NÚMERO 1

ENSAIOS
DEMOCRACIA
DIGITAL

PRIVACIDADE E INTERNET:

DESAFIOS PARA A DEMOCRACIA BRASILEIRA

DENNYS ANTONIALLI
FRANCISCO BRITO CRUZ

PLATAFORMA DEMOCRÁTICA
FUNDAÇÃO FHC
CENTRO EDELSTEIN

Realização

PRIVACIDADE E INTERNET:

DESAFIOS PARA A DEMOCRACIA BRASILEIRA

DENNYS ANTONIALLI
FRANCISCO BRITO CRUZ

Plataforma Democrática (www.plataformademocratica.org) é uma iniciativa da Fundação FHC e do Centro Edelstein de Pesquisas Sociais dedicada ao fortalecimento das instituições democráticas e da cultura na América Latina, através do debate pluralista de ideias sobre as transformações na sociedade e na política da região e do mundo.

Coleção: Ensaios Democracia Digital
Dirigida por Bernardo Sorj (Centro Edelstein de Pesquisas Sociais) e
Sergio Fausto (Fundação Fernando Henrique Cardoso)

Privacidade e Internet: desafios para a democracia brasileira
Texto no 1, Março de 2017
Dennys Antonialli e Francisco Brito Cruz

Edição da Fundação FHC/Centro Edelstein, 2017
Capa: Lisia Lemes

ÍNDICE

1. Sumário Executivo

1. A tecnologia, e sobretudo a Internet, passaram a intermediar grande parte das atividades da vida cotidiana, seja relações travadas entre usuários de Internet e o setor privado, seja nas relações travadas entre cidadãos e o setor público;

2. A Internet introduziu desafios adicionais para a proteção da privacidade dos usuários na medida em que propicia a utilização de sofisticados e silenciosos mecanismos de coleta e tratamento de dados pessoais;

3. A publicidade comportamental está na base de modelos de negócios amplamente adotados pelas empresas do setor de Internet, o que possibilita o seu oferecimento gratuito mas potencializa a exposição dos usuários de Internet a atividades de coleta de dados pessoais;

4. A estrutura globalizada da rede implica a transferência internacional de dados pessoais por parte de atores do setor privado e coloca em sobreposição modelos regulatórios diferentes, o que gera dificuldades de compatibilização;

5. A existência desses complexos bancos de dados a respeito de usuários de Internet e a multiplicação de dados e registros a seu res-

peito também desperta o interesse dos Estados, que passam a ver nessas informações uma possibilidade de aumentar suas capacidades de vigilância e de eficiência na gestão pública;

6. As prerrogativas de acesso a dados de usuários e a facilidade de coleta de dados e registros sobre a vida dos cidadãos exigem respostas regulatórias que garantam a privacidade dos cidadãos, sob pena de o aumento das capacidades de vigilância dos Estados inibir o exercício das liberdades públicas;

7. No que diz respeito às relações travadas com o setor privado, o ordenamento jurídico brasileiro não dispõe de um marco regulatório completo, capaz de oferecer respostas e balizas precisas para as atividades de coleta e tratamento de dados pessoais, sendo importante que se dê atenção para as propostas legislativas atualmente em debate no Congresso Nacional;

8. No que diz respeito às relações travadas com o setor público, embora o Marco Civil da Internet tenha estabelecido alguns direitos dos usuários, como a proteção da privacidade e da liberdade de expressão com a exigência de ordem judicial para o fornecimento de alguns tipos de registros, a aplicação dessas garantias pelos tribunais precisa ser feita com rigor sob pena de se alargarem muito as prerrogativas de acesso a dados de usuários por parte de autoridades, o que é prejudicial para o direito à privacidade;

9. A ausência de regulamentação específica em relação às atividades de coleta e tratamento de dados pessoais tanto por parte do setor privado quanto por parte do setor público deixa os cidadãos brasileiros muito expostos a violações de sua privacidade, sem remédios efetivos de responsabilização dos atores violadores.

2. Introdução

Já em 1890, *Warren e Brandeis* chamavam a atenção, em seu artigo "The right to privacy", para os riscos que as novas tecnologias, sobretudo no campo fotográfico, carregavam consigo[1]. O poder de capturar e eternizar imagens teria aberto caminho para formas mais invasivas de bisbilhotice da vida privada, na medida em que tornou possível compartilhar registros de momentos vivenciados por outras pessoas. A vida alheia passou a ser, desde então, alvo de escrutínio público e debate político. Em particular, aqueles que por qualquer motivo (fosse ele econômico, político ou social) conquistassem uma posição de destaque, eram constantemente "flagrados" e noticiados pelos jornais, o que, na visão dos autores, trazia sérios desafios para o direito à privacidade.

Mais de cem anos depois, a possibilidade de compartilhamento irrestrito de imagens e vídeos continua representando uma ameaça à privacidade. Essa ameaça ganhou novos contornos, seja com a chegada de tecnologias e dispositivos de captura de imagem muito mais sofisticados, como os drones 2, seja com a multiplicação de espaços e plataformas nos quais esses conteúdos podem ser postados, gerando, inclusive, novas formas de exposição e de violência. A divulgação de imagens íntimas não consentidas, fenômeno que se passou a chamar de "pornografia de vingança" *(revenge porn)*, por exemplo,

tem sido a causa de situações graves de abuso e violência que, em casos extremos, levaram vítimas até a cometer suicídio.[3] De forma similar, a multiplicação desses tipos de registros e a facilidade de encontrá-los por meio dos buscadores fez surgir um debate complexo a respeito do chamado "direito ao esquecimento", a partir do qual usuários poderiam demandar a remoção de notícias ou conteúdos ou a sua respectiva desindexação dos mecanismos de busca, isto é, impedir que esses conteúdos apareçam como resultados de busca.

Mas para além dos mecanismos de captura e compartilhamento de imagens, foi o aparecimento dos computadores e, mais tarde, da Internet, que exigiu uma redefinição da agenda de pesquisa em torno do direito à privacidade. A partir do momento em que passaram a ser possíveis a coleta e o tratamento automatizado de dados pessoais, cresceu o interesse, de empresas e Estados, em explorar as potencialidades desses novos tipos de recursos tecnológicos. Do lado das empresas, a possibilidade de construção de perfis detalhados dos hábitos e preferências de usuários[4] e do desenvolvimento de algoritmos preditivos (algoritmos preditivos são modelos matemáticos capazes de realizar inferências sobre hábitos e preferências dos usuários, geralmente em subsídio a processos de tomada de decisão automatizada) [5] permitiu repensar as formas de aproximação e de interação com os consumidores, além de abrir caminho para novos modelos de negócio, sobretudo aqueles baseados na publicidade comportamental. Do lado dos Estados, a possibilidade de ampliação do aparato de vigilância e controle dos cidadãos tem sido vista como uma exigência para o aumento da segurança pública e como uma alternativa para o aperfeiçoamento dos mecanismos de gestão.[6]

Nesse sentido, a interação dos cidadãos tanto com o setor público quanto com o setor privado passou a ser mediada pela tecnologia. Isso tem repercussões significativas não só para a sua privacidade, como também para a sua própria experiência democrática. De

posse de registros que revelam características tão sensíveis e detalhadas a respeito de sua personalidade, o usuário fica, por exemplo, cada vez mais exposto ao poder de manipulação que esses atores podem exercer.[7] A mesma exposição pode ser constatada em relação aos Estados, o que pode representar novas formas de controle e interferência no espaço público e no livre debate democrático. Por exemplo, durante as manifestações políticas de 2013, foi noticiada a organização, por agentes da polícia, das chamadas "Rondas Virtuais", a partir das quais eram feitas varreduras em perfis de redes sociais de suspeitos, o que culminou na prisão de mais de 20 manifestantes no Rio de Janeiro.[8]

No que diz respeito à propaganda política, é possível dizer que ela está cada vez mais segmentarizada em função dos perfis dos eleitores, sendo produzida em função de suas afinidades e preconceitos. Estudos demonstram, por exemplo, que eleitores podem ficar mais sugestionados a votar em determinados candidatos que tenham características faciais semelhantes com as suas próprias. De acordo com os experimentos realizados, a combinação sutil e, praticamente imperceptível, de fotos dos eleitores com fotos dos candidatos (em misturas geradas por computadores) poderia impactar a sua escolha política, especialmente em relação a candidatos desconhecidos.[9]

Em suma, o desenvolvimento dessas novas tecnologias nos coloca em um momento de inflexão histórica, no qual a privacidade e a autonomia dos indivíduos, elementos-chave para o livre exercício de suas liberdades públicas, estão sendo colocados em xeque por dispositivos tecnológicos que permitem construir sistemas de bombardeio de informação e de manipulação de suas susceptibilidades, tanto por parte do setor público quanto pelo setor privado, o que pode produzir resultados temerários para a sociedade democrática. O objetivo deste artigo é o de apresentar as principais tensões referentes ao direito à privacidade que se apresentam *(i)* na relação dos

usuários de Internet com as empresas; e *(ii)* na relação entre cidadãos e Estados, indicando, em ambos os casos, quais os principais modelos regulatórios adotados ao redor do mundo, com destaque para as questões e desafios no caso específico do Brasil.

3. Cidadania intermediada: setor privado

Desde sua abertura comercial, em 1993[10], a Internet, além da nítida revolução que representou para as formas de comunicação e interação social, passou a abarcar um número cada vez maior de atividades da vida cotidiana. De transações bancárias a consultas médicas, a Internet transformou a dinâmica de boa parte das relações sociais e comerciais. Isso pode ser constatado pelo crescente número de dispositivos que se conectam à Internet, movimento que se convencionou chamar de "Internet das coisas": automóveis[11], aviões[12], aparelhos de ginástica[13], relógios[14] e até mesmo objetos como garrafas de bebidas (por exemplo, os rótulos de garrafas do uísque "Johnnie Walker Blue Label" seriam capazes de detectar quando a garrafa foi aberta e enviar notificações e mensagens interativas para o dispositivo móvel do consumidor cadastrado)[15]. Muito além do que estar presente nos computadores, portanto, a Internet tem avançado rapidamente para diversas outras searas e instâncias da vida cotidiana.

Nesse sentido, na medida em que são executadas por meio de dispositivos conectados à Internet, as relações entre ser humano e setor privado estão cada vez mais *intermediadas* pela tecnologia.

Ryan Calo alerta para três consequências principais dessa intermediação: *(i)* a possibilidade de as empresas obterem registros sobre as preferências, formas de interação e engajamento dos consumidores; *(ii)* a possibilidade de se poder interferir na arquitetura de plataformas e dispositivos para influenciar essa interação; e *(iii)* a possibilidade de abordar os consumidores de forma proativa, ao invés de esperar que eles procurem pelas ofertas ou iniciem o contato com as empresas.[16]

Disso, percebe-se que a coleta e o tratamento de dados pessoais estão na base dessas relações, o que serve de subsídio não só para o desenvolvimento de técnicas avançadas de manipulação desses dados (o que se convencionou chamar de *big data*), como também para o surgimento de modelos de negócio calcados na publicidade digital. O resultado disso pode ser uma situação circular, na qual as escolhas e hábitos dos usuários determinam o seu contato com certos conteúdos publicitários, o que reforçaria padrões anteriores e restringiria o acesso dos indivíduos a alternativas ou opções mais inesperadas ou imprevisíveis. Isso traria menos heterogeneidade para os padrões de consumo. Do ponto de vista do acesso à informação e ao conhecimento, argumenta-se ocorrer fenômeno similar, com a criação de bolhas de interesse, dentro das quais os usuários teriam menos contato com opiniões divergentes.[17]

3.1. A monetização de dados pessoais como modelo de negócios

Muitos dos produtos e serviços oferecidos na Internet são gratuitos ou apresentam, no mínimo, versões gratuitas: redes sociais, *webmails*, plataformas de compartilhamento de imagens e vídeos ou inúmeras outras aplicações com funcionalidades variadas, como jogos e agregadores de informações.

