Provedores de acesso à Internet, dados pessoais e privacidade – para que regulação?

Graciela Baroni Selaimen*

*Quis custodiet ipsos custodes?***

SUMÁRIO

No Brasil há um vácuo regulatório no que diz respeito à privacidade na Internet e à retenção, uso e destino de dados de usuários de empresas de provimento de acesso e serviços Internet. Os cidadãos e cidadãs que navegam na rede ficam à mercê das políticas internas de cada provedor de acesso sobre o uso de seus "logs" —que incluem informações pessoais e hábitos de navegação. Estas informações, que têm crescente valor comercial, podem vir a ser uma fonte de renda ainda mais lucrativa que o próprio serviço de provimento de acesso e serviços Internet, uma vez que são elementos essenciais para práticas, por exemplo, de publicidade direcionada, o chamado *target advertising*— hoje um forte mercado baseado na Internet. Este estudo parte do pressuposto de que é possível harmonizar uma legislação de proteção à privacidade às prerrogativas intrínsecas à estrutura da operação dos provedores, que exigem a coleta e armazenamento de informações relativas ao uso dos seus serviços para fins de gerenciamento de suas redes e de seu negócio. Queremos apontar princípios e critérios que poderiam nortear políticas públicas de privacidade que respondam ao interesse público, aos direitos dos usuários, e ao mesmo tempo respeitem requisitos técnicos fundamentais para a operação dos provedores de acesso.

* Coordenadora do Instituto Nupef —*www.nupef.org.br* ?—, mestranda em Comunicação e Cultura na Escola de Comunicação da Universidade Federal do Rio de Janeiro; membro do *Multistakeholder Advisory Group* do Fórum de Governança da Internet.

** Quem observa os observadores? Frase de Juvenal, poeta romano autor de "As Sátiras".

Palavras-chave: privacidade, provedores de acesso e provedores de serviço à Internet, vigilância, políticas públicas, legislação e marcos regulatórios.

1. *Introdução*

Sabemos que nenhuma única instituição, grupo, indivíduo ou governo controla a Internet contemporânea. Todavia, isso não significa que ela não possa ou não esteja sendo controlada, de diferentes maneiras e em diversos níveis. A despeito do fato de a Internet ter sido construída numa modelagem baseada na descentralização, hoje ela é controlada direta e indiretamente por uma ampla gama de atores:[1] governos nacionais, côrtes judiciais, autoridades policiais, entidades reguladoras nacionais e internacionais, desenvolvedores de softwares, hardwares e engenheiros de computação, corporações multinacionais e conglomerados de mídia, anunciantes, gigantes da telecomunicação, provedores de acesso e provedores de serviços Internet, entre outros.

Pode-se dizer que o controle na Internet é disperso e relativamente descentralizado. Ainda que não exista um ponto único de controle, há pontos críticos nos caminhos e nos fluxos de informação na rede a partir dos quais diferentes formas de controle podem ser exercidas com significativa eficácia.

Os provedores de acesso e serviços Internet são um destes pontos: nodos tecnológicos fundamentais para a garantia ou a violação dos direitos dos usuários, predominantemente do direito à privacidade e à liberdade de expressão, em alguns países, o papel desempenhado pelos provedores comerciais pode ser estendido aos governos, como nas experiências recentes de implantação de territórios ou cidades digitais no Brasil —nas quais o governo local assume o papel de provedor de acesso e serviços Internet, como uma alternativa de democratização do acesso à Internet a uma maior parcela da população em localidades remotas ou fora do mapa de interesse das empresas de telecomunicações.

A falta de leis específicas para a proteção da privacidade na Internet abre espaço para o monitoramento indevido, o uso não

[1] Jonathan Zittrain explica bem os princípios da arquitetura da rede e suas formas de controle no artigo *Internet Points of Control,* publicado em *http://ssrn.com/abstract_id=388860*

autorizado e a comercialização de dados pessoais,[2] preferências e hábitos de navegação por diferentes atores que atuam na rede mundial —entre os quais os provedores de acesso ocupam um lugar de destaque.

A função dos provedores de acesso —de portas de entrada para a Internet— exige, como elemento fundamental para sua operação, um determinado nível de monitoramento e controle sobre as ações dos seus usuários, com coleta e armazenamento de informações relativas ao uso dos seus serviços. Os acordos feitos com os usuários sobre o destino e formas de utilização destes dados são estabelecidos nos contratos de prestação de serviço, que muitas vezes apresentam uma linguagem jurídica inacessível para o usuário leigo. A necessidade imperativa de contratar um provedor de acesso para chegar à Internet, juntamente com a falta de percepção a respeito do poder de vigilância e decisão delegado aos provedores sobre o uso de dados pessoais, torna o usuário comum extremamente vulnerável à violação da privacidade e ao uso indevido de seus dados. Acreditamos que só uma legislação específica para este setor pode garantir o respeito a direitos fundamentais dos usuários destes serviços —entre eles, o direito à privacidade—. Atualmente, não há nenhuma restrição legal no Brasil sobre a quantidade de dados que um provedor pode armazenar, ou sobre o tipo de dados que pode ser coletado e armazenado. Tampouco há regulação específica que busque evitar o uso não desejável de dados pessoais por parte destes atores.

As ameaças à privacidade na Internet têm suas origens em diversos fatores. A crescente divulgação de informações pessoais pelos consumidores permitem que as empresas coletem e processem dados extensivamente, e de forma cada vez mais detalhada e minuciosa. Ao mesmo tempo, cada vez mais os produtos oferecidos na Internet exigem dos consumidores interessados em adquiri-los o registro de usuário, a permissão para o uso de tecnologias de identificação, e a concordância com termos de uso que frequentemente ferem a privacidade dos usuários, ainda que veladamente.

[2] Tomamos como referência, ao utilizar o conceito 'dados pessoais', a definição adotada pelo Grupo de Trabalho sobre Proteção de Dados do Article 29 da Comissão Européia conforme o documento 01248/07/EN WP 136: Opinion 4/2007 on the concept of personal data.

De acordo com a organização inglesa Privacy International,[3] a realidade hoje é de que todos os maiores *players* da Internet fazem movimentos para estabelecer um nível de vigilância sobre os usuários que resulta em pouquíssima ou nenhuma escolha por parte destes últimos para fugir desta realidade —e há poucos mecanismos significativos de proteção da privacidade.

No mundo inteiro, cresce a percepção por parte de governos e empresas sobre o papel crítico dos provedores de acesso no controle sobre as atividades dos indivíduos na Internet e se intensifica o desenvolvimento de tecnologias e políticas de controle e vigilância. Algumas das tecnologias de vigilância mais eficazes hoje atuam especificamente no nível do provedor de acesso à Internet —um exemplo é o uso da tecnologia DPI (*Deep Packet Inspection,* inspeção profunda de pacotes). Como explica Ralph Bendrath:

> DPI é uma funcionalidade integrada às redes de comunicação digital que permite que o proprietário da rede física analise o tráfego Internet (os datagramas, em seu caminho pela rede) em tempo real e discrimine-o de acordo com o conteúdo encapsulado em cada datagrama.(...) A tecnologia DPI está no mercado desde 2002 e sua capacidade de análise de tráfego aumentou significativamente desde então. Hoje, o equipamento de DPI com mais capacidade pode sustentar um tráfego de 80 Gigabits por segundo (Anderson 2008). Isso permite que os provedores de acesso à Internet monitorem e discriminem o trafego de 20 mil assinantes de banda larga utilizando uma banda de 4 megabits por segundo cada —mesmo que estejam todos online ao mesmo tempo, utilizando 100 % de sua banda.

Além da capacidade tecnológica, se intensifica também a disposição política de governos para o exercício do controle sobre o uso da Internet pelos cidadãos a partir dos provedores de acesso. Ofereceremos exemplos sobre este cenário mais adiante. As empresas, por sua vez, sabem que os usuários facilmente optam por oferecer suas informações pessoais em troca de serviços gratuitos e de sua concordância em receber mensagens publicitárias. Muitas empresas adotam também a prática de analisar o conteúdo trafegado pelo/para o usuário e monetizar esse conteúdo. Será que ao concordar com isso os usuários sabem

[3] *http://www.privacyinternational.org*

que seus e-mails estão sendo sujeitos a mineração de dados muitas vezes em tempo real? Em discurso recente,[4] a Comissária Européia para o Consumo afirmou que "os dados pessoais são o novo combustível da Internet e a nova moeda do mundo digital" e chamou a atenção para o fato de que, atualmente, os consumidores têm pouca noção sobre que dados estão sendo coletados, como e quando são coletados, e para que finalidades são usados.

2. *Provedores de acesso à Internet e privacidade*

Provedores de acesso são os portões de entrada na Internet. Não é possível acessar a rede mundial sem a intermediação de um provedor. Como explica Marcel Leonardi:

> "...é muito comum a confusão entre provedores de *backbone*, provedores de acesso, provedores de correio eletrônico, provedores de hospedagem, provedores de conteúdo e provedores de informação, atividades completamente distintas que podem ser prestadas por uma mesma empresa a um mesmo usuário ou por diversas empresas, separadamente". Neste estudo, nos focamos na figura do provedor de acesso —entendido, como aquele que tem a função "de atribuir ao usuário, desde que entre eles exista essa obrigação, derivada de acordo entre as partes, um endereço IP para que o usuário possa se conectar à Internet e dela fazer uso, conforme sua vontade". [5]

Os provedores são um dos pontos mais críticos para a adoção de práticas de controle na Internet relativamente descentralizada. São eles um dos pontos de convergência de eixos de poder por onde se estabelecem práticas de controle na rede. Segundo Demont-Heinrich,[6] "mais de quarenta países restringem as capacidades de navegação na Internet de seus cidadãos no nível do provedor de acesso, incluindo algumas das poderosas democracias ocidentais, como a Alemanha". Esta tendência de controle por parte dos governos dos usos da Internet pelos cidadãos

[4] Meglena Kuneva, em seu discurso de abertura na mesa redonda Data Collection, Targeting and Profiling. Bruxelas, 31 de março de 2009.

[5] Brandini Barbagalo, Erica, citada por Leonardi, Marcel: *Responsabilidade civil dos provedores de serviços de Internet,* Juarez de Oliveira, 2005.

[6] Demont-Heinrich, Christof: "Central points of control and surveillance on a 'Decentralized', Net Internet Service Providers and Privacy and Freedom of Speech Online", IAMCR, 2002.

através dos provedores de acesso tem ganhado relevância crescente e suscitado o debate público. Vale mencionar a proposta recente do governo francês —a chamada lei Sarkozy— para limitar e punir o download de conteúdos protegidos por direitos de propriedade intelectual.

