> A INTERNET PERDEU
um de seus sonhadores

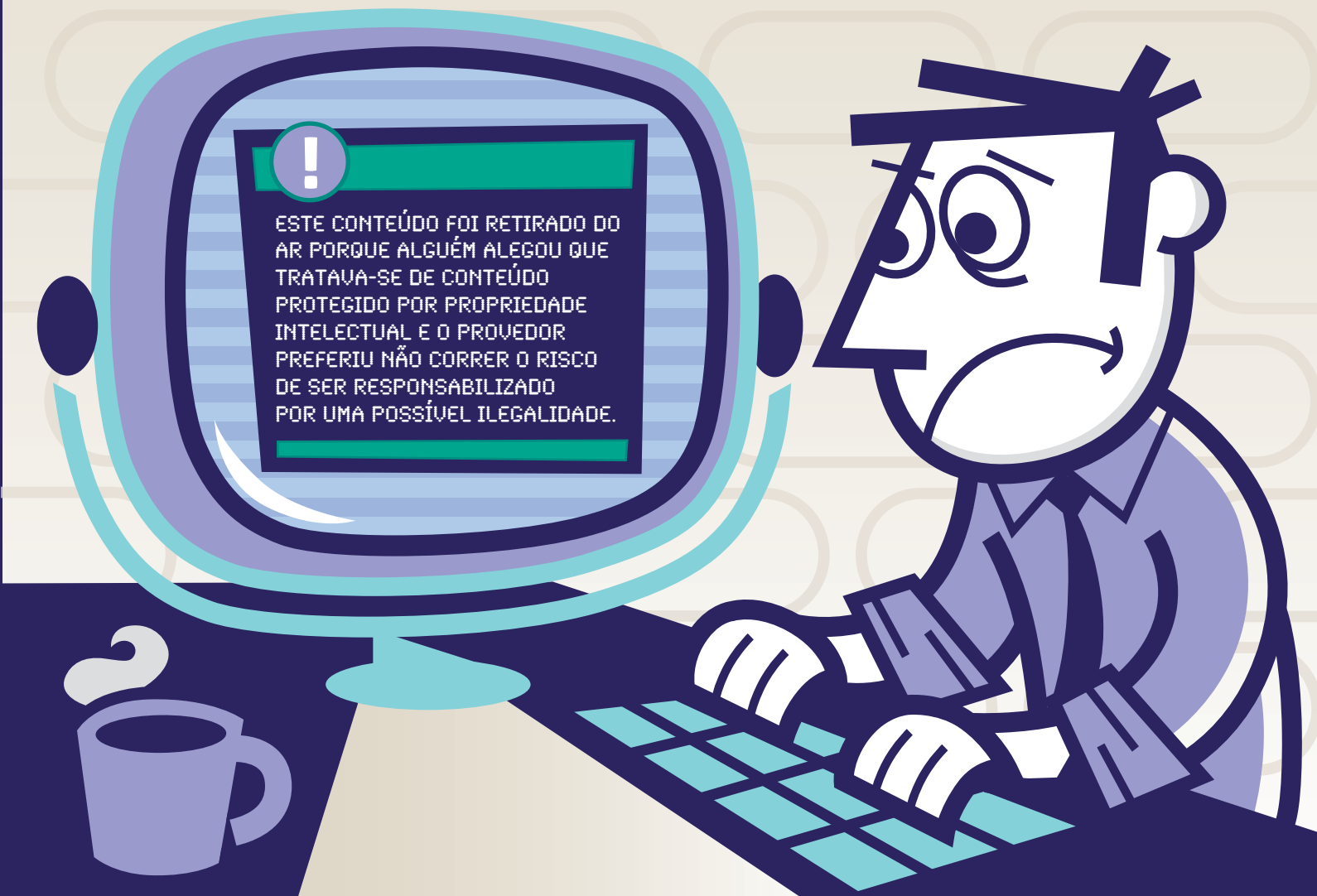
> SEGMENTAÇÃO COMPORTAMENTAL
e a lei holandesa

> DPI: ALGUÉM OBSERVA
quando você está on-line

poliTICs

Uma publicação do Instituto Nupef • fevereiro / 2013 • www.politics.org.br

Internet do futuro?



poliTICs nº 14

Índice

poliTICs

COORDENAÇÃO DO PROJETO GRACIELA SELAIMEN

EDITORES GRACIELA SELAIMEN, CARLOS A. AFONSO

CAPA, PROJETO GRÁFICO E DIAGRAMAÇÃO MONTE DESIGN

DISTRIBUIÇÃO VIVIANE GOMES

TRADUÇÕES RICARDO SILVEIRA

Esta é uma publicação do Instituto Nupef.

Versão digitalizada disponível em www.politics.org.br e no sítio do Nupef - www.nupef.org.br

Para enviar sugestões, críticas ou outros comentários: graciela@nupef.org.br

instituto nupef

Rua Sorocaba, 219 | 501 - parte | Botafogo | 22271-110

Rio de Janeiro RJ Brasil | telefone +55 21 2527-0294

Apoio:

FORD FOUNDATION

Strengthen democratic values, reduce poverty and injustice, promote international cooperation and advance human achievement

Google

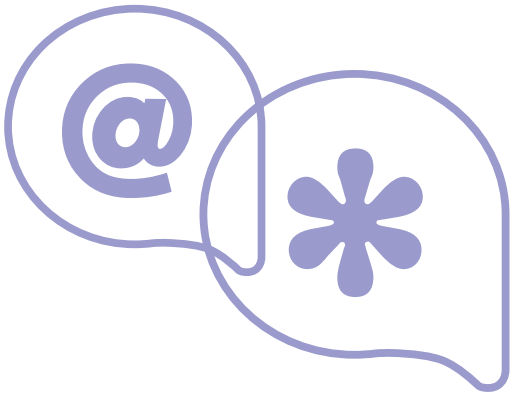
nic.br

Núcleo de Informação e Coordenação do Ponto BR

Os originais foram compostos com OpenOffice 3.X e GNU/Linux

ISSN: 1984-8803

A poliTICs procura aderir à terminologia e abreviaturas do Sistema Internacional de Unidades (SI), adotado pelo Instituto Nacional de Metrologia do Brasil (Inmetro). Assim, todos os textos são revisados para assegurar, na medida do possível e sem prejuizo ao conteúdo, aderência ao SI. Para mais informação: http://www.inmetro.gov.br/consumidor/unidLegaisMed.asp



Editorial

Esta edição da poliTICs traz visões, casos concretos e principalmente chamamentos importantes à reflexão sobre episódios recentes e processos atuais que impactam a vida de todas as pessoas. No rescaldo da Conferência Mundial sobre Telecomunicações Internacionais (a CMTI ou WCIT, na sigla em inglês, ocorrida em dezembro de 2012) e do evento que ocorreu às vésperas desta Conferência, no qual foram aprovados padrões internacionais para uso de DPI - tecnologia de inspeção profunda de pacotes -, é importante entender como esta tecnologia está sendo usada para inspecionar conteúdos que trafegam pela rede. Neste sentido, o artigo de Heesob Nam, ativista de defesa de direitos de usuários de TICs, é oportuno: mostra como as operadoras de telecomunicações da Coreia do Sul interferem no uso da Internet de seus clientes, utilizando a tecnologia DPI.

Monitoramento e vigilância também são tema do texto do pesquisador holandês Frederik Borgesius – mas, neste caso, a história a ser contada é de avanço na defesa de direitos: Frederik escreve sobre a recém-aprovada Lei Holandesa das Telecomunicações, que inova ao regular o uso de cookies para segmentação comportamental.

Um outro olhar importante sobre a CMTI/WCIT é oferecido por Jeferson Nacif, que acompanhou as negociações na Conferência como membro da delegação do governo brasileiro. Jeferson apresenta uma análise sobre o jogo político na CMTI/WCIT contextualizando-o principalmente sob a ótica da política externa brasileira na área de telecomunicações.

Pablo Ortellado escreve sobre um dos "nós" que travam o processo de aprovação do Marco Civil – as previsões de regulação para a retirada de conteúdos online que são alvo de disputas por questões de direito autoral. Ortellado explica como os mecanismos de retirada de conteúdos, conforme estão previstos no atual texto do Marco Civil, podem significar censura privada.

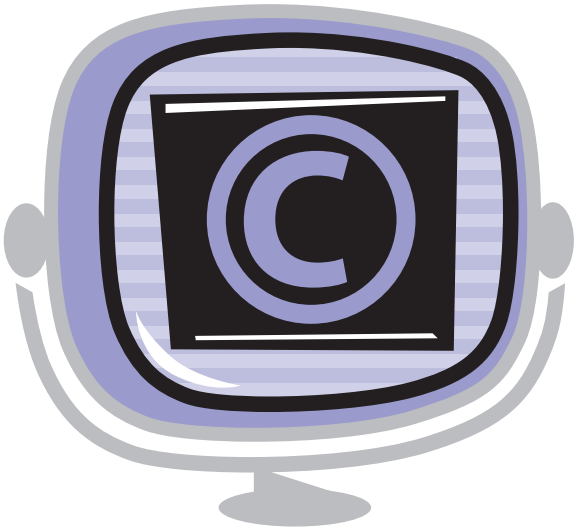
Não são apenas textos de leis progressistas que perecem sob a mão pesada dos detentores de direitos autorais. O artigo de Magaly Pazello – em memória de Aaron Schwarz, que cometeu suicídio em janeiro pressionado pela perseguição do governo dos EUA – ilustra o quão dramáticos podem ser os efeitos destas forças empenhadas a cercear e castigar, em nome da proteção de presumidas propriedades. ●

▶ Esperamos que você aprecie a leitura, participe e opine – o espaço está aberto em **www.politics.org.br**

Um abraço,

Graciela Selaimen – *Editora da poliTICs*

> **Pablo Ortellado** coordenador do Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (GPoPAI) da Universidade de São Paulo



Como regular a retirada de conteúdos reproduzidos sem autorização?

Considerações sobre o mecanismo de notificação e retirada

O Marco Civil da Internet, que deveria ter sido aprovado pela Câmara dos Deputados em dezembro, em conjunto com as leis de cibercrimes, terminou não sendo votado em 2012. O motivo foi uma forte pressão da indústria, que tentou alterar dispositivos relativos à guarda de registros e à melhor forma de regular a retirada de conteúdos que são alvos de disputas (principalmente reproduções não autorizadas de obras protegidas por direito autoral).

Embora pareça provável que a guarda de registros ficará do jeito que está no texto do projeto de lei (guarda de registros de conexão por 6 meses e guarda de registros optativa para provedores de serviço), os mecanismos de regulação da retirada de conteúdos pode sofrer uma revisão importante.

Basicamente, dois modelos estão sendo debatidos, opondo usuários a empresas. De um lado, empresas de conteúdo (como a Rede Globo) defendem o modelo americano do *notice and takedown* – ou notificação e retirada. De outro, ativistas e organizações preocupadas com os direitos dos usuários defendem um modelo de retirada mediante autorização judicial. Face às pressões, o relator do projeto na Câmara optou por empurrar a decisão para a reforma da Lei de Direito Autoral, o que pode significar a vitória da indústria.

Notificação e retirada é uma tradução da expressão *notice and takedown*, que é o nome dado ao mecanismo introduzido nos Estados Unidos por meio do *Digital Millennium Copyright Act* (DMCA) de 1998. O mecanismo busca regular as atividades das empresas provedoras de serviços Internet cujo conteúdo é inserido pelo usuário. Quando uma publicação por meio destas plataformas viola direitos autorais há incerteza sobre quem deve ser responsabilizado pela violação – se o prestador do serviço que oferece a plataforma, se o usuário que adiciona o conteúdo, ou ambos. O DMCA introduziu o conceito de notificação e retirada determinando responsabilidades por meio do seguinte procedimento:

1) o alegado titular dos direitos autorais, quando identifica uma suposta violação aos seus direitos, notifica o provedor de serviços;

2) o provedor tem duas opções: ou retira o conteúdo com a suposta violação (de maneira "expedita" – o que se entende como "em até 24 horas") ou mantém o conteúdo e assume responsabilidade por ele;

3) ao retirar o conteúdo, o provedor deve notificar o usuário (se for possível fazê-lo) que, por sua vez, pode contranotificar, assumindo ele (usuário) a responsabilidade pela publicação;

4) o conteúdo, neste último caso, é posto de volta no sítio Web se o titular do direito autoral não iniciar um processo contra o usuário em dez dias úteis.

Tudo ocorre na esfera extrajudicial, sem qualquer decisão da Justiça. Desta maneira, o DMCA buscou dar segurança jurídica aos serviços de Internet que se baseiam em conteúdos de usuários, ao mesmo tempo que fornece aos titulares de direito autoral um instrumento para impedir violações.

Embora em tese o mecanismo de notificação e retirada busque equilibrar o interesse dos titulares de direito autoral com o interesse dos provedores de serviço e dos usuários, na prática o mecanismo tem sido sistematicamente abusado pelos titulares.

A crítica consiste no fato de que o mecanismo de notificação e retirada cria, na prática, uma censura privada. No modelo americano, o detentor dos direitos autorais, ao notificar, faz simplesmente uma alegação de violação, na esfera extrajudicial, sem a verificação de um juiz. Os titulares tendem a interpretar a lei de maneira restritiva, minimizando, por exemplo, as possibilidades de usos livres conferidas pelas exceções e limitações dos direitos autorais (ou do *fair use*, no caso americano).

Assim, segundo estimativa da rede americana de clínicas de Direito Chilling Effects, (formada por clínicas das universidades de Harvard, Stanford, George Washington, entre outras) cerca de 60% das alegações de violação utilizando o *notice and takedown* são improcedentes, seja porque simplesmente não há violação (são usos cobertos pelo *fair use*), ou porque a violação não é de direito autoral (é de marca), ou porque os procedimentos formais não foram realizados de maneira adequada.

Apesar disso, os titulares conseguem atingir o objetivo de suprimir o conteúdo - já que os provedores de serviços Internet preferem retirar o conteúdo e notificar o usuário a enfrentar o ônus legal de mantê-lo.

