e do uso de aplicações? Diante de gigantes como Google e Facebook, que recolhem e manipulam grandes quantidades de informação pessoal, é possível uma internet sem violações de privacidade? Para responder, vamos discutir o Marco Civil sob os pontos de vista ético e legal. Ainda que a nova legislação esteja restrita ao Brasil, entendemos que o marco regulatório pode contagiar outros países a produzir mecanismos semelhantes para garantir os direitos civis no âmbito da internet.
PALAVRAS-CHAVE: Proteção de dados; Vigilância; Espionagem.

ABSTRACT
This article presents concerns about maintaining the privacy of users and journalists after the approval of the Marco Civil da Internet in April 2014. This law guarantees the privacy of navigation data and the use of applications? Faced with corporations like Google and Facebook, which collect and manipulate large amounts of personal information, is possible a secure internet? To answer, we will discuss the Marco Civil. Although the new legislation is restricted to Brazil, we believe that the regulatory framework can infect other countries to produce similar mechanisms to ensure civil rights in the internet.
KEYWORDS: Data protection; surveillance; Espionage.

As denúncias de espionagem global da National Security Agency (NSA), feitas pelo ex-agente de informação Edward Snowden, não alarmaram apenas os usuários da internet, mas toda a comunidade internacional. Os procedimentos do órgão de inteligência contrariavam acordos diplomáticos, violavam fronteiras internacionais, e ameaçavam a privacidade de governos, empresas e pessoas.

Em junho de 2013, quando as primeiras informações de Snowden vieram à tona, o WikiLeaks já havia produzido grandes vazamentos de dados sigilosos sobre ações dos Estados Unidos e seus aliados no Oriente Médio, e sobre uma quantidade monumental de comunicações oficiais da diplomacia norte-americana. Em julho de 2010, o WikiLeaks tornou públicas informações sobre ofensivas no Afeganistão, e em outubro, sobre o Iraque, apresentando o vídeo em que um helicóptero Apache atira e mata civis, inclusive funcionários da *Reuters*. A partir de novembro de 2010, o WikiLeaks associou-se ao *The New York Times*, *The Guardian*, *Le Monde*, *El País* e *Der Spiegel* para divulgar o impressionante volume de 251 mil mensagens despachadas pela diplomacia norte-americana em 180 países (LEIGH & HARDING, 2011; EL PAÍS, 2012).

Embora o WikiLeaks não fosse uma unanimidade (DOMSCHEIT-BERG, 2011), a repercussão de suas denúncias fortaleceu um debate internacional sobre o poder de alguns governos no novo ecossistema midiático global. Becerra y Lacunza (2012), por exemplo, filtraram as revelações para mostrar as relações perigosas entre meios de comunicação e governos na América Latina, notadamente Argentina, Peru, Chile, Colombia, Bolívia, Equador, Honduras, Venezuela, Brasil e México. Brevini, Hintz e McCurdy (2013) organizaram uma obra coletiva que detalha o legado do WikiLeaks para o futuro da comunicação, jornalismo e sociedade. Mais restritos, Christofoletti e Oliveira (2011) apontaram algumas implicações para a deontologia jornalística. Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn e Jérémie Zimmermann denunciaram os perigos para a liberdade num futuro próximo, onde a internet está totalmente integrada à vida social e amplamente dominada por corporações tecnológicas. Esses conglomerados recolhem, colecionam e comercializam dados de bilhões de pessoas no planeta. Aliados a governos, ajudam a compor um cenário de intensa vigilância eletrônica. Tentando equilibrar as relações, os autores reivindicam "privacidade para os fracos e transparência para os poderosos" (ASSANGE, 2013; 2015).

Espionagem global e violação de direitos

Os constrangimentos públicos provocados pelo grande vazamento de novembro de 2010 não impediu que outro rumoroso episódio acontecesse e expusesse a maior potência financeira e militar do planeta. O caso Snowden trouxe outros elementos para o debate global sobre política e tecnologia, sociedade e informação, transparência e privacidade.

Snowden informou ao repórter Glen Greenwald, do *The Guardian*, que a NSA ignorava seus limites constitucionais e vigiava cidadãos fora das fronteiras dos Estados Unidos, bem como espionava chefes de Estado. Foi revelado que a chanceler alemã Angela Merkel e os presidentes Antonio Pieña Nieto (México) e Dilma Rousseff (Brasil) tiveram seus celulares monitorados. A agência de inteligência coletou metadados das comunicações desses líderes e de assessores próximos, obtendo eventuais vantagens políticas e comerciais (HARDING, 2014).

Segundo Greenwald (2014), com a colaboração de empresas de tecnologia como Ap-

ple, Microsoft, Google, Verizon e Facebook, a NSA poderia acessar, coletar e analisar grandes quantidades de dados pessoais: tweets, posts de Facebook, conversas por Skype e chats, históricos de navegação, SMS, arquivos em Skydrive, metadados de telefonia móvel e até transações bancárias privadas. A agência seria capaz de identificar IPs, localizar rapidamente usuários, e fazer monitoramento de navegação em tempo real[1].

Mais recentemente, vieram à tona novos relatos de colaboração de empresas de telefonia com os esforços de espionagem do governo dos Estados Unidos. Segundo o *The New York Times*, a AT&T desde setembro de 2003 é parceira da NSA, e em 2011, começou a repassar diariamente para a agência mais de 1,1 bilhão de registros telefônicos de celulares norte-americanos[2].

Para Greenwald, vários fatores contribuíram para o abuso de poder da NSA: o clima de terror pós-11 de setembro, a criação de leis aumentando as prerrogativas do governo, a não necessidade de mandados judiciais para vigiar, e a cooperação de empresas de informática e telefonia de vários países. A instalação de dispositivos para captura de dados em cabos submarinos de comunicação, a facilitação na criptografia pelos próprios fabricantes de computadores, e a colocação de *backdoors* em modens seriam condições tecnológicas para violações quase imperceptíveis. Além disso, o Congresso dos Estados Unidos pouco controla as agências de inteligência do governo.

Indignada com as denúncias de Snowden sobre espionagem, a presidente brasileira Dilma Rousseff discursou na Assembleia Geral da Organização das Nações Unidas em setembro de 2013, denunciando violações à soberania e à privacidade de governos independentes e legítimos. Rousseff queixou-se também de espionagem industrial, já que a NSA havia interceptado informações restritas da maior empresa brasileira, a Petrobras (ROUSSEFF, 2013; WATTS, 2013). O presidente Barack Obama veio a público para atenuar o grau das denúncias, e o ex-agente de informação Edward Snowden se asilou na Rússia, temendo por segurança. À época, a presidente brasileira engrossou o tom das queixas e cancelou uma viagem oficial agendada para os Estados Unidos, o que estremeceu ainda mais as relações entre os dois países.

As denúncias de espionagem e violação de privacidade serviram de munição para que o governo brasileiro agilizasse a aprovação de um projeto de lei para regulamentar os direitos dos usuários da internet no Brasil. Chamado de Marco Civil da Internet, a proposta ingressou no Parlamento em 2011 e foi aprovada três anos depois, com intensas discussões (DEL BIANCO; BARBOSA, 2015).