No Brasil, o Projeto de Lei Substitutivo do Senador Eduardo Azeredo (PSDB-MG), que tipifica os crimes informáticos e os crimes cometidos via Internet, suscita reações apaixonadas tanto por parte de seus defensores como por parte de seus opositores. O Substitutivo apresentado pelo Senador Eduardo Azeredo aglutinou três projetos de lei que já tramitavam no Senado, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares.[7] Um dos pontos mais polêmicos do projeto é a necessidade de identificação eletrônica do usuário para acessar a Internet, e o armazenamento dos "logs"[8] do usuário pelos provedores de Internet. Há grandes resistência por parte da sociedade civil e de setores da academia, que alegam que o projeto viola a liberdade de expressão e oficializa o vigilantismo na Internet brasileira.

No rastro do PL 84/99, outros projetos de lei aparecem —no começo de junho de 2009, o PL 5361/2009, de autoria do deputado Bispo Gê Tenuta (DEM-SP), foi apresentado de forma discreta na Câmara dos Deputados. O projeto do Bispo Gê —que se diz motivado nesta iniciativa "por uma preocupação com a indústria cultural"— prevê punição ao usuário de Internet que quem for pego baixando arquivos protegidos por direitos autorais, nos mesmos moldes da lei Sarkozy: com a suspensão do seu acesso à rede. Segundo o texto do projeto, os provedores de internet seriam obrigados a vigiar o que o internauta faz, e se constatassem que um determinado usuário baixa ou compartilha arquivos de música, por exemplo, poderiam punir o usuário com a suspensão do acesso, sem necessitar para isso de ordem judicial. Por mais remota que seja hoje a possibilidade de aprovação deste projeto no Brasil —que é inconstitucional em vários pontos e entra em conflito até mesmo com a lei de direitos autorais brasileira—,[9] é interessante notar o crescente interesse dos parlamentares sobre as possibilidades de controle da Internet e sua percepção sobre o papel crítico que têm os provedores de Internet para a implementação de medidas neste sentido.

Segundo Paul Ohm,[10] até recentemente os provedores não se preocupavam muito em observar os usos e hábitos de navegação de seus clientes, até porque não dispunham de aparatos tecnológicos tão sofisticados quanto os que existem hoje. Ohm afirma que atualmente os provedores têm capacidade técnica de espionar seus usuários de maneiras jamais imaginadas. Enquanto isso, detentores de direitos de propriedade intelectual e empresas anunciantes têm pressionado direta e indiretamente os provedores para que os dados de seus usuários sejam revelados e/ou colocados à venda —e, observando a profusão recente de relatórios sobre o tema, os provedores têm cedido a esta tentação, e experimentado novas formas de vigilância. Para Ohm, esta é apenas a ponta do iceberg que anuncia uma onda sem precedentes de vigilância invasiva por parte de provedores de serviço e de acesso à Internet.

2.1. O funcionamento dos provedores de Internet e as possibilidades de monitoramento

O provedor de acesso à Internet conecta o usuário à Internet, fornecendo no ato da conexão um IP real com o qual a rede ou máquina do usuário passa a ser vista na Internet. Na regulação brasileira, este é chamado um "serviço de valor adicionado."[11]

7 Ver mais sobre este PL no site da Safernet: *http://www.safernet.org.br/site/institucional/projetos/obsleg/pl-azeredo*

8 Não há consenso sobre qual é a definição exatada de "logs". Neste texto, entendemos os "logs" como quaisquer registros que o provedor de Internet possa fazer a partir da conexão dos seus usuários: data e horário de conexão; tempo de conexão; sites visitados e serviços utilizados; etc.

9 As opiniões de diversos especialistas em direito informático sobre o PL 5361/2009 podem ser lidas em *http://www.estadao.com.br/noticias/tecnologia+link,brasil-pode-ter-sua-propria-lei-sarkozy,2785,0.shtm#*

10 Ohm, Paul: "The Rise and Fall of Invasive ISP Surveillance", University of Colorado Law School, September 2008.

11 Segundo a Anatel (Agência Nacional de Telecomunicações), Serviço de Valor Adicionado —SVA, definido no artigo 61 da LGT, é a atividade que acrescenta a um serviço de telecomunicações que lhe dá suporte - e com o qual não se confunde— novas utilidades relacionadas ao acesso, ao armazenamento, à apresentação, à movimentação ou à recuperação de informações. O SVA não constitui serviço de telecomunicações, classificando-se seu provedor como usuário do serviço de telecomunicações que lhe dá suporte. É assegurado aos interessados o uso das redes de serviços de telecomunicações para prestação de serviços de valor adicionado.

Hoje, na maioria das vezes, este serviço de provimento de acesso vem acompanhado de outros serviços —sediamento de sites, hospedagem de servidores, gerenciamento de contas de email, ferramentas para publicação e gerenciamento de conteúdos, etc.— os chamados serviços Internet, em vários países do mundo, os maiores provedores de acesso e serviços oferecem também conteúdos (alguns deles exclusivos aos assinantes) tais como fazem no Brasil os portais Terra, UOL, etc. Outro fato que ocorre com frequência —no Brasil e em outros países— é o de as operadoras de serviços de telecomunicações também fazerem o serviço de provimento de acesso à Internet,[12] prescindindo de outros provedores para isso. Este acúmulo de papéis por uma mesma empresa —de fornecedora de conexão física através da infraestrutura de telecomunicação e de fornecedora da conexão lógica como provedora de acesso à Internet— leva a um cenário de concentração ainda mais agudo, dado o modelo que resultou do processo de privatização do sistema de telecomunicações do país, na década de 90, no qual consórcios de grandes empresas internacionais detêm o monopólio dos serviços em cada uma das regiões do país.

O fato de os provedores de acesso à Internet serem tão visados por governos e empresas deve-se a um elemento central da

[12] Como explica Carlos Afonso: "According to prevailing legislation, recommended by the Brazilian Internet Management Committee (CGI)7 and regulated by ANATEL, a cable TV licensee or telephone operator that offers ADSL may connect its users to the internet, but access authentication must be done by an internet service provider (ISP). This is a result of legislation adopted in the country that separates the physical and logical infrastructure (data transmission methods) from the service layers, and prevents monopolies from developing. In practice, however, with the consolidation of companies and the convergence of technology, this rule has been systematically broken by cable TV operators and companies. Telefônica claims to operate ADSL services in over 900 municipalities in São Paulo, and is the owner of the service and content provider Internet Terra Networks; the cable TV quasi-monopoly Net Serviços, belonging to Organizações Globo and Telmex, offers internet services and content via its subsidiary Globo.com. It is not mandatory to take out a contract for connection and services from the same company, but it is obvious that these companies have many advantages when it comes to attracting users towards a single contract that encompasses all services (connection, email, access to information, etc.). This process has led to a consolidation in the provision of services and content, with the rapid disappearance of small-scale service providers". Afonso, C. Global Information Society Watch, 2007.

natureza da sua operação, que é o registro (e eventual manutenção destes registros) de acesso de seus clientes - dados que podem revelar detalhes sobre as comunicações e os hábitos de navegação dos assinantes.

O que são esses registros (logs) e o que se registra? Segundo Carlos Afonso, diretor executivo do Instituto Nupef e coordenador do projeto Tiwa,[13] os logs são basicamente de dois tipos:

– Registro de tempo, hora de início e hora de término, da conexão a um serviço de acesso à Internet (via linha discada, via ADSL, via rádio, etc.).

Esse registro é feito pelos provedores de acesso por razões contratuais e para monitorar a carga (intensidade de uso) dos sistemas. Os provedores de acesso têm um contrato com os usuários para prover o serviço (como o Velox da Oi, o Speedy da Telefónica, ou serviços similares via linha discada, ou rádio, etc.) e precisam desse registro para dirimir possíveis questionamentos sobre a efetiva prestação desses serviços. O contrato obriga à completa identificação fiscal e jurídica do cliente, dados que ficam registrados em cadastros. Os registros de cada conexão em geral contêm, além de dos dados de tempo e identificação do usuário contratante do serviço de acesso, o número IP[14] real (ou seja, "visível" por qualquer outra máquina na Internet) designado à máquina do usuário no período da conexão.

[13] O Tiwa é um provedor de serviços Internet, projeto originado do Alternex (primeiro provedor de serviços Internet no Brasil para a sociedade civil, criado no Ibase), posteriormente reorganizado como RitsNet (projeto que funcionou por doze anos na Rede de Informações para o Terceiro Setor).

[14] O IP, ou Internet Protocol, é um tipo específico de protocolo que foi projetado para criar ligações entre diferentes redes, possibilitando a intercomunicação entre dispositivos nelas presentes. Uma interligação entre diversas redes é normalmente chamada de internet. Cada computador numa determinada internet possui um número único, que o identifica dentre da mesma, chamado endereço IP. Pelo número de IP pode-se identificar o usuário de uma sessão de acesso à Internet. O número IP de origem em geral é o IP real designado pelo provedor de acesso a uma rede local, ou a uma máquina única) - através deste, pode-se determinar de imediato a origem geográfica, qual a rede de provimento de acesso etc. Esse IP de origem da visita é, portanto, cadastrado no registro do provedor junto com a informação de páginas visitadas. Este "rastro digital" leva facilmente (pelo menos do ponto de vista técnico) os dados desse registro ao responsável pela rede local para a qual estava designado aquele IP real nos períodos de visita registrados, bastando para isso que o interessado solicite (ou requisite) da respectiva operadora ou provedor de acesso os respectivos registros de acesso. No Brasil, o atendimento a este tipo de solicitação depende da "autoritatividade" ou força legal do solicitante.

– Registro de utilização de serviços de conteúdo via Internet (essencialmente páginas web de sítios, blogs, etc.).

Neste caso, o registro é feito pelos provedores de conteúdo por razões de mercado (ou para avaliar impacto). Por exemplo, o sítio do Fórum Social Mundial —que está hospedado no Tiwa—, tem um log de acesso para estimar seu impacto, possibilitando o conhecimento quanto a países de origem das visitas, número de visitas, que páginas são mais vistas etc. O mesmo fazem os sítios de provedores de conteúdo comerciais. Este registro contém em geral o número IP e os dados de tempo, e através de cruzamento com bases de dados de nomes e números (automaticamente feito pelos programas de registro), este número revela o país de origem. É o mesmo número IP cadastrado em algum lugar do planeta por um provedor de acesso desse usuário. Ou seja, em tese, é possível associar os dois registros.

Esses registros são feitos hoje de maneira independente na Internet brasileira. Não nos parece razoável a idéia de querer impedir legalmente que esses registros continuem, como propõem algumas das vozes que justificadamente buscam a defesa da privacidade e da liberdade na Internet, todavia sem compreender os detalhes tecnológicos da operação dos provedores e as demandas práticas deste tipo de negócio. No primeiro caso, por razões jurídicas (contratuais), é de interesse do usuário que esses registros existam (no caso de cobrança indevida ou falha na prestação de serviço pelo provedor, por exemplo). No segundo caso porque sem esses dados simplesmente se mata a "monetização" dos conteúdos, que é a base do modelo de negócios na Internet hoje em dia. Como garantir aos patrocinadores que um site é bem sucedido em termos de visitas e interessante em termos de origem de acessos, por exemplo?