A grande maioria dos modelos de negócio que viabilizam esse oferecimento gratuito de produtos e serviços está fundada na publicidade digital. Embora a lógica seja fundamentalmente a mesma daquela que financia a produção de conteúdos para parte da imprensa escrita e televisionada, qual seja a venda de espaços publicitários para anunciantes, o ambiente digital sofisticou muito a possibilidade de monetização desses espaços, fazendo que eles sejam também, muitas vezes, menos transparentes.

Isso porque a partir da coleta e tratamento de dados pessoais é possível segmentar usuários por grupos de interesse específicos e, portanto, direcionar os anúncios de forma mais eficiente. Nesse sentido, quanto mais usuários, mais valiosa a empresa se torna como veículo de divulgação de anúncios. Da mesma forma, quanto mais se sabe sobre o usuário, isto é, quanto mais dados sobre ele são coletados, maior é o grau de precisão com a qual a empresa pode determinar a relevância dos anúncios que lhe serão exibidos e, consequentemente, maior é o valor que pode ser cobrado para a sua exibição.[18]

Por essa razão, a coleta de dados pessoais é uma prática silenciosa que se tornou praxe entre as empresas do setor de internet.[19] Muitas vezes sem perceber, o usuário tem seus hábitos e preferências de navegação monitorados por meio da utilização de diversos mecanismos tecnológicos diferentes de coleta de dados, como os *cookies*. Os *cookies* são pequenos arquivos que podem ser enviados durante a comunicação estabelecida entre o dispositivo do usuário e o servidor do site que está sendo visitado. Esses arquivos nada mais são do que identificadores, que tornam possível reconhecer o dispositivo em visitas futuras e armazenar informações sobre suas preferências, por exemplo. É graças aos *cookies* que itens podem ser adicionados e mantidos em "carrinhos de compra" virtuais ou que preferências de exibição de páginas podem ser configuradas para visitas futuras. Chris Hoofnagle comenta a evolução des-

ses mecanismos, destacando as principais diferenças entre eles, tais como *flash cookies*, *evercookies*, *cookies* de terceiros, *web beacons* e *fingerprinting*. O autor ainda demonstra que algumas dessas tecnologias de coleta têm sido desenvolvidas para atuar de forma persistente, muitas vezes, inclusive, ignorando preferências expressas do usuário em não se submeter a essas práticas intrusivas. [20]

A partir do momento em que as empresas passam a ter acesso a esses tipos de dados sobre seus usuários, verdadeiros bancos de dados são criados, repletos de informações extremamente reveladoras sobre sua personalidade, tais como as palavras-chave buscadas, os sites visitados, as compras realizadas, os livros e as notícias lidas, a lista de amigos com quem mantém maior e menor contato e até mesmo os lugares por onde se passou[21]. A isso ainda se somam os arquivos que podem ficar armazenados nos servidores das empresas (*cloud computing*) ou os metadados, a partir dos quais inferências relevantes sobre o usuário também podem ser feitas.[22]

A segmentação dos usuários com base nesses dados e inferências levou ao desenvolvimento de complexos sistemas automatizados de alocação e exibição de anúncios, cujo funcionamento depende de mecanismos de "leilões". Inicialmente, esses mecanismos foram desenvolvidos para os anúncios oferecidos em buscadores, como Yahoo e Google. Basicamente, cada anunciante poderia propor um valor (lance) para a exibição de um determinado anúncio associado a uma palavra-chave (termo). A cada busca realizada pelo referido termo, o buscador considerava o lance do anunciante em comparação com os lances de outros anunciantes associados à mesma palavra-chave, como em um sistema tradicional de leilão. Os resultados de busca patrocinados (anúncios) eram então exibidos em ordem decrescente, ficando, no topo, o anúncio associado ao lance de maior valor e assim sucessivamente. Os anunciantes cujos anúncios recebessem cliques pagavam os valores com os quais haviam se comprometido (lance).[23]

Com o passar do tempo, mecanismos similares foram adotados para determinar quais anúncios seriam exibidos para cada usuário. Isso significa que, por trás da exibição de anúncios em quase todos os sites e plataformas da Internet, existe um complexo sistema automatizado de leilões, que é administrado por uma série de intermediários, como agências e redes de anunciantes ("Ad Networks"). Esses intermediários promovem a ligação entre os anunciantes, as plataformas e o usuário, na medida em que determinam quais anúncios serão exibidos para quais grupos de usuários.

Esse processo de segmentação e identificação das preferências de usuários com base na coleta e tratamento de dados pessoais desempenhado por uma complexa rede de intermediários preocupa os estudiosos do direito à privacidade por diversas razões, tais como: *(i)* a dificuldade de se dar ciência aos usuários sobre a utilização desses mecanismos de coleta e dos atores envolvidos nesse processo[24]; *(ii)* a insuficiência da noção de "consentimento informado" que se busca atingir por meio das políticas de privacidade, e a impossibilidade do usuário de não consentir, sob pena de não ter acesso ao serviço em algumas circunstâncias [25]; *(iii)* a possibilidade de cruzamento de informações entre diferentes bancos de dados, criando perfis cada vez mais completos[26]; *(iv)* a possibilidade de adoção de práticas discriminatórias na Internet com base em inferências sobre o usuário[27]; *(v)* a possibilidade de manipulação do usuário com base nas informações coletadas[28], entre outras.

Essas questões foram enfrentadas e reguladas de maneiras diferentes, especialmente no que tange aos limites definidos para a coleta e tratamento de dados pessoais, além da possibilidade de transferi-los para terceiros ou para outros países. As seções seguintes apresentam as principais características dos modelos adotados nos Estados Unidos, na Europa e no Brasil.

Por fim, vale lembrar que, além da via normativa, isto é, do

direito, a própria arquitetura da Internet também pode servir como instrumento de regulação. Por exemplo, podem ser instaladas extensões ao navegador do usuário que protegem a sua privacidade impedindo o envio de *cookies*, por exemplo. A proposta de criação do "Do Not Track" nos Estados Unidos seguiu essa concepção.[29] Nessa linha, o conceito de "*privacy by design*" foi idealizado como um conjunto de princípios que prega a incorporação de mecanismos e opções de configuração padrão que garantem, por meio da tecnologia, uma experiência de navegação menos intrusiva à privacidade do usuário.[30]

Contudo, por mais que esses mecanismos possam empoderar o usuário e possibilitar uma maior proteção da sua privacidade independentemente da adoção de um arcabouço jurídico para fazê-lo, o poder de "escolha" dos usuários ainda é muito reduzido nesses casos. Há diversos sites que exigem a aceitação do envio de cookies para a utilização de todas as funcionalidades ou exibição de todos os seus conteúdos, por exemplo.

3.2. A privacidade e a sua proteção: o modelo dos Estados Unidos

O modelo regulatório adotado nos Estados Unidos pode ser definido como fragmentado e de auto-regulamentação. Em primeiro lugar, fragmentado porque as leis que tratam do tema da coleta e tratamento de dados pessoais são apenas aplicáveis a setores específicos e bem diversificados: há leis que regulamentam a coleta e tratamento de dados financeiros[31], ligados à saúde[32], a crianças menores de treze anos[33] ou até mesmo ao histórico de vídeos alugados em locadoras.[34]

Boa parte dessas leis foi aprovada em resposta às crescentes discussões a respeito da necessidade de tutela da privacidade em

face do desenvolvimento da tecnologia, sobretudo das capacidades de processamento automatizado de dados pelos computadores.

Além dessas legislações setoriais, há, ainda, para alguns casos específicos, legislações estaduais aplicáveis[35] e legislações federais que tocam o tema da coleta e uso de dados pessoais. Contudo, no caso das legislações federais, que poderiam ser mais abrangentes, seu escopo de aplicação ficou limitado aos órgãos da administração pública federal, como o *Privacy Act of 1974*[36] e o *Freedom of Information Act (FOIA)*.[37]

Fora do alcance dessas legislações e dos segmentos por elas abrangidos, a coleta e tratamento de dados pessoais por atores do setor privado não são regulamentados no âmbito federal de forma genérica, o que confere considerável discricionariedade por parte daqueles que desejam colocar essas operações em prática.

Dessa forma, fica sob competência da Comissão Federal de Comércio ("Federal Trade Commission") a investigação de práticas "injustas ou enganosas" em relação ao consumidor no que diz respeito à sua privacidade.[38] De acordo com o entendimento da Comissão, basicamente, toda coleta e tratamento de dados pessoais deve cumprir os requisitos de *ciência e escolha*.[39]

Em outras palavras, isso significa dizer que é possível realizar a coleta e tratamento de dados pessoais livremente, desde que o usuário seja informado e tenha alguma opção para evitar a prática (mecanismos de "*opt-out*"). É pela liberdade que esse sistema confere às empresas no desenho de suas políticas de privacidade que se costuma dizer que ele está calcado na auto-regulamentação.[40]

Por vezes já se discutiu a adoção de uma legislação federal genérica que regulamentasse o tema nos Estados Unidos, impondo limites e regras mais concretas à coleta e tratamento de dados pessoais por parte das empresas. Nessas discussões, entretanto, costumam prevalecer os argumentos de que o modelo regulatório atual

é o que garante a capacidade de inovação e competitividade das empresas do setor de Internet.[41]

3.3. A privacidade e a sua proteção: o modelo da União Europeia

O modelo regulatório adotado pelos países da União Europeia é o legislativo, isto é, baseado na aprovação de uma lei. Nele, portanto, adota-se um regime geral de proteção de dados pessoais, geralmente consubstanciado em uma lei, genérica, que estabelece parâmetros mínimos que devem ser respeitados para coleta e tratamento desses dados (leis de proteção de dados). Nesses casos, portanto, não há liberdade irrestrita da iniciativa privada para moldar e implementar suas políticas de privacidade. A fiscalização e controle costumam ser feitos por órgãos especiais ("autoridades de garantia"), cujas competências e atribuições também costumam estar definidos nessas legislações.