Em abril de 2014, o Marco Civil da Internet tornou-se lei no Brasil, estabelecendo direitos básicos para o usuário, determinando contrapartidas dos provedores de serviços, e definindo responsabilidades de setores públicos. Mas pode-se afirmar que o Marco Civil garanta a privacidade das pessoas? A nova lei oferece instrumentos para cidadãos e jornalistas resguardarem seus dados de navegação e de aplicações? Como lidar com conglomerados globais de tecnologia - como Google e Facebook -, que atuam na escala de bilhões de pessoas e ignoram fronteiras nacionais? É possível que organizações jornalísticas e usuários preservem seus dados pessoais? Temos uma in-

1 As reportagens renderam o Prêmio Pulitzer de 2014 (http://www.pulitzer.org/citation/2014-Public-Service) e o documentário "CitizenFour", de Laura Poitras, sobre o encontro com Snowden em Hong Kong e as denúncias globais ganhou o Oscar 2015 (http://www1.folha.uol.com.br/ilustrada/2015/02/1593404-citizenfour-sobre-edward-snowden-vence-o-oscar-de-melhor-documentario.shtml).

2 Ver <http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0> Acessado em 29 de agosto de 2015.

ternet segura?

Uma privacidade agonizante

Greenberg (2012) lembra que a atuação de vazadores de informação não é uma novidade na política dos Estados Unidos. O autor remete a Daniel Ellsberg, responsável pelos chamados "Pentagon Papers" na década de 1970, para atualizar o debate em torno dessas controversas figuras. À época, o então funcionário do Pentágono repassou de forma clandestina 14 mil páginas de documentos secretos para *The New York Times*, revelando fatos obscuros da Guerra do Vietnã. Greenberg avalia o cenário composto por WikiLeaks, OpenLeaks, GlobaLeaks e iniciativas semelhantes, e parece que o mundo está longe de ver o fim dos vazadores.

Denunciantes ou delatores, patriotas ou traidores, esses personagens têm influenciado o debate público sobre limites para os poderosos. No caso da privacidade de dados, entendemos que a batalha está apenas começando, pois os usuários despertaram para o tema tardiamente.
É importante frisar que a privacidade é uma invenção humana, e essa criação muda com o tempo e a geografia, demonstram Habermas (1984), Ariès e Duby (1990, 1991a, 1991b, 1992a, 1992b), Giddens (1993), entre outros. Da dicotomia entre o que era social/reservado à oposição transparente/secreto, as transformações observadas contagiam costumes, disposição arquitetônica, organização política, etc.

As mutações mostram-se mais drásticas e dinâmicas nas últimas décadas, com um acirramento do processo de individualização, a disseminação de uma cultura do eu, e a busca de uma "redenção social" (BAUMAN, 2001). Para Prior e Sousa (2014:11, 13), na atualidade, verificamos "uma verdadeira democratização da intimidade" por um lado, e a "incessante necessidade de aprovação e diversão relativamente ao meio envolvente". Conforme os autores, "assiste-se à exposição orgulhosa do individual, do emocional e do secreto enquanto categorias que permaneciam, até aqui, na esfera íntima" (*idem*). Tal exposição é intensificada pelas tecnologias de informação e pelas redes sociais digitais, espelhos atuais do eu e da exaltação do indivíduo singular.

Estaríamos, então, abrindo mão do que nos acostumamos a chamar de privacidade?

Há uma década, Koops & Leenes (2005) já apontavam alguns danos à privacidade no que se refere aos códigos computacionais, sistemas e algoritmos. Para eles, temas como interceptação de dados por telecomunicações, geolocalização e criptografia mereceriam mais atenção de usuários e provedores, pois sua evolução contribuiria para uma "erosão da privacidade". Para contê-la, os autores sugerem que governos exijam - a exemplo do meio ambiente -, "declarações de impacto à privacidade" de novos produtos e serviços. E que haja esforços para sensibilizar cidadãos, governos e desenvolvedores sobre a importância da privacidade. Este "é, de fato, um primeiro passo crucial para frear a espiral descendente da erosão da privacidade que é, em parte, resultado de uma miopia" (*op.cit.*: 188). Se o usuário não vê o que está perdendo, não tem porque se importar.

O perigo alardeado por Koops & Leenes foi anteriormente sinalizado por Sykes (1999) e Whitaker (1999), entre outros, que não economizam tintas para pintar um cenário terminal. O panorama é composto por sociedades dominadas pela tecnologia, onde governos e empresas exercem extrema vigilância e controle social, e o usuário ignora

REVISTA ECO PÓS | ISSN 2175-8689 | AS FORMAS DO ARTÍFICIO | V. 18 | N. 3 | 2015 | PERSPECTIVAS

os riscos, conformando-se com comodismos técnicos. Falência das políticas de privacidade e termos de uso[3], perda de controle de dados em serviços de email[4], mudanças nos protocolos de privacidade de redes sociais[5] e até mesmo "experimentos emocionais" no Facebook[6] já foram motivos de denúncias e controvérsias anos atrás.

A temperatura vem subindo ultimamente. Em setembro de 2014, WikiLeaks denunciou o uso do FinFisher, software de espionagem usado por governos para vigiar ativistas, dissidentes políticos e jornalistas[7]. Quatro meses depois, em janeiro de 2015, o WikiLeaks acusou o Google de ter facilitado as autoridades dos Estados Unidos o acesso ao correio eletrônico de três de seus responsáveis. A Justiça norte-americana confirmou que está investigando o coletivo[8]. Dois meses depois, em março, a Wikimedia, organização responsável pela Wikipedia, juntou-se à American Civil Liberties Union e outras sete entidades para a abertura de um processo contra NSA e o Departamento de Justiça dos Estados Unidos. A acusação é de violação da 1ª e 4ª Emendas da Constituição na medida em que se configura a prática de "vigilância upstream", monitoramento de comunicações com sujeitos não norte-americanos, potencialmente provocando embaraços a assuntos de segurança nacional, geopolítica ou relações exteriores[9]. As queixas não são exageradas, afinal a NSA e a *Government Communications Headquarters* (GCHQ) – a análoga agência britânica – têm condições de vigiar cidadãos não apenas nos domínios da internet, mas também em suas comunicações por dispositivos móveis[10].

O rosto mais visível e conhecido do WikiLeaks não poupa cargas contra o governo norte-americano, suas agências de inteligência e os grandes conglomerados de mídia e tecnologia. Para Julian Assange, o negócio de Google, Facebook e demais gigantes do setor é "a destruição industrial da privacidade"[11].

Além das declarações mais radicais, chamam a atenção também relatórios como o da American Civil Liberties Union & Human Rights Watch (2014) sobre como o monitoramento em larga escala empreendido pelos Estados Unidos pode afetar a liberdade de expressão, o jornalismo, a lei e a própria democracia! O prestigioso Pew Research Center divulgou em dezembro de 2014 um alentado documento onde tenta entrever o que poderia ser o futuro da privacidade em tempos tão sombrios como os nossos[12]. No caso dos conglomerados midiáticos e de tecnologia, os alertas vêm de Pariser (2012), que aponta como o usuário está cada vez mais preso numa bolha de filtros de Google e Facebook. Waters & Ackerman (2011), Tello (2013), Yang, Brown & Braun (2014), e Marwick & boyd (2014) preocupam-se com o gerenciamento de dados priva-

3 Privacy Policies Are Dead, Privacy Watchdog Says. Disponível em < http://readwrite.com/2011/01/07/privacy_policies_are_dead_privacy_watchdog_says> Acessado em 09 de dezembro de 2014.

4 La verdade sobre la falta de privacidade em Gmail. Disponível em < http://www.enter.co/cultura-digital/redes-sociales/la-verdad-sobre-la-falta-de-privacidad-en-gmail/> Acessado em 15 de dezembro de 2014.

5 Mais detalhes em <http://blogs.estadao.com.br/link/o-xereta/> e http://www.clasesdeperiodismo.com/2010/05/13/la-privacidad-en-facebook-infografia/

6 Privacy watchdog files complaint over Facebook emotion experiment. Disponível em < http://www.theguardian.com/technology/2014/jul/04/privacy-watchdog-files-complaint-over-facebook-emotion-experiment> Acessado em 12 de janeiro de 2015.