A questão que propomos neste estudo é que deve haver um meio termo, que é possível e desejável um marco regulatório que ao mesmo tempo respeite estas características intrínsecas à operação dos provedores de Internet, e também assegure que os empreendedores que acumulam esses dados (os "guardiães dos logs") não os usarão para quaisquer propósitos, para uso próprio ou em conluio com terceiros, sem o pleno conhecimento, a anuência do usuário e respeitando o seu direito à privacidade e à autodeterminação informativa.

2.2. **Concentração do mercado e propriedade cruzada**

Nos primeiros anos da Internet comercial, havia centenas de provedores de acesso e serviços Internet no Brasil, oferecendo acesso discado a assinantes através de serviços de telefonia fixa. Segundo a Rede Nacional de Pesquisa (RNP),[15] em 1997 o Brasil contava com cerca de 600 provedores de acesso. No final do ano 2000, eram 150, uma diminuição sensível, seguindo uma tendência mundial de oligopolização dos serviços da Internet. Esta concentração do mercado é mais intensa em se tratando de banda larga: em 2006, os grandes provedores (Terra, Brasil Telecom Internet e UOL) conquistaram uma fatia de 64 % deste mercado no Brasil. Esta realidade era anunciada por alguns autores desde o início da década: Irina Dimitrieva[16] há nove anos já expressava sua preocupação com a tendência de fusões entre empresas de Internet, quando afirmava que "no futuro, apenas um punhado de empresas privadas controlarão as comunicações online".

Entre os grandes provedores, há um número significativo que é parte de grandes conglomerados de mídia brasileiros - como as empresas Globo, o grupo Abril Folha, etc. Esta realidade é um dos reflexos do que costuma ser chamado um "cipoal regulatório"[17] do setor de Comunicação Social do país, que permite, entre outras situações, a ocorrência da propriedade cruzada de meios. Este fato torna ainda mais crítica a possibilidade de monitoramento do uso da Internet por parte de grupos empresariais gigantescos na área de comunicação e entretenimento. O registro e processamento dos usos e hábitos de navegação do internauta é um prato cheio e apetitoso para as empresas que operam estes provedores —que, segundo Ohms, hoje sofrem de uma síndrome de "inveja do Google". A Google mostrou

[15] Dados divulgados na revista *ComCiência - http://www.rnp.br/noticias/imprensa/2001/not-imp-010310.html*

[16] Dimitrieva, Irina: "Will Tomorrow be Free? Application of State Action Doctrine to Private Internet Providers", em *http://books.google.com.br/books?id=wSfvdWIm3ykC&pg=PA3&lpg=PA3&dq=dmitrieva+irina+will+tomorrow+be+free%3F&source=bl&ots=_Tv_cL2tJb&sig=ZTnOgOCMPTyOBT960WTlEb6A-Q&hl=pt-BR&ei=TDk5SpPPI4Sktge6y43eDA&sa=X&oi=book_result&ct=result&resnum=1#PPA5,M1*

[17] O termo "cipoal regulatório" foi concebido por José Leite, conselheiro da Agência Nacional de Telecomunicações - Anatel.

como a monetização do comportamento dos usuários— a partir do uso eficiente de seus dados, do "rastro" que deixam na Web —pode transformar completamente o perfil e a dimensão do negócio de determinadas empresas na Internet. Para este autor, o sucesso da Google redefiniu as expectativas a respeito da lucratividade na Web— e também a respeito da privacidade online. Ohms afirma que os provedores hoje tentam replicar a invejável lucratividade que a Google obteve a partir dos preciosos dados que revelam padrões de consumo e comportamentos na Internet.

3. *O que pode ser feito com os dados coletados e armazenados*

Já vimos que o papel dos provedores de acesso —de portas de entrada para a Internet— exige, como elemento fundamental para sua operação, um determinado nível de controle e sobre as ações dos seus usuários, com coleta e armazenamento de informações relativas ao uso dos seus serviços. Os acordos feitos com os usuários sobre o destino e formas de utilização destes dados são geralmente estabelecidos nos contratos de prestação de serviço, que muitas vezes apresentam uma linguagem jurídica inacessível para o usuário leigo. A necessidade imperativa de contratar um provedor de acesso para chegar à Internet, juntamente com a falta de percepção a respeito do poder de vigilância e decisão sobre o uso de dados pessoais delegado aos provedores torna o usuário comum extremamente vulnerável à vigilância digital, à violação da privacidade e ao uso indevido de seus dados.

Entendemos por vigilância digital o "monitoramento sistemático, automatizado e à distância de ações e informações de indivíduos no ciberespaço, com o fim de conhecer e intervir nas suas condutas ou escolhas possíveis". Quatro processos se destacam nas práticas de vigilância digital: os mecanismos de coleta, monitoramento e arquivo de informação; os sistemas de classificação e conhecimento dos dados; os procedimentos de individualização e produção de identidades; as formas de controle sobre as escolhas e ações dos indivíduos (Bruno, 2008).

É importante compreender a enorme capacidade de vigilância que os provedores de Internet podem exercer sobre os dados dos seus usuários. Para isso, é útil uma explicação sobre como

as informações trafegam nas redes digitais. Como explica Carlos Afonso.[18]

> "Todas as informações que circulam na Internet são decompostas em pacotes de dados (os datagramas), que são enviados por um ou mais caminhos ao destino, onde são recompostos para formar o conjunto de dados original – uma mensagem, uma imagem, um documento, ou mesmo um fluxo de vídeo ou voz, em resumo, qualquer conteúdo que tenha trânsito na info-rede. Hoje, tecnologias existentes e de custo irrisório para operadoras de infovias[19] ("backbones"), graças aos protocolos atualmente em utilização, como o TCP/IP permitem que fluxos de datagramas possam ser integralmente recompostos, formando mensagens de email (com ou sem anexos), fluxos de telefonia ou vídeo digital, dados de navegação Web, transferência de arquivos em redes "peer-to-peer" (P2P), etc.
>
> Essas tecnologias permitem que os datagramas sejam identificados por tipo de aplicativo (FTP, HTTP, SMTP, fluxos VoIP, conexões terminais SSH etc.) e sejam quantificados ou mesmo armazenados na íntegra em bases de dados. Tecnologias de identificação e cópia de datagramas empregadas pela National Security Agency (NSA) estão disponíveis comercialmente para as operadoras de infovias ou qualquer outra organização que deseje praticar algum tipo de controle ou censura sobre o tráfego de datagramas que passe por sua rede. A combinação dessas tecnologias —chamadas "packet sniffers"— com gerenciadores de tráfego IP (os "traffic shapers") dá um excepcional poder e controle sobre o conteúdo trafegado na Internet às operadoras de infovias.
>
> Em geral, ações de controle, censura ou qualificação do tráfego podem ser difíceis de detectar por um usuário não especialista ou alguém que não seja particularmente teimoso. Todavia, equipamentos de mercado (a custos da ordem de US$ 50 mil) podem controlar ou vigiar um volume de tráfego comparável à soma de todas as infovias

[18] Afonso, Carlos: "Todos os datagramas são iguais perante a rede! Instituto", Nupef, 2007. Disponível em *http://www.nupef.org.br/publicacoes.htm*

[19] N.A.: Cabe ressaltar que no Brasil as operadoras de infovias também podem desempenhar o papel de provedores de acesso e serviços à Internet.

da maioria dos países".

A EPIC afirma que o fato de os provedores serem capazes de compilar um volume tão significativo de dados sobre os assinantes os coloca em uma posição de destaque para interesses externos que invariavelmente tentarão acessar os dados. Quanto mais dados eles coletam acerca dos assinantes para interesses comerciais, maior é o interesse que geram nas autoridades que querem obter este tipo de informações.

3.1. **Target advertising e a monetização dos logs**

Não é somente o interesse das autoridades que é despertado pelo enorme potencial de monitoramento, coleta e armazenamento de dados por parte dos provedores. A monetização destes dados tem surgido como um modelo de negócios muitas vezes mais lucrativo que o próprio serviço de provimento de acesso à Internet.

Sabemos da necessidade de registro e armazenamento dos dados de logs por parte dos provedores, com vistas à manutenção da segurança da rede e da estabilidade do fluxo de tráfego, entre outros aspectos inerentes à sua operação. Todavia, não se pode negar que também existem fortes incentivos econômicos para que os provedores compilem dados sobre assinantes, embora muitos provedores assumam o compromisso de não divulgar dados individuais ou, em alguns casos, agregar dados sobre seus assinantes de outras fontes, alguns provedores forjam relações estreitas com empresas de marketing. Demont-Heinrich cita exemplos de empresas norte-americanas como a Predictive Networks e a Compete.com, que recolhem e analizam dados dos consumidores através de provedores. Os dados coletados são posteriormente utilizados em campanhas de marketing segmentadas na Internet. Este autor também afirma que a maioria dos provedores alega ter um compromisso com a proteção da privacidade de seus usuários. Todavia, segundo ele, nos Estados Unidos já é comum algumas destas empresas tentarem capitalizar os temores quanto à violação da privacidade em suas campanhas de publicidade.

O relatório[20] da Federal Trade Comission norteamericana sobre *target advertising*, de fevereiro de 2009 define esta prática:

[20] Disponivel em *http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf*

> "Publicidade online envolve o monitoramento do comportamento dos consumidores na Internet a fim de enviar peças de publicidade adequadas aos seus hábitos e interesses. A prática, que normalmente é invisível para os consumidores, permite que as empresas alinhem os seus anúncios mais estreitamente aos interesses de seu público alvo, inferidos através de monitoramento, em muitos casos, as informações recolhidas não são pessoalmente identificáveis no sentido tradicional do termo – isto é, as informações não incluem o nome do consumidor, endereço físico, ou outro meio que poderia ser utilizado para identificar o consumidor no mundo offline".

Este conjunto de informações coletadas formam o que se costuma chamar de perfil digital, que pode ser compartilhado, combinado e analisado através do uso de técnicas de mineração de dados. Estes perfis são hoje os principais "ingredientes" para a publicidade online e para a segmentação comportamental. Apesar de não serem necessariamente associados a um nome e/ou endereço, sabemos que é possível inferir a verdadeira identidade do usuário por trás do perfil. Assim afirmou Anne Carblanc, Administradora principal da Information Computer and Communications Policy Division, da Organização para a Cooperação Econômica e Desenvolvimento (OECD) em workshop[21] realizado na reunião do IGF de 2008, em Hyderabad. Segundo ela, a coleta de dados e construção de perfis irá alimentar o rápido crescimento da publicidade na Internet, partindo de receitas de US$ 21,7 bilhões em 2007 para US$ 50,3 bilhões em 2011 - uma taxa de crescimento anual de mais de 24 %. Anne afirmou que isso se deve ao aprimoramento das tecnologias de coleta e mineração de dados, à expansão do acesso à Internet banda larga e ao barateamento dos custos de armazenamento dos dados. Carblanc chamou a atenção para o fato de que a captura de dados para fins mercadológicos no nível do provedor de acesso é uma tendência emergente.