Embora o Brasil ainda não tenha formalmente este mecanismo, já enfrentamos notificações extrajudiciais em massa, que servem como teste de ensaio para a sua introdução formal. A Associação Brasileira de Direito Reprográfico (ABDR), por exemplo, faz milhares de notificações extrajudiciais a provedores de serviço Internet (cerca de dez mil por mês) solicitando a retirada de links para downloads de livros. São notificações que alegam que determinada obra do catálogo de uma editora filiada está sendo publicada on-line sem autorização - e que se não houver ações para retirar a publicação da Internet, medidas judiciais serão tomadas em face dos provedores. Os provedores então, para não assumir o ônus judicial, quase sempre retiram o conteúdo (ao ponto de a ABDR utilizar a retirada de conteúdo como indicador de sucesso do seu trabalho).

É muito provável que um número significativo dessas retiradas feitas sem decisão judicial sejam improcedentes, seja pelo fato de a editora filiada à ABDR não ter mais os direitos da obra (porque o contrato com o autor expirou), seja porque a publicação on-line da obra pode estar coberta por exceções e limitações aos direitos autorais, sobretudo após a recente decisão do Superior Tribunal de Justiça (STJ) que indicou que as limitações na atual lei são exemplificativas, ou seja, nem todas as limitações estão expressamente previstas na lei.

A alternativa ao mecanismo de notificação e retirada que é defendida por usuários e ativistas é a proposta que saiu dos debates do Marco Civil. A proposta determinava a retirada de conteúdos sob disputa apenas por via judicial, ou seja, os provedores de serviço não seriam responsáveis por conteúdos gerados por usuários, a não ser que uma ordem judicial de retirada de conteúdo específico deixasse de ser cumprida. A redação era a seguinte:

Art. 14 - O provedor de conexão à Internet não será responsabilizado por danos decorrentes de conteúdo gerado por terceiros.

Art. 15 - Salvo disposição legal em contrário, o provedor de aplicações de Internet somente poderá ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente.

Parágrafo único - A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

A redação original do Marco Civil da Internet oferecia duas garantias importantes. A primeira, era a garantia de que os provedores não fossem considerados responsáveis pelos conteúdos publicados por terceiros, o que retirava qualquer estímulo para que as empresas censurassem preventivamente seus usuários. A segunda, era a garantia de que a retirada de conteúdos só aconteceria mediante ordem de um juiz que, ao fazê-lo, deveria levar em conta se o solicitante é de fato o titular do conteúdo supostamente infringente e se a queixa dele efetivamente procedia. Isso garantiria que solicitações abusivas de retirada de conteúdo não seriam recorrentes.

No entanto, no fogo cruzado que opôs usuários e empresas de direito autoral, o relator do projeto na Câmara terminou com uma redação esquiva, que empurrava para a lei de direito autoral o mecanismo de retirada de conteúdos infringentes. A redação que propôs é a seguinte:

Art. 15 - Com o intuito de assegurar a liberdade de expressão e evitar a censura, o provedor de aplicações de Internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

> A crítica consiste no fato de que o mecanismo de notificação e retirada cria, na prática, uma censura privada.

§ 1º - A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º - O disposto neste artigo não se aplica quando se tratar de infração a direitos de autor ou a direitos conexos.

Aparentemente, o artigo 15 oferece uma solução mediada pelo judiciário como querem os usuários. Mas o parágrafo segundo diz que isso não se aplica a direito autoral, justamente o caso mais importante. Como só há basicamente esses dois modelos, o de notificação e retirada (com algumas variantes, como

> É muito provável que um número significativo dessas retiradas feitas sem decisão judicial sejam improcedentes

o modelo canadense de notificação e notificação) e o de decisão judicial, a exclusão do direito autoral indica que para os casos de disputas envolvendo direito autoral, o abusivo modelo de notificação e retirada prevalecerá.

A suspeita é reforçada pela inclusão feita no anteprojeto de reforma da lei de direito autoral, durante a gestão de Ana de Hollanda, de um dispositivo de notificação e retirada. Esse dispositivo, muito parecido com o americano, estabelece o seguinte procedimento: o titular do direito autoral notifica o provedor de serviço; o provedor de serviço retira o conteúdo; o usuário é avisado que o seu conteúdo foi retirado; se discorda da exclusão, o usuário pode contranotificar, assumindo a responsabilidade do conteúdo e restabelecendo o conteúdo suprimido. Veja abaixo a redação proposta:

Art. 105-A - Os provedores de aplicações de Internet poderão ser responsabilizados solidariamente, nos termos do art. 105, por danos decorrentes da colocação à disposição do público de obras e fonogramas por terceiros, sem autorização de seus titulares, se notificados pelo titular ofendido ou mandatário e não tomarem as providências para, no âmbito do seu serviço e dentro de prazo razoável, tornar indisponível o conteúdo apontado como infringente.

§ 1º - Os provedores de aplicações de Internet devem oferecer de forma ostensiva ao menos um canal eletrônico dedicado ao recebimento de notificações e contranotificações, sendo facultada a criação de mecanismo automatizado para atender aos procedimentos dispostos nesta Seção.

§ 2º - A notificação de que trata o caput deste artigo deverá conter, sob pena de invalidade:

I – identificação do notificante, incluindo seu nome completo, seus números de registro civil e fiscal e dados atuais para contato;

II – data e hora de envio;

III – identificação clara e específica do conteúdo

apontado como infringente, que permita a localização inequívoca do material pelo notificado;

IV – descrição da relação entre o notificante e o conteúdo apontado como infringente; e

V – justificativa jurídica para a remoção.

§ 3º - Ao tornar indisponível o acesso ao conteúdo, caberá aos provedores de aplicações de Internet informar o fato ao responsável pela colocação à disposição do público, comunicando-lhe o teor da notificação de remoção e fixando prazo razoável para a eliminação definitiva do conteúdo infringente.

§ 4º - Caso o responsável pelo conteúdo infringente não seja identificável ou não possa ser localizado, e desde que presentes os requisitos de validade da notificação, cabe aos provedores de aplicações de Internet manter o bloqueio.

§ 5º - É facultado ao responsável pela colocação à disposição do público, observados os requisitos do § 2o, contranotificar os provedores de aplicações de Internet, requerendo a manutenção do conteúdo e assumindo a responsabilidade exclusiva pelos eventuais danos causados a terceiros, caso em que caberá aos provedores de aplicações de Internet o dever de restabelecer o acesso ao conteúdo indisponibilizado e informar ao notificante o restabelecimento.

§ 6º - Qualquer outra pessoa interessada, física ou jurídica, observados os requisitos do § 2o, poderá contranotificar os provedores de aplicações de Internet, assumindo a responsabilidade pela manutenção do conteúdo.

§ 7º - Tanto o notificante quanto o contranotificante respondem, nos termos da lei, por informações falsas, errôneas e pelo abuso ou má-fé.

§ 8º - Os usuários que detenham poderes de moderação sobre o conteúdo de terceiros se equiparam aos provedores de aplicações de Internet para efeitos do disposto neste artigo.

O mecanismo de notificação e retirada proposto pelo Ministério da Cultura tem algumas melhorias em relação ao modelo americano: a solicitação tem que ser formalmente embasada e o restabelecimento de conteúdo fruto de contranotificação é imediato. No entanto, o mecanismo segue sendo privado, sem nenhuma autorização ou supervisão judicial. Além disso, como o procedimento é simples e sem ônus econômico, as empresas titulares de direito autoral são estimuladas a fazer notificações vazias ou mal embasadas; em contrapartida, os provedores de serviço são estimulados a aceitar todas as notificações, já que o ônus de não as aceitarem é a responsabilização civil ou criminal. O resultado será o mesmo que nos Estados Unidos: solicitações improcedentes em massa sendo acatadas, gerando censura privada de discursos protegidos pela lei. ●

> **Frederik Zuiderveen Borgesius** pesquisador do Instituto para o Direito da Informação (IViR), Universidade de Amsterdã

Segmentação Comportamental,

Do Not Track e o desenvolvimento jurídico europeu e holandês

A segmentação comportamental (*behavioral targeting*) é o monitoramento que se faz do comportamento das pessoas na Internet ao longo do tempo, para usar as informações recolhidas com o intuito de dirigir-lhes publicidade conforme as inferências a respeito de seus interesses. Este tipo de negócio cresceu a ponto de tornar-se um mercado que movimenta milhões e milhões de dólares. Há empresas que reúnem os perfis de centenas de milhões de usuários da Internet. As entidades reguladoras do mundo inteiro se debatem quanto a regular, ou deixar de regular, e como agir com relação à segmentação comportamental.

No dia 01 de janeiro de 2013, a versão final da Lei Holandesa das Telecomunicações entrou em vigor. Ela implementa a "cláusula dos cookies" a partir das emendas realizadas em cima da Diretiva "Privacidade e Comunicações Eletrônicas"[1]. O dispositivo holandês só permite o armazenamento e a leitura de cookies

1. Diretiva 2002/58/EC de 12 de julho de 2002 relativa ao processamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (Diretiva sobre privacidade e comunicações eletrônicas) (Diário Oficial L 201, 31/07/2002 P. 0037 – 0047), conforme emendas dadas pela Diretiva 2006/24/EC [a Diretiva sobre Retenção de Dados], e a Diretiva 2009/136/EC [a Diretiva dos Direitos do Cidadão]. Este artigo usa o texto consolidado da Diretiva "Privacidade e Comunicações Eletrônicas".

quando o usuário, uma vez informado, dá o seu consentimento. As empresas não podem inferir que houve consentimento a partir das configurações padrão de um navegador. Para facilitar a leitura, neste artigo falamos de cookies, mas o dispositivo holandês não se aplica só a eles, como também a outras tecnologias, tais como os leitores biométricos.[2]

A legislatura holandesa também deu um passo inédito, introduzindo uma premissa jurídica sobre o rastreamento de cookies para segmentação comportamental. Presume-se que esse uso dos cookies desencadeie o processamento de dados pessoais, onde se aplica plenamente, portanto, a lei da proteção de dados pessoais.

:: OS COOKIES E A SEGMENTAÇÃO COMPORTAMENTAL

A segmentação comportamental é o monitoramento que se faz do comportamento das pessoas na Internet ao longo do tempo para usar as informações recolhidas com o intuito de dirigir-lhes publicidade conforme as inferências a respeito de seus interesses. Num exemplo simplificado, uma empresa pode assumir que um usuário da Internet que costuma visitar sítios sobre receitas de cozinha seja um entusiasta da gastronomia. Quando visitar um sítio de notícias, esse usuário poderá se deparar com anúncios de restaurantes ou livros de receitas. Ao visitar o mesmo sítio de notícias, alguém que leia muitos blogs de assuntos jurídicos pode se deparar com anúncios de livros de direito.

A segmentação comportamental pode beneficiar empresas e consumidores, mas também traz à baila preocupações acerca da privacidade. As empresas podem compilar perfis detalhados dos usuários da Internet com base no que eles lêem, que vídeos assistem, que buscas fazem etc.

Para realizar a segmentação comportamental, diversas tecnologias podem ser usadas – entre elas, os cookies, utilizados por muitas empresas.

O cookie é um pequeno arquivo de texto que um editor de sítios na Internet armazena no computador ou no smartphone de um usuário para reconhecer aquele dispositivo. Esses editores usam cookies para, por exemplo, lembrar o conteúdo de um carrinho de compras ("cookies de usuário" ou "*first party cookies*"). Normalmente, esses cookies são relativos à "sessão", pois desaparecem depois que o usuário fecha o navegador. As empresas que atuam na segmentação comportamental costumam usar cookies persistentes para reconhecer os usuários em momentos futuros. Aquelas que publicam anúncios num sítio, como as redes de propaganda, podem colocar e ler também esses cookies persistentes ("cookies de terceiros" ou "*third party cookies*"). Resulta daí que uma rede de propaganda pode acompanhar o comportamento de um usuário da Internet em todos os sítios nos quais ela publica anúncios. Este artigo se refere a cookies que são usados para segmentação comportamental, como cookies de rastreamento.

2. O texto original em holandês pode ser encontrado em: http://wetten.overheid.nl/BWBR0009950.

:: A DISCUSSÃO EUROPEIA SOBRE A REGULAÇÃO DE COOKIES

Esta seção faz um apanhado geral da discussão europeia sobre a regulação de cookies, concentrando-se na Diretiva "Privacidade e Comunicações Eletrônicas". Essa lei da União Europeia de 2002 trata da proteção da privacidade no setor das comunicações eletrônicas. O Artigo 5.3 regula o uso de cookies, escutas web (*web bugs*), identificadores ocultos e outras tecnologias semelhantes[3]. As primeiras propostas para a versão de 2002 do Artigo 5.3 exigiam que as empresas pedissem consentimento antes de colocar em ação certos tipos de cookie. Depois do lobby feito junto à indústria de marketing on-line, a versão final do Artigo 5.3 usou palavreado ambíguo sobre um "direito à recusa"[4]. Costuma-se interpretar a versão de 2002 do Artigo 5.3 como uma exigência que as empresas ofereçam às pessoas a possibilidade de se opor ao uso de cookies (um sistema de escolhas livres). A versão de 2002 não deixava de exigir que as empresas informassem aos usuários qual era o uso dos cookies.

Em 2009, a Diretiva "Direitos dos Cidadãos"[5] fez emendas à Diretiva "Privacidade e Comunicações Eletrônicas". O novo Artigo 5.3 só permite o armazenamento e a leitura de cookies depois que o usuário, informado, dá o seu consentimento (note-se que certos cookies estão isentos da exigência do consentimento[6]). Em suma, o Artigo 5.3 requer um consentimento prévio por parte do usuário. Entretanto, uma frase do considerando 66 da Diretiva "Direitos do Cidadão" gerou muita confusão e discussão:

> *Onde for tecnicamente possível e eficaz, conforme os dispositivos pertinentes [da Diretiva "Proteção de Dados Pessoais"], o consentimento do usuário para o procedimento pode ser expresso através das configurações apropriadas de um navegador ou de outro aplicativo.*

A maior parte dos navegadores oferece ao usuário a possibilidade de bloquear os cookies de usuário, os cookies de terceiros, ou todos os cookies. Algumas pessoas concluem que, a partir do considerando 66, as configurações padrão do navegador podem expressar consentimento. Outras dizem que é possível inferir o consentimento para instalação de cookies a partir das configurações do navegador. Essa divergência de opiniões causou muitos debates na Europa.