7 Ver: http://www.clasesdeperiodismo.com/2014/09/15/wikileaks-filtra-detalles-sobre-el-software-para-espiar-periodistas/ Acessado em 31/01/2015.

8 Ver: http://www.clasesdeperiodismo.com/2015/01/26/wikileaks-acusa-a-google-de-permitir-el-acceso-a-sus-correos/ Acessado em 12/03/2015.

9 Ver: http://www.observatoriodaimprensa.com.br/news/view/criadores_da_wikipedia_processam_a_nsa / Acessado em 01/04/2015.

10 Ver: http://fndc.org.br/clipping/nsa-e-aliados-tem-chaves-criptograficas-para-ouvir-celulares-em-todo-o-mundo-940483/ Acessado em 01/04/2015.

11 No artigo "Who should own the internet?", publicado originalmente no The New York Times em dezembro de 2014 e reproduzido em outros jornais. Disponível em <http://www.nytimes.com/2014/12/04/opinion/julian-assange-on-living-in-a-surveillance-society.html?_r=4> Acessado em 25/01/2015.

12 http://www.nytimes.com/2014/12/04/opinion/julian-assange-on-living-in-a-surveillance-society.html?_r=4> Acessado em 25/01/2015.

REVISTA ECO PÓS | ISSN 2175-8689 | AS FORMAS DO ARTÍFICIO | V. 18 | N. 3 | 2015 | PERSPECTIVAS

dos na maior rede social do planeta.

A regulação da Internet e a busca de um equilíbrio maior entre os atores da rede passam inevitavelmente pela discussão de regras de uso, garantias, proteções e contrapartidas. Guardia Crespo (2014), por exemplo, analisa a realidade boliviana e detecta falhas que constrangem os direitos de intimidade e privacidade, entre outros. Para o autor, o combate passa pela formulação de leis que equilibrem os processos de interação entre usuários, empresas, desenvolvedores e governos, regulando direitos e obrigações, preservando direitos civis e a liberdade de expressão.

As preocupações com a ausência de limites dos grandes conglomerados de tecnologia e com suas atuações predatórias têm provocado reações de importantes organismos multilaterais, como a Organização das Nações Unidas, que no final de março de 2015 criou uma relatoria especial sobre o direito à privacidade. A iniciativa foi resultado da ação direta de Brasil e Alemanha junto ao Conselho de Direitos Humanos da ONU, e tem como base o artigo 12 da Declaração Universal dos Direitos Humanos e o artigo 17 do Pacto Internacional sobre os Direitos Civis e Políticos. A relatoria especial poderá monitorar o vigilantismo global, fazer missões in loco, apresentar denúncias de violação da privacidade e recomendar ajustes a governos e outros atores diretamente envolvidos .

Neste contexto, o caso brasileiro do Marco Civil da Internet nos parece adequado para analisar potencialidades e fragilidades desses dispositivos numa arena tão controversa.

Regulação da internet

No Brasil, a exemplo de outros países, a intimidade é um direito fundamental, previsto na legislação superior. Conforme a Constituição Federal (BRASIL, 2015), "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas" (artigo 5º, inciso X), e a privacidade está entre os direitos e garantias fundamentais de todos os cidadãos. Sigilos bancário, fiscal e de correspondência, também previstos em lei, respaldam e fortalecem o direito à intimidade. A interceptação de dados (inclusive por vias eletrônicas) é uma violação desse direito, conforme a Constituição (artigo 5º, inciso XII) e a Lei nº 9296/96, que regulamenta o tema.

Intimidade e privacidade estão ligadas à capacidade do indivíduo de se reservar, buscar proteção de ambientes e situações públicas, enfim, ser deixado em paz. A intimidade varia de sujeito para sujeito, mas sua demanda se mostra universal. Do ponto de vista das doutrinas jurídicas, o direito à intimidade é resultado da consagração do princípio da dignidade humana. Isto é, ele é uma das exigências básicas para que o ser humano tenha uma vida digna em sociedade. Em meio ao cenário de convergência midiática e de intensificação das tecnologias de informação e comunicação, a privacidade ganha novos contornos porque se tornam mais complexas as formas de gerenciamento da vida íntima e da imagem pública. Isto é, existem hoje muitas maneiras de exibir o que antes circulava de forma restrita, aumentando a necessidade de mais cuidados para a preservação dos próprios dados.

Em termos estatísticos, o Brasil é um grande mercado para a indústria de produtos e serviços de tecnologia. Tem uma população estimada em 204 milhões de pessoas, conforme dados de agosto de 2015 do Instituto Brasileiro de Geografia e Estatística

REVISTA ECO PÓS | ISSN 2175-8689 | AS FORMAS DO ARTÍFICIO | V. 18 | N. 3 | 2015 | PERSPECTIVAS

(IBGE). Pesquisa Nacional por Amostragem Domiciliar (PNAD) do mesmo órgão apontava que 50,1% dos habitantes tinham acesso à internet em setembro de 2014. Observa-se também que percentuais de uso e acesso vêm subindo gradativamente, impulsionados por ações governamentais (como o Plano Nacional de Banda Larga, que pretende universalizar a internet até 2018) e pela popularização de computadores, notebooks, tablets e telefones celulares. Segundo a Agência Nacional de Telecomunicações (Anatel), em julho de 2015, estavam ativas 281,5 milhões de linhas de celulares no país, três quartos delas de aparelhos pré-pagos. Mais de 76% dos jovens entre 15 e 17 anos afirmam usar internet. É neste cenário que o debate sobre privacidade e regulação da internet ganha peso na democracia e na busca por justiça social no país.

Em 2009, o Comitê Gestor da Internet (CGI-BR) formulou documento com princípios para governança e uso da internet no país. Com dez pontos, a resolução enaltece a liberdade, privacidade e direitos humanos, governança democrática e colaborativa, universalidade, diversidade, inovação, neutralidade de rede, inimputabilidade da rede, funcionalidade, segurança e estabilidade, padronização e interoperabilidade, ambiente legal e regulatório (CGI, 2009). A proposta auxiliou o governo a elaborar projeto de lei para regular o setor, e em 2010 e 2011, foram promovidas audiências públicas que discutiram o texto inicial.

Segurado (2011) descreveu o processo colaborativo do debate antes da apreciação, votação e aprovação do projeto de lei que originou o marco regulatório. Ferreira (2014), por sua vez, investigou de que forma convergiam a agenda governamental e a agenda brasileira de regulação da internet. A atuação de atores visíveis e invisíveis, os debates acerca de propostas como a Lei de Cibercrimes (a chamada Lei Azeredo, rechaçada) e movimentos internacionais ajudaram a criar uma janela de oportunidade para a emergência do Marco Civil. Uma plataforma eletrônica recolheu cerca de duas mil sugestões da sociedade, e uma comissão de especialistas sistematizou o conteúdo, dando nova redação ao projeto. Bragatto, Sampaio e Nicolás (2015a; 2015b) avaliam que foi um processo democrático de consulta, tanto no formato quanto na execução, apesar da restrição de público. Para além de um gesto democrático, Parode, Zapata e Bentz (2015) consideram que a abertura do governo para uma discussão pública em plataforma digital do texto da lei significa "uma renovação ética". Examinando o projeto de lei que se tornaria o Marco Civil da Internet, Boff e Fortes (2014) avaliaram a privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental, calcado na Constituição Federal e outros dispositivos.