[21] Workshop 83 - *The Future of Online Privacy: "Online advertising and behavioral targeting*", organizado pela Electronic Privacy Information Center (EPIC), pelo Center for Media and Communications Studies (CMCS), pela Central European University (CEU) em colaboração com a DiploFoundation. Relatório disponível em *http://www.intgovforum.org/cms/Contributions 2009/Workshop-Report-IGF-vf.pdf*.

No mesmo evento, Kristina Irion, Professora Auxiliar do Departamento de Políticas Públicas da Universidade da Europa Central (CEU), afirmou que a segmentação comportamental ainda dá seus primeiros passos. Segundo ela, há uma forte tendência para a massiva coleta de dados pessoais ainda em preparação e esta deve ser uma preocupação na área de proteção da privacidade, uma vez que não há política eficaz ou outro instrumento de combate à concentração de coleta de dados.

A exposição do indivíduo que está por trás do internauta desafia as salvaguardas à privacidade hoje existentes. O mercado dos dossiês digitais é um setor que cresce e se consolida, uma tendência que parece escapar a qualquer controle da privacidade na Internet.

Os efeitos e impactos da coleta massiva de dados para fins mercadológicos é descrita por Tal Z. Zarsky, no artigo *Online privacy, tailoring and persuasion*.

> "Essa coleta é possível graças à diminuição dos custos associados ao incremento da capacidade de memória do computador e à armazenagem dos dados, o que permite às empresas salvar muitos terabytes de informação - os quais, na verdade, não têm utilidade aparente. A crescente coleta de dados também é facilitada pela constante melhoria das infraestruturas de comunicação, que permitem o fluxo cada vez maior de informações pessoais de forma rápida e eficaz a partir do seu local de coleta para outros locais, onde são armazenadas".

Há diversas ferramentas que permitem que os provedores façam o rastreamento de cada ação do usuário online, registrando suas sessões de utilização da internet e os endereços IP visitados, portanto, é perfeitamente possível a um provedor de Internet exercer uma vigilância constante e onipresente. Os provedores podem saber onde seus usuários buscam informações, que tipo de informações buscam e consomem, que serviços e produtos consomem e utilizam, em que horários, delineando assim padrões, de forma muito apurada. Com esses dados em mãos, é possível construir um extenso perfil de cada usuário. Este perfil provê às empresas fornecedoras de conteúdos e serviços dados suficientes para mapear de modo eficaz as preferências, interesses, hábitos e, eventualmente, até características pessoais dos usuários monitorados, e serve como uma base sólida para as fases subsequentes de análise de utilização dos dados coletados.

Zarsky explica que, para além da mera coleta e armazenamento, o uso eficiente de informações pessoais é possível através da introdução de meios avançados de análise de dados. Estas novas ferramentas permitem às empresas capitalizar o grande volume de dados sob seu controle.

3.2. **Mineração de dados, construção de perfis e predição de condutas**

Evidentemente, a capacidade de recolher uma grande quantidade de informações pessoais é quase inútil, se estes dados não puderem ser utilizados. A coleta de dados relativos a cada sessão de uso de cada internauta cria enormes bases de dados com milhares de milhões de entradas. As empresas que coletam os dados, ansiosas para utilizar esta informação —consideradas por muitos uma mina de ouro— podem não saber por onde começar a analisar estes dados, e podem não ter os recursos humanos para fazer face a esta proeza. Estas e outras dificuldades em analisar vastas bases de dados levaram ao desenvolvimento de uma nova geração de ferramentas para análise de dados, geralmente conhecidas como *Knowledge Discovery in Databases* (KDD). O desenvolvimento destas novas ferramentas tem sido possível graças aos progressos significativos nas áreas de ciência da computação e matemática. Estas aplicações não exigem que um analista faça uma consulta inicial ou sugira a forma como os dados devem ser divididos em subseções, em vez disso, essas aplicações empregam sofisticados algoritmos computacionais que podem ser executados através de toda a base de dados automaticamente, em busca de padrões e de correlações específicas entre vários fatores.

Além disso, as ferramentas de mineração de dados e de *profiling* podem exercer funções tanto descritivas quanto preditivas. Elas permitem a utilização de informações parciais sobre usuários específicos para fazer suposições sobre suas ações futuras, ao combinarem os seus dados com padrões e agrupamentos de dados derivados de informações coletadas anteriormente. Assim, fornecedores de conteúdos e serviços podem utilizar ferramentas de mineração de dados e de *profiling* para predizer os gostos e preferências dos usuários e assim influenciar condutas.

Conforme Fernanda Bruno, os padrões e regularidades daí extraídos permitem visualizar domínios com certa homogeneidade

interna e fronteiras externas —de interesses, comportamentos, traços psicológicos— que de outro modo ficariam indefinidos ou fora do nosso campo de atenção. Assumem assim um formato mais dócil, calculável, legitimado e orientando intervenções diversas. Perfis de criminosos, consumidores, profissionais, doentes físicos ou mentais, tipos psicológicos ou comportamentais apresentam-se como padrões que ao mesmo tempo ordenam e objetivam a multiplicidade humana, legitimando formas de governá-la.

Enfim, estas ferramentas transformam a grande quantidade de informações pessoais coletadas em fontes gerenciáveis de conhecimento e de percepção. Zarsky ressalta que este processo de três níveis (de coleta, análise e uso de dados pessoais), deve ser encarado como um ciclo contínuo que está constantemente sendo reavaliado e refinado, assim formando um ciclo de retroalimentação no processo de oferta de conteúdos e serviços personalizados para cada usuário específico.

Conhecimentos específicos sobre traços de personalidade e preferências de cada usuário podem informar anunciantes sobre que tipo de respostas emocionais específicas eles devem tentar provocar no consumidor para estimulá-lo a agir numa determinada direção. O constante monitoramento dos usos e condutas dos consumidores municiam os anunciantes sobre que estímulos induzir para obter a resposta desejada. Quando terceiros —neste caso, anunciantes e fornecedores de conteúdos e serviços— têm em suas mãos estas poderosas ferramentas de persuasão, os direitos dos indivíduos à autonomia de pensamento e de ação podem ser comprometidos, em outras palavras, quando os consumidores são bombardeados com mensagens de marketing e publicidade especialmente adaptados, capazes de capitalizar sobre a sua vulnerabilidade e tirando proveito dos seus pontos fracos, é possível que as suas atitudes e escolhas subsequentes não sejam as mesmas que teriam sido adotadas se estes consumidores tivessem a oportunidade de refletir sobre elas sem tanta interferência.

A capacidade de categorizar a conduta dos indivíduos não implica somente na possibilidade de influenciar condutas presentes, mas também na possibilidade de simular comportamentos futuros. "O perfil é uma simulação pontual de identidades que ao se anunciar tem uma efetividade performativa e proativa, fazendo passar à realidade o que era apenas uma potencialidade.

Aí reside uma última característica importante –a performatividade do perfil, que opera segundo um formato próximo ao oracular" (Bruno, 2006).

Essa vigilância digital sistemática, embora tratada como um tema emergente no IGF, já era alvo de estudos em 2002. Os pesquisadores Roland T. Rust, P. K. Kannan and Na Peng, no artigo *The Customer Economics of Internet Privacy* concluem que, se a privacidade for deixada entregue às forças do mercado, no futuro a privacidade será um forte mercado. Todavia, a abordagem destes autores sugere que não apenas os dossiês digitais serão um produto altamente vendável, mas que a defesa da privacidade, em si mesma, se tornará um produto. Ou seja, a privacidade vai tornar-se um bem tão escasso, que emergirá uma "indústria da privacidade". Conforme se torna mais e mais difícil usufruir de privacidade no mundo das redes digitais, sua garantia e manutenção se tornará cada vez mais cara.

O modelo econômico desenvolvido por Rust, Kannan e Na Peng sugere a emergência de um mercado de privacidade que permitirá que os clientes comprem um certo grau de privacidade, num mundo em que se torna cada vez mais fácil para as empresas obter informações sobre os indivíduos público-alvo.

Ambas as perspectivas —a de comercialização de dados e perfis, e a de comercialização da própria privacidade— oferecem visões de uma Internet onde o usuário é mercadoria, não um indivíduo que deve ter garantidos seus direitos fundamentais. Conforme afirmou Meglena Kuneva, em seu discurso de abertura na mesa redonda[22] *Data Collection, Targeting and Profiling*, "do ponto de vista das comunicações comerciais, a World Wide Web está se tornando a world 'wide west'. E isso pode ser muito prejudicial".

4. *Disputas legais e políticas para acesso, retenção e uso de dados pessoais: alguns cenários*

Em 2008, a notícia de que três dos maiores provedores de Internet do Reino Unido (Virgin Media, BT and TalkTalk) decidiram vender o histórico de navegação de seus usuários para uma "agência de anúncios" online —o Phorm— mobilizou a mídia

[22] Realizada na abertura do European Consumer Summit 2009 em Bruxelas, março de 2009.

britânica, as organizações de defesa dos consumidores, e as entidades que defendem direitos na Internet.[23] A parceria entre os provedores e o Phorm significava que todo o conteúdo das páginas visitadas pelos usuários destes provedores seria acessível ao Phorm, que, a partir dos hábitos de navegação e interesses dos usuários, cria perfis para o envio de anúncios focados, o chamado '*targeted advertising*'. Os provedores, por sua vez, recebem uma porcentagem dos lucros obtidos com cada "click" nos anúncios oferecidos. Esta relação com o Phorm não foi divulgada pelos provedores aos usuários, e não foi oferecida nenhuma alternativa do tipo "*opt out*" para este monitoramento. No auge do debate, a Foundation for Information Policy Research (FIPR), formada por um grupo de especialistas em questões ligadas a políticas de Internet, escreveu uma carta[24] ao Commissário de Informações britânico argumentando que o sistema de anúncios direcionados do Phorm é ilegal. Segundo o site estaria "testando" o sistema do Phorm desde 2006, sem informar os usuários. Os protestos e ameaças de grupos de usuários e ativistas não intimidaram o Phorm. O executivo da empresa, Virasb Vahidi, garantiu: "Conforme você navega, nós somos capazes de categorizar todas as suas ações na Internet. Na verdade nós conseguimos ver a Internet toda".[25]

Ao mesmo tempo em organizações não governamentais apelam a agências de governo por medidas de proteção aos usuários de Internet, o governo do Reino Unido também é alvo de críticas e denúncias com relação à violação da privacidade dos cidadãos.