3. Ver considerandos 24 e 25 da Diretiva "Privacidade e Comunicações Eletrônicas", e os considerandos 65 e 66 da Diretiva "Direitos do Cidadão" 2009/136.
4. S.M. Kierkegaard, 'Lobbyism and the 'opt in'/'opt out' cookie controversy. How the cookies (almost) crumbled: privacy & lobbyism' (2010) Computer Law & Security Report 2005-21, p. 310-322. 5. Diretiva 2009/136 de 25 de novembro de 2009. 6. O Artigo 5.3 da versão final da Diretiva "Privacidade e Comunicações Eletrônicas" diz: "Os EstadosMembros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Diretiva 95/46/CE [Data Protection Directive], nomeadamente sobre os objetivos do processamento. Tal não impede o armazenamento técnico ou o acesso que tenha como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrônicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador."

:: ARGUMENTOS CONTRA O USO DAS CONFIGURAÇÕES DOS NAVEGADORES ATUAIS COMO UM MECANISMO DE CONSENTIMENTO

Alguns argumentos foram apresentados para que sejam rejeitadas as configurações do navegador como mecanismo de consentimento. O considerando 66 da Diretiva "Direitos do Cidadão" diz que, de fato, "o consentimento do usuário, que autoriza o processamento, pode ser expresso usando-se as configurações apropriadas de um navegador ou de outro aplicativo." Mas o considerando acrescenta que o consentimento precisa ser dado "em conformidade com os dispositivos pertinentes da [Diretiva "Proteção de Dados Pessoais"]". A palavra "consentimento" está definida na Diretiva "Proteção de Dados Pessoais"[7]. O consentimento deve ser (i) informado, (ii) específico, (iii) dado de livre e espontânea vontade, e (iv) a indicação do desejo de uma pessoa. Essas quatro exigências fornecem argumentos contra o uso das configurações de um navegador como mecanismo de consentimento, conforme explica-se abaixo.

Primeiro, o consentimento deve ser informado. As informações relevantes não devem ficar ocultas do usuário numa política de privacidade. Se os usuários aceitam grandes quantidades de cookies simplesmente porque não mudam as configurações de seu navegador, esse fato não pode ser considerado um consentimento informado.

Segundo, o consentimento precisa ser específico. Por exemplo, o consentimento para que dados pessoais sejam usados com propósitos comerciais não deve ser aceito. Alguns navegadores aceitam todos os cookies como padrão, inclusive os de rastreamento. Se um navegador aceita todos os cookies de usuário ou todos os cookies de terceiros, a escolha do usuário não é específica.

Terceiro, é preciso que as pessoas expressem sua vontade de dar consentimento. A não-ação do usuário dificilmente poderá ser considerada um consentimento. Além disso, as pessoas precisam ter ciência de que estão expressando uma vontade. Em princípio, a expressão de uma vontade pode ser dada de qualquer forma, e também pode ser dada de maneira implícita. Mas é improvável que todas as pessoas que *deixam* de ajustar seus navegadores com esse propósito estejam dando consentimento para todas as formas de cookies. O Tribunal de Justiça da União Europeia confirma que chegar à conclusão de que houve o consentimento não é algo trivial[8]. Portanto, as configurações de um navegador provavelmente não poderão atender às exigências de consentimento explicitadas na Diretiva "Proteção de Dados Pessoais".

Quarto, o consentimento deve ser dado de livre e espontânea vontade; portanto, o consentimento dado sob pressão não é válido. Se o usuário ajusta seu navegador para rejeitar todos os cookies, não conseguirá usar muitos dos serviços da Internet.

7. Artigo 2(h) da Diretiva de Proteção de Dados (Diretiva 95/46/EC de 24 de outubro de 1995). O considerando 17 da Diretiva "Privacidade e Comunicações Eletrônicas" se refere à Diretiva de Proteção de Dados para a definição do consentimento. 8. ECJ: Case C-92/09 and C-93/09 *Volker und Markus Schecke GbR* [2010], para 63. ECJ: Case C112/11, ebookers.com [2012].

Entretanto, se o navegador for configurado para aceitar os cookies de usuário, também aceitará cookies de rastreamento. Além disso, algumas empresas levam os navegadores que aceitam cookies de usuário a aceitar também os cookies de rastreamento[9]. Em suma, não dá para ter certeza se os usuários realmente têm a liberdade de configurar seus navegadores para rejeitar todos os cookies.[10]

É importante ressaltar que o Tribunal de Justiça da União Europeia diz que a Diretiva "Privacidade e Comunicações Eletrônicas" deve ser interpretada juntamente com os direitos fundamentais.[11] A Diretiva "Privacidade e Comunicações Eletrônicas" visa proteger o direito à privacidade, o direito à proteção dos dados pessoais e a confidencialidade das comunicações. Todos esses direitos estão incluídos na Carta dos Direitos Fundamentais da União Europeia. O considerando 24 do preâmbulo da Diretiva "Privacidade e Comunicações Eletrônicas" diz que os aparelhos dos usuários "fazem parte da esfera privada de usuários, que requerem proteção conforme a Convenção Europeia para a Proteção dos Direitos Humanos e as Liberdades Fundamentais." O Tribunal Europeu dos Direitos Humanos interpreta o direito ao amplo respeito pela vida privada. Além disso, a Carta e outros Tratados da União Europeia enfatizam a importância de garantir-se um elevado nível de proteção ao consumidor[12]. Em suma, as leis na União Europeia requerem uma interpretação da Diretiva "Privacidade e Comunicações Eletrônicas" pela ótica da privacidade.

Por outro lado, a proteção de dados pessoais e o direito à privacidade não são absolutos. Os Estados-membros devem atingir um equilíbrio justo entre os direitos fundamentais ao aplicar as diretivas. As empresas que empregam cookies também poderiam invocar um direito fundamental da Carta: "a liberdade de tocar uma empresa em conformidade com o direito da União e as leis e práticas nacionais" [13]- embora seja pouco plausível que a liberdade de tocar uma empresa implique no direito de armazenar cookies nos aparelhos das pessoas sem o consentimento adequado. Em suma, aceitar as configurações padrão do navegador como consentimento para o uso de cookies é um tanto difícil de conciliar com a lei na União Europeia.

:: ARGUMENTOS A FAVOR DO USO DAS CONFIGURAÇÕES DOS NAVEGADORES ATUAIS COMO UM MECANISMO DE CONSENTIMENTO

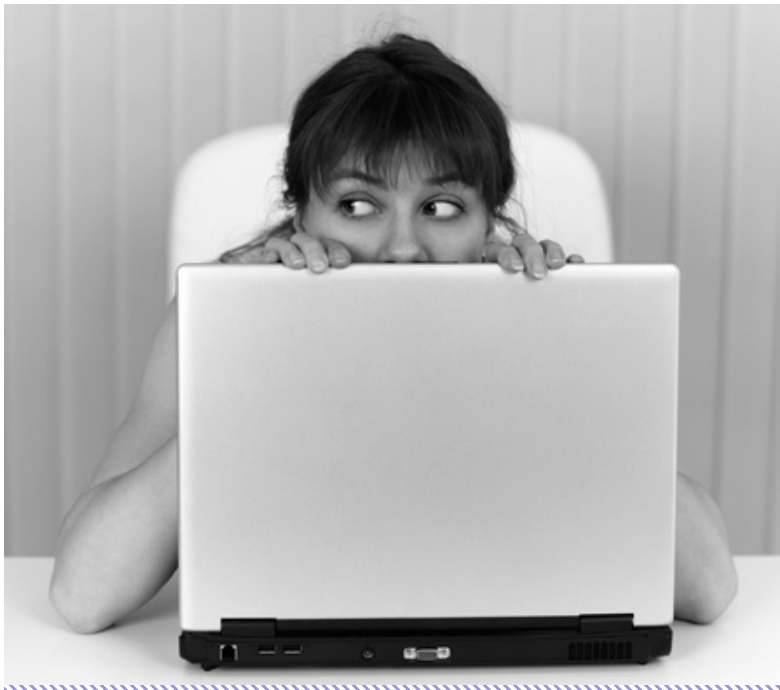
Há quem seja a favor do uso das configurações padrão dos navegadores como um mecanismo de consentimento. Os argumentos podem ser

9. J. Mayer, Safari Trackers (Web Policy, 17 de fevereiro de 2012), http://webpolicy.org/2012/02/17/safari-trackers; B. Krishnamurthy & C. Wills, 'Privacy diffusion on the web: a longitudinal perspective' (2009) WWW '09: Proceedings of the 18th international conference on World wide web, ACM, 2009, p. 544.
10. Grupo de Trabalho do Artigo 29, 'Opinião 2/2010 sobre publicidade baseada em segmentação comportamental' (WP 171, 22 June 2010); Grupo de Trabalho do Artigo 29, 'Opinião 15/2011 sobre a definição de consentimento' (WP 187, 13 July 2011). O Grupo de Trabalho do Artigo 29 foi instituído pelo artigo 29.o da Diretiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de proteção dos dados e da privacidade. As suas atribuições estão descritas no artigo 30.o da Diretiva 95/46/CE e no artigo 15.o da Diretiva 2002/58/CE. 11. ECJ: Caso C-275/06, *Promusicae* [2008], par. 67-68, and dictum. Ver também o considerando 62 da Diretiva de Direitos dos Cidadãos 2009/136. 12. Ver artigos 38 e 51(1) da Carta dos Direitos Fundamentais da União Europeia, e artigos 12, 114(3) e 169 do Tratado sobre o Funcionamento da União Europeia. 13. Artigo 16 da Carta de Direitos Fundamentais da União Europeia.

resumidos assim: primeiro, as pessoas que não mudam as configurações de seus navegadores consentem implicitamente com o armazenamento de cookies em seus computadores. O *Interactive Advertising Bureau* do Reino Unido diz, por exemplo: "Acreditamos que as configurações padrão do navegador possam ser equivalentes a 'consentimento' conforme disposto em nosso considerando 66" (ênfase original).[14]

Segundo, há quem tema que os usuários da Internet sejam bombardeados com pop-ups pedindo consentimento se as configurações do navegador não forem suficientes para sinalizar consentimento. Assim, navegar pela Internet seria um pesadelo. Ficaria difícil conciliar isso com o considerando 66 da Diretiva "Direitos do Cidadão", que pede uma solução de fácil uso para o usuário: "Os métodos de fornecer informação e oferecer o direito a recusar devem ser o mais fácil possível para o usuário."

Terceiro, os pop-ups talvez não consigam passar a informação de maneira significativa para o usuário. Muitos são os que clicam em "Concordo" com qualquer declaração que lhes seja apresentada. Esta situação pode piorar se as pessoas começarem a ver mais pop-ups aparecendo em suas janelas. Portanto, a lei não seria eficaz no sentido de proteger a privacidade dos usuários. Há até quem argumente que os usuários podem clicar distraidamente num *spyware* ou num vírus se passarem a ter de aceitar muitos pop-ups. Por outro lado: se as configurações do navegador expressam consentimento, isso pode implicar, para terceiros, na premissa de que os usuários consentem com a instalação de *spyware* uma vez que seus navegadores não bloqueiam *spyware*.[15] Ainda assim, é preciso



Muitos são os que clicam em "Concordo" com qualquer declaração que lhes seja apresentada.

14. Interactive Advertising Bureau, Resposta da IAB UK à consulta do Department for Business, Innovation & Skills sobre a implementação da revisão do marco das comunicações eletrônicas na UE (IAB 1 de dezembro de 2010, www.iabuk.net/sites/default/files/IABUKresponsetoBISconsultationonimplementingthe-revisedEUElectronicCommunicationsFramework_7427_0.pdf), p. 2. 15. N.A.N.M. Van Eijk e outros, A bite too big: Dilemma's bij de implementatie van de Cookiewet in Nederland, TNO-report no. 35473. http://www.ivir.nl/publicaties/vaneijk/A_bite_too_big.pdf, p. 63.

verificar se os pop-ups vão conseguir informar direito os usuários.

Quarto, as pessoas podem acabar clicando em "não" para o rastreamento de cookies usados para fazer segmentação comportamental quando se depararem com um pedido de consentimento. Isso reduziria a receita oriunda de anúncios, e poderia acabar com a oferta gratuita de alguns serviços. Outro argumento pertinente é que uma regulamentação sobre cookies forte demais é ruim para a competitividade dos provedores de conteúdos europeus na Internet e outras empresas que utilizem cookies. Por exemplo, os sítios norte-americanos podem ignorar a regra da União Europeia.

Quinto, a lei não explica como as empresas devem obter o consentimento. Há quem diga que não está clara a maneira como as empresas devem cumprir a lei, se não quiserem usar os pop-ups. Isso seria prejudicial para a segurança jurídica.

Em suma, há argumentos para duvidar da razoabilidade da regra do consentimento para cookies na Diretiva "Privacidade e Comunicações Eletrônicas". Alguns desses argumentos são usados a favor da aceitação das configurações padrão do navegador como mecanismo de consentimento. É difícil avaliar o argumento de que o rastreamento dos cookies é necessário para a publicidade que financia os serviços de Internet, afinal também pode haver anúncios que não dependam do monitoramento do comportamento das pessoas na Internet. Além disso, é rara a pesquisa independente em torno da renda gerada a partir da segmentação comportamental [16]. E mais, não parece plausível que a importância da renda oriunda de publicidade venha a ditar a interpretação de uma diretiva.

O temor de que surja uma avalanche de pop-ups parece ser o argumento mais convincente em favor da aceitação das configurações dos navegadores atuais como um mecanismo de consentimento. Mas esse temor pode estar algo exagerado, pois certos tipos de cookies estão isentos da exigência de consentimento. É possível construir sítios Web sem cookies que precisem de consentimento. Além disso, os usuários da Internet só precisam dar consentimento para um cookie específico uma vez. Não obstante, ficar constantemente clicando em pop-ups para desativá-los não parece nada atraente.