Na verdade, o modelo se consolidou na Europa após a aprovação da Diretiva 95/46/CE, de 24 de outubro de 1995, que impôs a todos os Estados membros da União Europeia a obrigação de assegurar, em seus ordenamentos jurídicos nacionais, a proteção do direito à privacidade em conformidade com os parâmetros mínimos estabelecidos na Diretiva.[42]

Muito antes da aprovação da Diretiva, entretanto, alguns países já adotavam legislações nesse sentido. Desde 1973, a Suécia tem uma lei de proteção de dados pessoais (*Datalagen*); desde 1977, a Alemanha (*Bundesdatenschutzgesetz*). É interessante notar, nesse sentido, que a partir da aprovação da Diretiva, não só os demais países membros da União Europeia passaram a adotar o modelo legislativo, como também muitos outros países ao redor do mundo:

hoje, mais de cem países adotam legislações de proteção de dados pessoais. [43]

Parte da razão pela qual o modelo legislativo ganhou aderência mundial se deve a uma característica da própria Diretiva, que, ao regular a transferência internacional de dados pessoais, autoriza a sua realização apenas *"para países terceiros que assegurem um nível de proteção adequado"*.[44] Isso significa dizer que empresas de países localizados fora da União Europeia que desejassem coletar e transferir dados de cidadãos europeus para tratamento deveriam comprovar um nível adequado de proteção. A forma mais fácil de se fazer isso era, então, adotar legislações que estivessem alinhadas, substancialmente, com as exigências da Diretiva, facilitando as operações dessas empresas de fora da União Europeia,

Para avaliar a adequação dos níveis de proteção adotados em outros países fora da região, a Diretiva europeia criou um "Grupo de Trabalho" , cujos resultados serão apresentados a seguir.[45]

3.3.1. Dificuldades de compatibilização: a transferência internacional de dados

A existência dos referidos modelos nacionais distintos de regulação gera incerteza para as empresas do setor de Internet, que atuam a nível global, que teriam que respeitar, concomitantemente, diferentes graus de proteção conferidos ao direito à privacidade, especialmente se se considerar que as atividades de coleta e tratamento de dados envolvem, frequentemente, a transferência desses dados entre países diferentes. Tal tarefa exigiria não só o estudo detalhado das peculiaridades de cada ordenamento jurídico, como também a criação de um sistema de coleta de dados pessoais diferente para cada país, de acordo com a localização do usuário, deter-

minada pelo seu endereço de IP, por exemplo. Considerando que praticamente todos os *websites* realizam algum tipo de coleta de dados, a exigência poderia representar uma barreira técnica e econômica para que muitos deles pudessem se estabelecer.

Como visto, no caso dos Estados Unidos, não há legislação de proteção de dados que garanta os parâmetros mínimos de proteção exigidos pela Diretiva europeia 95/46/EC, o que gerou um impasse em relação à possibilidade de transferência de dados entre as duas regiões. Sem a garantia de um nível adequado de proteção, empresas estadunidenses não poderiam transferir dados de cidadãos europeus para fora da União Europeia, o que inviabilizaria os modelos de negócios de muitas das empresas de Internet atuantes no mercado europeu.

Para equacionar essa situação, em 21 de julho de 2000, o Grupo de Trabalho celebrou um acordo bilateral com o Departamento de Comércio dos Estados Unidos a partir do qual as empresas estadunidenses poderiam declarar adotar níveis de proteção de privacidade adequados, isto é, que estavam em conformidade com as exigências da Diretiva ("Safe Harbor").[46] Essa declaração estava baseada em alguns princípios[47] e era suficiente para incluir as empresas em uma lista, autorizando-as a transferir dados coletados de cidadãos europeus ("US-EU Safe Harbor List").[48]

Por ser de participação voluntária e por se basear na mera declaração das empresas participantes, sem um sistema de verificação por parte do Departamento de Comércio, durante sua vigência, o sistema sofreu diversas críticas.[49]

Pouco mais de quinze anos depois de sua entrada em vigor, em 06 de outubro de 2015, o acordo foi invalidado pela Corte de Justiça Europeia em um caso envolvendo um cidadão austríaco que questionara a validade do acordo para a proteção do seu direito à privacidade. De acordo com a decisão, o acordo não pode ser consi-

derado um mecanismo válido de "adequação" aos níveis de proteção exigidas pela Diretiva para transferência de dados de cidadãos europeus para os Estados Unidos.[50]

Com o acordo invalidado, Estados Unidos e União Europeia iniciaram as negociações para a elaboração de um novo sistema que possibilitasse a transferência de dados entre as duas regiões. Em 12 de julho de 2016, foi anunciada a aprovação de uma versão reformulada do acordo ("Privacy Shield"). Comparado com o "Safe Harbor", pouca coisa mudou em relação ao sistema de auto-declaração das empresas, que continuam tendo que certificar sua "adequação" aos níveis de proteção europeus com base nos mesmos sete princípios anteriormente adotados. A diferença principal do acordo está na exigência de mecanismos de fiscalização por parte do Departamento de Comércio dos Estados Unidos e da Comissão Federal de Comércio em relação ao cumprimento dessas certificações, além de abrir espaço para formas mais eficazes de reclamação e denúncias de violação por parte dos cidadãos europeus.[51] Desde 01 de agosto de 2016, o Departamento de Comércio dos Estados Unidos está aceitando as certificações em conformidade com o novo acordo.

Vale lembrar que os acordos vigoram apenas entre Estados Unidos e União Europeia, não havendo mecanismos significativos semelhantes em relação a outros países. O tópico seguinte apresenta as características da regulamentação existente no Brasil.

3.4. A privacidade e a sua proteção: para onde caminha o Brasil

No Brasil, a privacidade recebe tutela constitucional nos incisos X e XII do artigo 5º da Constituição Federal. Figuram como parte dos direitos dos brasileiros a proteção da vida privada, da intimida-

de e a inviolabilidade dos sigilos de correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas (este último violável em casos de investigações ou processos criminais, na forma de lei). Para se efetivar, entretanto, tal proteção constitucional necessita de legislação que lhe dê suporte, concretizando tal proteção genérica em regras específicas de tutela da privacidade em face do complexo ecossistema empresarial de coleta e tratamento de dados pessoais já descrito.

A despeito da grande utilização de produtos e serviços na Internet pelos brasileiros - especialmente aqueles que tem como cerne de seus modelos de negócio a coleta e processamento de dados pessoais para posterior direcionamento de publicidade -, a regulamentação infraconstitucional do tema ainda é tímida. No plano infraconstitucional, as regras que existem podem ser localizadas em *(i)* leis setoriais esparsas, e *(ii)* na Lei nº 12.965, de 23 de abril de 2014 ("Marco Civil da Internet"), acompanhada de seu decreto regulamentador ("Decreto nº 8771, de 11 de maio de 2016").

Leis setoriais[52] trazem algumas disposições aplicáveis à Internet. Na área de telecomunicações, por exemplo, a Lei Geral do setor estabelece a proteção da privacidade e da inviolabilidade das comunicações como deveres a serem seguidos pelas prestadoras, mas sem dispor sobre o assunto mais especificamente. Tais disposições gerais da LGT trazem mais dúvidas do que soluções nos casos mais recentes que envolveram as prestadoras de serviço de telecomunicações e o direito à privacidade. Nesses casos[53], a legislação de defesa do consumidor e o seu sistema de fiscalização foram os fundamentos que subsidiaram a ação de proteção da privacidade por parte do Poder Público.

Os casos até agora mais notáveis são o de notificação (e multa, ao menos em um deles), por parte do Ministério da Justiça (mais especificamente a Secretaria Nacional do Consumidor, órgão que en-

cabeça o Sistema Nacional de Defesa do Consumidor), da Oi e da Telefônica/Vivo em razão de coleta e tratamento de dados de usuários sem prévia informação ou consentimento. No caso da Oi, a situação envolveu investigação de parcerias firmadas em 2010 entre a empresa britânica Phorm, desenvolvedora de um software que monitorava toda a navegação dos consumidores, e empresas de telecomunicações brasileiras. A Oi foi multada em 3,5 milhões de reais no caso, por violar os direitos de informação e privacidade dos consumidores. Mais recentemente, no início de 2015, a Telefônica/Vivo também foi notificada pelo Ministério da Justiça por anunciar publicamente a implementação do serviço "Smart Steps", que coletaria informações de geolocalização dos celulares clientes da empresa para geração de relatórios e análises, possivelmente com fins econômicos.

Nesse contexto, a Secretaria Nacional do Consumidor ("SENACON") ocupa um papel relevante nas discussões que envolvem a proteção do direito à privacidade no Brasil, em especial por coordenar a fiscalização das disposições do Código de Defesa do Consumidor usadas para constranger empresas que concentram intensa atividade de coleta e tratamento de dados pessoais. Tal tendência se confirma pela proeminência de tal agência perante as discussões que culminaram na Lei do Cadastro Positivo (de grande importância na discussão de proteção ao consumidor), por um lado, e em seu protagonismo dentro do Executivo no processo de elaboração de um anteprojeto de lei de proteção de dados pessoais, tratado mais adiante.

O Marco Civil da Internet (Lei 12.965/2014), por sua vez, concentra uma série de disposições bastante importantes relativas à proteção da privacidade dos usuários de Internet no Brasil.

O Marco Civil da Internet é considerado paradigmático em termos de elaboração normativa por ter sido fruto de um processo de intenso debate público fomentado pelo Poder Executivo entre 2009 e

2011. Neste período, o Ministério da Justiça, em parceria com a Fundação Getúlio Vargas, disponibilizou uma plataforma na Internet para coletar contribuições e fomentar o debate entre cidadãos, empresas e organizações. O processo culminou na propositura de um projeto de lei ao Congresso Nacional e ficou reconhecido como referência internacional de participação multissetorial na elaboração de regras e diretrizes para a governança da Internet. Tal projeto de lei levava à consideração do Legislativo arranjos que resolviam os temas mais tocados na plataforma de debates, nominalmente a responsabilidade de empresas de Internet por conteúdo gerado por seus usuários, a retenção de registros de navegação por parte de tais empresas e a neutralidade de rede, questão ligada às regras de gerência da infraestrutura de telecomunicações[54].

Foi apenas na etapa final da tramitação do projeto de lei no Legislativo (2012-2014) que a coleta e tratamento de dados pessoais por parte do setor privado foi incluída na discussão do Marco Civil da Internet. Esta inclusão teve como fator catalisador as revelações do ex-funcionário da Agência Nacional de Segurança (NSA) dos Estados Unidos, Edward Snowden. Ao revelar que o setor de inteligência estadunidense lograva acesso legal (decorrente de ordem judicial, mesmo que sigilosa, genérica ou ligada a questões de segurança nacional) ou forçado (a partir de acesso privilegiado à infraestrutura de cabeamento necessária para o funcionamento de tais serviços digitais em rede) aos servidores de boa parte das maiores empresas de Internet, Snowden tomou as manchetes. O processo se agudizou quando as revelações chegaram ao alto escalão do governo federal: o ex-agente revelara que até mesmo o telefone celular da então Presidente da República, Dilma Rousseff, havia sido espionado, bem como a rede interna da maior empresa estatal do país, a Petrobrás.

O chamado "efeito Snowden" abriu uma janela de oportunidade política para que o texto do projeto de lei fosse emendado

com regras genéricas dirigidas à proteção dos dados pessoais dos usuários de Internet brasileiros. O Congresso Nacional, sensibilizado pelas revelações, referendou a ideia, que foi encampada pelo deputado relator do projeto, Alessandro Molon (PT-RJ, à época). Como resposta à espionagem estadunidense proporcionada pela emergência do setor de Internet baseado naquele país, o texto aprovado pelo Congresso Nacional dispõe que é necessário o consentimento livre e expresso do usuário para a coleta de seus dados pessoais (art. 7º, IX), bem como exige que sejam prestadas informações claras e completas sobre o uso desses dados, permitido apenas para finalidades lícitas, explícitas em contrato com os usuários e que justifiquem a sua coleta (art. 7º, VIII). A lei também estabeleceu que cidadãos podem requerer às tais empresas a exclusão definitiva de dados pessoais após o término de relação entre as partes.