Em agosto de 2011, o Poder Executivo entrou com a proposta na Câmara Federal, e o projeto foi à votação pela primeira vez em julho de 2012. Apesar de receber apoio público de entidades e ciberativistas célebres, sem quórum no Congresso, o projeto foi retirado de pauta. Sua votação foi adiada outras vezes, enquanto as empresas de telecomunicações e informática faziam pressão contrária a sua aprovação. No segundo semestre de 2013, com as denúncias de Edward Snowden, o Marco Civil da Internet passou a ser prioridade para o governo Dilma Rousseff, que teve dificuldades para unir sua base parlamentar em torno do tema[13].

Após queixas na ONU, a presidente brasileira queria dar um recado global, aprovando uma legislação que protegesse os usuários e comprometesse governos e empresas. O

13 Um dos episódios mais ruidosos foi protagonizado pelo deputado Eduardo Cunha (PMDB-RJ), que liderou o grupo que ajudou a impedir a votação mais de uma vez. Mesmo fazendo parte da base aliada, Cunha contrariou a orientação do partido e arregimentou parlamentares na estratégia de obstrução. Cunha imporia nova derrota ao governo em janeiro de 2015 quando se tornou presidente da Câmara Federal, vencendo com margem folgada. Meses depois, o deputado alardearia publicamente "estar na oposição".

Brasil sediaria em abril de 2014 o NetMundial (Encontro Multissetorial Global Sobre o Futuro da Governança da Internet), oportunidade única para essa demonstração. Em março daquele ano, o projeto de lei do Marco Civil da Internet foi aprovado na Câmara Federal e, no mês seguinte, confirmado no Senado, tornando-se lei no dia de abertura do tão esperado evento.

O surgimento do Marco Civil da Internet foi o maior trunfo do governo Rousseff no campo da comunicação em seu primeiro mandato. Criticada pela descontinuidade das políticas públicas de seu antecessor, Luiz Inácio Lula da Silva, e pelas poucas ações na área, a presidente deu o primeiro passo para uma regulamentação no setor. Mas o Marco ainda carece de leis que especifiquem alguns aspectos importantes, como a neutralidade de rede.

O lugar da privacidade no Marco Civil

A lei nº 12.965, de 23 de abril de 2014, chamada de Marco Civil da Internet, é composta por 32 artigos, organizados em cinco capítulos: disposições preliminares, direitos e garantias dos usuários, provisão de conexão e de aplicações de internet, atuação do poder público e disposições finais.

Nas disposições preliminares, a lei reverbera os princípios anteriormente elaborados pelo CGI-BR (2009) para orientar a finalidade social da internet e seu papel na emancipação individual e coletiva, e lista um curto glossário de termos técnicos mencionados ao longo de seu texto.

No Capítulo II, o artigo 7º da lei assegura ao usuário a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; garante o sigilo do fluxo de suas comunicações pela internet (exceto a quebra do sigilo por ordem judicial); mantém o sigilo das comunicações privadas armazenadas, e proíbe o fornecimento a terceiros dos dados pessoais dos usuários, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado. Segundo a lei, são ainda direitos do usuário ter informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, e solicitar a exclusão definitiva de seus dados das aplicações de internet, quando encerradas as relações com o provedor de serviços.

O Marco Civil também estende ao usuário os direitos da legislação de proteção ao consumidor. A afirmação dos direitos e a definição clara do que a internet representa para o convívio social atual nos parecem ser aspectos muito positivos para os usuários, o que permite entrever que o Marco seguiu uma orientação majoritária do usuário e não mercadológica. Neste sentido, a norma tem um espírito cidadão e não mercantil, um avanço no que tange ao escopo e ao histórico de grande parte da legislação brasileira. O Capítulo III – que trata da provisão de conexão e de aplicações de internet – é o mais sensível para a análise que nos propomos, já que ele se desdobra em seções que abordam a proteção aos registros, aos dados pessoais e às comunicações privadas, a guarda dos registros de conexão, a requisição judicial dos registros, e a responsabilidade por danos derivados de conteúdos gerados por terceiros. O capítulo também aborda outro aspecto preocupante na matéria, a neutralidade da rede, que não trataremos aqui.

O artigo 10 determina que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, assim como de dados pessoais e do conteúdo de comunicações privadas, devem se reger pela preservação da intimidade, da vida privada, da honra e da imagem das pessoas direta ou indiretamente envolvidas. Mandados judiciais podem permitir que o provedor dos serviços apresente tais dados. Conforme a lei, medidas e procedimentos de segurança e sigilo devem ser informados de forma clara pelo provedor aos usuários, "respeitado seu direito de confidencialidade quanto a segredos empresariais", condição ampla e que pode se constituir numa brecha perigosa para a não informação devida. Um exemplo: alegando manter sigilo empresarial sobre suas práticas no setor, o Google pode não tornar muito claro aos usuários o funcionamento de seu serviço de e-mail - o Gmail -, fragilizando a prerrogativa da lei.

Conforme o artigo seguinte – 11 -, devem ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros "em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional". A salvaguarda se faz necessária num ambiente dominado por corporações transnacionais, sediadas em países com regras muito flexíveis quando não omissas. Neste sentido, o Marco Civil garante um fórum nacional de dissolução de litígios, mais uma garantia aos usuários numa eventual disputa assimétrica.

Apesar disso, os parágrafos 3º e 4º do mesmo artigo permitem novas brechas quando obrigam os fornecedores a prestar informações quanto ao cumprimento da legislação, mas não definem como tais infrações serão apuradas. O Marco Civil posterga tais detalhes a uma futura regulamentação, mas permanecem as dúvidas: Quem irá fiscalizar os provedores de serviços? O usuário e o governo podem confiar na boa fé dos players do mercado e esperar que eles atendam aos protocolos previstos? Como deve funcionar a instância de fiscalização desses atendimentos? Corporações transnacionais de tecnologia vão contrariar seus interesses para atender às exigências das autoridades brasileiras? Jornalistas contarão com proteções especiais?

O Marco Civil menciona sanções cíveis, criminais e administrativas, e define quatro tipos de penalidades, que podem ser aplicadas isoladas ou cumulativas (art. 12): a) advertência, com indicação de prazo para medidas corretivas; b) multa de até 10% do faturamento anual do grupo econômico no país; c) suspensão temporária das atividades; d) proibição das atividades no país.

A lei determina ainda que cabe ao administrador do sistema manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, e que sua manutenção não pode ser transferida a terceiros. A medida inibe comércio ou vazamento de dados, mas a legislação é falha quando não define sanções em caso de descumprimento. Conforme o parágrafo 6º do artigo 12, para definir as penalidades "serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência". Um grau de subjetividade bastante perigoso.

Segurado, Lima e Ameni (2014) compararam o Marco Civil brasileiro a dispositivos análogos de outros quatro países - Chile, Espanha, França e Estados Unidos – no que

afetam a neutralidade de rede, a privacidade e a proteção a direitos autorais[14]. Interessa-nos discutir aqui possíveis impactos à privacidade e, neste sentido, os autores lembram que "os defensores da garantia da privacidade na internet argumentam que a guarda de registro de acessos dos *logs* (dados de conexão) deve ser realizada pela Justiça mediante suspeita de crime, e não de forma indiscriminada. Caso contrário, é violação da privacidade e cerceamento da liberdade de expressão e de comunicação" (p.9). Os autores se referem ao artigo 15 da lei, que obriga o provedor a manter os logs sob sigilo, em ambiente seguro e controlado por seis meses.