:: DO NOT TRACK

O Tribunal de Justiça da União Europeia tem a palavra final sobre a interpretação que se deve dar à Diretiva "Privacidade e Comunicações Eletrônicas". Não obstante, a comissária Kroes já deu sua interpretação. Ela sugere que um sistema de *Do Not Track* possibilitaria às empresas o cumprimento da Diretiva "Privacidade e Comunicações Eletrônicas"[17]. Uma opção de *Do Not Track*[18] nos navegadores deveria permitir que os usuários sinalizassem que

16. J. R. Mayer & J. C. Mitchell, "Third-Party Web Tracking: Policy and Technology", IEEE Security & Privacy, novembro/dezembro de 2012.
17. Neelie Kroes é Vice-Presidente da Comissão Europeia responsável pela Agenda Digital. Ver "Online privacy – reinforcing trust and confidence", comunicado de imprensa divulgado durante o Online Tracking Protection & Browsers Workshop, em junho de 2011, Bruxelas (http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/461). 18. N.E.: Do Not Track é uma proposta tecnológica e política que permite ao usuário da Web optar por não aceitar o rastreamento feito por terceiras partes através de um cabeçalho no protocolo http que sinaliza sua opção. Ver em http://donottrack.us/

não querem ser rastreados a partir dos sítios que visitam na Internet.

O Consórcio World Wide Web é uma comunidade internacional onde as organizações membro cooperam para a elaboração de padrões na Internet. Desde novembro de 2011, um Grupo de Trabalho de Proteção contra o Rastreamento, formado por essa comunidade, está envolvido numa discussão sobre uma norma *Do Not Track*[19]. Basicamente, essa norma deverá permitir que as pessoas rejeitem o rastreamento.

Uma norma assim permitiria que as pessoas sinalizassem com seus navegadores que não querem ser rastreadas. Uma empresa que receba um sinal "Não me rastreiem" deve responder: "OK, não vou rastreá-lo". Mas se a empresa continuar rastreando o usuário depois de uma resposta assim, a lei deve ser acionada. Por exemplo, as autoridades responsáveis pela proteção ao consumidor devem poder interferir se uma empresa descumprir a promessa que fez ao responder "Não vou rastreá-lo".

Mas como um sistema *Do Not Track* poderia ajudar as empresas a cumprir a regra do consentimento do Artigo 5.3 da Diretiva "Privacidade e Comunicações Eletrônicas"? Talvez seja possível um acordo nos seguintes moldes: as empresas devem deixar de rastrear os usuários europeus da Internet que não configurarem uma preferência de *Do Not Track*. Se alguém sinalizar para uma empresa "Sim, pode me rastrear" depois de receber informações suficientes sobre o assunto, essa empresa poderá colocar um cookie de rastreamento. Portanto, na Europa, deixar de configurar uma preferência teria o mesmo efeito que configurar uma preferência por *Do Not Track*. Nos países onde a lei não exija consentimento, as empresas ficam livres para rastrear as pessoas que não determinarem essa preferência.

As propostas em favor de uma norma do tipo *Do Not Track* excluem o rastreamento dentro de um mesmo sítio. Portanto, a norma permitiria que empresas como a Amazon ou o Facebook analisem o comportamento das pessoas dentro de seu próprio sítio, mesmo que as pessoas acionem o sinal de *Do Not Track*. Por outro lado, a regra de consentimento da Diretiva "Privacidade e Comunicações Eletrônicas" também se aplica a cookies de rastreamento de usuário.

Um dos principais pontos de discórdia é se o *Do Not Track* significa "Bloqueio de Coleta" (não use tecnologias de rastreamento) ou simplesmente "Não use para segmentação de comportamento" (continue coletando dados mas pare de mostrar a publicidade direcionada). Outra discórdia é se devem ser respeitados os navegadores que utilizem *Do Not Track* como padrão. Algumas empresas de publicidade dizem que a adoção de *Do Not Track* como padrão pelo navegador pode ser ignorada pois ela não expressam a vontade do usuário. No momento em que escrevi estas linhas, o Grupo de Trabalho sobre a Proteção contra o Rastreamento não tinha chegado a um consenso ainda.

19. Ver a discussão na lista pública de e-mails do Grupo de Trabalho sobre Do Not Track do Consórcio World Wide Web: http://lists.w3.org/Archives/Public/public-tracking/.

Resumindo, a discussão jurídica sobre os cookies e a segmentação comportamental na Europa foi lançada em 2009 como emendas à Diretiva "Privacidade e Comunicações Eletrônicas". A discussão se concentra na maneira como as empresas devem obter o consentimento dos usuários da Internet para instalarem seus cookies. O principal ponto de discórdia é se os navegadores atuais são ajustados para indicar consentimento para o uso de cookies. Há argumentos contra e a favor da aceitação das configurações dos atuais navegadores como um mecanismo de consentimento. O debate ainda não terminou. Enquanto isso, está sendo discutido um sistema de *Do Not Track*, mas ainda não ficou clara a maneira como isso ajudaria as empresas a cumprir a Diretiva "Privacidade e Comunicações Eletrônicas".

:: ANÁLISE DA LEI HOLANDESA DE TELECOMUNICAÇÕES

Nos Países Baixos, a regra do consentimento para a Diretiva "Privacidade e Comunicações Eletrônicas" está implementada no Artigo 11.7a da Lei Holandesa de Telecomunicações. A regra geral determina que as empresas que querem armazenar ou rastrear um cookie no aparelho do usuário devem: (a) dar ao usuário informações claras e completas sobre o propósito daquele cookie, e (b) obter consentimento do usuário[20].

Ficam isentadas da exigência de consentimento duas categorias de cookies funcionais. Primeiro, não é necessário consentimento para cookies cujo único propósito seja o transporte de uma comunicação através de uma rede eletrônica de comunicações. Um exemplo seriam os cookies necessários para rotear a informação dentro da rede. Segundo, não é necessário consentimento para um cookie que seja estritamente necessário para a prestação de um serviço que o usuário tenha solicitado. Por exemplo, um cookie para um carrinho de compras digital.

O elemento mais marcante da implementação holandesa é uma premissa da lei sobre os cookies de rastreamento: presume-se que o uso desses cookies leve ao processamento de dados pessoais. Portanto, aplica-se a Lei Holandesa de Proteção de Dados Pessoais. Na maioria dos casos, isso significa que a empresa lançadora do cookie deva obter consentimento prévio do usuário sem existência de ambiguidades. O ônus da prova recai sobre as empresas que empreguem os cookies de rastreamento, no sentido de provarem que não processam dados pessoais.

Assim como o Artigo 5.3 da Diretiva "Privacidade e Comunicações Eletrônicas", o Artigo 11.7 da Lei Holandesa de Telecomunicações tem um escopo amplo. Ele se aplica a qualquer "armazenamento de informação" ou "acesso a informação já armazenada" no equipamento terminal de um usuário.

20. Para ver uma versão em inglês da provisão: F. Zuiderveen Borgesius, Behavioral Targeting: Legal Developments in Europe and the Netherlands, paper elaborado para o workshop Do Not Track do W3C, novembro de 2012, www.ivir.nl/publications/borgesius/Position_paper_W3C.pdf, p. 5.

Esse equipamento terminal do usuário inclui, por exemplo, computadores e smartphones. O dispositivo holandês se aplica a qualquer informação armazenada ou acessada no aparelho do usuário, como cookies, *spyware* e vírus. Por exemplo, os reguladores holandeses já aplicaram o antecessor do Artigo 11.7a a um *spyware*. O histórico legislativo mostra que o Artigo 11.7a também se aplica a identificadores biométricos e a acesso a informações num decodificador de TV digital para segmentação comportamental[21].

O parágrafo 2 enfatiza que as exigências de informação e consentimento também se aplicam quando alguém instala, por outros meios que não a Internet, software capaz de armazenar ou acessar informações no aparelho de um usuário através da Internet. Um exemplo disso seria uma empresa distribuindo CDs com software que lhe dê acesso a informações no computador do usuário após a instalação. O dispositivo se aplicaria, por exemplo, aos CDs distribuídos pela SONY em 2005, que instalavam *spyware* no computador das pessoas.

:: REGRA PRINCIPAL: CONSENTIMENTO INFORMADO

A regra geral no Artigo 11.7a da Lei de Telecomunicações basicamente copia o Artigo 5.3 da versão final da Diretiva "Privacidade e Comunicações Eletrônicas". Uma empresa que queira acessar informações armazenadas no equipamento terminal de um usuário, ou que queira armazenar informações nesse equipamento, deverá dar ao usuário informações claras, pelo menos sobre o propósito do cookie, e deverá também obter o consentimento do mesmo. Em suma, cookies só são permitidos após consentimento informado por parte do usuário. Há, entretanto, uma discussão sobre exceções a essa regra.

> O ônus da prova recai sobre as empresas que empreguem os cookies de rastreamento, no sentido de provarem que não processam dados pessoais.

As informações prestadas ao usuário devem ser "claras e completas" e devem estar "em conformidade com a Lei de Proteção de Dados Pessoais". As empresas devem, no mínimo, explicar o propósito de um cookie. A Lei de Proteção de Dados Pessoais exige que as empresas forneçam mais informações detalhadas, caso isso seja necessário para assegurar um processamento justo e legítimo dos dados.

Organizações como o *Interactive Advertising Bureau* holandês fizeram lobby em prol de uma

21. Eerste Kamer, vergaderjaar 2011–2012, 32 549, G, 17 February 2012, p. 4-6.

implementação que aceitaria as configurações padrão do navegador como consentimento[22].
Os legisladores holandeses não seguiram a sugestão. O memorial explicativo das emendas à Lei das Telecomunicações diz que os navegadores atuais não são adequados para dar consentimento.
Por exemplo, muitos deles aceitam cookies como padrão. Os legisladores acrescentaram que existe a possibilidade de navegadores que venham a oferecer funções para a expressão do consentimento. Eles não explicaram como as empresas devem obter o consentimento para cookies, mas convocam as empresas do ramo da propaganda on-line para encontrar uma solução viável.

A Agência Nacional holandesa encarregada das telecomunicações, a OPTA, diz que o consentimento pode ser obtido através de uma janela pop-up. Diz também que um anunciante na Internet pode negar acesso a visitantes que não aceitem um cookie. É possível questionar se o usuário dá consentimento "de livre e espontânea vontade" em casos assim.
Por outro lado, o considerando 25 do preâmbulo da Diretiva "Privacidade e Comunicações Eletrônicas" permite que anunciantes na Internet condicionem o acesso "com base numa aceitação bem-informada acerca de um cookie ou de um dispositivo semelhante, se ele for usado para um propósito legítimo."

As empresas não precisam pedir novo consentimento para visitantes que estejam voltando ao seu sítio Web. Se um usuário dá o seu consentimento para que ela armazene um cookie permanente, o consentimento permanece válido durante toda a vida útil do cookie, conforme a OPTA. Assim, as pessoas só precisam dar consentimento uma vez a um cookie desse tipo.
Com isso, minimiza-se o risco de uma avalanche de pop-ups de consentimento. Além disso, muitos cookies estão isentos da exigência de consentimento. Em suma, o dispositivo holandês somente permite o armazenamento e a leitura de cookies depois do consentimento informado do usuário, a menos que se aplique uma exceção.

:: DUAS EXCEÇÕES À EXIGÊNCIA DE CONSENTIMENTO

Assim como na Diretiva "Privacidade e Comunicações Eletrônicas", o dispositivo holandês isenta duas categorias de cookies da exigência de consentimento. Primeiro, uma empresa que queira armazenar ou ler informações "com o único propósito de transportar uma comunicação através de uma rede de comunicações eletrônicas" não precisa obter o consentimento prévio. Uma segunda exceção se refere a cookies que são "estritamente necessários" para "a prestação de um serviço da sociedade da informação solicitado pelo usuário".
Um serviço da sociedade da informação significa, grosso modo: um serviço prestado via Internet[23].

22. Ver: Interactive Advertising Bureau, IAB Europe urges EU Member States to consider negative impact of an overly strict consent for cookies (www.iabeurope.eu/news/iab-europe-urges-eu-member-states-to-consider-negative-impact-of-an-overly-strict-consent-for-cookies.aspx). 23. O Artigo 1(2) da Diretiva 98/34/EC define assim um serviço da sociedade da informação : "qualquer serviço remunerado normalmente prestado à distância, por meios eletrônicos e mediante a solicitação individual do usuário do serviço." Este artigo está implementado no Artigo 3:15d do Código Civil Holandês.

Um exemplo seria um cookie para um carrinho de compras digital.

O Grupo de Trabalho do Artigo 29 emitiu um parecer sobre as isenções da exigência de consentimento[24]. Os pareceres do Grupo de Trabalho não têm força de lei, mas influenciam, uma vez que o Grupo de Trabalho é formado por representantes das autoridades responsáveis pela proteção de dados dos estados membros e pelo Supervisor Europeu para a Proteção de Dados, e normalmente toma decisões por consenso.

O Grupo de Trabalho usa uma interpretação estreita dos cookies que são necessários para transportar uma comunicação. Para ser isenta, a transmissão de uma comunicação através de uma rede de comunicações eletrônicas precisa ficar impossibilitada sem o cookie. O Grupo de Trabalho também dá exemplos de cookies que são estritamente necessários para um serviço de Internet solicitado pelo usuário. A saber, um cookie necessário para um carrinho de compras digital, para um procedimento de login, ou para lembrar as preferências de idioma estabelecidas pelo usuário.

O Grupo de Trabalho confirma que certos tipos de cookies não são isentados da exigência de consentimento. A exigência de consentimento prévio dado por um usuário informado se aplica ao rastreamento com cookies tais como os que são usados para a segmentação comportamental. O consentimento é exigido para outros cookies de terceiros que também são usados para a publicidade. A regra do consentimento se aplica ainda a muitos cookies que são usados pelos sítios de redes sociais para rastrear os usuários quando estes navegam pela Internet.

:: PREMISSA LEGAL ACERCA DOS COOKIES DE RASTREAMENTO

Durante o processo legislativo, o Parlamento Holandês acrescentou uma emenda relativa ao uso de cookies de rastreamento e tecnologias semelhantes. Entende-se que esse uso de cookies envolva o processamento de "dados pessoais". A premissa legal reverte o ônus da prova. Cabe às empresas que empregam os cookies de rastreamento provar que não processam dados pessoais. A Lei Holandesa parece ser a primeira do mundo que parte de uma premissa jurídica desse tipo para os cookies de rastreamento - o Artigo 11.7a traz a seguinte redação:

Qualquer atividade mencionada no preâmbulo, com vistas a coletar, analisar ou combinar informações sobre o uso que um assinante ou usuário faz dos vários serviços da sociedade da informação, com propósitos comerciais, idealísticos ou de caridade, é tida como processamento de dados pessoais, conforme definido no Artigo 1(b) da Lei de Proteção de Dados.