Por fim, esse "efeito" também foi responsável pela inclusão de regras de "fiscalização". O artigo 11, acrescentado após negociação entre o relator e o Executivo, dispõe que *"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, deverão 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"*. A lei prevê, inclusive, sanções que podem ser aplicadas em casos de violação desta norma[55].

As regras estabelecidas no Marco Civil estão distantes, entretanto, do arcabouço estabelecido nas legislações gerais de proteção de dados geralmente adotadas no modelo legislativo europeu que se mencionou acima, seja em termos legais ou de fiscalização por parte do Estado. Não há menção sobre uma série de questões-chave tratadas em exaustão por esses arranjos normativos.

Apesar disso, já há algum tempo existem discussões no sentido de instituir, no âmbito nacional, uma Lei de Proteção de Dados Pessoais, acompanhada de um sistema de fiscalização correspondente. Uma proposta de marco normativo foi incluído na agenda do Ministério da Justiça já em 2011, na esteira dos citados escândalos envolvendo prestadoras de serviço de telecomunicações e a coleta e tratamento de dados pessoais. Neste ano, o Ministério promoveu um debate público a respeito de um anteprojeto de lei. Após o Marco Civil ter monopolizado as discussões entre os setores interessados na regulação do ambiente digital entre 2011 e 2014 o tema voltou à tona em 2015. Foi no início desse ano, 2016, que uma nova versão do anteprojeto foi novamente levada a debate público, em conjunto com uma proposta de decreto regulamentador do texto do Marco Civil da Internet.

O decreto resultante deste processo, de número 8771/2016, trouxe a primeira definição de "dado pessoal" contida na legislação brasileira, mesmo após controvérsias de que não seria o diploma adequado para conter tal definição. As definições de "dado pessoal" e de "tratamento de dados pessoais" são as mesmas presentes nas propostas legislativas de proteção de dados pessoais encampadas pelo mesmo Ministério da Justiça e encaminhadas ao Legislativo.

A consulta pública em relação ao anteprojeto produziu uma série de mudanças no texto. Possivelmente, a mudança mais significativa foi a inclusão do "legítimo interesse do responsável pelo tratamento de dados pessoais" como uma hipótese que autoriza o tratamento dos dados, dispositivo criticado por organizações da sociedade civil organizada e de defesa dos direitos do consumidor[56]. O texto seguiu para o Legislativo após a consolidação deste processo de negociação capitaneado pela SENACON, passando a tramitar sob o número 5276/2016. No Congresso, porém, já havia outros dois projetos propostos por parlamentares que também endereçavam a ma-

téria, um na Câmara e outro no Senado. A despeito de seu apensamento a um projeto de matiz radicalmente diferente (e mais branda), o projeto de lei nº 4060/2012, há especial relevância em este projeto de lei ter sido proposto pelo Executivo.

Isso porque, por exigência da Constituição Federal, é de iniciativa privativa do Presidente da República a criação de órgãos da Administração Pública (Art. 61,§ 1º, e). Nesse sentido, o projeto 5276/2016 é o único que pode instituir um órgão específico para atuar na fiscalização das atividades ligadas ao direito à privacidade (tarefa desempenhada pelas autoridades de garantia em países que adotam o modelo legislativo).

Apesar das divergências a respeito dos detalhes administrativos de sua estrutura, uma autoridade central federal e independente de proteção de dados pessoais é ponto pacífico entre setores radicalmente opostos durante a consulta pública – o setor privado e a sociedade civil. Para as empresas, o receio é que a legislação seja aplicada de forma heterogênea e espontânea por diferentes autoridades locais e regionais, o que elevaria o risco e seu custo de adequação à regulação. Por sua vez, a sociedade civil teme que a lei "não pegue", ou seja, que a fiscalização não aconteça caso não haja um efetivo de técnicos dedicados ao tema, bem como uma autoridade com poder de polícia e, portanto, de aplicar sanções.

Mesmo que a matéria seja atual e fruto de um debate prévio, os projetos de lei que regram a proteção de dados pessoais ainda têm um longo caminho de tramitação pela frente. Esta lacuna normativa abre espaço para que questões cheguem ao Judiciário sem que haja balizas específicas e pensadas para os dilemas inseridos por inovações tecnológicas. Em diferentes casos, magistrados têm apresentado concepções díspares em relação à aplicação dos dispositivos constitucionais, das regras genéricas do Marco Civil ou das disposições "emprestadas" das leis setoriais.

Dois casos podem servir de exemplo para ilustrar a disparidade das decisões emitidas pela Justiça. No primeiro, o Tribunal de Justiça do Rio Grande do Sul (TJ-RS) decidiu[57]que a venda de dados pessoais como nome, CPF ou endereço, ainda que sem consentimento, não é ilícita. Isso porque esses dados não seriam sensíveis. Segundo a interpretação do Tribunal, mereceriam proteção apenas os dados que poderiam gerar discriminação, "como orientação política, religiosa ou sexual". A falta de "comprovação de dano" com a venda também serviu de fundamento para a decisão.

No outro extremo, o Ministério Público Federal teve acolhido um pedido para bloqueio do site "Tudo Sobre Todos", que realizava atividade muito similar àquela do caso julgado pelo Tribunal de Justiça do Rio Grande do Sul, qual seja a comercialização de dados pessoais sem o consentimento dos seus titulares[58]. Na visão do magistrado da 1ª Vara Federal do Rio Grande do Norte, a atividade é ilícita.

As decisões ganharam repercussão nacional e datam do mesmo ano, 2015. Sua disparidade suscita dúvidas relevantes quanto à interpretação da proteção constitucional à intimidade e à vida privada no contexto digital, especialmente em face dos riscos associados às novas técnicas de cruzamento de bancos de dados e de uso de algoritmos.

4. Cidadania mediada: o setor público

Na seção anterior, descreveu-se de que forma os modelos de negócios baseados na publicidade digital, que envolvem a coleta e tratamento de dados pessoais, repercutem na tutela do direito à privacidade. Além disso, foram apresentadas as principais características dos modelos regulatórios adotados para lidar com as relações travadas entre usuários e empresas, com destaque para o Brasil, que ainda dispõe de poucos dispositivos nesse sentido. O objetivo desta seção é ilustrar como a regulação dessas questões também interfere de maneira direta na relação entre cidadão e Estado, acrescentando novas formas de potencial violação ao seu direito à privacidade.

As denúncias realizadas, em junho de 2013, por Edward Snowden, a respeito do aparato de vigilância implementado pela Agência de Segurança Nacional dos Estados Unidos (NSA) tornaram palpável e explícita a relação entre o desenvolvimento de técnicas de vigilância em massa, de um lado, e o ecossistema de coleta de dados pessoais como parte de um modelo de negócio, de outro. A confecção, por parte do setor privado, de repositórios com gigantesca quantidade de registros de navegação, de preferências, de fotos ou de atividade na rede despertou um enorme interesse por parte do

Estado. Uma vez cientes da existência desses bancos de informações, os Estados passaram a demandar, cada vez mais, prerrogativas de acesso a esses dados, como subsídios importantes para os processos de investigação e de persecução penal.

Ao mesmo tempo, o próprio Estado administra (em seus órgãos e subdivisões) uma série de bancos de dados potencialmente sensíveis. A atividade administrativa é permeada pela necessidade de coleta e tratamento de dados pessoais, um ponto nevrálgico em termos de eficiência das políticas públicas que tenham escala. Exemplos não faltam: o cadastro biométrico eleitoral e o banco de dados de prontuários médicos do sistema público de saúde indicam que a informatização das mais diversas áreas trouxe dilemas próprios da área de proteção de dados pessoais para o núcleo da Administração Pública.

Nesse sentido, são dois os principais pontos de atenção no que diz respeito ao tema da vigilância do Estado e a proteção de dados pessoais: *(i)* o aumento das prerrogativas de acesso a dados de usuários mantidos por empresas; e *(ii)* o aumento das possibilidades de coleta e tratamento de dados pessoais pelo próprio Estado.

4.1. Antagonismo ou cooperação: prerrogativas do Estado de acesso a dados dos cidadãos

A recente onda de ataques e atentados terroristas ao redor do mundo tem suscitado inúmeras discussões sobre as necessidades de aumento das capacidades de vigilância dos Estados. Na França, o Estado decretou estado de emergência, o que aumentou consideravelmente as prerrogativas de investigação por parte das autoridades.[59] Na Alemanha, discutem-se reformas legislativas para

tornar mais céleres os processos de investigação.[60] No Reino Unido, foi aprovada, em 16 de novembro de 2016, uma das legislações mais agressivas em termos de vigilância do mundo.[61] Nos Estados Unidos, desde os ataques de 11 de setembro, foi encampada uma intensa reforma legislativa para fortalecer o aparato de vigilância nacional, o que se consubstanciou, principalmente, na aprovação do "USA Patriot Act".[62]

Em comum, todas essas medidas se apoiam no aumento das prerrogativas de acesso a dados de usuários de Internet por parte das autoridades. Esses dados, até então concentrados nas mãos das empresas, tal como já se descreveu, passam a ser objetos de desejo dos Estados, que advogam por medidas mais invasivas em nome da segurança nacional.