O Joseph Rowntree Reform Trust[26] (JRRT) lançou em 2008 um relatório onde aponta que os planos do governo britânico para a construção de uma base de dados única contendo, entre outras, informações sobre todas as comunicações dos britânicos, incluiria a proposta de interceptar, no nível do provedor de serviço Internet, todos os cabeçalhos de email dos usuários, o histórico de sites visitados e mesmo o histórico de ligações telefônicas, entre outros dados. O documento avisava que os cidadãos não estão "nem servidos nem protegidos pelos cada vez mais complexos e invasivos registro e armazenamento de informações pessoais que invadem todos os aspectos de nossas vidas". No total, 46 bases de dados mantidas pelo governo britânico foram analisadas pelo JRRT —o que também incluiu a *National DNA Database* e o *National Identity Register*—. Estas bases de dados foram, então, agrupadas em três categorias: Vermelho, Laranja e Verde. A categoria Verde reúne bases de dados consideradas eficazes, proporcionais e necessárias, construídas sobre bases legais que protegem contra a invasão da privacidade. Mesmo assim, algumas delas apresentam problemas operacionais. A categoria Vermelho inclui bases de dados profundamente intrusivas - algumas delas possivelmente ilegais sob o ponto de vista dos direitos humanos e de leis de proteção de dados. Segundo este estudo, muitas destas bases de dados deveriam ser totalmente redesenhadas, por trem sido construídas sem o consentimento dos cidadãos, por não tratarem adequadamente dados sensíveis, por questões operacionais, entre outros motivos. Por exemplo, a *National DNA Database* foi condenada pela Corte Européia de Direitos Humanos. Segundo o JRRT, hoje mais de dois terços da população britânica não confia no governo com relação à coleta e uso dos seus dados pessoais.

A proposta da super base de dados foi retirada pelo governo britânico em abril de 2009[27] devido à pressão dos grupos de defesa da privacidade. Entretanto, a Secretária de Governo Jacqui Smith continua levando adiante a proposta de rastrear toda chamada telefônica, mensagem de email e visita a website sob o pretexto de combater o terrorismo e os crimes cibernéticos como parte do programa *Interception Modernisation Programme.*[28] Assim, em lugar de coletar todos estes dados e armazená-los em uma única base de dados, os dados serão coletados e armazenados por cada provedor de Internet, por 12 meses. Estes dados incluem informações sobre hora, duração e destino de chama-

23 Como por exemplo, a mobilização BadPhorm: *http://www.badphorm.co.uk/page.php?2 e a Anti-Phorm League: http://www.antiphormleague.com/index.php*

24 A carta está publicada em *http://www.fipr.org/080317icoletter.html*

25 Ver em Clayton, Richard: The Phorm Webwise System, *http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf*

26 *O relatório pode ser lido em http://www.jrrt.org.uk*

27 Ver matéria do jornal *Daily Telegraph*: *http://www.telegraph.co.uk/news/newstopics/politics/5230459/National-database-dropped-but-all-our-communications-will-still-be-monitored.html*

28 Comentários sobre esta iniciativa podem ser lidos em *https://publicaffairs.linx.net/news/?cat=5*. O documento publicado para a consulta pública sobre este programa (aberta até 20 de julho de 2009) está em *http://www.homeoffice.gov.uk/about-us/haveyoursay/current-consultations/*

das telefônicas e contatos via Internet, bem como visitas a websites. As autoridades britânicas garantem que os conteúdos das comunicações não serão vigiados e armazenados. Os custos que recairão sobre os provedores para esta operação e armazenamento serão cobertos pelo poder público, e pagos com os impostos da população vigiada.

Após seis anos de implementação do programa *Transformational Government*[29] no Reino Unido, o número de bases de dados classificadas como Verde é incrivelmente baixo: apenas 6, em 46 (menos de 15 %). A *Communications Database* está incluída na categoria Vermelho. Esta base de dados pode ser consultada por todas as agências de inteligência do Reino Unido, por 52 forças policiais, por instituições prisionais e por 510 autoridades públicas diversas. No ano de 2007 foram feitas 519.260 solicitações de dados a esta base.

A despeito da medida aprovada pelo parlamento europeu no dia 6 de maio de 2009, que proíbe que os governos integrantes da União Européia cortem a conexão de internet de cidadãos sem antes passar por um tribunal de Justiça, a assembléia Legislativa da França aprovou em 12 de maio (por 296 votos a 233) um projeto de lei que permitiria desativar as conexões de Internet de usuários que fossem pegos repetidamente fazendo download ilegal de filmes e música. O projeto de lei criaria a primeira agência governamental para rastrear e punir piratas online —especialistas acreditam se tratar da primeira do gênero em todo o mundo—. Todavia, a tarefa de monitorar os usuários ficaria a cargo dos órgãos de defesa da indústria do entretenimento, que contariam, para isso, com as informações fornecidas pelos provedores de Internet, em 10 de junho o Conselho Constitucional francês considerou a lei inconstitucional. Entre os aspectos da lei rejeitados pelo Conselho Constitucional, está a possibilidade de a suspensão da conexão à Internet ser determinada por uma comissão administrativa. Na lei francesa, esta é

[29] O programa 'Transformational Government' foi criado para tornar serviços públicos mais eficientes e baratos – por conta disso, nos últimos anos, o govern britânico construiu ou ampliou muitas bases de dados centrais que agrupam informações sobre diversos aspectos das vidas dos cidadãos, desde dados sobre saúde, educação, até informações sobre o pagamento de impostos, seguridade social, etc. Este programa vem sendo seguidamente questionado sobre sua eficiência, eficácia, legalidade, custos e respeito à privacidade.

uma prerrogativa exclusiva de juízes. Entretanto, a ministra da Cultura da França, Christine Albanel, afirma que a queda de braço continua – o governo vai adequar a lei às regras do Conselho Constitucional, de modo que a decisão final sobre a suspensão da conexão à Internet seja de um juiz, mas a política de monitoramento do uso da Internet será mantida.

O projeto de lei francês previa que os acusados de pirataria online receberiam dois emails de aviso sobre sua prática "criminosa", seguidos de uma notificação oficial. Se os downloads ilegais continuassem a ser feitos pelos infratores dentro de um período de um ano após os avisos, o acesso à internet dessas pessoas seria cortado por um período que vai de dois meses a um ano – período durante o qual as pessoas punidas deveriam continuar a pagar pela manutenção do serviço, mesmo inativo.

A proposta de sanções após três avisos de infração a direitos de propriedade intelectual e copyright é comumente chamada de legislação "3-strikes". A indústria do entretenimento faz lobby no mundo inteiro para a implementação deste tipo de legislação –na qual os provedores de Internet têm papel central. Segundo Cory Doctorow,[30] esta política *3-strikes* é uma modalidade que consta do —ainda secreto— *Anti-Counterfeiting Trade Agreement*, que está sendo discutido pelos Estados Unidos, pelo Canadá, pelo Japão, pela União Européia e por outros países ricos a portas fechadas.

A adoção deste tipo de vigilantismo e punição a usuários de Internet não se limita à União Européia: na Nova Zelândia, o parlamento chegou a aprovar a Lei 92A, também uma proposta de legislação "3-strikes", mas diante da intensa pressão de intelectuais, artistas e grupos defensores de direitos na Internet, o governo viu-se obrigado a recuar. No Canadá, um Tribunal Superior do estado de Ontario[31] determinou que os endereços de IP deve ser tratados da mesma forma que endereços residenciais —portanto, as pessoas não deveriam ter nenhuma expectativa quanto à privacidade de suas atividades online—. Isso significa que no Canadá a polícia poderia requisitar informações aos provedores de Internet sobre as atividades de seus usuários sem

[30] Ver os comentários de Doctorow sobre o tema no blog Boing Boing - *http://www.boingboing.net/2009/05/07/eu-kills-3-strikes-i.html#previouspost*

[31] Notícia publicada em *http://arstechnica.com/tech-policy/news/2009/02/canadian-judge-no-expectation-of-privacy-in-online-tasks.ars*

necessitar para isso de um processo ou autorização judicial. Segundo a juíza Leitch, do Tribunal Superior de Ontario, o *Personal Information Protection Electronics Documents Act* do Canadá permite que provedores de Internet forneçam informações sobre os IPs a qualquer "autoridade" sem necessidade do devido processo legal.

Nos Estados Unidos, desde 1994 os provedores de Internet são obrigados por lei a fornecer dados dos usuários às autoridade. O CALEA —*Communications Assistance for Law Enforcement Act*— foi fruto de intenso lobby do Departamento de Justiça norte-americano junto ao Congresso. Esta lei determina que provedores de Internet são obrigados a adequar suas infraestruturas para auxiliar prontamente as autoridades em atividades de monitoramento dos usuários. Após 2001 os programas de vigilância e controle dos cidadãos —dentro e fora da Internet— chegaram a níveis de invasão que violam escancaradamente os direitos humanos. É fato que, quando se trata de vigilância na Internet, os provedores são um ponto de convergência para as ações das autoridades policiais e do Departamento de Segurança. Não podemos nos deter aqui para citar cada uma das ações de vigilância da Internet pelo governo norte-americano, mas sugerimos uma visita ao sítio da EPIC[32] para um panorama abrangente das disputas entre governo e entidades civis que defendem direitos naquele país.

No que diz respeito à parceria entre provedores de internet e empresas especializadas em *target advertising* nos EUA, um exemplo recente que chama a atenção é a operação da empresa NebuAd. Um relatório lançado em 2008 pela Free Press e pela Public Knowledge mostra que a NebuAd, atuando em conjunto com provedores de Internet norte-americanos, atacaram a liberdade de escolha dos usuários/consumidores, de maneira insidiosa e invisível.

No Brasil, tramita no Congresso Nacional o Projeto de Lei 84/99, também conhecido como "Projeto Azeredo". Este projeto de lei prevê, entre outras coisas, que os provedores de Internet retenham e guardem por um período de três anos todos os dados relativos à comunicação de seus usuários. O texto do projeto também prevê que os provedores devem ser responsáveis por denunciar possíveis crimes e atividades suspeitas de seus usuários —atribuindo aos provedores um papel de polícia—. O projeto de lei não menciona em nenhum ponto a proteção da privacidade dos usuários de Internet e também não prevê limites e critérios para a guarda —e possível uso— dos "logs"; apenas determina que as empresas guardem de forma protegida essas informações e só as disponibilizem com ordem judicial.

[32] *http://www.epic.org*

O relatório[33] "Legislação sobre Internet no Brasil", produzido pela Consultoria Legislativa da Área XIV - Comunicação Social, Informática, Telecomunicações, Sistema Postal, Ciência e Tecnologia do Congresso Nacional e divulgado em 4 de junho de 2009, afirma, sobre o PL 84/99:

> "(...) tramita na Câmara dos Deputados o Projeto de Lei nº 84/99, que tipifica tanto os crimes informáticos como os crimes cometidos via rede. O projeto original, de autoria do Deputado Luiz Piauhylino, teve parecer aprovado no Senado e retorno para votação na Câmara, estando submetido ao exame de três comissões. O parecer, do senador Eduardo Azeredo, penaliza, com reclusão ou multa, crimes como: acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado; obtenção, transferência ou fornecimento não autorizado de dado ou informação; divulgação ou utilização indevida de informações e dados pessoais; inserção ou difusão de código malicioso; inserção ou difusão de código malicioso seguido de dano; estelionato eletrônico; atentado contra a segurança de serviço de utilidade pública; interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado; falsificação de dado eletrônico ou documento público ou particular; divulgação ou utilização indevida de informações e dados pessoais; falsificação de documento e favor ao inimigo.
>
> Entre os principais pontos do projeto, como a tipificação de crimes, um dos pontos mais polêmicos é a necessidade de identificação eletrônica do usuário, a cada acesos, bem como armazenamento dos passos do usuário na rede. Há grandes resistência por parte de internau-

[33] Disponível em *http://www2.camara.gov.br/internet/homeagencia/materias.html?pk=135826*

tas e setores da academia, que alegam que o projeto viola a liberdade de expressão, o anonimato e implanta o vigilantismo na internet. O movimento contrário ao projeto de lei é encabeçado pelo professor da Universidade de São Paulo, Sérgio Amadeo.