24. Grupo de Trabalho do Artigo 29, 'Opinião 04/2012 sobre Exceções ao Consentimento para Cookies' (WP 194, 7 de junho de 2012).

A frase "atividade mencionada no preâmbulo" refere-se a acessar informações armazenadas no equipamento terminal de um usuário ou a armazenar informações no equipamento terminal de um usuário, através de redes de comunicações eletrônicas. Um "serviço da sociedade da informação" é identificado de forma ampla. A definição cobre a maior parte dos serviços de Internet, inclusive os gratuitos. Um exemplo do "uso de vários serviços da sociedade da informação" seria a visita a variados sítios na Internet.

Portanto, se uma empresa quiser acessar ou armazenar informações para rastrear pessoas em vários serviços de Internet, a premissa jurídica se aplica. A frase "com propósitos comerciais, idealísticos ou de caridade" significa, grosso modo: com propósitos de marketing direto. O escopo da frase holandesa é um tanto mais amplo, e também inclui mensagens voltadas para angariar verbas, por exemplo. O memorial explicativo diz que a premissa legal visa assegurar que a Lei de Proteção de Dados se aplique quando uma empresa emprega cookies de rastreamento.

O memorial explicativo diz que uma empresa precisa obter um consentimento do usuário sem ambiguidade antes de colocar um cookie de rastreamento. O governo holandês mais tarde disse que, em princípio, outras bases além do consentimento sem ambiguidade poderiam legitimar o processamento de dados pessoais de natureza não sensível. Entretanto, o Grupo de Trabalho sugere que o processamento de dados pessoais para segmentação comportamental raramente pode ser legitimado por outro embasamento que não o "consentimento sem ambiguidade" do usuário. Se uma empresa processa dados pessoais, ela precisa cumprir com todos os princípios relativos à proteção de dados. Por exemplo, as empresas devem evitar a coleta de dados excessivos ou sigilosos.

A premissa legal entrou em vigor em 1 de janeiro de 2013, embora o resto do dispositivo já esteja em vigor desde junho de 2012. O Senado Holandês disse que esse retardo poderia permitir que a indústria de marketing on-line apresentasse um sistema fácil de usar para a obtenção do consentimento, por exemplo, elaborando uma norma palpável para o *Do Not Track*.

:: FISCALIZAÇÃO E EFEITO EXTRATERRITORIAL

Quem precisa cumprir o Artigo 11.7a da Lei Holandesa de Telecomunicações? O Parágrafo 1 diz: "qualquer um" que queira acessar informações armazenadas no aparelho de um usuário, ou que queira armazenar informações no aparelho de um usuário.

O dispositivo holandês se aplica a empresas que não estejam sediadas nos Países Baixos? Este assunto é complicado. A OPTA, autoridade responsável pelas telecomunicações, supervisiona

o cumprimento da Lei Holandesa de Telecomunicações. Conforme essa entidade, o Artigo 11.7a também se aplica a anunciantes estrangeiros na Internet. O texto da Diretiva "Privacidade e Comunicações Eletrônicas" permite essa interpretação.

Outra questão a se discutir é quem deve pedir o consentimento do usuário. Se um usuário visita um sítio de notícias e vinte empresas de segmentação comportamental colocam cookies espalhados pelo sítio, quem deve pedir o consentimento do usuário? A OPTA diz que um anunciante na Internet compartilha a responsabilidade com terceiros que espalhem cookies pelo seu sítio. Isso se alinha com o conselho anterior do Grupo de Trabalho do Artigo 29.

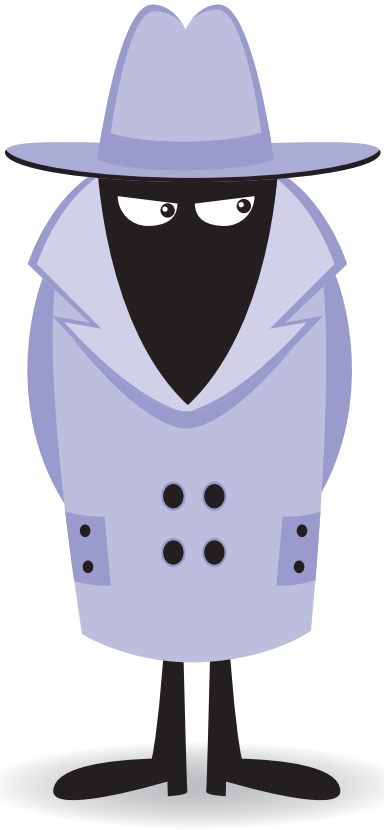
Os reguladores holandeses não começaram a fazer cumprir a lei ainda. A OPTA tem autoridade para aplicar multas de até 450.000 euros pelo seu descumprimento. Se uma empresa processa "dados pessoais", aplica-se a Lei de Proteção de Dados. Nesse caso, uma segunda autoridade reguladora entra em cena. A Autoridade Holandesa de Proteção de Dados supervisiona o cumprimento da Lei de Proteção de Dados. A Autoridade de Proteção de Dados não precisará provar que uma empresa usando um cookie de rastreamento processa dados pessoais. Caberá à empresa provar que não o faz. A Autoridade de Proteção de Dados não pode aplicar multas pelo descumprimento do dispositivo holandês a respeito dos cookies. Mas pode aplicar vultosas penalidades preventivas se uma empresa desobedecer suas ordens administrativas.

:: CONCLUSÃO

Este artigo analisou as novas regras holandesas sobre cookies e tecnologias semelhantes. Primeiro, foi abordada a discussão europeia sobre a regulação da segmentação comportamental e dos cookies. Na Europa, a discussão está centrada na maneira como as empresas devem obter o consentimento dos usuários.

Nos Países Baixos, o Artigo 5.3 da Diretiva "Privacidade e Comunicações Eletrônicas" está implementado na Lei Holandesa das Telecomunicações. O dispositivo holandês, que também se aplica a empresas fora dos Países Baixos, só permite o armazenamento e leitura de cookies e arquivos assemelhados depois de o usuário emitir um consentimento informado. As empresas não podem inferir consentimento a partir das configurações padrão dos navegadores atuais. O legislador holandês acrescentou uma premissa legal sobre o rastreamento de cookies e tecnologias semelhantes. Presume-se que usar cookies dessa maneira envolva o processamento de dados pessoais. Ainda não está clara a maneira como a Lei Holandesa vai ser aplicada. Ela poderá trazer más notícias para empresas que empreguem cookies de rastreamento e tecnologias semelhantes, especialmente se outros países resolverem seguir o caminho holandês. ●

> **Heesob Nam** Diretor Executivo da Open Net



Alguém observa enquanto você está on-line: experiências da Coreia do Sul

:: PREÂMBULO

Por Carlos Afonso – Diretor Executivo do Instituto Nupef

A luta pelo Marco Civil da Internet no Brasil não terminou - pelo contrário, será acirrada nos próximos meses e no momento a vantagem pende para as operadoras de telecomunicações (contra a neutralidade da rede), apoiadas por alguns setores do governo federal, e para as empresas de midia (que defendem a responsabilização de intermediários e a retirada arbitrária de conteúdo da rede sem o devido processo legal).

O experimento conhecido como "verme de Morris", no final de 1988, revelou a extrema vulnerabilidade da rede originalmente concebida, e desencadeou uma infinidade de processos para estabelecer mecanismos de proteção[1]. Podemos dizer que Robert Morris, hoje professor do MIT, "expulsou a Internet do Paraíso". Surgiram então as *firewalls* em servidores e em computadores caseiros, as técnicas de monitoramento e controle, e uma gigantesca indústria de antivírus.

1. Ver em http://en.wikipedia.org/wiki/Morris_worm

Inevitavelmente descobriu-se que esse monitoramento poderia também permitir uso comercial ou político da bisbilhotagem, levando aos sistemas atualmente existentes de monitoramento e manipulação do tráfego de rede.

A neutralidade da rede tem sido rotineiramente violada na chamada "camada de enlace" da Internet - através da qual qualquer computador é conectado à Internet. A conexão é um serviço dominado pelas operadoras de telecomunicações, seja via cabo da TV por assinatura, ou através da linha telefônica, ou ainda por rádio digital (celulares, tablets, conexões via provedores wi-fi, conexões via satélite e outros). O texto de Heesob Nam sobre a bisbilhotagem do tráfego Internet na Coreia do Sul é revelador de uma situação rotineira em todo o mundo - o emprego de técnicas de inspeção profunda de datagramas (*deep packet inspection* ou DPI) para fins de controle, censura e eventual monetização do perfil de navegação dos usuários.

A violação de direitos na camada de enlace por parte das operadoras e grandes provedores vem de longe. Lembremos do caso AT&T denunciado pela Electronic Frontier Foundation (EFF) em 2006, de espionagem massiva de dados dos usuários a serviço da National Security Agency (NSA) dos EUA[2]. Nesse mesmo período surgiam denúncias de bloqueio do tráfego do Skype na rede da Brasil Telecom[3]. Coincidentemente, a BR Telecom utilizava o mesmo software que a AT&T usava para a bisbilhotagem de datagramas.

Em julho de 2012 o cientista-chefe da APNIC, Geoff Huston, denunciou a Telstra (principal operadora de telecomunicações da Austrália) exatamente por isso: praticar DPI sobre o tráfego de dados de seus usuários, catalogar os perfis de navegação e repassar esse cadastro a uma empresa canadense especializada em mineração de dados e monetização de perfis, a Netsweeper[4]. Essa escandalosa violação de privacidade (que pode até colocar em risco a segurança pessoal de milhares de usuários) foi reconhecida pela Telstra, que afirma não ter feito nada ilegal — o que indica que continuará a violar a privacidade de seus usuários e a adotar outras formas arbitrárias de controle sobre os dados trafegados por sua rede.

Em dezembro de 2012 a União Internacional das Telecomunicações (UIT/ITU), através de seu organismo que define padrões (ITU-T), aprovou em sessões fechadas uma norma para a bisbilhotagem dos dados que trafegam na camada de enlace. A norma Y.2770 sacramenta a DPI, estabelecendo um conjunto detalhado de regras para monitorar, inspecionar e manipular cada datagrama que passa por essa camada. Destina-se especialmente às empresas que produzem equipamentos e software de bisbilhotagem utilizados pelas operadoras e provedores.

Ao mesmo tempo, na Conferência Mundial sobre Telecomunicações Internacionais (WCIT),

2. Ver em http://www.wired.com/science/discoveries/news/2006/04/70619 3. Ver em http://www.abusar.org.br/skype_brt.html
4. Ver em http://www.potaroo.net/ispcol/2012-07/allyourpackets.html. Ver também http://bit.ly/LQtYR4

89 países (entre os quais o Brasil) assinaram um novo tratado para regulação das telecomunicações (ITR), que requer a aderência aos padrões aprovados pelo ITU-T. Consultados sobre esse padrão de bisbilhotagem, membros da Anatel insistem que o Brasil assinou o tratado mas não está obrigado a cumpri-lo em sua totalidade e tampouco a seguir sem ressalvas a normatização respectiva. Isso é estranho - tratados internacionais são vinculativos. Que partes, que normas, que determinações o Brasil seguirá ou deixará de seguir?

Mesmo que a aprovação dos novos ITRs tenha sido na prática um fracasso (dos 193 Estados membros da UIT, uma maioria de 104 países não assinou ou absteve-se, entre estes os EUA, a Europa e Japão), qualquer país filiado ou não à UIT acaba seguindo os padrões desta, muitos dos quais têm crucial relevância para a operação da rede - exemplos são os padrões da série G.X para codificação da comunicação digital via ADSL ou via rádio digital, os codecs para transmissão de voz e vídeo, e muitos outros. Afinal, a Internet está "montada" em uma estrutura de telecomunicações normatizada por essa agência da ONU. A norma Y.2770 pertence à série Y.27X, dedicada à segurança das redes.

A assinatura do tratado por parte do Brasil, especialmente no momento delicado e muito difícil em que tentamos aprovar o Marco Civil com forte oposição de lobbies poderosos, deu a impressão que o Brasil disse ao mundo: ainda não aprovamos o Marco Civil, mas por coerência (ou por vinculação ao tratado) agora pelo menos a neutralidade da rede desaparecerá dele.

Mas não nos iludamos: a Coreia do Sul, a Austrália e os EUA não assinaram o tratado e são exemplos marcantes de violação da neutralidade da rede desde bem antes da normatização da ITU-T. Isso fica bem claro no artigo de Heesob. Vamos a ele.

:: INTRODUÇÃO

A Inspeção Profunda de Pacotes (conhecida como DPI, sigla em inglês de *Deep Packet Inspection*) é uma tecnologia que permite a um observador saber quem você é e o que você está fazendo online. Esta tecnologia não é neutra - no sentido de que tem sido desenvolvida e adotada por aqueles que tiram proveitos da possibilidade de vigiar em função de seu próprios interesses. Um destes interesses é ganhar o controle sobre os usuários da Internet; outro é o lucro comercial. O Estado, normalmente os órgãos do Executivo, beneficia-se da DPI, pois através dela obtém uma quantidade inimaginável de informações sobre as pessoas, o que é essencial para controlá-las. O propósito dos interesses comerciais ao usar a tecnologia DPI é simples: ganhar mais dinheiro. Com a DPI as empresas podem fazer mais dinheiro, expulsando concorrentes do mercado ou tirando melhor proveito de oportunidades para atrair mais clientes.

Durante os últimos quatro ou cinco anos, nós, sul-coreanos, testemunhamos inúmeras histórias de adoção da tecnologia DPI, utilizada tanto para a vigilância do Estado como também para a vigilância

por parte de empresas. Este artigo tem como objetivo compartilhar as nossas experiências e lições. A história apresentada aqui não é uma história de sucesso. Ao contrário, mostra que o debate em curso sobre tecnologias de vigilância e seu resultado dependem em grande medida da reação dos defensores de uma Internet livre e aberta.