No Brasil, para além da ausência de marco normativo que estabeleça regras básicas relativas a cuidados com a proteção de dados dos cidadãos por parte de entes estatais, estudos recentes apontam para a opacidade na atividade de vigilância empreendida pelo Estado brasileiro.[63] Em linhas gerais, o rigor da lei parece surgir apenas nas ocasiões em que autoridades como a Polícia e o Ministério Público – referendados por uma ordem judicial – buscam acesso a dados de cidadãos em face de intermediários privados. Este arranjo é exemplificado nas tabelas abaixo, que esquematizam os limites à vigilância sobre as comunicações e dados no Brasil e as prerrogativas de acesso a esses dados instituídas na regulamentação vigente:

Tabela 1: prerrogativas de acesso a dados por parte de autoridades[64]

VIGILÂNCIA DO ESTADO BRASILEIRO SOBRE AS COMUNICAÇÕES			
Fim/ Autoridade(s)	**Regulação das Telecomunicações (ANATEL)**	***Law enforcement* (autoridades policiais, Ministério Público, juízes e CPIs)**	**Inteligência (ABIN)**
OBRIGAÇÕES DE GUARDA DE DADOS	Resoluções 426/05, 477/07 e 614/13 da ANATEL obrigam que dados relativos à prestação de serviço de telefonia fixa e móvel sejam guardados por prestadoras por no mínimo 5 anos e que dados relativos à conexão à internet sejam guardados por provedores prazo mínimo de 1 ano.	A lei 12.850/13 (art. 17) impõe a guarda de "registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas" a empresas concessionárias de telefonia fixa e móvel por 5 anos.	Não há obrigação de guarda para fins de inteligência.
		A lei 12.965/14 (arts.13 e 15) impõe a guarda de registros de conexão à Internet por 1 ano a todos os provedores de conexão e a guarda de registros de acesso a aplicações a provedores de aplicações com fins econômicos por 6 meses.	
ACESSO A DADOS GUARDADOS (informações cadastrais e metadados)	No exercício de poderes fiscalizatórios (art. 8, Lei 9472/97), a ANATEL pode acessar documentos fiscais, que contém informações cadastrais e registros, por requisição às prestadoras de serviço. Atualmente, há desenvolvimento de infraestrutura que permita acesso direto e irrestrito online, baseada no art. 38 da Resolução 596/12.	Pelas leis 9.613/98 (art. 17-B) e 12.850/13 (art. 15), no caso de informações cadastrais de usuários de telefonia, o acesso pode ocorrer mediante simples requisição de autoridades policiais ou Ministério Público às prestadoras. O acesso a registros telefônicos e outros metadados gerados no uso de telefonia (localização) não possui regulamentação legal específica: ocorre mediante ordem judicial para fins de produção de prova. Pelo MS 23452/RJ do STF, acesso a registros telefônicos também pode ocorrer no âmbito de CPIs.	Poderes de requisição e de requerimento de dados da ABIN inexistentes. Possibilidade de acesso indireto pelo Sisbin, nos termos dos arts.6, V e 6-A do Decreto 4.376/02.
		Pela lei 12.965/14, o acesso a informações cadastrais de assinantes de provedores de conexão e de usuários de aplicações de Internet pode ocorrer mediante requisição de autoridades competentes (art. 10, § 3º). No caso de registros de conexão à Internet e acesso a aplicações, o acesso deve ocorrer por ordem judicial quando houver fundados indícios de ocorrência de ilícito e utilidade dos registros à investigação ou instrução probatória, com necessidade de determinação de período específico (art. 22).	
ACESSO A COMUNICAÇÕES DOCUMENTADAS	Resoluções da ANATEL permitem acesso a gravações de ligações a serviços de atendimento ao cliente de prestadores de serviço de telecomunicações.	A lei 12.965/14 permite acesso a comunicações privadas registradas ocorridas por aplicações de Internet por ordem judicial (art. 7, III). Segundo RE 418.416-8/SC julgado pelo STF, o mandado de busca e apreensão legitimiza o acesso a dados armazenados em computadores.	Poderes de requisição e de requerimento de dados da ABIN inexistentes. Possibilidade de acesso indireto pelo Sisbin (arts.6, V e 6-A do Decreto 4.376/02).

INTERCEPTAÇÕES	Prerrogativa de realização e competência de requerimento de interceptações inexistentes.	Pela lei 9.296/96, interceptações de comunicações telefônicas e de sistemas de informática e telemática podem ocorrer mediante ordem judicial, de ofício ou por requerimento de autoridade policial ou do Ministério Público, quando há indícios razoáveis de autoria ou participação em infração penal punida com pena de reclusão e indisponibilidade de outros meios de produção de prova (arts 1 e 2). Lei 12.965/14 permite interceptação de fluxo de comunicações via Internet na forma da lei 9.296/96. Resoluções do CNJ e do CNMP especificam critérios a serem observados em pedidos e decisões.	Prerrogativa de realização e competência de requerimento de interceptações inexistentes. Lei 9.296/96 não estende tais poderes à ABIN. Possibilidade de cooperação pelo Sisbin (arts.6, V e 6-A do Decreto 4.376/02).

Tabela 2: limites às prerrogativas de vigilância[65]

LIMITES À VIGILÂNCIA SOBRE AS COMUNICAÇÕES NO BRASIL	
DIREITOS	Constituição Federal protege a liberdade de expressão, a intimidade e o sigilo das comunicações (art. 5º incisos IX, X e XI).
	Leis nº 9.472/97 (arts. 3º, V e IX, e 72) e nº 12.965/14 (art. 7º) garantem os direitos ao sigilo das comunicações e à privacidade no uso de telefonia e Internet.
	Não há testes consagrados, de aplicação uniformizada na jurisprudência e na doutrina, para avaliação da constitucionalidade de restrições a esses direitos.
	O art. 5º, § 2º da Constituição Federal dispõe que direitos e garantias expressos nela não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais de que o Brasil faça parte. Fazem parte do bloco de constitucionalidade, contudo, apenas tratados e convenções internacionais sobre direitos humanos aprovados em regime equivalente ao de emendas constitucionais, pelo art. 5º, § 3º.
REMÉDIOS	Em casos de violação a direitos, o cidadão pode impetrar habeas corpus ou mandado de segurança, previstos na Constituição (art. 5º, LXVIII e LXIX), ou propor ação ordinária.
GARANTIAS	A Constituição Federal garante o devido processo legal, o contraditório e a ampla defesa, e a presunção de inocência (art. 5º, LIV, LV e LVII). O Código de Processo Penal ordena que o juiz observe os princípios da adequação, da necessidade e da proporcionalidade ao ordenar produção de provas (art. 156). O mesmo vale para a apreciação de pedidos de medidas cautelares de produção de provas (art. 282). Intimação do atingido deve sempre ocorrer "ressalvados casos de urgência e de perigo de ineficácia" (art. 282, § 3º).
	Pela Constituição Federal (art. 5º, LVI) e pelo Código de Processo Penal (art. 157) são inadmissíveis provas obtidas por meios ilícitos, contrariando a Constituição ou a lei. Não podem ser aproveitadas.
SANÇÕES	Art. 10 da Lei nº 9.296/96 criminaliza interceptações ilegais e quebra de segredo de justiça. Pena: reclusão de 2 a 4 anos e multa.
	Art. 156-A do Código Penal criminaliza invasão a dispositivo informático com fim de obter dados. Pena: detenção de 3 meses a 1 ano, e multa. Se daí decorrer acesso a conteúdo de comunicação privada, a pena é reclusão de 6 meses a 2 anos, e multa.

Das tabelas, cumpre destacar o conjunto de garantias estabelecido pelo Marco Civil da Internet, que consagrou a exigência de ordem judicial para o acesso a dados de identificação de usuários de Internet no Brasil (como registros de acesso a aplicações de Internet e registros de conexão).

Com a aprovação da lei, o que se esperava era consolidar uma aplicação rigorosa desse crivo judicial, resguardando a privacidade de usuários de Internet, que só deveriam ser identificados em circunstâncias de fundados indícios da ocorrência de ato ilícito e com justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória (art. 22).

A exigência desse crivo judicial para a identificação de usuários também tem repercussões para a liberdade de expressão. Isso porque, se se considerar que há um direito irrestrito e genérico de identificação dos usuários de Internet por quaisquer manifestações ou conteúdos divulgados na Internet, aumentam as possibilidades de intimidação e constrangimento dos usuários.

Nesse sentido, além do rigor judicial para só determinar a entrega de dados de identificação no caso de preenchimento dos requisitos mencionados acima, há um papel importante a ser desempenhado pelos provedores de aplicações de Internet (como Facebook e Google) e também pelos provedores de conexão à Internet (como NET, VIVO e TIM). No dois casos, questionar pedidos abusivos de dados de usuários ou recorrer de decisões judiciais pouco rigorosas pode ajudar a fomentar uma cultura de valorização do direito à privacidade e, consequentemente, do direito à liberdade de expressão[66]. Em relação às práticas e políticas de proteção a dados de usuários adotadas pelos provedores de conexão à Internet no Brasil, o InternetLab realiza avaliação anual por meio do projeto "Quem defende seus dados?", cujos resultados podem ser consultados no endereço www.quemdefendeseusdados.org.br.

Após as eleições de 2014 (e, a partir de algumas leituras, da composição do Congresso Nacional ter se tornado bastante mais conservadora em relação aos anos anteriores[67]), as garantias estabelecidas pelo Marco Civil, entretanto, ficaram sob ataque. Como se pode notar por uma série de iniciativas encampadas nos últimos anos, uma ofensiva pela retirada de travas para o acesso a dados por autoridades estatais e pela ampliação da retenção obrigatória de informações dos usuários para futuras investigações dominou a agenda legislativa nesta área.

Essa ofensiva pode ser ilustrada por alguns exemplos. A tramitação do projeto de lei 215/2015 – chamado por setores da sociedade civil organizada de "PL Espião" – pela Comissão de Constituição, Justiça e Cidadania da Câmara dos Deputados, por exemplo, levantou receios de acadêmicos da área[68], por concentrar uma série de propostas que envolviam a obrigação de coleta e guarda de dados cadastrais de usuários e sua disponibilização sem ordem judicial para quaisquer casos. Uma intenção explicita dos parlamentares era a facilitação de procedimentos de identificação de usuários em razão da proliferação de "ofensas à honra" na Internet.

Essa mesma preocupação permeou os trabalhos da chamada Comissão Parlamentar de Inquérito (CPI) de Crimes Cibernéticos, criada também na Câmara. A CPI estava lastreada em um requerimento que fazia menção à uma fraude grave bancária e foi palco de uma série de discussões que não necessariamente guardavam relações entre si (como a militância política virtual e o combate à pornografia infantil). Seu relatório final foi no mesmo sentido que a tramitação do PL 215/2015: deu força a iniciativas que modificavam o Marco Civil[69] para afastar o controle judicial da coleta de dados pessoais de usuários de Internet junto ao setor privado[70].

Recentemente, o clima entre as autoridades de investigação e o Judiciário, de um lado, e as empresas provedoras de aplicações

de Internet, de outro, tem se acirrado. A retórica e o requerimento de medidas jurídicas dissuasórias bastante extremas (como os recentes bloqueios de sites e aplicativos, marcadamente do mensageiro *WhatsApp*) pode indicar uma incessante busca dos bancos de dados mantidos por tais intermediários. Esses bloqueios estão inseridos em uma complexa trama de impasses políticos e jurídicos[71] e decorrem de diversos tipos de resistências criadas pelas empresas, sejam elas de ordem técnica (como a adoção de sistemas criptográficos que não permitem a interceptação de mensagens) ou jurisdicional (com o argumento de que o dado requerido estaria armazenado por outra pessoa jurídica foram do território nacional). Independentemente da motivação – e, portanto, da razoabilidade – das resistências, os bloqueios têm evidenciado um processo de antagonismo entre ambos setores, catalisado pela avidez de autoridades do Estado pela franquia de um acesso facilitado à qualquer informação gerada no uso de aplicações de Internet.

4.2. Eficiência ou vigilância: a coleta de dados direta por parte do setor público

É próprio da atividade de gestão pública manter registros sobre o cadastro e a identificação de cidadãos ou sobre a utilização de serviços públicos. São dados como esses que permitem administrar os processos eleitorais ou calcular e ajustar tarifas no setor de transportes, por exemplo. Na medida em que é guardião desses dados, o Estado deve zelar para não comprometer sua segurança, prevenindo vazamentos e o acesso desautorizado de terceiros, e criar mecanismos que impeçam a sua utilização para finalidades não regulamentadas por lei.