Em 28 de maio de 2008, o Conselho de Altos Estudos e Avaliação Tecnológica promoveu o 'Seminário Internacional Crimes Cibernéticos e Investigações Digitais', no qual especialistas defenderam a tipificação urgente dos crimes cometidos na Internet. O Ministério da Justiça, em razão do papel da Polícia Federal de coibir o crime cibernético, chegou a divulgar minuta de projeto de lei, é favorável à identificação prévia do usuário e com a tipificação de vários crimes. Mas depois recuou. O seminário também foi palco das pressões para que o Brasil faça sua adesão à chamada Convenção de Budapeste, o mais notório diploma sobre o controle da Internet no mundo."

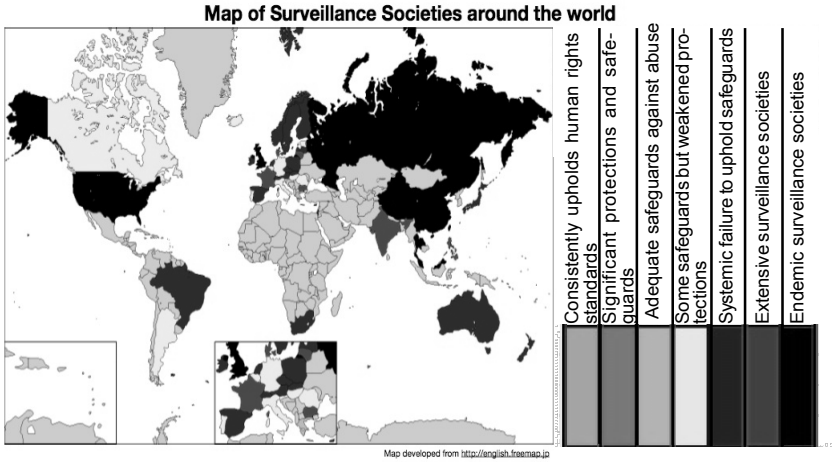
São muitas as pressões no Congresso Nacional para que o Brasil faça sua adesão à Convenção de Budapeste, embora o Ministério das Relações Exteriores argumente que o Brasil não costuma aderir a Convenções de cujas discussões não participou, como é o caso desta. Todavia, não se vê surgir no debate público ou nos debates no Congresso Nacional nenhuma menção aos compromissos assumidos pelo Brasil com relação à proteção de dados e defesa da privacidade, como faz na Declaración de Santa Cruz de la Sierra[34]—que expressa, em seu artigo 45: "Por isso, estamos conscientes de que a protecção de dados pessoais é um direito fundamental e destacamos a importância das medidas regulatórias ibero-americanas de protecção da privacidade dos cidadãos, contidas na Declaração de Antígua, que criou a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa comunidade".

O PL 84/99 prevê que os provedores de Internet, além de serem responsáveis pela retenção e armazenamento de dados de seus usuários, sejam também responsáveis pela segurança do armazenamento destes dados, pelo período de três anos. Para

[34] Declaração apresentada ao final da *XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno*, em 2003, na qual o Brasil é signatário. O documento está em *http://www.oei.es/xiiicumbredec.htm*

muitos provedores pequenos, isso significaria a inviabilidade de sua operação, por se tratar de um processo oneroso, que exige adequações técnicas e de infraestrutura, contratação de pessoal especializado em segurança, entre outros fatores.

Em se tratando da capacidade de garantir salvaguardas ao direito à privacidade, o Brasil aparece como um dos países com piores registros neste quesito, em pesquisa realizada pela organização inglesa Privacy International, em parceria com a norte-americana EPIC.[35] Desde 1997 esta pesquisa é realizada anualmente e hoje é considerada uma das mais elucidativas em termos de análise global do direito à privacidade. Este trabalho analisa o cenário de vigilância, monitoramento e proteção da privacidade em mais de 70 países.



Os países marcados em vermelho no mapa são aqueles que sistematicamente falham em garantir salvaguardas ao direito à privacidade a seus cidadãos.

Entre os piores países no ranking, de acordo com diferentes critérios, o Brasil aparece duas vezes: no critério *Privacy Enforcement* e no critério *Surveillance of medical, financial and movement.*

5. *Regulação e/ou regulamentação –o que é necessário?*

A Constituição Federal brasileira afirma o direito à privacidade como direito fundamental e prevê ressarcimento indeni-

[35] Os resultados de 2007 pode ser vistos em *http://www.privacyinternational.org/phr*

zatório em caso de danos materiais e morais que resultem de eventual violação a esse direito. Apesar de estar consagrado na Constituição, o direito à privacidade —especialmente na Internet— ainda é um campo incipiente. Pode-se afirmar que o Brasil "engatinha", em termos da produção de normas e da criação de instâncias de proteção deste direito. A legislação brasileira conta com instrumentos específicos para garantir o acesso a informações pessoais mantidas pelos governo, como o Habeas Data, e instrumentos para a defesa do consumidor —o Código de Defesa do Consumidor—. É comum o posicionamento, por parte de autoridades e ativistas dedicados ao combate ao cibercrime, que o Código de Defesa do Consumidor dá conta das questões relativas ao uso ético pelas empresas de dados pessoais de consumidores. Todavia, no entender de muitos advogados e ativistas que se dedicam à defesa da privacidade nas redes digitais, esta lei não alcança toda a complexidade do cenário atual, no qual a maior parte da coleta, armazenamento, uso, processamento de dados pessoais é realizada de forma invisível, por mecanismos camuflados na própria infraestrutura da rede e dos serviços online, e na maioria das vezes colocados em prática sem a consciência e consentimento do internauta.

O fato é que, no Brasil, falta regulação específica para a proteção de dados, em entrevistas que realizamos nesta pesquisa com representantes de associações provedores de acesso, foi consensual a percepção de que o processo de formulação das leis não acompanha o ritmo da inovação tecnológica. O relatório "Legislação sobre Internet no Brasil"[36] também toca neste ponto, ao fazer a recomendação de que "qualquer tentativa de regulação deve ser feita de maneira parcimoniosa e reduzida, sob pena de obsolescência da lei, em razão do dinamismo tecnológico".

Para os representantes da Abranet —Associação Brasileira de Provedores de Internet— assim como para um dos representantes dos provedores no Comitê Gestor da Internet no Brasil (CGI.br), os caminhos para uma maior proteção da privacidade dos usuários são: a autorregulamentação e a educação dos usuários. A adesão dos empresários a códigos de autorregulamentação é vista por estes atores como a melhor forma de regulação

[36] Relatório divulgado em junho de 2009 pela Consultoria Legislativa da Área XIV. Comunicação Social, Informática, Telecomunicações, Sistema Postal, Ciência e Tecnologia do Congresso Nacional.

para este setor —devendo ser levados à Justiça somente os casos que transcenderem a abrangência destes códigos—. Um argumento recorrente entre os que adotam esta visão é o de que "a Internet só evoluiu —e continua evoluindo— porque não depende de burocracia".

Assim, este discurso propõe a transferência da responsabilidade sobre a proteção da privacidade em grande parte para o usuário –que precisa ser "educado" para um uso mais consciente e para a oferta mais cuidadosa de seus dados; ao mesmo tempo, minimiza a necessidade da regulação, ao sugerir que a autorregulamentação é suficiente para a prevalência de posturas éticas quanto à coleta e o tratamento de dados pessoais no mercado de provimento de acesso e serviços Internet.

Para muitos provedores, uma estratégia bastante positiva seria a criação de um órgão de autorregulamentação, a exemplo do CONAR —Conselho Nacional de Autorregulamentação Publicitária—,[37] uma ONG encarregada de fazer valer o Código Brasileiro de Autorregulamentação Publicitária e que arbitra sobre processos éticos neste setor. A Abranet chegou a formular o seu próprio código de autorregulamentação,[38] que foi apresentado ao Comitê Gestor da Internet no Brasil e mesmo a alguns parlamentares —mas este documento até hoje não foi oficialmente "reconhecido" pelo CGI.br.

Sobre a proposta de autorregulamentação por parte de empresas de Internet, é interessante observar que este é um posicionamento recorrente por parte de representantes do setor privado e discutido em diversos fóruns e espaços dedicados ao debate sobre políticas de Internet e sobre a governança da rede mundial, em relação a este posicionamento, em mensagem recente à lista de discussões do *Internet Governance Caucus*, Parminder Jeet Singh, da organização indiana It for Change, cita Lawrence Lessig e complementa:

> "(...) here is the quote of Lawrence Lessig preceding the one which I sent earlier. But I think one big problem here is imagining companies as the leaders in public policymaking. You know, companies are in the business

[37] *http://www.conar.org.br/*

[38] Este documento esteve publicado no site da Abranet até março de 2009. No entanto, no momento de redação deste relatório, o *link* para o documento *(http://www.site.abranet.org.br/index.php?id=140*) não funcionava.

of making money. And if we begin to imagine a world where we trust companies to do good public policy, then we're fools, because they'll do good public policy when it makes sense for them from a financial perspective to do it, but when it doesn't make sense for them from a financial perspective to do it, they won't.

What he says is simple and generally universally accepted. Adam Smith said long ago. "People of the same trade seldom meet together… but the conversation ends in a conspiracy against the public. What does it say about industry-led 'regulatory systems'.

However the fact that such simple truths have to be re-asserted, but still ignored by many, speaks of the new forms of power that big corporations increasingly have to change our frames of thought and action, in some very basic and oft hidden ways. It becomes difficult to separate which actors, willy nilly, become agents of such new forms of dominations, but an introspection on this issue may be useful".[39]

O advogado e especialista em direito informático Seiiti Arata apontava bem a fragilidade dos argumentos em prol da autorregulamentação como forma exclusiva de balancear direitos e deveres nas relações online, em artigo publicado em 2004:[40]

> "Diante da dita crise do Estado soberano, não raro são discutidas propostas de autorregulação para as relações intermediadas pela internet buscando agilidade, constante atualização com o progresso tecnológico e garantia de conhecimento específico de importantes peculiaridades do setor econômico para a normatização de suas relações jurídicas.
>
> Apesar de apresentar grandes vantagens, não se deve esquecer que sua estrutura somente será firme na medida da solidez do interesse em que as condutas previstas sejam respeitadas.