Para efeitos de contextualização sobre a indústria de telecomunicações da Coreia, é importante assinalar que para prestar serviços de telecomunicações ou ser provedor de serviços de acesso à Internet é preciso antes obter uma aprovação da autoridade reguladora. Em setembro de 2012, havia 119 provedores de acesso no país. Entretanto, o mercado é dominado por três grandes provedores: Korea Telecom (KT), SK Telecom e LG U + . São estes os principais atores quando se fala na implantação das tecnologias DPI.

:: VIGILÂNCIA DO ESTADO: AS ESCUTAS NA INTERNET

Na Coreia a prática de escuta é estritamente proibida por lei. Conforme a Lei de Proteção da Privacidade das Comunicações (CPPA, por sua sigla em inglês), promulgada em 1993, escutas referem-se a qualquer ato de conhecer ou gravar o conteúdo das comunicações eletrônicas de outros usando-se dispositivos mecânicos ou eletrônicos[5]. A definição de "comunicações eletrônicas" é ampla: cobre qualquer transmissão ou recebimento de qualquer tipo de som, texto, vídeo ou sinal por meio de fio, por redes sem fio, por fibra óptica ou qualquer outro meio eletrônico. Qualquer pessoa que efetua escuta telefônica sem autorização judicial e sem o devido processo legal pode ser condenada a pena de prisão de até dez anos ou a suspensão de qualificação de até cinco anos. Não é permitida a pena pecuniária no lugar da prisão. Autoridades como promotores de justiça, oficiais da polícia e de agências de informação não são exceção.

No entanto, a proibição estrita de escutas telefônicas não garante a total proteção da privacidade das comunicações. Para escutas telefônicas legais, a CPPA exige que as autoridades executoras da lei obtenham uma permissão judicial (ou uma aprovação do presidente, nos casos em que estrangeiros estão envolvidos), especificando como inspecionar, o que será inspecionado, por quanto tempo e em que medida a inspeção deve ser feita. No entanto, as autoridades policiais têm encontrado facilidade para obter dos tribunais a permissão de inspeção.

Por exemplo, em 2011, o Serviço de Inteligência Nacional (SIN) fez escutas telefônicas em 6.840 números de telefone. Isso equivale a 95,4% do total de inspeções feitas no país por autoridades encarregadas da aplicação das leis[6]. Este número reflete apenas a vigilância realizada por intermédio de provedores de Internet, a pedido do SIN - o que significa que a inspeção realizada pelo SIN

5. É interessante observar que a CPPA define "o ato de inibir a transmissão ou recepção na comunicação eletrônica alheia" como escuta. A nossa história legislativa falha em lançar luz sobre o significado desta frase e não há jurisprudência sobre este tipo de situação. 6. Ver em http://www.mediaus.co.kr/news/articleView.html?idxno=24942

sem passar pelos provedores não é contabilizada (note-se que o SIN possui mais de 30 equipamentos de inspeção, conforme foi revelado em 2010 por uma investigação do Congresso). De acordo com Della, um dos ativistas de privacidade mais proeminentes na Coreia do Sul, as autoridades que fazem investigação estão utilizando cada vez mais a Internet como alvo de suas escutas. Em 2011, o percentual de escutas na Internet foi superior a 60% do total de escutas realizada em serviços de telecomunicações. As autoridades investigadoras observaram os e-mails dos suspeitos e toda a sua navegação na Web. As ações de inspeção na comunicação móvel vão além de nossa imaginação. Quando algo suspeito acontece em uma determinada área, as autoridades policiais inspecionam todas as estações móveis dentro daquela área. Somente no ano de 2010, cerca de 39 milhões de números de telefones móveis foram inspecionados na Coreia.

Durante muito tempo após a promulgação da CPPA, em 1993, não sabíamos se a inspeção autorizada pelos tribunais (que é chamada de "medidas restritivas sobre a comunicação", nos termos da lei) incluía inspeção profunda de pacotes. Entretanto, durante um julgamento criminal em 2009, foi revelado que o SIN havia inspecionado cada mensagem de e-mail, toda a navegação na Internet e todas as conversas telefônicas do suspeito. Em outro caso, ficou provado que o SIN realizou inspeção profunda de pacotes por cerca de seis anos - de julho de 2003 a junho de 2009. Nesta situação, o SIN conseguiu obter a permissão da corte 36 vezes para inspecionar a mesma pessoa sob a mesma suspeita, que estava relacionada à Coreia do Norte. Surpreendentemente, o tribunal permitiu a inspeção da linha de Internet instalada na casa do suspeito, de duas contas de e-mail do suspeito, e da linha de conexão à Internet do local de trabalho do suspeito. Isso significa que o SIN pode capturar todos os pacotes que fluem através das conexões e assistir remotamente e em tempo real tudo o que está sendo exibido na tela do computador da pessoa.

Este caso causou polêmica sobre a legalidade da inspeção de pacotes. Em 2010, os membros da Assembleia Nacional organizaram uma discussão aberta, demonstrando como a inspeção de pacotes funciona. Os participantes da discussão podiam

Somente no ano de 2010, cerca de 39 milhões de números de telefones móveis foram inspecionados na Coreia.

ver cada mensagem de e-mail e até mesmo a senha que um usuário digitou para entrar num programa de mensagens instantâneas – estes dados foram capturados e exibidos na tela do sistema de DPI. Alguns legisladores apresentaram projetos de lei para limitar a inspeção legal de pacotes. Uma proposta foi a de permitir a inspeção de pacotes somente quando um observador autorizado estiver presente.

Todavia os esforços legislativos não se concretizaram. Por isso, em 29 de março de 2011, defensores dos direitos humanos levaram o caso para o Tribunal Constitucional argumentando que a inspeção profunda de pacotes é inconstitucional porque a autorização judicial permitindo a inspeção de pacotes é equivalente ao mandado genérico de busca e apreensão, que é proibido[7]. Note-se que o argumento deles não era o de limitar o âmbito do que é admissível em se tratando de DPI. Também não se tratava de aprimorar a vigilância judicial sobre o governo em questões envolvendo DPI. O argumento era simples e claro: a permissão para uso de DPI, por si só, é inconstitucional.

De acordo com a nossa constituição, um mandado judicial deve ser de alcance limitado, ou seja, deve especificar qual pessoa será inspecionada. No entanto, a inspeção profunda de pacotes em uma conexão de Internet permite a inspeção da comunicação de outras pessoas que compartilham a conexão, o que é comum em se tratando de conexão à Internet. Além disso, o controle deve ser limitado a certas comunicações - aquelas que são relevantes para o crime sendo investigado. Todavia esta relevância não pode ser determinada até que os investigadores olhem para o conjunto das comunicações feitas através daquela conexão e decidam que parte da comunicação é relevante. Portanto, o mandado que permite a DPI equivale a um mandado "genérico", que é inconstitucional - os freios e contrapesos judiciais não podem ser postos em prática, quando se trata de DPI.

:: MARKETING E DPI – O PHORM E A PUBLICIDADE DIRECIONADA

O uso de DPI para fins comerciais é outra ameaça à privacidade. Um exemplo que merece atenção é o uso de DPI para publicidade direcionada, que foi chamado em 2009 pela Korea Telecom de "QOOK SmartWeb[8]." A KT desenvolveu este sistema com base no sistema Webwise do Phorm[9], e tornou público o fato de que a KT já colocou em prática um serviço experimental desta tecnologia tendo como alvo milhares de clientes que vivem em Seul.

Muitas organizações da sociedade civil e especialistas expressaram suas preocupações sobre a potencial violação do direito à privacidade dos usuários porque a publicidade direcionada da KT baseava-se na inspeção e análise de termos

7. Este caso envolve um indivíduo que é professor numa escola secundária e trabalha para o Sindicato Coreano de Professores e Trabalhadores da Educação. A suspeita sobre ele era a de notória "apreciação" pela Coreia do Norte. 8. "QOOK" é uma marca do serviço de conexão à Internet da KT. 9. Para detalhes sobre o Webwise, visite http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf

de busca e comportamentos online dos usuários. Enquanto a KT, o Phorm e seus advogados argumentaram que não havia ameaça à privacidade porque o serviço foi aplicado apenas àqueles que consentiram ser alvo de seu uso, as organizações da sociedade civil obtiveram sucesso em mostrar que a publicidade direcionada viola a CPPA, que proíbe qualquer ato que busque conhecer e gravar a comunicação eletrônica alheia.

:: USO DE DPI EM BENEFÍCIO DO PROVEDOR DE SERVIÇOS INTERNET: O CASO DA SMART TV

Provedores de acesso à Internet usam a tecnologia DPI para seu próprio benefício. Eles anseiam por garantir suas vantagens de mercado da maneira que for possível, mesmo que isso signifique sufocar a concorrência.

Em 10 de fevereiro de 2012, a Korea Telecom bloqueou uma conexão à Internet feita através da smart TV da Samsung. De acordo com a KT, seu bloqueio foi legítimo, porque era muito provável que a smart TV gerasse tráfego excessivo (diz-se que a smart TV gera tráfego de 5 a 15 vezes maior do que a IPTV). Mas este argumento não foi razoável, porque a KT não bloqueou a smart TV da LG Electronics[10]. A Korea Telecom argumentou que tentou negociar com a Samsung sobre a taxa de uso de sua rede, mas a Samsung não quis negociar. Em 2010 e 2011, a Samsung vendeu cerca de 750.000 aparelhos de smart TV na Coreia e, para o serviço de smart TV, tinha 77 servidores alocados nos EUA e linhas alugadas da AT&T.

A KT pôde bloquear o tráfego de smart TV, simplesmente capturando pacotes com endereço de destino dirigidos para os servidores da Samsung e derrubando-os em seus quatro roteadores centrais localizados em Seul[11]. No dia seguinte, a Samsung foi à justiça e pediu uma liminar para proibir a KT de fazer este bloqueio - e o governo coreano, ou seja, a Korea Communications Commission (KCC) interveio no caso. Além disso, a opinião pública estava contra a KT.

Finalmente, em 14 de fevereiro de 2012, a KT suspendeu sua sanção à smart TV da Samsung, e

10. No terceiro trimeste de 2011, o market share da smart TV da LG era de 14.4% enquanto que o da smart TV da Samsung era de 22.5%.
11. Os roteadores eram modelo GSR12316 e o endereço IP bloqueado foi o 210.118.88.200.

a KCC decidiu em 4 de maio que o bloqueio da KT violara a Lei de Empresas de Telecomunicações, pelo fato de ter sido feito apenas ao tráfego da smart TV da Samsung e não ao tráfego da LG. Além disso, o bloqueio foi feito sem aviso prévio aos assinantes.

:: USO DE DPI E SERVIÇOS DE VOIP MÓVEL

O debate sobre serviços de voz sobre IP móvel (VoIP móvel) em 2012 mostrou como o DPI foi usado para o benefício das operadoras de telefonia, solapando o princípio da neutralidade da rede. O serviço KakaoTalk, que foi lançado em 2010 e tinha, em janeiro de 2013, cerca de 70 milhões de assinantes (sendo que 35 milhões só na Coreia), é uma aplicação de software para dispositivos móveis que permite aos usuários enviar e receber mensagens, incluindo textos, fotos e vídeos. No ano passado, a KakaoTalk começou a oferecer também o serviço de chamadas gratuitas através de voz sobre IP. Mas as principais operadoras de telecom – a SK Telecom, a Korea Telecom e a LG U + - todas prestadoras de serviços de telefonia e de VoIP móvel, não perderam um minuto sequer. No dia seguinte ao lançamento do serviço de chamada gratuita da KakaoTalk , as três empresas estrangularam o tráfego de mVoIP da Kakao.

Segundo pesquisa da KakaoTalk, a taxa de perda de qualidade do serviço no primeiro dia de funcionamento do VoIPmóvel foi de aproximadamente um por cento – o que significa pouca dificuldade nas ligações. No entanto, a partir do segundo dia, a taxa de perda disparou para 20 por cento no caso da SK Telecom – e 54 por cento no caso da LG U + – , tornando a qualidade das ligações via Kakao demasiado pobre, impossibilitando a comunicação.

Ao contrário do caso da smart TV, a autoridade reguladora (KCC) apenas assistiu inerte, dizendo que a situação deveria ser resolvida de acordo com os mecanismos de autorregulação do mercado. Mas aos olhos dos defensores da neutralidade da rede, o bloqueio arbitrário de tráfego VoIP por parte dos grandes provedores de acesso à Internet é anti-competitivo e viola a Lei de Negócios de Telecomunicações, assim como ocorreu no caso da smart TV da Samsung.

Aproveitando a oportunidade, várias organizações da sociedade civil, especialistas e ativistas lançaram o Fórum dos Usuários para a Neutralidade da Rede (chamado de nnForum) e tomaram diversas medidas. Por exemplo, o nnForum pediu ao Conselho Nacional de Auditoria e Inspeção para investigar a KCC por negligência e abandono de funções, e levou a SK Telecom e a KT à entidade reguladora e à Comissão de Comércio Justo, apontando que estas empresas utilizaram mal seu poder de mercado à custa dos interesses dos consumidores. O nnForum também foi bem sucedido em tornar o princípio da neutralidade da rede uma das questões mais controversas durante a campanha das eleições presidenciais de dezembro de 2012.

:: USO DE DPI E AS REDES P2P

Este caso também envolve a Korea Telecom. Desde junho de 2012 a KT vinha planejando bloquear o tráfego de P2P em sua rede - e fez um contrato com a Sandvine[12] para testar seus serviços. Diz-se que a KT pagou três bilhões de wons sul-coreanos (KRW)[13] para a Sandvine pelo teste do serviço de rastreamento de conexões Internet e que iria passar a usar definitivamente o equipamento da Sandvine no final de 2012, pagando em torno de KRW 80 bilhões.