No caso do Brasil, não é difícil encontrar exemplos que ilustram de que forma a falta de uma regulamentação robusta de proteção de dados pessoais acaba potencializando situações de manipulação inadequada ou indesejável desses dados. Em 2013, por exemplo, noticiou-se amplamente um acordo celebrado entre o Tribunal de Justiça Eleitoral e a Serasa Experian, autorizando o compartilhamento de dados cadastrais dos cidadãos junto à Justiça Eleitoral com a empresa. De posse dos dados, especialmente aqueles relativos à filiação, a empresa poderia enriquecer de forma significativa seus bancos de dados, que seriam posteriormente comercializados. Na época, a grande repercussão que o caso atingiu obrigou o Tribunal a rever o acordo, declarando-o como cancelado pouco tempo depois de sua divulgação.[72]

Um outro exemplo diz respeito aos dados gerados a partir do uso de cartões como o "Bilhete Único", que facilitam o pagamento adiantado de viagens no sistema de transporte público de metrópoles brasileiras. Em São Paulo, a empresa pública responsável pela administração do serviço sequer divulgou sua política de privacidade para a coleta e tratamento de informações sobre as viagens dos usuários, que podem revelar detalhes do dia a dia de todos os usuários de seu sistema de transporte público.[73]

Mais um caso que toca a questão envolve os bancos de dados para aquisição de remédios a baixo custo no programa federal "Farmácia Popular". Este programa de descontos permitiu que empresas privadas de "gestão de programas de benefícios em medicamentos" coletassem e armazenassem uma série de informações sensíveis de cidadãos sem a sua organização ou supervisão de uma autoridade.[74]

Como se percebe, a discussão de proteção de dados travada no âmbito do setor público carrega uma série de peculiaridades. A obrigatoriedade (ou inevitabilidade) de fornecimento de certos dados (como aqueles advindos do uso e sistemas ou serviços públicos

inescapáveis, como o de saúde, de mobilidade ou de previdência) é uma das característica que torna a coleta significativamente diferente dos casos típicos do setor privado, marcados pela necessidade de obtenção do consentimento.

Nesse sentido, é importante haver balizas claras que impeçam a utilização desses dados para finalidades diferentes daquelas originalmente previstas. No caso do Bilhete Único, por exemplo, dados sobre rotas e trajetos de cidadãos poderiam vir a ser de interesse da guarda municipal para finalidades de vigilância, o que extrapolaria a finalidade de coleta desses dados para gerenciar a cobrança das tarifas pela utilização do sistema de transporte público.

O compartilhamento de dados entre órgãos da Administração Pública foi tema de recente regulamentação no Brasil. O decreto nº 8789, de 01 de julho de 2016, disciplina o compartilhamento de bases de dados entre órgãos e entidades federais. Sua motivação é a de que o compartilhamento serve à "amplificação de oferta de serviços públicos", "formulação e monitoramento de políticas públicas", "fiscalização de benefícios" e "melhoria da fidedignidade de dados" (art. 2º).

Nesse sentido, abre caminho para a utilização de técnicas de *big data* para aprimorar a gestão pública e aperfeiçoar os mecanismos de fiscalização. Um exemplo seria a possibilidade de cruzamento de dados de diferentes bancos de dados para "conferência", o que permitiria um maior controle sobre a concessão, pagamento ou fiscalização de benefícios.[75] No caso do programa Bolsa Família, por exemplo, isso ajudaria a combater fraudes na medida em que tornaria possível a verificação do cumprimento dos requisitos pelo cruzamento de dados, o que também foi noticiado pela imprensa.[76]

Analisando os termos do decreto, Jacqueline Abreu chama a atenção para a falta de mecanismos que resguardem a privacidade dos cidadãos e garantam a transparência das atividades. Para ela,

"um programa de compartilhamento de dados não pode só ser justificado em termos de eficiência da gestão do Estado, como o governo até agora o fez. Ele precisa instituir garantias aos indivíduos afetados".[77] Sobretudo diante da falta de uma lei geral de proteção de dados pessoais no Brasil, Jacqueline Abreu conclui que é preocupante que o decreto não se ocupe dessas questões.

5. Conclusão

O direito à privacidade tem múltiplas intersecções com o exercício das liberdades públicas. Nesse sentido, é impossível dissociar esse direito das condições de vida e participação democrática dos cidadãos, seja na sua interface com o poder público, seja nas suas interações sociais e/ou de acesso à informação, cada vez mais mediadas por atores privados, proprietários e desenvolvedores de plataformas como as redes sociais ou motores de busca.

Do ponto de vista das relações travadas com o setor privado, o presente artigo argumenta que *(i)* a arquitetura da Internet permite que sejam adotadas técnicas não-transparentes de coleta, tratamento e usos de dados pessoais, o que aumenta a vulnerabilidade dos usuários perante esses atores; *(ii)* as tecnologias de monitoramento e coleta de dados implicam a transferência irrestrita de dados ao redor do mundo, exigindo a adoção de modelos regulatórios que sejam compatíveis entre si; *(iii)* o fato de os modelos de negócios que financiam o oferecimento de produtos e serviços gratuitos estarem calcados justamente na coleta e tratamento de dados pessoais exige que sejam colocadas balizas regulatórias para a realização dessas atividades, sob pena de se manter fragilizada a proteção do direito à privacidade.

Nesse contexto, os desafios para a realidade brasileira são os de *(i)* aprovar um marco regulatório de proteção de dados pessoais,

com o objetivo de estabelecer parâmetros para as atividades de coleta, tratamento e transferências internacionais de dados pessoais desempenhadas por atores privados e que envolvem usuários brasileiros; *(ii)* promover a conscientização dos usuários em relação aos modelos de negócios praticados por essas empresas e dos impactos que isso gera em relação à sua autonomia; e *(iii)* criar nas instituições brasileiras, sobretudo entre os membros do Poder Judiciário, uma cultura de valorização do direito à privacidade, garantindo que a aplicação do eventual marco regulatório adotado venha a ser implementado com rigor.

Do ponto de vista das relações travadas com o setor público, o presente artigo indica que *(i)* o Brasil está inserido em um contexto mundial de avanço de propostas invasivas de vigilância, que apostam no aumento das capacidades de investigação e controle do Estado em nome do que cada governo considera como segurança nacional; *(ii)* o Poder Público tem feito cada vez mais uso de ferramentas de coleta e tratamento de dados pessoais para desempenho das suas funções como gestor público, o que abre caminho para novas formas de compartilhamento e uso dos dados e registros gerados nessas atividades para fins de vigilância e persecução criminal; e *(iii)* o aumento dessas prerrogativas de coleta e acesso a dados de usuários mantidos por atores privados ameaça as liberdades democráticas na medida em que possibilita maior controle por parte do Estado.

Nesse contexto, os desafios para a realidade brasileira são os de *(i)* regulamentar a utilização de dados pessoais coletados pelo próprio Poder Público, estabelecendo, inclusive, limites rigorosos para o seu compartilhamento entre órgãos da Administração; *(ii)* preservar as garantias estabelecidas no Marco Civil da Internet, mantendo o crivo judicial como baliza para a quebra da privacidade dos usuários e o consequente acesso a dados pessoais que estejam nas mãos de atores privados; e *(iii)* promover uma cultura de valorização

do direito à privacidade como premissa para o exercício das liberdades democráticas, especialmente no âmbito de instituições como o Poder Judiciário, o Ministério Público e a Polícia.

6. Bibliografia

ABREU, Jacqueline de Souza, O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?, JOTA.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys M. "Vigilância das comunicações pelo estado brasileiro e a proteção a direitos fundamentais" – Electronic Frontier Foundation / InternetLab, 2015.

ANDERSON, Chris, *FREE: The Future of a Radical Price*, New York: Hyperion, 2009.

ANTONIALLI, Dennys M. Indenizações por dano moral ameaçam liberdade para se fazer humor na Internet, Consultor Jurídico, 31/08/2016, disponível em http://www.conjur.com.br/2016-ago-31/dennys-antonialli-dano-moral-ameaca-liberdade-humor-internet.

_____."Watch your virtual steps: an empirical study of the use of tracking technologies in different regulatory regimes". *Stanford Journal of Civil Rights and Civil Liberties*, v. VIII, 2012.

BAILENSON, J. N.; IYENGAR, S.; YEE, N.; *et al*. Facial Similarity between Voters and Candidates Causes Influence. **Public Opinion Quarterly**, v. 72, n. 5, p. 935–961, 2008.

BRANDEIS, Louis / WAREN, Samuel, "The right to privacy", *Harvard Law Review* IV (1890).

BRASIL, Portal. **Governo coloca em prática ação para barrar fraudes no Bolsa Família**. Portal Brasil. Disponível em: <http://www.brasil.gov.br/cidadania-e-justica/2016/07/governo-coloca-em-pratica-acao-para-barrar-fraudes-no-bolsa-familia>. Acesso em: 21 nov. 2016.

BRILL, Julie, "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions" (20.01.2014), <disponível em **http://www.ftc.gov/system/files/documents/public_statements/202151/140220princetonbigdata_0.pdf**, último acesso em 26.10.2016>.

BRITO CRUZ, Francisco, Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet, Universidade de São Paulo, dissertação de mestrado, 2015.

BUTLER, Brandon. **BMW's vision for a world of connected cars**. Network World. Disponível em: <http://www.networkworld.com/article/3072687/mobile-wireless/bmw-s-vision-for-a-world-of-connected-cars.html>. Acesso em: 21 nov. 2016.

CALO, Ryan, Digital market manipulation, The George Washington Law Review, vol. 82, 2013.

CAVOUKIAN, Ann, Privacy By Design: The Seven Foundational Principles (2009), <disponível em **http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf**, último acesso em 26.6.2014>.

CRAWFORD, Kate / SCHULTZ, Jason, Big Data Due Process: Toward a Framework to Reddress Predictive Privacy Harms.

CRAWFORD, Susan / GOLDSMITH, Stephen, The Responsive City, Jossey-Bass, 2014.

EDELMAN et. al, Internet Advertising and the Generalized Second-Price Auction: Selling Billions of Dollars Worth of Keywords, The American Economic Review 97 1 (2007).

French lawmakers extend state of emergency after Nice attack. **Reuters**, 2016.

Disponível em: <http://www.reuters.com/article/us-europe-attacks-nice-idUSKCN10009V>. Acesso em: 21 nov. 2016.

GONÇALVES, Antonio Felipe de Almeida. **Balões para segurança da Olimpíada são destaque — Ministério da Justiça e Cidadania**. Disponível em: <http://www.justica.gov.br/sua-seguranca/grandes-eventos/imprensa/baloes-para-seguranca-da-olimpiada-sao-destaque>. Acesso em: 19 nov. 2016.

GREENLEAF, Graham, Global Tables of Data Privacy Laws and Bills (3rd Ed, June 2013) (June 16, 2013). UNSW Law Research Paper No. 2013-39.

GRUMAN, Galen. **Apple Watch: The Internet of things' new frontier**. InfoWorld. Disponível em: <http://www.infoworld.com/article/2608996/consumer-electronics/article.html>. Acesso em: 21 nov. 2016.

HICKS, Jennifer. **Johnnie Walker Smart Bottle Debuts At Mobile World Congress**. Forbes. Disponível em: <http://www.forbes.com/sites/jenniferhicks/2015/03/02/johnnie-walker-smart-bottle-debuts-at-mobile-world-congress/>. Acesso em: 21 nov. 2016.