Silveira (2014) explica que, "apesar de o Marco Civil ser a lei mais avançada do mundo na garantia dos direitos individuais na rede, de assegurar a neutralidade como princípio central da internet livre, de ter sido formulada de modo colaborativo", para ser aprovada na Câmara Federal, foi necessário fazer concessões, o que levou o relator da matéria, o deputado Alessandro Molon (PT-RJ) a "incorporar no projeto alguns dispositivos nocivos à defesa da privacidade". A obrigatoriamente da guarda dos logs é um desses enxertos indesejáveis, já que a lei

> ao obrigar – ao invés de restringir – a guarda de logs de aplicação, está ampliando e legalizando esse mercado de observação e análise de nossas vidas que é feito pela redução crescente da privacidade e da intimidade dos cidadãos. Mesmo restringindo a obrigatoriedade de guarda das informações às pessoas jurídicas com fins econômicos, ela expandirá o mercado de vigilância (SILVEIRA, 2014, p. 06).

Neste aspecto em particular, o Marco Civil recua diante das pressões para que haja uma vigilância maior dos atos do usuário, deixando escapar a privacidade pelos dedos da lei. Silveira aponta mais uma fragilidade no artigo 15:

> A busca da defesa da privacidade como direito fundamental da comunicação em rede se choca com parte da dinâmica da economia informacional, pois nossos dados de navegação são extremamente valiosos. O armazenamento desses dados de navegação nos torna completamente fragilizados diante de grandes corporações e de segmentos políticos autoritários que ocupam a máquina de Estado. Outro grande problema do Artigo 15 é que após os seis meses em que os dados devem estar "guardados sob sigilo, em ambiente controlado e de segurança", poderá ocorrer a troca dos mesmos com empresas especializadas em processar informações de navegação e realizar cruzamentos inaceitáveis, pois comprometem completamente nossa intimidade. Repare que apesar do texto do Artigo 15 enfatizar que a segurança dos dados armazenados é fundamental, ela só seria efetiva para o cidadão se seus dados não pudessem ser reunidos e armazenados." (op.cit.)

Como se trata de um item a ser regulamentado ainda, sob a forma de decreto presidencial, certos ativistas defendem o veto do artigo ou nova consulta pública em plataformas online para que a população participe dessas decisões.

Um aspecto positivo do Marco é o impedimento da guarda dos "registros de acesso

14 Em seu comparativo, os autores concluem que a privacidade, a segurança e a vigilância encontram as posições mais retrógradas nos Estados Unidos, seguidos da França e Espanha. A partir dos ataques de 11 de setembro de 2001, os EUA adotaram controle e espionagem cada vez maior da internet e de ligações telefônicas, não somente de seus cidadãos, mas de vários países do mundo, incluindo o Brasil. A legislação dos Estados Unidos oferece grandes perigos à privacidade. Os norte-americanos contam com dispositivos legais como o Patriot Act, a Communications for Law Enforcement Act (CALEA, lei de auxílio das comunicações para a aplicação do direito) e a Foreign Intelligence Surveillance Act (FISA, lei de vigilância de inteligência estrangeira), que garantem prerrogativas de grande intrusão na vida de cidadãos. Embora vigentes apenas naquele território, essas leis podem ser invocadas em situações específicas envolvendo estrangeiros e, pior, contagiar países aliados a adotarem legislações análogas, ampliando o cerco à intimidade online. Ainda conforme Segurado, Lima e Ameni (2014), França e Espanha acompanham os Estados Unidos nos últimos anos e vêm defendendo a necessidade de maior controle da internet pelos governos em parceria com as corporações.

a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, e de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular" (artigo 16). É cada vez mais comum que, para utilizar um determinado aplicativo ou sistema, o usuário seja "convidado" a fazer o login pelo Google, Facebook ou assemelhados. Apresentada como uma facilidade - já que é uma alternativa mais rápida do que fazer novo cadastro - a operação permite comutação de dados entre os provedores, fragilizando sua privacidade. Embora Facebook, Twitter e outros peçam a anuência do usuário – através de cliques expressando sua concordância com termos de uso -, observa-se que o comportamento padrão do usuário é buscar sua conveniência, muitas vezes, não lendo tais documentos, ignorando as condições a que está submetido. A proibição expressa no artigo 16 é salutar, mas não se pode ignorar que ela dependa de mais cuidados técnicos, jurídicos e até mesmo educacionais para ser concretamente aplicável. O mesmo se dá com os dados "excessivos em relação à finalidade" contratada. A definição deriva para um terreno muito subjetivo...

A assunção de que o poder público – em suas variantes geográficas e institucionais – deve zelar pelo assunto é outro aspecto positivo do Marco Civil, embora ele contenha uma fragilidade visível: dilui tal responsabilidade nos vários setores do Estado, o que provoca alguma miopia no usuário: a quem recorrer diante de violações à regra?

Considerações finais

A regulação da Internet parte do Marco Civil de 2014, mas ainda depende do detalhamento de alguns aspectos, como a neutralidade de rede, privacidade, sigilo das comunicações e a proteção de registros e dados pessoais.

Segundo o artigo 9º, cabe à presidência da República – com apoio da Agência Nacional de Telecomunicações (Anatel) e do Comitê Gestor da Internet (CGI-BR) - editar decreto com regras para a neutralidade de rede e outros dispositivos. Respondendo a críticas da oposição, o governo Rousseff incentivou mecanismos para debates públicos do tema.

Em dezembro de 2014, o Comitê Gestor da Internet criou um formulário eletrônico para colher sugestões (http://marcocivil.cgi.br/). Na sequência, um grupo de trabalho multissetorial deve sistematizar os dados e promover reuniões públicas para discutir a minuta do documento a ser endereçado ao governo. O formulário eletrônico permite que sejam encaminhadas sugestões para definições técnicas, neutralidade de rede, proteção aos registros, dados pessoais e comunicações privadas, guarda de registros de conexão, guarda de registros de acesso a aplicações de internet na provisão de aplicações, etc..

No final de janeiro de 2015, o Ministério da Justiça criou plataformas específicas para recolher contribuições para o decreto de regulamentação do Marco Civil (http://participacao.mj.gov.br/marcocivil/) e para o projeto de lei de Proteção de Dados Pessoais (http://participacao.mj.gov.br/dadospessoais/). A primeira plataforma não tinha um texto base, mas eixos de discussão. Mas a que trata da proteção de dados pessoais ofereceu um texto, elaborado a partir dos debates de 2010 e 2011. Em resumo, o projeto objetiva a assegurar ao cidadão direitos básicos sobre seus próprios dados pessoais, ainda que armazenados em bancos fora do país. Com isso, dá controle sobre como suas informações pessoais são utilizadas, seja por organização, empresa ou

governo, prevê maior transparência, segurança e responsabilidade no uso dos dados, inclusive podendo exigir reparações diante de violação. Vazamentos, dados sensíveis, consentimento dos usuários, transferência internacional de dados, entre outros aspectos também são abordados pelo texto de base.

No final de março de 2015, foi a vez da Agência Nacional de Telecomunicações (Anatel) abrir seu canal público para recolher sugestões à regulamentação do Marco Civil[15]. A consulta iria escorar o posicionamento da agência reguladora na matéria, conforme previsto no artigo 9º do marco regulatório.

As contribuições também vêm por vias não estatais. Quinze organizações não-governamentais e coletivos ativistas formularam um documento de 28 páginas com propostas específicas para os eixos da privacidade e da liberdade de expressão. Entre os signatários estão Artigo 19, Intervozes, Ciranda Internacional da Comunicação Compartilhada e Instituto Brasileiro de Defesa do Consumidor (Idec)[16].

Nem bem foi regulamentado, o Marco Civil da Internet corre o risco de ser adulterado por novos projetos de lei, como é o caso do PL 215, que tramita na Câmara Federal e, que em síntese, permite que o Ministério Público e autoridades policiais tenham autonomia para acessar dados de usuários sem autorização judicial[17]. A medida pode afetar a privacidade dos cidadãos na internet e reeditar discussões acerca de limites de poder do MP e das polícias em investigações, por exemplo.