[39] Este é um trecho de mensagem enviada à lista do Internet Governance Caucus em junho de 2009, *http://lists.cpsr.org/lists/info/governance.*

[40] Arata, Seiiti: "Internet e autorregulação: temas atuais, responsabilidade e crimes em *http://www.jusbrasil.com.br/noticias/4240/internet-e-autoregulacao-temas-atuais-responsabilidade-e-crimes.*

> De fato, as técnicas coercitivas que a autorregulação conta, por si só, não seriam suficientes para a desejada segurança jurídica. A conformidade da conduta às regras da autorregulação somente é observada enquanto existe uma conveniência, um equilíbrio favorável no sistema de sticks and carrots, das possíveis punições e dos benefícios que podem ser auferidos".

Neste ponto, é importante termos claro o que se quer dizer com os conceitos de 'regulação' e 'autorregulamentação'. Cabe bem a explicação oferecida por Gustavo Gindre, que cita o Dicionário Michaelis de Língua Portuguesa (1998), onde se define o ato de regular como "relativo a regras, jurídica e simetricamente estabelecidas, bem proporcionais, equilibradas, […]". Já regulamentação é o "ato de escrever e publicar o conjunto de normas que uma associação vai acatar". Gindre mostra que ambos os termos dizem respeito a regras:

> "O segundo, no entanto, manifesta a necessidade de estabelecer um código de normas (escritas e publicadas). O primeiro, por outro lado, aponta para a necessidade de proporção e equilíbrio, e não menciona nenhuma exigência explícita de codificação. A busca de equilíbrio e proporção remete-nos a um processo constante, dinâmico, e não ao mero desenvolvimento de um código que pretende ser tão eterno quanto possível. Regulamentação diz respeito ao conjunto de instrumentos jurídicos, tais como a Constituição, leis complementares e ordinárias, decretos, ordens executivas, normas, estatutos, códigos e assim por diante. Regular envolve o processo de regulamentação (e é importante reconhecer isso), mas vai além dele. É um leque mais vasto de práticas que visam acompanhar e interferir num dado processo, numa base diária, com intenções claras e bem definidas. Para isso, instrumentos legais podem ser utilizados, mas também várias outras 'ferramentas sociais'".

No nosso entendimento, a falta de regulação na área de privacidade e proteção de dados ajuda a criar distorções e mesmo uma falsa impressão de segurança entre os usuários de Internet. Isso porque muitos provedores de Internet criam suas próprias políticas de privacidade —que, publicadas em seus sites ou anexadas a contratos comerciais, acabam por ser o único

instrumento ao qual os usuários podem recorrer—. Como afirma o advogado Tiago Farina Marcos,[41] políticas de privacidade claras no sítios web passam a ser essenciais na captação de clientes, e devem informar o usuário de forma bastante objetiva sobre o tipo de informações que serão coletadas, o modo como será realizada a coleta dos dados, como os dados serão gerenciados, os motivos pelos quais serão armazenados em bancos de dados, a possibilidade de cruzamento das informações coletadas junto a terceiros etc. Mas o advogado lembra que estas "políticas de privacidade" são na verdade contratos de prestação de serviços, e como tal estão subordinados aos preceitos estabelecidos no Código Civil, e notadamente no Código de Defesa do Consumidor:

> "Art. 54: Contrato de adesão é aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas *unilateralmente* pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo" (grifo nosso).

Não há nenhuma garantia de proteção de direitos em contratos, mas sim acordos: ou o usuário aceita seus termos —sejam eles razoáveis ou não— ou deixa de utilizar o serviço oferecido. Uma questão complexa em relação às politicas de privacidade da maioria das empresas é a tendência à opacidade e inacessibilidade destes documentos – em geral, o acesso a estas políticas não ocupa lugar de destaque nos sites; os textos utilizam uma linguagem jurídica difícil, muitas vezes incompreensível para o usuário leigo; os documentos são extensos e, caso o usuário esteja realmente precisando do serviço (afinal, precisa da autenticação de um provedor para conectar-se à Internet), não restam muitas alternativas além de clicar no botão "aceito os termos do contrato".

Em termos de legislação para a proteção da privacidade de dados, o Brasil está em posição bastante atrasada em relação ao outros países. O vácuo regulatório que percebemos é endossado pelo advogado Ariel Foina,[42] quando diz que:

> "a questão da privacidade de dados no Brasil, especialmente quando se fala de privacidade na Internet ou em sistemas eletrônicos —excetuada a transmissão de dados— costuma ser reduzida a dois aspectos fundamentais: as relações de consumo, com seu conseqüente direito à informação, e a correção das informações armazenadas em bancos de dados.
>
> Tal redução geralmente decorre de uma situação jurídica brasileira muito singular, se observados outros países: o fato de que as únicas ferramentas legais que tratam de privacidade de informações no Brasil serem o Código de Defesa do Consumidor e a Constituição Federal quando trata das garantias e da via do hábeas-data. Desta míngua de normas, resulta a freqüente posição, comum entre juristas e operadores do direito, de que há a necessidade de se estabelecer critérios e leis destinados ao controle de quais dados pessoais e informações relativas ao comportamento do indivíduo na rede podem ser armazenados e utilizados por terceiros, especialmente quanto à forma como o indivíduo toma conhecimento e anui com tal uso e armazenamento".

[41] No artigo "Comércio de dados pessoais, privacidade e Internet", publicado na revista *Jus Navegandi*: *http://jus2.uol.com.br/doutrina/texto.asp?id=5667*

[42] Foina, Ariel: "Do panóptico ao 'Big Brother' - por uma política pública para a privacidade de dados no Brasil", Revista PoliTICs, julho de 2009.

Para que se possa falar na defesa do direito à privacidade online no Brasil e na efetiva possibilidade de defesa dos usuários em casos de coleta e uso indevido de dados pessoais, consideramos necessário um marco regulatório que demarque as possibilidades e limites de obtenção e uso de dados pessoais por governos e empresas, ainda que reconhecendo o valor e legitimidade de iniciativas de autorregulamentação em curso.

6. *Conclusões e recomendações*

Para nós fica claro, ao concluir este estudo, que não é por acaso que nos dias de hoje os provedores de Internet são um dos principais alvos das iniciativas de vigilância, monitoramento e controle de usuários de Internet, tanto por parte de governos em diversos países do mundo, quanto por parte de empresas.

Como pontos centrais de acesso à rede mundial de computadores, através da oferta de infraestrutura e serviços, os provedores de Internet são indispensáveis portas de entrada ao espaço público que é hoje a Internet. Assim, podem desempenhar um papel fundamental na promoção deste espaço como um ambiente democrático, inclusivo, onde as relações entre indivíduos, grupos de pessoas, organizações, governos, etc. se baseiem em critérios,

direitos e princípios acordados nas legislações nacionais, nos tratados, resoluções e convenções internacionais, e em outros instrumentos supranacionais de defesa de direitos. Por outro lado, também podem ser pontos de concentração de iniciativas de vigilância e controle —seja para fins comerciais, seja para fins de controle governamental e até mesmo para fins de delação e punição de atividades online consideradas ilegais.

Acreditamos que estamos hoje diante de uma encruzilhada, no que diz respeito à manutenção do caráter aberto, libertário e não-hierárquico da Internet conforme ela foi criada, conforme expressamos na cerimônia de abertura do Fórum de Governança da Internet em Hyderabad, 2008:

> "Hoy hacemos frente a una oposición ideológica entre dos tendencias principales que se manifiestan en los distintos estratos de internet. Una de ellas apunta a profundizar el libre flujo de la información, la construcción de los ámbitos comunitarios, ampliando el espacio y el dominio público en el uso y desarrollo de internet. La otra apunta a controlar, a restringir el acceso a la información y su circulación, a inspeccionar y contener su libre desarrollo a fin de favorecer los procesos económicos basados en la apropiación privada del conocimiento y las infraestructuras por las que circula la información, amenazando la naturaleza pública e igualitaria de internet".[43]

Enfatizamos que a garantia de direitos —dentro e fora da Internet— deve passar pela consolidação de leis e marcos regulatórios baseados nos princípios que fundamentam a Declaração dos Direitos Humanos. Especificamente no que diz respeito ao direito à privacidade e à proteção de dados pessoais, consideramos essenciais as iniciativas que têm por objetivo o fortalecimento do caráter universal do direito à privacidade e à proteção de dados e a harmonização de marcos regulatórios nesta área, seja mediante a adoção de instrumentos supranacionais de caráter vinculante, assim como mediante a adoção de leis nacionais que consagrem estes direitos.

[43] Selaimen, Graciela: Discurso na abertura do IGF 2008 na Índia. Publicado em *http://lac.derechos.apc.org/es.shtml?apc=he_1&x=5539240*

Recomendamos o desenvolvimento de uma convenção universal para a proteção dos indivíduos com relação à privacidade e à coleta e processamento de dados pessoais. Ressaltamos a importância da Resolução apresentada ao final da 30a Conferência Internacional de Autoridades de Proteção de Dados e Privacidade, em 18 de outubro de 2008,[44] especialmente quando apela às Nações Unidas que prepare um instrumento legal vinculante que claramente estabeleça em detalhe os direitos à privacidade e à proteção de dados como direitos humanos exigíveis e inalienáveis.

Outra recomendação que fazemos é que a consolidação de um marco regulatório nacional para a proteção do direito à privacidade e a proteção de dados pessoais seja orientada pelos princípios elencados nas Diretrizes para a Proteção de Dados na Comunidade Iberoamericana, desenvolvidas pela Rede Iberoamericana de Proteção de Dados. Além de um marco regulatório conforme estas diretrizes, recomendamos que seja criada no Brasil uma autoridade encarregada de zelar pelo seu cumprimento, à qual os cidadãos possam apelar e que tenha poderes de inspeção e investigação sobre o tratamento dados a estes direitos. "Esta autoridade deverá ser capaz de impor medidas que garantam a efetividade destes direitos, tais como sanções em caso de sua violação ou, pelo menos, que tenha a capacidade para instar aos tribunais a imposição de medidas nos casos em que se verifique o descumprimento da normativa nacional de proteção de dados e da privacidade".[45]

Em nível nacional, recomendamos também que o desenvolvimento de qualquer instrumento de regulação para a Internet seja baseado nos seguintes Princípios para a Internet no Brasil – formulados pelo Comitê Gestor da Internet no Brasil e apresentados em junho de 2009:

1. Liberdade, privacidade e direitos humanos: O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.

[44] Documento disponível em *http://www.privacyconference2008.org*

[45] Conforme o texto das Diretrizes para a Proteção de Dados na Comunidade Iberoamericana. Disponível em *https://www.agpd.es/portalweb/internacional/relaciones_iberoamerica/seminario_cartagena/common/pdfs/Documento_de_Directrices_de_armonizacion_final.pdf*

2. Governança democrática e colaborativa: A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.
3. Universalidade: O acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em beneficio de todos.
4. Diversidade: A diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores.
5. Inovação: A governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso.
6. Neutralidade da rede: Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento.
7. Inimputabilidade da rede: O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos.
8. Funcionalidade, segurança e estabilidade: A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.
9. Padronização e interoperabilidade: A Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento.
10. Ambiente legal e regulatório: O ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração.