HOOFNAGLE, Chris Jay ***et al***, Behavioral Advertising: The Offer You Cannot Refuse, Harvard Law and Policy Review 6, 2012.

JANSEN, Sue Curry. The Streisand Effect and Censorship Backfire. 2015. Disponível em: <http://sal.muhlenberg.edu:8080/librarydspace/handle/10718/2589>. Acesso em: 19 nov. 2016.

Justiça Eleitoral repassa dados de 141 milhões de brasileiros para a Serasa - Política. Estadão. Disponível em: <http://politica.estadao.com.br/noticias/geral,justica-eleitoral-repassa-dados-de-141-milhoes-de-brasileiros-para-a-serasa,1061255>. Acesso em: 21 nov. 2016.

LOVE, Brian / PICY, Emile, French lawmakers extend state of emergency after Nice attack, **Reuters**, 2016.

McDONALD, Aleecia M. / CRANOR, Lorrie Faith, *The Cost of Reading Privacy Policies*, A Journal of Law and Policy for The Information Society 543, 544, 564 (2008).

PARISER, Eli. The filter bubble: what the Internet is hiding from you. London: Viking/Penguin Press, 2011.

RATLIFF, James D.; RUBINFELD, Daniel L. Online advertising: Defining relevant markets. **Journal of Competition Law and Economics**, v. 6, n. 3, p. 653–686, 2010.

SOLTANI, Ashkan, et al., *Flash Cookies and Privacy* (Working Paper, 2009), <disponível em http://ssrn.com/abstract=1446862., último acesso em 20.10.2016>.

SOPRANA, Paula. *CPI de Crimes Cibernéticos "mutila" o Marco Civil da Internet?* Revista Época, 01/04/2016. Disponível em: http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/04/cpi-de-crimes-ciberneticos-quer-alterar-marco-civil-da-internet-no-brasil.html. Acessado em 18/11/2016.

SPTrans não divulga política de privacidade do bilhete único. CartaCapital. Disponível em: <http://www.cartacapital.com.br/sociedade/sptrans-nao-divulga-politica-de-privacidade-do-bilhete-unico-4526.html>. Acesso em: 21 nov. 2016.

TORY. **Farmácia Popular: falta transparência sobre uso de dados médicos.** CartaCapital. Disponível em: <http://www.cartacapital.com.br/sociedade/farmacia-popular-falta-transparencia-sobre-uso-de-dados-medicos>. Acesso em: 21 nov. 2016.

The Connected Aircraft: Beyond Passenger Entertainment and Into Flight Operations. Avionics Today. Disponível em: <http://interactive.avionicstoday.com/the-connected-aircraft/>. Acesso em: 21 nov. 2016.

The Government just passed the most extreme surveillance law in history – say goodbye to your privacy. The Independent. Disponível em: <http://www.independent.co.uk/voices/snoopers-charter-theresa-may-online-privacy-investigatory-powers-act-a7426461.html>. Acesso em: 21 nov. 2016.

TURNER, Zeke, Germans Reconsider Tough Privacy Laws After Terrorist Attacks, **Wall Street Journal,** 2016.

VALENTE, Mariana Giorgetti; NERIS, Natália; RUIZ, Juliana Pacetta; BULGARELLI, Lucas. O Corpo é o Código: estratégias jurídicas de enfrentamento ao revenge porn no Brasil. InternetLab: São Paulo, 2016.

Wahoo Fitness Announces GymConnect: Treadmill integration & control. Disponível em: <https://www.dcrainmaker.com/2016/01/announces-gymconnect-integration.html>. Acesso em: 21 nov. 2016.

What is the USA Patriot Web. Disponível em: <https://www.justice.gov/archive/ll/highlights.htm>. Acesso em: 21 nov. 2016.

WIRTHMAN, Lisa, What Your Cellphone Is Telling Retailers About You, Forbes EmcVoice (16.12.2013) <disponível em http://www.forbes.com/sites/emc/2013/12/16/what-your-cellphone-is-telling-retailers-about-you/, último acesso em 21.10.2016>.

Notas

1 Cf. BRANDEIS, Louis / WAREN, Samuel, "The right to privacy", *Harvard Law Review* IV (1890).

2 A utilização de dispositivos como esses permite, por exemplo, a captura de imagens de alta resolução à distância, como foi o caso que envolveu a cantora Barbra Streisand que, em 2003, teve sua casa sobrevoada e fotografada por um desses dispositivos. Ao pretender impedir a divulgação das imagens em jornais e tabloides, a cantora acabou chamando mais atenção para o caso, o que potencializou a sua divulgação. Cf. JANSEN, Sue Curry / MARTIN, Brian, The Streisand Effect and Censorship Backfire, International Journal of Communication 9, 2015, p.656-671. Para além da invasão de privacidade de pessoas públicas ou famosas, esses dispositivos também assumiram importantes aplicações no campo da vigilância para fins de segurança pública. Cf. GONÇALVES, Antonio Felipe de Almeida, **Balões para segurança da Olimpíada são destaque — Ministério da Justiça e Cidadania**, disponível em: <http://www.justica.gov.br/sua-seguranca/grandes-eventos/imprensa/baloes-para-seguranca-da-olimpiada-sao-destaque>, acesso em: 01 out. 2016.

3 Cf. VALENTE, Mariana Giorgetti; NERIS, Natália; RUIZ, Juliana Pacetta; BULGARELLI, Lucas. O Corpo é o Código: estratégias jurídicas de enfrentamento ao revenge porn no Brasil. InternetLab: São Paulo, 2016, p.2.

4 Cf. HOOFNAGLE, Chris Jay *et al*, Behavioral Advertising: The Offer You Cannot Refuse, Harvard Law and Policy Review 6, 2012.

5 Cf. Kate Crawford / Jason Schultz, Big Data Due Process: Toward a Framework to Reddress Predictive Privacy Harms.

6 Muito da discussão sobre "cidades inteligentes" passa por como aproveitar os dados gerados para a melhoria da gestão dos espaços públicos urbanos. Cf. CRAWFORD, Susan / GOLDSMITH, Stephen, The Responsive City, Jossey-Bass, 2014.

7 Estudo sugere, por exemplo, que anunciantes de cosméticos e produtos de beleza concentrem seus esforços publicitários na parte da manhã das segundas-feira quando, de acordo com as conclusões da pesquisa, as mulheres se sentem menos atraentes. Cf. CALO, Ryan. Digital Market Manipulation. The George Washington Law Review, vol. 82, 2013, p. 996.

8 Cf. ABREU, Jacqueline de Souza; ANTONIALLI, Dennys M. "Vigilância das comunicações pelo estado brasileiro e a proteção a direitos fundamentais" – Electronic Frontier Foundation / InternetLab, 2015. (Relatório de pesquisa), disponível em http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf, pp.35-36.

9 Cf. BAILENSON, Jeremy et. al. Facial similarities between voters and candidates cause influence. **Public Opinion Quarterly**, v. 72, n. 5, p. 935–961, 2008.

10 RATLIFF, James D.; RUBINFELD, Daniel L., Online advertising: Defining relevant markets, **Journal of Competition Law and Economics**, v. 6, n. 3, p. 653–686, 2010, p. 655. (esclarecendo que a abertura comercial da rede se deu por uma nova interpretação das políticas de uso aceitável (Acceptable Use Policy) da National Science Foundation, que até então só admitia seu uso para propósitos relacionados à pesquisa e à educação.)

11 Cf. BUTLER, Brandon, **BMW's vision for a world of connected cars**, Network World, disponível em: <http://www.networkworld.com/article/3072687/mobile-wireless/bmw-s-vision-for-a-world-of-connected-cars.html>, acesso em: 17 nov. 2016.

12 Cf. **The Connected Aircraft: Beyond Passenger Entertainment and Into Flight Operations, Avionics Today**, disponível em: <http://interactive.avionicstoday.com/the-connected-aircraft/>, acesso em: 17 nov. 2016.

13 Cf. Wahoo Fitness Announces GymConnect: Treadmill integration & control, disponível em https://www.dcrainmaker.com/2016/01/announces-gymconnect-integration.html, acesso em: 17 nov. 2016.

14 Cf. GRUMAN, Galen, **Apple Watch: The Internet of things' new frontier**, InfoWorld, disponível em: <http://www.infoworld.com/article/2608996/consumer-electronics/article.html>, acesso em: 17 nov. 2016.

15 Cf. HICKS, Jennifer, **Johnnie Walker Smart Bottle Debuts At Mobile World Congress**, Forbes, disponível em: <http://www.forbes.com/sites/jenniferhicks/2015/03/02/johnnie-walker-smart-bottle-debuts-at-mobile-world-congress/>, acesso em: 17 nov. 2016.

16 Cf. CALO, Ryan, Digital market manipulation, The George Washington Law Review, vol. 82, 2013, p. 1003–1005.

17 Cf. PARISER, Eli. The filter bubble: what the Internet is hiding from you. London: Viking/Penguin Press, 2011.

18 Cf. ANDERSON, Chris, *FREE: The Future of a Radical Price,* New York: Hyperion, 2009.

19 Pesquisa realizada em 2009 já indicava que todos os 100 sites mais visitados no mundo utilizavam *cookies* para a coleta de dados pessoais, por exemplo. Cf. SOLTANI, Ashkan, et al., *Flash Cookies and Privacy* (Working Paper, 2009), <disponível em http://ssrn.com/abstract=1446862. , último acesso em 20.10.2016>.

20 Cf. Chris Hoofnagle et al., "Behavioral Advertising: The Offer You Cannot Refuse", pp. 291-294.

21 Isso se tornou possível com a incorporação de mecanismos de identificação geográfica aos aplicativos de aparelho celular, por exemplo. Cf. WIRTHMAN, Lisa, What Your Cellphone Is Telling Retailers About You, Forbes EmcVoice (16.12.2013) <disponível em http://www.forbes.com/sites/emc/2013/12/16/what-your-cellphone-is-telling-retailers-about-you/ , último acesso em 21.10.2016>.

22 Um exemplo disso é o projeto "Immersion", desenvolvido pelo MIT Media Lab e que demonstra quantas informações relevantes podem ser

extraídas pela simples combinação entre os remetentes e destinatários presentes na sua caixa de *e-mail*. Cf. https://immersion.media.mit.edu/

23 Cf. EDELMAN et. al, Internet Advertising and the Generalized Second-Price Auction: Selling Billions of Dollars Worth of Keywords, p. 245-246.

24 Cf. Solon Barocas / Helen Nissenbaum, On Notice: The Trouble with Notice and Consent Order 1–6 (2009) (unpublished manuscript), <disponível em http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf, último acesso em 26.10.2016>.

25 Cf. McDONALD, Aleecia M. / CRANOR, Lorrie Faith, *The Cost of Reading Privacy Policies*, A Journal of Law and Policy for The Information Society 543, 544, 564 (2008).

26 Cf. BRILL, Julie, "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions" (20.01.2014), <disponível em http://www.ftc.gov/system/files/documents/public_statements/202151/140220princetonbigdata_0.pdf, último acesso em 26.10.2016>.