Um ano após o surgimento do Marco Civil, a sociedade busca formas de se ajustar à nova realidade. O Ministério Público Federal do Rio de Janeiro, por exemplo, recomendou que Apple e Google só disponibilizassem em suas lojas aplicativos que acatassem a Constituição e a nova lei. O motivador foi o Secret, aplicativo que permitia publicar "segredos" de terceiros sem a identificação dos publicadores[18]. A Apple buscou adequações e a Google chegou a obter liberação do produto na justiça, sinalizando quão tensas podem ser as relações daqui para frente.

O marco da internet deve provocar mais reacomodações, prevê Prado (2014):

> Em termos de política pública, os líderes de governo terão que estabelecer entendimentos claros sobre os riscos de privacidade que acompanham a "Internet das Coisas". A capacidade de colocar sensores em praticamente qualquer lugar, para observar o tráfego em uma rua residencial ou para monitorar o uso de energia elétrica de uma casa, sem dúvida, levantam sérias preocupações sobre como toda essa informação será utilizada. Percebendo os benefícios da "Internet das Coisas" no policiamento, por exemplo, pode se exigir um nível sem precedentes de vigilância que a comunidade pode rejeitar. Os reguladores terão de construir um consenso sobre quais as proteções que poderiam ser colocadas para a "Internet das Coisas" e trabalhar através das fronteiras e diferentes níveis de governo para garantir que essas proteções podem e vão ser amplamente aplicadas.

15 Ver<http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/starthtm?infoid=39294&sid=11#.VRytMlxJKIJ> Acessado em 01/04/2015.

16 A proposta pode ser conferida em < http://artigo19.org/wp-content/uploads/2015/03/mciprivacidade.pdf> Acessado em 2/04/2015.

17 Ver <http://fndc.org.br/clipping/projeto-de-lei-em-discussao-na-camara-pode-afetar-privacidade-de-internautas-943579/> Acessado em 01 de setembro de 2015.

18 Importante lembrar que a empresa gerenciadora do aplicativo tem acesso aos metadados de seus usuários o que lhe garante grande poder e total conhecimento dos tais "segredos" a serem publicados. Se lembrada com frequência, esta condição levaria muitos usuários a pensar duas vezes antes de se logar ou de utilizar o aplicativo...

Segundo o autor, governos como o dos Estados Unidos e do Reino Unido já estão se antecipando e discutindo bases para proteger dados dos usuários em tempos de intensa vigilância[19]. O Brasil ainda engatinha nos debates sobre a privacidade na era do Big Data[20], embora alguns usuários já manifestem bastante desconfiança no uso de certos serviços dedicados[21]. Em outras palavras, existe muito ainda a se fazer nesse campo...

Fuchs (2011) já havia sinalizado alguns dos desafios que deveremos enfrentar a partir do espalhamento sem precedentes das redes sociais e das TICs. Bruno (2013) expande a discussão à medida em que oferece um extenso levantamento das tecnologias que permitem não apenas o monitoramento das pessoas por governos e corporações, mas também a sedução de se tornar mais um na esteira do que chama de "vigilância distribuída". As ofensivas contra a privacidade parecem vir de todas as partes...

Em agosto de 2015, o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas apresentou dados preliminares de uma pesquisa com 50 plataformas online, apontando para o fato de que dois terços delas (66%) coletam mais dados do que precisam[22]. No mesmo período, o site Suporte Ninja divulgou dados de análise do tráfego do Windows 10, atestando que a nova versão do sistema operacional da Microsoft, coleta e envia a servidores da empresa uma quantidade "bastante alarmante" de dados, mesmo com as configurações estritas de privacidade[23]. Nos últimos meses, a Microsoft vem incentivando os usuários de seus sistemas a atualizarem suas versões do Windows...

Para concluir, é importante retomar os questionamentos que nos orientaram até aqui. O primeiro perguntava se o Marco Civil garante a privacidade dos usuários. Seria ingênuo pensar que uma lei resolva um conjunto de complexidades como esta. As normas surgem quando o consenso está distante e as reflexões éticas não foram suficientes para criar um ambiente de equilíbrio. A lei prescreve condutas, mas isso não impede seu desacato ou manipulação. Em outras palavras, o Marco Civil é um ponto de partida importante, mas a instauração de uma nova ordem na internet no Brasil vai depender de outros esforços, também nos campos da educação e da cultura.

A segunda pergunta ansiava por saber se o Marco oferece instrumentos para cidadãos e jornalistas resguardarem seus dados de navegação e de aplicações. A resposta é afirmativa, embora algumas dessas armas sejam ainda débeis. Daí a importância do momento atual, quando se busca regulamentar a lei. Os dispositivos auxiliares da lei terão que expressar os interesses dos usuários, reforçando a figura da privacidade e enaltecendo a intimidade como direito inalienável de base para a internet. Se os próximos capítulos jurídicos seguirem essa direção, haverá mais equilíbrio nas relações entre usuários, fornecedores de serviços, governos e outras partes interessadas.

Entretanto, profissionais da informação já recorrem a softwares e sistemas que "borram" suas pegadas na internet e dificultam o monitoramento das agências de in-

19 Para mais informações, ver: http://zip.net/blqLGl e http://zip.net/bdqMy7

20 Para ampliar o debate, ver: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=37488&sid=4#.VRr6oOHW4gt Acessado em 20/03/2015.

21 Maioria dos paulistanos não confia nos provedores: Disponível em <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=37397&sid=97#.VRsCp-HW4gt > Acessado em 01/04/2015.

22 Ver <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=40452&sid=4> Acessado em 31 de agosto de 2015.

23 Ver <http://suporteninja.com/microsoft-analise-de-trafego-do-windows-10-para-quais-servidores-ele-envia-suas-informacoes/?fb_ref=Default> Acessado em 01 de setembro de 2015.

teligência. A intensificação da criptografia para troca de mensagens e pacotes de dados, a adoção de precauções mais severas nos contatos com as fontes e esforços para uma especialização de jornalistas em cibersegurança estão se tornando procedimentos cada vez mais comuns e necessários[24]. Duas soluções são bastante usadas por jornalistas: o TOR - um navegador que prioriza o anonimato do usuário e "embaralha" sua localização para sistemas vigilantes[25] - e o Pretty Good Privacy (PGP) – sistema que encriptação de mensagens que permite trocas mais seguras entre as chaves dos usuários. Este dispositivo foi, inclusive, utilizado pelo jornalista Glen Greenwald e por Edward Snowden para suas comunicações iniciais[26]. Empresas de mídia começam a se preocupar com tais cuidados, como é o caso da BBC, cujo programa de formação e reciclagem de jornalistas repassa orientações de cibersegurança e privacidade a seus repórteres[27].

A paranoia contagia outros contingentes de usuários[28]. Ao longo dos últimos dois anos, a mesma BBC já publicou diversas reportagens instruindo seus públicos a como intensificar sua privacidade na internet e nas redes sociais[29]. Em março de 2015, o Pew Research Center divulgou uma pesquisa sobre a reação dos adultos norte-americanos diante das muitas denúncias sobre vigilantismo cibernético. Entre os resultados, verificou-se que uma parcela limitada das pessoas mudou seu comportamento diante dos monitoramentos, e apenas 25% delas passou a usar senhas mais complexas na internet. A pesquisa mostra que a maioria desconhece soluções que aumentem sua privacidade on line, como o uso de sistemas de restringem o rastreamento online.