Não se sabe como a KT pode bloquear o tráfego P2P. Ao consultar o centro de informações da KT foi-me assegurado que eles não olham o conteúdo dos pacotes de informações dos assinantes. Em vez disso, eles simplesmente tornam invisíveis aos prestadores de serviços P2P as informações sobre assinantes que instalaram programas clientes para a entrega da grade P2P. A entrega da rede P2P é implementada por programas específicos distribuídos por provedores de serviços Internet ou por prestadores de serviços de armazenamento de arquivos online. O que eu ouvi de um funcionário da KT (que está no comando da gestão de tráfego P2P da empresa) é que a tecnologia específica para implementar a gestão do tráfego P2P na rede da Korea Telecom é segredo comercial e que eles só olham para os endereços contidos no cabeçalho IP e não para o número da porta.

Ao contrário de outras práticas comuns de restrições ao tráfego P2P[14], o caso KT tem pouco a ver com a gestão de congestionamento de tráfego ou com proteção de direitos autorais. A KT considera que todos os indivíduos que instalaram o programa cliente de P2P não são assinantes individuais: são assinantes corporativos que devem pagar taxas maiores para a utilização de rede da KT, uma vez que a utilizam para fins comerciais.

Até o momento em que este artigo foi escrito, a KT não parecia ter implementado seu plano. Uma possível razão para isso pode ser o trabalho que o KCC está realizando, de um esboço de padrão para a gestão e utilização racional de redes de comunicação, que visa definir os detalhes da "orientação para a neutralidade de rede e para o gerenciamento do tráfego da Internet." Para a Korea Telecom, seria melhor para sua reputação esperar até que a norma seja promulgada, porque o projeto da agência reguladora parece legitimar o seu bloqueio de VoIP móvel e de tráfego P2P. Na verdade, o projeto de lei enumera a restrição de VoIP móvel como uma das formas admissíveis de gerenciamento de tráfego. Membros de organizações da sociedade civil criticaram este projeto pela falta de transparência no seu processo de elaboração, uma vez que deixou-se de ouvir os diversos interessados, incluindo os usuários finais, tornando o gerenciamento de tráfego uma chave-mestra nas mãos dos provedores de acesso à Internet. ●

12. N.E. Empresa asiática que oferece produtos e serviços para provedores de Internet, entre eles plataformas tecnológicas para gerenciamento de tráfego. Ver em http://www.sandvine.com 13. N.E.: o que equivale a aproximadamente três milhões de dólares. 14. De acordo com BEREC (*A view of traffic management and other practices resulting in restrictions to the open Internet in Europe*, 29 May 2012), as restrições reportadas com mais frequência são o bloqueio e/ou o "estrangulamento" do tráfego P2P tanto em redes fixas quanto em redes móveis em função do gerenciamento de congestionamentos do tráfego nas redes.

A Internet perdeu um de seus mais brilhantes sonhadores[1]

Magaly Pazello pesquisadora do Emerge — Centro de Pesquisa e Produção em Comunicação e Emergência da Universidade Federal Fluminense (UFF).

O suicídio de Aaron Swartz, em Nova Iorque, no dia 11 de janeiro de 2013, teve enorme repercussão. Esse trágico evento ultrapassa a dor da família, dos amigos e daqueles que o admiravam. É trágico em diversas dimensões. A dor foi acompanhada de espanto e indignação contra os excessos inadmissíveis do poder legal em um país como os Estados Unidos, onde presume-se que os princípios constitucionais são respeitados e fazem parte do cotidiano das pessoas. A indignação foi explícita contra a pequenez de espírito dos responsáveis por uma das instituições acadêmicas mais respeitadas do mundo - o Massachusetts Institute of Technology (MIT), que tornou-se um dos protagonistas dos eventos que levaram Aaron ao suicídio.

A repercussão da tragédia não foi devido ao fato de tratar-se de um rapaz de 26 anos, que gozava de alguma popularidade, ou porque Aaron ousou enfrentar a milionária indústria da privatização do conhecimento. A repercussão, o espanto, a profunda tristeza e a indignação são sentimentos que se entrelaçam diante do fato de que a Internet perdeu um de seus mais brilhantes sonhadores.

Embora a maioria de nós não tenha ideia, somos todos beneficiários, de algum modo, das criações de Aaron Swartz. Desde muito cedo ele contribuiu para o aperfeiçoamento da Internet, sem com isso ficar famoso e milionário, como aconteceu com outros que estamos acostumados a ver na grande mídia. O seu prodígio era conscientemente posto a favor do bem comum, seguindo a onda boa dos trabalhos colaborativos, abertos e livres. Trabalhando com Tim Berners-Lee (o cara que criou a Web), no famoso Massachusetts Institute of Technology (MIT) - que mais tarde seria protagonista dos eventos que o levaram ao suicídio -, Aaron ajudou a desenvolver e popularizar padrões para o compartilhamento de dados na Web.

Ainda assim, inicialmente os meios de comunicação insistiram em sublinhar a depressão como o signo mais relevante na tentativa de compreender o suicídio de Aaron Swartz, mas este argumento não convenceu: muitas vozes se levantaram para dizer, criticamente, que disso não se tratava, que estávamos diante de algo maior. Danna Boyd escreveu[2]: *Para o bem ou para o mal, ao longo dos anos, eu conheci muitas pessoas que cometeram suicídio. Eu observei essas pessoas lutarem contra a depressão profunda, mas, por fim, fazem essa escolha. Lutei contra os meus próprios demônios, para entender isso. Parte do que me entristece e atordoa na morte de Aaron é o fato de que desta vez foi diferente.*

1. Artigo baseado em texto, da mesma autora, publicado pelo blog Viomundo em 14 de janeiro de 2013. Ver em http://www.viomundo.com.br/falatorio/magaly-pazello--aaron-swartz-perda-inestimavel.html 2. Ver em http://www.zephoria.org/thoughts/archives/2013/01/13/aaron-swartz.html

Lawrence Lessig, ainda sob o impacto da notícia, firmemente denunciou as intimidações sofridas por Aaron, (as quais a família confirmou através de uma declaração pública): *Ele era brilhante, e engraçado. Um menino prodígio. Uma alma, uma consciência, a fonte de uma pergunta que eu fiz a mim mesmo um milhão de vezes: O que Aaron pensaria? Essa pessoa se foi hoje, levada ao limite por algo que uma sociedade decente só poderia chamar bullying.*[3]

Tatiana de Mello Dias, do jornal *O Estado de São Paulo*, resumiu de forma certeira: *Poucas pessoas traduziram tão bem a época em que nós estamos vivendo quanto Aaron Swartz*[4]. Eliane Brum, da revista *Época*, reflete sobre a dimensão social e cultural da decisão de Aaron Swartz: *Isso faz com que possamos pensar que sua morte é também, simbolicamente, um fracasso da geração a qual pertenço. Essa geração que testemunhou o nascimento da internet, que está decidindo — na maioria dos casos por omissão — como o conhecimento vai circular dentro dela e que, por ter crescido num mundo sem ela, nem chega a compreender totalmente o que está em jogo. E por isso deixa a geração de Aaron tão só*[5].

O que a grande mídia nos Estados Unidos demorou a reconhecer é que esse rapaz enfrentou e sofreu penosamente os efeitos da máquina de moer do Departamento de Justiça dos Estados Unidos. Acusado de "roubar" milhões de artigos científicos, ele foi arrolado num processo judicial que poderia resultar em 35 anos de prisão e multa milionária. No centro desse processo se instalou uma séria controvérsia que deixou uma marca indelével sobre o direito de todas as pessoas ao acesso ao conhecimento e à informação, ao livre exercício dos direitos civis e das liberdades individuais. Os eventos que levaram à sua morte, contudo, vão além e se incrustam no próprio sistema de justiça, no modelo de desenvolvimento e nas políticas de Estado. Algo que igualmente atinge a todos nós, embora de diferentes modos.

A trajetória de Aaron Swartz é singular e merece ser conhecida. Aos 13 anos ele foi o ganhador do ArsDigita Prize, uma competição para jovens criadores de sítios Web não-comerciais que fossem úteis, colaborativos e voltados para atividades educacionais. O prêmio incluiu uma visita ao famoso MIT. Aos 14 anos, Aaron integrou a equipe de criadores do RSS 1.0[6], uma sigla cujo significado é conhecido por poucas pessoas, mas que dá nome a uma tecnologia largamente utilizada por quem navega na Internet. Trata-se de um agregador de conteúdos, um recurso que, hoje, contribui para a disponibilização de informação em redes sociais e que é utilizado em várias outras soluções de compartilhamento de dados. Além disso, tem a qualidade de ser um recurso criado a partir de um padrão simples e de ser adaptável a qualquer plataforma.

Nesse momento, Aaron já frequentava convenções e eventos onde os grandes nomes da

3. Ver em http://www.boingboing.net/2013/01/12/lessig-on-the-dojs-vindictiv.html 4. Ver em http://blogs.estadao.com.br/tatiana-dias/nao-foi-em-vao--aaron-swartz 5. Ver em http://revistaepoca.globo.com/Sociedade/eliane-brum/noticia/2013/01/perdao-aaron-swartz.html 6. Os *feeds* RSS oferecem conteúdo Web ou resumos de conteúdo juntamente com os *links* para as versões completas deste conteúdo e outros metadados. Ver em http://pt.wikipedia.org/wiki/RSS

Internet estavam presentes. Com um computador muito velho e sua inteligência exuberante cativou os pensadores mais influentes da Internet como Cory Doctorow e Lawrence Lessig. Assim aos 15 anos, integrou a equipe que concebeu as licenças Creative Commons, a audaciosa alternativa às amarras do tradicional direito de autor e da rapinagem realizada em nome da propriedade intelectual.

Em seguida Aaron lançou-se num vôo solo ao criar uma *start-up*, que depois se fundiu à rede social Reddit, onde ele desenvolveu a plataforma que levaria esta rede ao sucesso. O desenho desta plataforma também resultou na base de sítios Web *Open Library*, ou seja, bibliotecas abertas, e no *Archive.org*, uma espécie de "máquina do tempo da Internet". Esta foi sua vida e sua bandeira a partir de então: o acesso ao conhecimento e à informação, a oferta online gratuita de conteúdos através de plataformas abertas, o desenvolvimento técnico dessas plataformas. Em seu trabalho Aaron dedicou-se especialmente a promover o acesso ao conhecimento e à informação pública, principalmente quando gerados a partir de recursos públicos. Sua genialidade está presente em dezenas de projetos semelhantes. Porém, suas atividades profissionais nunca visaram à obtenção de lucro e promoção pessoal. Era a luta contra a privatização do conhecimento e em defesa da liberdade de expressão e da privacidade o seu maior interesse.

Seu talento não parava aí. Era comentarista de arte e cultura. Criou com Taryn Simon o *Image Atlas*[7], um pioneiro sistema online interativo que permite visualizar diferenças e similaridades culturais através da indexação de imagens utilizando resultados de mecanismos de busca mundiais. Aaron é também autor de diversos artigos sobre uma gama variada de assuntos, tinha predileção pelo tema da influência de grandes agentes financeiros sobre as instituições - incluindo as fundações, a mídia, a própria política e a opinião pública. Entre 2010 e 2011, foi bolsista do Laboratório de Ética do Centro Edmond J. Safra na Harvard University, onde pesquisava sobre corrupção institucional. Fundou e era líder do *DemandProgress.org*, uma plataforma inteligente de ciberativismo para fiscalização de processos legislativos e pressão para avanços nas políticas públicas.

Aaron dedicou-se especialmente a promover o acesso ao conhecimento e à informação pública, principalmente quando gerados a partir de recursos públicos.

7. Ver em http://imageatlas.org e http://www.newmuseum.org/exhibitions/view/taryn-simon-cultural-differences

Aaron foi uma das vozes fortes contra o Stop Online Piracy Act (SOPA), o projeto de lei contra a pirataria online proposto pelas poderosas empresas fonográficas, de cinema, juntamente com outros empreendimentos do setor de propriedade intelectual e direitos de autor. Mas não era só isso. O SOPA, de fato, iria endurecer as leis a tal ponto, que até mesmo mencionar um texto num blog poderia ser considerado um ato ilegal, estrangulando o direito à liberdade de expressão e o debate, assim como a criatividade.

Em suas atividades como pesquisador, Aaron, junto com Shireen Barday, "baixou" e analisou por volta de 440 mil artigos acadêmicos da área de Direito para determinar o tipo de financiamento que os autores receberam. Os resultados, publicados no *Stanford Law Review*, o levaram a trilhar os caminhos por onde seguiam os fundos públicos para pesquisa. Por causa de sua capacidade de processar grandes quantidades de dados era requisitado para colaborar com vários outros pesquisadores. Disto resultou o projeto *theinfo.org*, que chamou a atenção do Departamento de Justiça dos Estados Unidos. E aqui começa a saga que terminaria tragicamente.

O *theinfo.org* tornou livre e aberto o acesso a uma imensa base de dados públicos somente disponível gratuitamente através de máquinas instaladas em 17 bibliotecas em todo o país. As pessoas interessadas eram obrigadas a deslocar-se até os pontos de acesso ou, então, a pagar 10 centavos por peça. A base de dados oferecida pelo *theinfo.org* tem aproximadamente 20 milhões de páginas da Corte Federal, algo de tirar o fôlego. Aaron deixou muita gente brava com essa façanha, a ponto de tornar-se alvo de investigação pelo FBI – o que, contudo, não gerou consequências.

Mas a história foi bem diferente com o Massachusetts Institute of Technology (MIT). Ainda no Laboratório de Ética de Harvard, em 2011, Aaron usou o acesso aberto do MIT para coletar por volta de 4,8 milhões de artigos científicos, incluindo arquivos da base JSTOR, muito conhecida no mundo acadêmico. O caso passou a ser conhecido pelo público quando ele foi preso, em julho de 2011.

A controvérsia sobre este caso – houve grande debate sobre a ação de Aaron, se teria sido roubo ou não - foi substituída pelo debate sobre a cobrança por artigos científicos referentes a pesquisas financiadas com dinheiro público: um debate sobre a mercantilização e privatização do conhecimento científico, direitos de autor e os custos para tornar esses materiais disponíveis. Uma campanha de apoio a Aaron surgiu com força e o manifesto *Guerrilla Open Access*[8], escrito por ele em 2008, ganhou visibilidade outra vez.