Consideramos que estes princípios devem ser levados em conta em qualquer atividade na Internet, por representantes de todos os grupos de interesse: empresas, governos, sociedade civil, academia, comunidade técnica, usuários.

Especificamente em relação a marcos regulatórios e políticas públicas relativos à proteção da privacidade de usuários de provedores de acesso e serviços Internet, sugerimos as orientações do Council of Europe desenvolvidas em parceria com a European Internet Services Providers Association (EuroISPA), no documento "Human Rights Guidelines for Internet Service Providers".[46] Este documento oferece um conjunto de recomendações para que provedores de Internet desenvolvam suas atividades sob um marco de direitos humanos. Reconhecendo a centralidade dos provedores nas sociedades conectadas em redes digitais, este trabalho enfatiza a impotância do reconhecimento, pelos provedores, sobre o impacto que suas decisões, práticas e políticas podem ter sobre os direitos fundamentais dos usuários. Evidentemente, estas recomendações devem ser adequadas aos marcos regulatórios nacionais, quando houver. Assim, o documento do CoE e da EuroISPA recomenda, entre outras coisas,[47] que os provedores:

- Estabeleçam procedimentos apropriados e usem as tecnologias disponíveis para proteger a privacidade de seus usuários, bem como o sigilo de conteúdos e dados transmitidos em suas redes, especialmente assegurando a integridade dos dados, a confidencialidade e a segurança fisica e lógica da rede e dos serviços providos através suas redes. O nível de proteção deve ser adaptado ao tipo de serviço provido.
- Ofereçam suficiente informação e orientação aos seus consumidores sobre os meios técnicos que eles possam utilizar para protegerem-se contra riscos à segurança de seus dados e comunicações (tais como ferramentas anti-*spyware, firewalls*, tecnologia de encriptação ou assinaturas digitais, etc.).
- Em caso de implementarem ações relativas à comunicação de seus usuários (tais como permitir a interceptação ou o monitoramento das mensagens de email de usuári-

[46] Documento produzido em 2008. Publicado em *http://www.euroispa.org/*

[47] Destacamos aqui um número de recomendações específicas sobre a proteção da privacidade, mas sugerimos que também as outras recomendações apresentadas no "Human Rights Guidelines for Internet Service Providers" sejam consideradas na formulação de marcos regulatórios para a proteção da privacidade de usuários de Internet, ou na reformulação de regulação existente, quando houver e quando for necessário.

os), tais ações só devem ser tomadas em caso de obrigação imposta pela justiça, sob ordens ou instruções específicas de uma autoridade pública competente, feitas de acordo com a lei. Não monitorem ativamente o conteúdo das comunicações em suas redes. Além disso, a exclusão ou modificação que qualquer correspondência dos usuários (e.g. por filtros de spam) deve depender de consentimento explícito do usuário antes que tal medida seja posta em prática.

– Não revelem a identidade de usuários, o tráfego de seus dados ou o conteúdo de dados acessados por eles a terceiros, a não ser sob ordem judicial ou seguindo ordens específicas da autoridade pública competente feitas de acordo com a lei. Solicitações desta natureza feitas por entes de fora do país devem ser respondidas através das autoridades competentes em cada país.
– Informem seus usuários sobre em quais circunstâncias o provedor estará sujeito à obrigação legal de revelar suas identificações, dados de conexão e tráfego, mediante solicitação de autoridades. Tal informação pode ser oferecida especialmente por associações de provedores. Se receberem alguma requisição para divulgar tais dados, os provedores devem certificar-se da autenticidade da solicitação, e de que é feita pela autoridade competente de acordo com o que determina a lei.
– Não coletem, processem ou armazenem dados sobre usuários, a não ser que isso seja necessário para propósitos explícitos, específicos e legítimos, de acordo com as leis de proteção de dados. Não armazenem dados por mais tempo do que requerido pela lei, ou por mais tempo do que seja necessário para alcançar o propósito deste processamento de dados.
– Não usem dados pessoais para seus próprios propósitos comerciais ou mercadológicos, a menos que o usuário em questão, após ser informado, tenha consentido com esta prática, e que este consentimento não tenha sido revogado. Não tornem nenhum dado pessoal publicamente disponível.

Além destas recomendações, uma prática que consideramos bastante recomendável é a adoção de ícones que expressem as políticas de privacidade de cada site, a exemplo dos ícones do

projeto Creative Commons - hoje mundialmente utilizados. Acreditamos que com a adoção deste tipo de estratégia de divulgação, as políticas de privacidade fiquem mais acessíveis e compreensíveis por qualquer pessoa, se divulgadas em espaços de destaque nos sites dos provedores. Iniciativas desta natureza têm a vantagem de oferecerem escolhas aos usuários de forma simples e acessível; permitirem múltiplas combinações, de acordo com o contexto e com as possibilidades de cada provedor; e funcionarem em âmbito internacional, uma vez que são compreensíveis por pessoas de diferentes grupos linguísticos. Um exemplo do uso de ícones para informar políticas de privacidade é o que está publicado no blog netzpolitik.[48]

REFERÊNCIAS BIBLIOGRÁFICAS

Afonso, Carlos: *Global Information Society Watch 2007,* Associação Para o Progresso das Comunicações, HIVOS, Instituto do Terceiro Mundo, Uruguai, 2007. *http://www.giswatch.org/gisw2007/*

—: "Todos os datagramas são iguais perante a rede!", Instituto Nupef, Rio de Janeiro, 2007. *http://www.nupef.org.br/publicacoes.htm*

Arata, Seiiti: "Internet e autorregulação: temas atuais, responsabilidade e crimes", Jus Brasil, São Paulo, 2004. *http://www.jusbrasil.com.br/noticias/4240/internet-e-auto-regulacao-temas-atuais-responsabilidade-e-crimes*

Bendrath, Ralph: *Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection,* International Studies Annual Convention, New York City, 2009.

Brasil, Constituição da República Federativa do Brasil de 1988, em *http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm.*

Brasil: Código de Defesa do Consumidor, *http://www.mj.gov.br/DPDC/data/Pages/MJ7E3E5AAEITEMID736B189700174E618C00EF8DA589D98CPTBRNN.htm*

Bruno, Fernanda, *et al.: O Oráculo de Mountain View: o Google e sua cartografia do ciberespaço,* vol. 6, ap 1-21, Ecompós, Brasília, 2006.

—: "Monitoramento, Classificação e Controle nos Dispositivos de Vigilância Digital", XVII Encontro da Compós na UNIP, São Paulo, 2008.

Clayton, Richard: "The Phorm 'Webwise' System", Light Blue Touchpaper, 2008. em *http://www.lightbluetouchpaper.org/2008/04/04/thephorm-webwise-system/*

[48] *http://netzpolitik.org/best-of-netzpolitikorg/*

Comitê Gestor da Internet no Brasil (CGI.br.): *Decálogo de Princípios para a Internet no Brasil,* São Paulo, 2009.

Cumbre Iberoamericana de Jefes de Estado y de Gobierno, *Declaración de Santa Cruz de la Sierra,* Santa Cruz de la Sierra, 2003, em *http://www.oei.es/xiiicumbredec.htm*

Demont-Heinrich, Christof: "Central points of control and surveillance on a 'Decentralized' Net Internet Service Providers and Privacy and Freedom of Speech Online", vol. 4, nº 4, Info, 2002 , pp. 32-42.

Dimitrieva, Irina: "Will Tomorrow be Free? Application of State Action Doctrine to Private Internet Providers", em I Vogelsang & B Compaine (eds), *The Internet Upheaval: raising questions, seeking answers in communications policy*, MIT Press, Cambridge, 2000.

EPIC, Center for Media and Communications Studies, Central European University: *The Future of Online Privacy: online advertising and behavioral targeting.* Hyderabad: Internet Governance Forum, 2008. *http://www.intgovforum.org/cms/Contributions2009/Workshop-Report-IGF-vf.pdf*

EUROISPA e CoE: *Human Rights Guidelines for Internet Service Providers.*2008, em *http://www.euroispa.org*

FOINA, Ariel: "Do panóptico ao 'Big Brother' - por uma política pública para a privacidade de dados no Brasil", revista PoliTICs, Rio de Janeiro, 2009*, http://www.politics.org.br*

FTC Staff Report: *Self-Regulatory Principles For Online Behavioral Advertising,* Washington: FTC, 2009, *http://www.ftc.gov/opa/2009/02/behavad.shtm*

Gilbert, Daphne; Kerr, Ian e McGill, Jena: "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers", Ottawa, 2008. *Criminal Law Quarterly* 469-507, em *http://ssrn.com/abstract=1302544*

Gindre, Gustavo: *Agenda Regulatória: uma proposta para o debate,* Rio de Janeiro, 2008.

Goldsmith, Jack L., e Wu, Tim: *Who Controls the Internet? Illusions of a Borderless World,* Oxford University Press, New York, 2006.

IBDI - Instituto Brasileiro de Direito da Informática. *Lista de Discussões do IBDI - Direito, Informação e Tecnologias, http://www.ibdi.org.br*

Kuneva, Meglena: *Roundtable: Keynote Speech at Brussels* (2009), em: *http://epic.org/redirect/ 041309_ECCA_Meglena_Roundtable.html.*

Leonardi, Marcel: *Responsabilidade Civil dos Provedores de Serviços de Internet,* Juarez de Oliveira, São Paulo, 2005.

Matos, Tiago F.: "Comércio de dados pessoais, privacidade e Internet", *Jus Navegandi,* São Paulo, 2003. *http://jus2.uol.com.br/doutrina/texto.asp?id=5667*

OHM, Paul: "The Rise and Fall of Invasive ISP Surveillance", *University of Illinois Law Review,* 2009, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261344*

RED Iberoamericana de Protección de Datos. "Directrices para la Armonización de la Protección de Datos em la Comunidad Iberoamericana" (2007). *https://www.agpd.es/portalweb/internacional/relaciones_iberoamerica/seminario_cartagena/common/pdfs/Documento_de_Directrices_de_armoni zacion_final.pdf*

RNP, "A Internet no Brasil", Revista ComCiência, Rio de Janeiro, 2001. *http://www.rnp.br/noticias/imprensa/2001/not-imp-010310.html*

Rust, Roland, Kannan, P., Peng, Na: *The Customer Economics of Internet Privacy,* vol. 30, nº 4, Academy of Marketing Science Journal, Londres, pp. 455-64.

Selaimen, Graciela: *Discurso na abertura do IGF 2008, na Índia.* Publicado em *http://lac.derechos.apc.org/es.shtml?apc=he_1&x=5539240*

Solove, Daniel: *The digital person,* Nova Iorque, New York University Press, 2004.

Zarsky, Tal: "Online Privacy, Tailoring, and Persuasion", em *Privacy and Technologies of Identity - A Cross_Disciplinary Conversation,* Strandburg, Katherina, y Stan Raicu, Daniela (eds.), Chapter 12, pp. 209-224, Springer, 2006, em *http://ssrn.com/abstract=946428*

Zittrain, Jonathan: "Internet Points of Control", *Boston College Law Review,* Boston, *http://ssrn.com/abstract_id=388860*