27 Cf. CRAWFORD, Kate / SCHULTZ, Jason, Big Data Due Process: Toward a Framework to Reddress Predictive Privacy Harms.

28 Cf. CALO, Ryan, Digital Market Manipulation, George Washington Law Review 82 (2014).

29 Para mais informações a respeito do funcionamento do mecanismo, cf. Jules Polonetsky / Omar Tene, "To track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising, *Minnesota Journal of Law, Science and Technology* 13 (2012), pp. 320-322.

30 Cf. CAVOUKIAN, Ann, Privacy By Design: The Seven Foundational Principles (2009), <disponível em http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf , último acesso em 26.6.2014>.

31 Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 12 U.S.C. §§ 3401-3422.

32 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

33 Children's Online Privacy Protection Act of 1998, Pub. L. No. 106-170, 15 U.S.C.

34 Video Privacy Protection Act of 1998, Pub. L. 100-618, 18 U.S.C. §§ 2710-2711.

35 É o exemplo da lei de privacidade do estado da Califórnia. Cf. "The California Online Privacy Protection Act".

36 A legislação exige que órgãos da administração pública federal coletem apenas os dados estritamente necessários para o desempenho de suas atividades e estabeleçam procedimentos para resguardar a sua segurança, por exemplo. Cf. 5 U.S.C. parag. 552a(e)(1)-(5).

37 A legislação exclui a possibilidade de acesso do público a documentos que contenham informações pessoais, como registros médicos (5 U.S.C. parag. 552(b) (6)) e registros ligados à segurança pública (5 U.S.C. parag. 552(b) (7)).

38 Cf. Seção 5 do "Federal Trade Commission Act".

39 Cf. Fair Information Privacy Principles, <disponível em http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf, último acesso em 26.6.2014>.

40 Para mais detalhes sobre o histórico de desenvolvimento do regime de auto-regulamentação nos Estados Unidos, cf. Daniel Solove / Woodrow Hartzog, "The FTC and The New Common Law of Privacy", *Columbia Law Review* 114 (2014), pp.1-15.

41 A esse respeito, cf. Marsha Blackburn, "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?: Hearing Before the Subcomm. on Commerce, Mfg. & Trade f the H. Comm. Of Energy and Commerce", 112th Cong. 4 (2012).

42 Cf. Artigo 1o da Diretiva 95/46/CE do Parlamento Europeu, de 24.8.1995. A Diretiva 95/46/EC passou por um processo de reformulação, tendo dado origem ao Regulamento Geral de Proteção de Dados Pessoais, aprovado em 27 de abril de 2016, e que entrará em vigor em 25 de maio de 2018. Para mais detalhes sobre o processo de reforma dos parâmetros regulatórios na União Europeia e as principais mudanças que serão introduzidas em 2018, cf. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

43 É o caso, por exemplo, de Canadá, México, Nova Zelândia, África do Sul, Austrália, Argentina, Colômbia, Chile, etc. Para uma lista completa dos países que adotam legislações de proteção de dados pessoais, cf. GREENLEAF, Graham, Global Tables of Data Privacy Laws and Bills (3rd Ed, June 2013) (June 16, 2013). UNSW Law Research Paper No. 2013-39, <disponível em http://ssrn.com/abstract=2280875, último acesso em 26.10.2016>.

44 Cf. Artigo 25 da Diretiva 95/46/CE do Parlamento Europeu, de 24.8.1995.

45 Cf. Artigo 30, 1, b, da Diretiva 95/46/CE do Parlamento Europeu, de 24.8.1995.

46 Cf. US-EU Safe Harbor Frameworks, <disponível em http://www.export.gov/safeharbor/eu/eg_main_018476.asp.

47 O "Safe Harbor" elegia sete princípios: notificação, consentimento, acesso, segurança, restrição de transferências subsequentes, limitação de finalidade e direito de reparação.

48 A lista com as empresas participantes pode ser encontrada no endereço https://safeharbor.export.gov/list.aspx

49 Cf. Jules Polonetsky / Christopher Wolf, The US-EU Safe Harbor: An Analysis of the Framework's Effectiveness in Protecting Personal Privacy, Future of Privacy Forum (2013), <disponível em http://www.futureofprivacy.org/wp-content/uploads/FPF-Safe-Harbor-Report.pdf, último acesso em 30.10.2016>.

50 Cf. Corte de Justiça Europeia, Caso C362/14, disponível em http://curia.europa.eu/juris/document/ document jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031

51 Cf. Privacy Shield Agreement, disponível em http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf

52 Referidamente as leis do Cadastro Positivo (Lei 12.414/2011), o Código de Defesa do Consumidor (8.078/1990), e a Lei Geral de Telecomunicações (Lei 9.472/1997).

53 Fontes: http://oglobo.globo.com/economia/defesa-do-consumidor/oi-multada-em-35-milhoes-por-invasao-de-privacidade-feita-por-velox-13348505 e http://www.justica.gov.br/noticias/ministerio-da-justica-notifica-telefonica-vivo-por-servico-smart-steps

54 As afirmações referentes ao processo de elaboração e tramitação do Marco Civil da Internet podem ser encontradas em BRITO CRUZ, Francisco, Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet, Universidade de São Paulo, dissertação de mestrado, 2015.

55 A interpretação da aplicação destas sanções tem causado ampla divergência no Judiciário brasileiro. Juízes e autoridades de persecução penal têm entendido que o descumprimento de determinações judiciais abre espaço para requerer, por exemplo, o bloqueio de tais aplicações de Internet. É o caso de algumas das recentes ordens de suspensão do aplicativo de mensagens WhatsApp, contestadas ao Supremo Tribunal Federal na ADPF 403 e na ADI 5527.

56 Debate exemplificado na controvérsia entre o diretor de políticas públicas do Google Brasil, Marcel Leonardi, e a representante do Coletivo Intervozes, Veridiana Alimonti, em seus comentários sobre o tema na Semana Especial sobre Proteção de Dados Pessoais produzida pelo InternetLab, cf. http://www.internetlab.org.br/pt/semana-especial-protecao-de-dados-pessoais/

57 Apelação TJ-RS nº 0208925-06.2014.8.21.7000.

58 Processo nº 0805175-58.2015.4.05.8400.

59 Cf. LOVE, Brian / PICY, Emile, French lawmakers extend state of emergency after Nice attack, **Reuters**, 2016.

60 Cf. TURNER, Zeke, Germans Reconsider Tough Privacy Laws After Terrorist Attacks, **Wall Street Journal**, 2016.

61 Cf. **The Government just passed the most extreme surveillance law in history – say goodbye to your privacy**, The Independent, disponível em: <http://www.independent.co.uk/voices/snoopers-charter-theresa-may-online-privacy-investigatory-powers-act-a7426461.html>, acesso em: 20 nov. 2016.

62 Cf. **What is the USA Patriot Web**, disponível em: <https://www.justice.gov/archive/ll/highlights.htm>, acesso em: 20 nov. 2016.

63 Cf. ABREU, Jacqueline de Souza; ANTONIALLI, Dennys M. "Vigilância das comunicações pelo estado brasileiro e a proteção a direitos fundamentais" – Electronic Frontier Foundation / InternetLab, 2015. (Relatório de pesquisa), disponível em http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf

64 Cf. ABREU, Jacqueline de Souza; ANTONIALLI, Dennys M. "Vigilância das comunicações pelo estado brasileiro e a proteção a direitos fundamentais" – Electronic Frontier Foundation / InternetLab, 2015. (Relatório de pesquisa), disponível em http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf

65 Cf. ABREU, Jacqueline de Souza; ANTONIALLI, Dennys M. "Vigilância das comunicações pelo estado brasileiro e a proteção a direitos fundamentais" – Electronic Frontier Foundation / InternetLab, 2015. (Relatório de pesquisa), disponível em http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf

66 Em pesquisa realizada pelo InternetLab sobre liberdade de expressão e conteúdos humorísticos na Internet, constatou-se um desprestígio do direito à liberdade de expressão em relação a outros direitos, como honra e imagem, o que chama a atenção para os casos de identificação de usuários de Internet por conteúdos veiculados como forma de constrangimento. Cf. ANTONIALLI, Dennys. Indenizações por dano moral ameaçam liberdade para se fazer humor na Internet. Consultor Jurídico, 31/08/2016, disponível em http://www.conjur.com.br/2016-ago-31/dennys-antonialli-dano-moral-ameaca-liberdade-humor-internet, acesso em 10 de dezembro de 2016.

67 Conforme o Departamento Intersindical de Assessoria Parlamentar (DIAP). Fonte: Valor Econômico, 2015, disponível em: http://www.valor.com.br/politica/3843910/nova-composicao-do-congresso-e-mais-conservadora-desde-1964, acesso em 20 nov. 2016.

68 InternetLab, 2015, disponível em: http://www.internetlab.org.br/pt/noticias/pesquisadores-questionam-medidas-de-pl-sobre-crimes-contra-a-honra-na-internet/, acesso em 18 nov. 2016.

69 Cf. SOPRANA, Paula. *CPI de Crimes Cibernéticos "mutila" o Marco Civil da Internet?* Revista Época, 01/04/2016. Disponível em: http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/04/cpi-de-crimes-ciberneticos-quer-alterar-marco-civil-da-internet-no-brasil.html. Acessado em 18/11/2016.

70 Outros projetos e leis aprovadas seguem na mesma direção, como a Lei Antiterrorismo (n. 13.260/2016, que estabelece que podem ser considerados terroristas ataques cibernéticos e, portanto, submetidos a seu regime peculiar e extremo de persecução criminal) e o projeto de lei do Senado Federal n. 730/2015, também dirigido à retirada da ordem judicial para acesso a dados de usuários.

71 InternetLab. *Bloqueios.info*. Sítio eletrônico, 2016.

72 Cf. **Justiça Eleitoral repassa dados de 141 milhões de brasileiros para a Serasa - Política**, Estadão, disponível em: <http://politica.estadao.com.

br/noticias/geral,justica-eleitoral-repassa-dados-de-141-milhoes-de-brasileiros-para-a-serasa,1061255>, acesso em: 18 nov. 2016.

73 Cf. **SPTrans não divulga política de privacidade do bilhete único**, CartaCapital, disponível em: <http://www.cartacapital.com.br/sociedade/sptrans-nao-divulga-politica-de-privacidade-do-bilhete-unico-4526.html>, acesso em: 19 nov. 2016.

74 Cf. TORY, **Farmácia Popular: falta transparência sobre uso de dados médicos**, CartaCapital, disponível em: <http://www.cartacapital.com.br/sociedade/farmacia-popular-falta-transparencia-sobre-uso-de-dados-medicos>, acesso em: 19 nov. 2016.

75 Cf. ABREU, Jacqueline de Souza, **O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?**, JOTA, disponível em: <http://jota.info/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro>, acesso em: 19 nov. 2016.

76 Cf. BRASIL, Portal, **Governo coloca em prática ação para barrar fraudes no Bolsa Família,** Portal Brasil, disponível em: <http://www.brasil.gov.br/cidadania-e-justica/2016/07/governo-coloca-em-pratica-acao-para-barrar-fraudes-no-bolsa-familia>, acesso em: 19 nov. 2016.

77 Cf. ABREU, Jacqueline de Souza, **O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?**, JOTA, disponível em: <http://jota.info/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro>, acesso em: 19 nov. 2016.