A pesquisa do Pew aponta que o público se divide quando indagado sobre a legitimidade do uso de programas de vigilância pelas autoridades governamentais: 82% dizem ser aceitável monitorar as comunicações de suspeitos de terrorismo, 60% defendem o monitoramento de líderes americanos (mesmo percentual para os estrangeiros) e 54% consideram aceitável a vigilância de cidadãos estrangeiros. Entretanto, 57% acham inaceitável que o governo monitore os próprios norte-americanos.

Um pouco mais da metade dos sujeitos da pesquisa (52%) se descreveram como "muito preocupados" ou "um pouco preocupados" com a vigilância do governo dos dados dos americanos e das comunicações eletrônicas. Parcelas próximas de um terço demonstram apreensão sobre o monitoramento de telefones celulares (37%) e de suas atividades em redes sociais como Facebook e Twitter (31%)[30].

Os cidadãos brasileiros reagiram com mais ênfase à escalada da cibervigilância, conforme mostra pesquisa feita pela YouGov sob encomenda da Anistia Internacional: 65% reprovam monitoramento e vigilância de governos sobre dados de internet e de telefonia da população, e 78% rejeitam a ideia de que as empresas de tecnologia devem repassar informações aos governos. O índice foi o maior entre os treze países ou-

24 O jornalista argentino Pablo Mancini chegou a elaborar um manual para repórteres na condição de vigiados: "Cryptoperiodismo". Disponível em <http://cryptoperiodismo.org> Acessado em 10/01/2015.
25 Ver: <https://www.wefightcensorship.org/article/improve-your-privacy-and-security-internet-using-torhtml.html> Acessado em 01/12/2014.
26 Outras cinco alternativas de segurança estão em http://www.clasesdeperiodismo.com/2014/09/21/privacidad-y-seguridad-con-estas-5-herramientas/ Acessado em 10/03/2015.
27 Ver: http://www.bbc.co.uk/blogs/collegeofjournalism/entries/386cc28a-80ff-4f06-958d-b44db31b49bf Acessado em 01/04/2015.
28 Na Bélgica, a comissão de privacidade local arrastou o Facebook para os tribunais em junho de 2015, alegando desrespeito às leis europeias e do país sobre o rastreamento de usuários para fins comerciais. Ver <http://www.theguardian.com/technology/2015/jun/15/belgium-facebook-court-privacy-breaches-ads> Acessado em 29 de agosto de 2015.
29 Ver: http://www.bbc.co.uk/portuguese/noticias/2015/03/150227_vert_fut_privacidade_internet_ml Acessado em 11/03/2015.
30 A pesquisa foi feita a partir de entrevistas com 475 pessoas acima dos 18 anos, entre 26 de novembro de 2014 e 3 de janeiro de 2015. O relatório completo pode ser acessado em http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/ Acessado em 30/03/2015.

vidos na pesquisa. Quando perguntados sobre a espionagem norte-americana, 80% dos respondentes brasileiros foram críticos, segunda maior taxa, atrás da Alemanha (81%), outro país atingido conforme os relatos de Edward Snowden[31].

Retornando aos nossos questionamentos: Como lidar com conglomerados globais de tecnologia - como Google e Facebook -, que atuam na escala de bilhões de pessoas e ignoram fronteiras nacionais? Esta terceira questão é bastante concreta, e o Estado pode usar mais o seu poder como moderador das relações econômicas, fazendo prevalecer os interesses da coletividade. O usuário, por sua vez, também pode atuar com mais diligência na condição de consumidor, exigindo o atendimento à lei e as condições de mercado do país. Jornalistas deveriam se engajar mais também.

Com o Marco Civil, temos uma internet segura? A resposta é não. Nossa internet é tão insegura quanto o mundo que habitamos. É claro que o marco regulatório não se propunha a um dispositivo de proteção do usuário, mas de garantias fundamentais de sua condição. No entanto, esperar que o ciberespaço possa ter proteções mínimas é legítimo e extensivo a todos os usuários.Neste sentido, não basta que o cidadão exija dos governos mecanismos de segurança. É preciso participar das discussões e decisões que ajudam a moldar a internet, assumindo uma postura de protagonismo compartilhado, abandonando a "bolha de filtros" (PARISER, 2012). Isto é, são tentadoras as muitas comodidades técnicas, mas o usuário não pode delegar a empresas ou a governos o gerenciamento de seus dados pessoais e da sua vida íntima. Não pode abrir mão de seus direitos, interesses e privacidade. Tais imperativos ganham maior contorno no caso dos jornalistas, profissionais que lidam diariamente com dados, influenciam vidas alheias e necessitam de salvaguardas ainda maiores para a proteção de suas privacidades. Se um repórter não contar com tais garantias, como poderá atuar de forma desembaraçada dentro e fora da internet? Acreditamos que esses profissionais dependam e precisem de garantias adicionais neste ambiente para assegurar segurança pessoal e independência editorial.

Uma advertência de Silveira (2014) dá uma dimensão do que está em jogo quando nos dispomos a discutir privacidade nas sociedades contemporâneas:

> Quanto maior o direito à privacidade que conseguirmos exercer nas redes menor será o tamanho da economia da vigilância e da venda de nossos dados de navegação para o processamento em big data centers. Se os direitos à privacidade avançarem, avançarão com eles as condições básicas para as disputas democráticas e para o controle da sociedade sobre o poder. A redução da privacidade implica no aumento do poder das corporações e de grupos que querem o controle não democrático do Estado.

Embora o Marco Civil da Internet se restrinja ao território brasileiro, observa-se que seu surgimento pode contagiar outros países a criar proteções aos direitos civis no ambiente da rede. A privacidade como a conhecemos, pode estar mudando, mas vamos saber em breve se iremos descartá-la por completo ou redesenhá-la. Avaliar iniciativas como o Marco Civil e os movimentos da sociedade comprometida nos ajudam a entender melhor o que viveremos a seguir.

Referências Bibliográficas

31 Mais informações em <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=39185&sid=18#.VR1A-plxJKIK> Acessado em 29/03/2015.

AMERICAN CIVIL LIBERTIES UNION; HUMAN RIGHTS WATCH. **"With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy",** 2014. Disponible en <http://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf> Consultado en 15/12/2014.
PRADO, Eduardo. **"Internet das Coisas vai obrigar mudanças no Marco Civil da Internet"**. Convergência Digital, 09/09/2014. Disponible en <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=37768&sid=15#.VNTCbXa9XUl> Consultado en 06/02/2015.
ARIÈS, Philipe; DUBY, Georges (orgs.). **História da Vida Privada 1: do Império Romano ao Ano Mil.** São Paulo: Cia das Letras, 1990
_____. **História da Vida Privada 2: da Europa Feudal à Renascença.** São Paulo: Cia das Letras, 1991a.
_____. **História da Vida Privada 3: da Renascença ao Século das Luzes.** São Paulo: Cia das Letras, 1991b.
_____. **História da Vida Privada 4: da Revolução Francesa à Primeira Guerra.** São Paulo: Cia das Letras, 1992a.
_____. **História da Vida Privada 5: da Primeira Guerra a nossos dias.** São Paulo: Cia das Letras, 1992b.
ASSANGE, Julian. **Cypherpunks: liberdade e o futuro da internet.** São Paulo: Boitempo, 2013.
_____. **Quando o Google encontrou o WikiLeaks.** São Paulo: Boitempo, 2015.
BAUMAN, Zygmunt. **Modernidade líquida.** Rio de Janeiro: Zahar, 2001.
BECERRA, Martín; LACUNZA, Sebastián. **WikiMediaLeaks: La relación entre medios y gobiernos de América Latina bajo el prisma de los cables de WikiLeaks.** Buenos Aires: Ediciones B, 2012
BOFF, Salete Oro; FORTES, Vinícius Borges. **A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil.** Sequência. Vol. 35, nº 68, junho de 2014, pp. 109-128
BRAGATTO, Rachel Callai; SAMPAIO, Rafael Cardoso; NICOLÁS, Maria Alejandra. **"A segunda fase da consulta do marco civil da internet: como foi construída, quem participou e quais os impactos?"** Revista Eptic, vol. 17, nº 1, janeiro-abril de 2015, pp.236-255.
_____. **"Inovadora e democrática. Mas e daí? Uma análise da primeira fase da consulta online sobre o Marco Civil da Internet".** Política & Sociedade, Florianópolis, vol. 14, nº 29, janeiro-abril de 2015, pp. 125-150.
BRASIL. **Lei nº 9296, de 24 de julho de 1996.** Disponible em <http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm> Consultado em 20/01/2015.
_____. **Lei nº 12.965, de 23 de abril de 2014. Marco Civil da internet.** Disponíble en http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Consultado em 10/12/2014.
_____. **Constituição da República Federativa do Brasil de 1988.** Disponible em < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Consultado em 20/01/2015.
BREVINI, Benedetta; HINTZ, Arne; McCURDY, Patrick (ed.). **Beyond WikiLeaks: implications for the future of communications, journalism and society.** London: Plagrave Macmillan, 2013.
BRUNO, Fernanda. **Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade.** Porto Alegre: EdiPUCRS, 2013.
CGI-BR. **Resolução CGI-br/RES/2009/003/P.** Disponible en <http://cgi.br/resolucoes/documento/2009/003> Consultado em 20/12/2014.
CHRISTOFOLETTI, Rogério; OLIVEIRA, Cândida. **"Jornalismo pós-Wikileaks: deontologia em temos de vazamentos globais de informação".** Contemporânea, vol. 9, n. 2, 2011, pp. 86-100. Disponível em <https://monitorando.files.wordpress.com/2011/08/wikileaks-christofoletti-e-oliveira.pdf> Consultado em 02/02/2015.
DEL BIANCO, Nelia Rodrigues; BARBOSA, Marcelo Mendes. **"O marco civil da internet e a neutralidade de rede: dilemas, debates e impasses relacionados a este princípio na tramitação do projeto de lei".** Revista Eptic, vol. 17, nº 1, janeiro-abril, 2015, pp.5-19.
DOMSCHEIT-BERG, Daniel. **Os bastidores do WikiLeaks.** Rio de Janeiro: Campus Elsevier.
EL PAÍS (2012). **Las revelaciones de Wikileaks.** Madrid: El País Selección, 2011.
FERREIRA, Juliana Nolasco. **Acessando a rede: um olhar sobre a formação de uma agenda de regulação da internet no Brasil.** Dissertação (Mestrado em Administração Pública), Escola de Administração de Empresas de São Paulo. Fundação Getúlio Vargas, 2014.
FUCHS, C. **Internet and Surveillance: The Challenges of Web 2.0 and Social Media.** New York: Routledge, 2011.
GIDDENS, Anthony. **A transformação da intimidade: sexualidade, amor & erotismo nas sociedades modernas.** São Paulo: UNESP, 1993.
GREENBERG, Andy. **This machine kills secrets. How wikileakers, hactivists and cypherpunks aim to free the world's information.** London: Dutton, 2012.

GREENWALD, Glenn. **Sem lugar para se esconder. Edward Snowden, a NSA, e a espionagem do governo norte-americano.** São Paulo: Sextante, 2014.
GUARDIA CRESPO, Marcelo. **"No te metas en mi vida, privacidad e intimidad en los medios".** Punto Cero, Ano 19 – Nº 28 –1, 2014, pp. 33-44.
HABERMAS, Jurgen. **Mudança estrutural da esfera publica :investigações quanto a uma categoria da sociedade burguesa.** Rio de Janeiro: Tempo Brasileiro, 1984.
HARDING, Luke. **Os arquivos Snowden. A história secreta do homem mais procurado do mundo**. Rio de Janeiro: Leya, 2014.
KOOPS, Bert-Jaap; LEENES, Ronald. "'Code' and the Slow Erosion of Privacy",12 Mich. Telecomm. Tech. L. Rev. 115, 2005. Disponible en<http://www.mttlr.org/voltwelve/koops&leenes.pdf> Consultado em 10/01/2015.
LEIGH, David; HARDING, Luke. **Wikileaks – a guerra de Julian Assange contra os segredos de Estado.** Campinas: Verus, 2011.
MARWICK, Alice E.; boyd, danah. **"Networked privacy: How teenagers negotiate context in social media".** New Media Society, vol. 16(7), 2014, pp. 1051-1067.
PARISER, Eli. **O filtro invisível. O que a internet está escondendo de você.** Rio de Janeiro: Zahar, 2012.
PARODE, Fábio; ZAPATA, Maximiliano; BENTZ, Ione. **Processo de participação coletiva na internet: uma ética para o ciberespaço.** Veritas. Porto Alegre, v. 60, nº 1, janeiro-abril, 2015, pp. 36-46.
PRIOR, Hélder; SOUSA, João Carlos. **"A mudança estrutural do Público e do Privado".** Observatorio (OBS*) Journal, Vol.8, nº 3, 2014, pp. 01-16.
ROUSSEFF, Dilma. **Discurso da Presidente da República Dilma Rouseff na abertura do Debate Geral da 68ª Assembleia Geral das Nações Unidas** – Nova Iorque/EUA. Palácio do Planalto – Presidência da República, Brasília, 2013. Disponiblen en < http://www2.planalto.gov.br/imprensa/discursos/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua > Consultado en: 15/02/2015.
SEGURADO, Rosemary. **O debate sobre o Marco Civil da Internet.** In: IV Congresso Compolítica, Rio de Janeiro, 2011.
SEGURADO, Rosemary; LIMA, Carolina Silva Mandú de; AMENI, Cauê S. **Regulamentação da internet: perspectiva comparada entre Brasil,** Chile, Espanha, EUA e França. História, Ciências, Saúde – Manguinhos, Rio de Janeiro, 2014, pp. 1-21.
SILVEIRA, Sergio Amadeu da. **Marco Civil e a proteção da privacidade.** ComCiência, nº 158, Campinas: 10/05/2014. Disponível em http://www.comciencia.br/comciencia/?section=8&edicao=99&id=1208 Acessado em 31/08/2015.
SYKES, Charles J.. **The End of Privacy: The Attack on Personal Rights at Home, at Work, On-Line, and in Court.** New York: Saint-Martin Press, 1999.
TELLO, Lucía. **"Intimacy and «Extimacy» in Social Networks. Ethical Boundaries of Facebook".** Comunicar, nº 41, vol. XXI, 2013, pp: 205-213.
WATER, Susan; ACKERMAN, James. **"Exploring Privacy Management on Facebook: Motivations and Perceived Consequences of Voluntary Disclosure".** Journal of Computer-Mediated Communication, vol. 17, 2011, pp: 101–115.
WATTS, Jonathan. **"NSA accused of spying on Brazilian oil company Petrobras".** The Guardian, 9 de setembro de 2013. Disponible em <http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras> Consultado en 01/02/2015
WHITAKER, Reg. **The End of Privacy: ow Total Surveillance Is Becoming a Reality.** New York: The New Press, 1999.
YANG, Chia-chen; BROWN, B. Bradford; BRAUN, Michael T. Braun. **"From Facebook to cell calls: Layers of electronic intimacy in college students' interpersonal relationships".** New media & society, Vol. 16(1), 2014, pp: 5–23.