Segundo a ONG Electronic Frontier Foundation, embora os métodos de Aaron fossem provocativos, os seus objetivos eram justos. Ele lutava para libertar a literatura científica de um sistema de publicação

8.Ver em http://archive.org/details/GuerillaOpenAccessManifesto. Uma tradução para o português está em http://www.laparola.com.br/aaron-swartz-e-o--manifesto-da-guerrilla-open-access

que tornava inacessível essa produção para a maior parte das pessoas que realmente pagaram por isso, quer dizer, todas as pessoas que pagam impostos. Essa luta deveria ser apoiada por todos.

As coisas começaram a tomar outros rumos com o declínio do debate nos meses seguintes. Após a devolução das cópias digitais dos artigos, a JSTOR decidiu não apresentar queixa contra Aaron. Mas a façanha, desta vez, resultou num processo por crime cibernético, levado adiante pelo governo dos Estados Unidos, municiado pelo MIT. Em seu desabafo, Lawrence Lessig escreveu:

> *Logo no início, para seu grande mérito, a JSTOR compreendeu que era "apropriado" desistir: eles declinaram a dar prosseguimento à sua própria ação contra Aaron e pediram ao governo para fazer o mesmo. O MIT, para sua grande vergonha, não foi claro, e então a promotora teve a desculpa que ela precisava para continuar sua guerra contra o "criminoso" que nós amamos e conhecemos como Aaron.*[9]

O Departamento de Justiça dos Estados Unidos interpretou a ação de Aaron como crime de roubo e a demanda foi levada ao grande júri, que decidiu que ele deveria ir a julgamento. Então, a máquina de fazer moer do governo começou a funcionar.

Primeiramente, Aaron foi acusado de quatro crimes - todos relativos à violação de sistema informático. Depois, o Departamento de Justiça, numa atitude de "exemplaridade", acrescentou mais nove acusações, todas contidas na Lei de Abuso e Fraude Informática, e atos de conspiração. Sem ver nenhuma oposição a esse acréscimo por parte de seus pares, a ira da promotora Carmen Ortiz ganhou uma proporção injustificada e desmesurada. A acusação de conspiração foi a cereja do bolo. Em uma sociedade marcada por recentes atos terroristas, conspirador é sinônimo de inimigo mortal da nação. Aclamada como uma promotora corajosa por enfrentar crimes de corrupção e de colarinho branco, Ortiz se voltou contra Aaron.

Inúmeras vozes vieram a público desmontar a acusação de Ortiz e explicar por que era injustificada. Entre essas vozes destaca-se a de Alex Stamos, especialista em crimes cibernéticos, que pacientemente revela a verdade sobre o "crime" em seu blog.[10] Stamos simplesmente explica por que nada do que foi imposto como acusação - seja o roubo, seja a invasão de computadores ou o mais estapafúrdio, a conspiração -, poderia ser imputado a Aaron. Mesmo tendo sido contratado para ajudar na defesa de Aaron, Stamos oferece seu currículo e biografia para afirmar que a análise que havia feito sobre o caso goza da necessária isenção legal e ética. Todos os itens analisados por Stamos tratam exclusivamente dos procedimentos técnicos utilizados por Aaron frente à arquitetura de rede do MIT. Ele explica que Aaron não invadiu a rede,

9. Ver em http://boingboing.net/2013/01/12/lessig-on-the-dojs-vindictiv.html 10. Ver em http://unhandled.com/2013/01/12/the-truth-about-aaron-swartzs-crime

simplesmente porque a rede é aberta a qualquer pessoa que esteja no campus, independentemente de ser aluno, docente ou funcionário do MIT.

Porém, o efeito cascata das acusações resultaram na possibilidade real de Aaron Swartz ser condenado a 35 anos de prisão e a pagar multa de um milhão de dólares![11] Afirmou Lawrence Lessig:

> *Aqui, é onde nós precisamos de um melhor sentido de justiça e de vergonha. O que é ultrajante nesta história não é apenas [o que aconteceu com] Aaron. É também o absurdo do comportamento da promotora. Bem desde o início, o governo trabalhou tão duro quanto pôde para caracterizar o que Aaron fez da forma mais extrema e absurda. A "propriedade" que Aaron "roubou", segundo nós fomos informados, valia "milhão de dólares" — com a dica, e então a sugestão, de que o seu objetivo era obter lucro com o seu crime. Mas qualquer um que diga que se pode ganhar dinheiro com um estoque de ARTIGOS ACADÊMICOS é idiota ou mentiroso. Estava claro que disso não se tratava, mas o nosso governo continuou a pressionar como se tivesse agarrado terroristas do 11/09 com a boca na botija.*

Não consigo imaginar o que se passou com esse rapaz de personalidade introvertida, apresentando um quadro de depressão, à medida que a data do julgamento se aproximava. Sua solidão, seu medo diante deste quadro kafkiano. Sua morte me pareceu, daqui de longe, uma forma de exílio — como o exílio do protagonista das tragédias gregas. A morte é a condenação ao exílio da República que não permite a existência dos poetas.

No sábado após a morte de Aaron, ainda sob o impacto do acontecimento, sua família fez um comunicado público, culpando as autoridades judiciais e o MIT. O documento afirma que essa morte não é apenas uma tragédia pessoal, mas sim "um produto de um sistema de justiça criminal repleto de intimidações", o qual iria punir uma pessoa por um alegado crime que não fez vítimas.

O funeral, realizado em 15 de janeiro, em Illinois, contou apenas com a família e pessoas muito próximas — mas ao redor do mundo foram realizados tributos em seu nome. Um memorial online foi construído: *aaronsw.com*. A comunidade ciberativista criou uma página web[12] com o objetivo de ser um grande e espontâneo repositório de produção acadêmica colocada à disposição de todas as pessoas de forma gratuita e aberta. Todas as pessoas são convidadas a disponibilizar ali seus trabalhos em qualquer idioma. No twitter, a *hashtag* *#pdftribute* ajudou a organizar as contribuições.

O JSTOR publicou suas condolências[13] imediatamente e o MIT anunciou[14] que vai investigar sua responsabilidade na morte de Aaron, mas este anúncio já não tem nenhum efeito.

11. Ver artigo na revista online Techdirt em http://goo.gl/2Z3hW 12. Ver em http://pdftribute.net 13. Em http://about.jstor.org/statement-swartz
14. Em http://www.theverge.com/2013/1/13/3873352/mit-announces-internal-investigation-into-its-role-in-aaron-swartz

Aaron Swartz

Ainda durante a perseguição da Dra. Carmen Ortiz, foi negado o pedido de revisão das acusações. Entretanto, com a mobilização de distintas vozes – comunidade acadêmica, ciberativistas, mídia alternativa, blogueiros, artistas, pessoas proeminentes etc. –, com a repercussão internacional após a morte de Aaron e com os tributos realizados em várias cidades dos Estados Unidos, a cena mudou. A morte de Aaron, ao que tudo indica, não terá sido em vão - uma luz no fim do túnel parece se acender.

Em fevereiro, ativistas da Internet e políticos de ambos partidos, Republicano e Democrata, acordaram reformar o Computer Fraud and Abuse Act em nome de Aaron Swartz. As emendas serão chamadas de Lei Aaron e têm como objetivo descriminalizar alguns dos artigos da Lei contra Fraude – prevenindo, deste modo, futuros processos contra pessoas que foram autorizadas a ter acesso à informação mas que utilizaram de meios atípicos para seu acesso. Parlamentares que tiveram a oportunidade de conhecer Aaron discursaram no Congresso Nacional e declararam que o acesso à informação deveria ser considerado um direito humano.

O mais difícil, no entanto, será rever as práticas acusatórias empregadas pelo Departamento de Justiça. As intimidações, o excesso das acusações e a pressão sobre o suposto criminoso a partir do uso das penalizações máximas é corrente em todo o país. Estas práticas são muito criticadas, mas sem êxito: se há críticas, há também apoio, tanto interno quanto externo. Essa será uma discussão de mais largo prazo.

Aaron não foi o primeiro caso de suicídio de um jovem hacker exageradamente acusado e intimidado pelo Departamento de Justiça. Jonathan James também cometeu suicídio[15], em 2008, aos 24 anos, em meio a uma acusação feita pelo Serviço Secreto dos Estados Unidos de que estaria envolvido com o caso TJX Hacker. Tanto Jonathan quanto Aaron sofreram intimidações da mesma pessoa, o Assistente da Promotoria Stephen Heymann.

Tim Wu, professor da Escola de Direito da Universidade de Columbia, levanta a questão de forma contundente: *Hoje, promotores pensam que eles têm permissão para tratar quem vaza informações como se fossem chefões do crime ou terroristas. Numa época onde nossas fronteiras são digitais, o sistema criminal ameaça algo intangível mas incrivelmente valioso. Ameaça o vigor juvenil, a perspectiva diferente, a liberdade de quebrar algumas regras e não ser condenado ou arruinado para o resto da vida. Swartz era um excêntrico impetuoso que podia ter sido um dos grandes inovadores e criadores de nosso futuro. Agora nós nunca saberemos.*[16]

15. Ver em http://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html
16. Ver em http://www.newyorker.com/online/blogs/newsdesk/2013/01/everyone-interesting-is-a-felon.html

:: E O QUE NÓS AQUI NO BRASIL TEMOS COM ISSO?

A Internet foi concebida como uma plataforma sem fronteiras físicas e territoriais. E quando ocorre um evento, triste ou alegre, seja onde for, que está relacionado ao âmago do funcionamento desse incrível sistema, isso nos interessa.
O aperfeiçoamento técnico da Internet e seu sistema regulatório são também de grande interesse de todos, sobretudo quando este aperfeiçoamento está relacionado com o acesso ao conhecimento e à informação, ao livre[17] exercício dos direitos civis e das liberdades individuais.

Em relação à produção científica, vale lembrar que o governo brasileiro tem tido uma participação importante na formação de uma cultura de acesso aberto e gratuito - embora de maneira, por vezes, contraditória.

Deixando as idiossincrasias de lado… a área de saúde é um bom exemplo de acesso aberto e compartilhado ao conhecimento com a instalação, no Brasil, da BIREME[18], em 1967 - cujo objetivo é contribuir com o desenvolvimento da saúde "fortalecendo e ampliando o fluxo de informação em ciências da Saúde". A partir dela, surgiu em 2002 o projeto Scielo[19], uma biblioteca eletrônica que abrange uma coleção selecionada de periódicos científicos brasileiros que se expande pela América Latina.

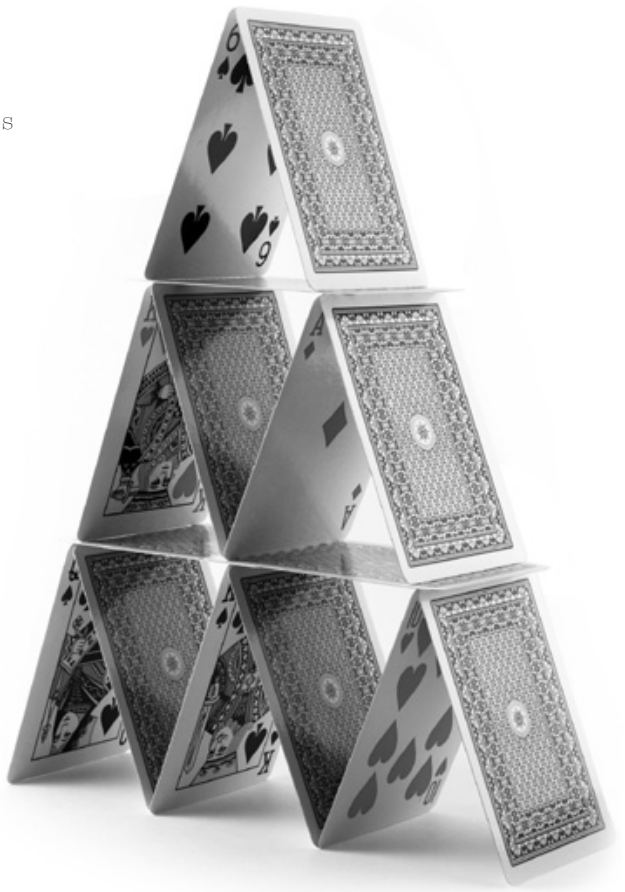
No início dos anos 2000, em consonância com a o debate global, é lançado o *Manifesto Brasileiro de Apoio ao Acesso Livre à Informação Científica*[20] com vários setores e órgãos do governo brasileiro entre os apoiadores da iniciativa.

Contudo, a sucessão de eventos desde a cópia dos milhares de artigos científicos até o processo judicial e o incremento da pena — resultando na absurda possibilidade de Aaron ser condenado a 35 anos de prisão mais multa — serve de alerta para a necessidade de nós mesmos repensarmos e revisarmos estrategicamente as recentes leis aprovadas no nosso Congresso Nacional sobre cibercrime. Também é o momento para refletirmos com mais atenção sobre a debilidade política e conceitual a que chegou o Marco Civil, e sobre os *imbroglios* com a lei de direito autoral[21]. Para este marco legal não há sinais de melhora por parte de Marta Suplicy.

Nós não estamos distantes de absurdos como o caso de Aaron! Em terras tupiniquins outros absurdos já acontecem por causa do uso excessivo, de um lado, das leis de difamação e persistência das leis de desacato[22] e, de outro, com a chamada proteção do direito de autor (*copyrights*). Um bom exemplo é a perseguição às copiadoras nas faculdades de todo o Brasil, utilizando-se força policial como na captura de criminosos - em um país onde livros são caros, onde não há incentivo para a reimpressão de obras raras ou esgotadas nem políticas que estimulem publicações a preços mais em conta. ●

17. Ver em http://regional.bvsalud.org/php/index.php 18. Ver em http://regional.bvsalud.org/bvs/bireme/P/mision.htm 19. Ver em http://www.scielo.br/scielo.php?script=sci_home&lng=pt&nrm=iso 20. Ver em http://www.ead.fiocruz.br/noticias/index.cfm?matid=25400 21. N.E.: Ver mais no artigo de Pablo Ortellado que abre esta edição da *poliTICs*. 22. Ver em http://artigo19.org/?cat=79

> **Jeferson Fued Nacif** Chefe da Assessoria Internacional da Agência Nacional de Telecomunicações



Uma análise da CMTI 2012

A política externa brasileira nos últimos anos, talvez desde a redemocratização, tem se pautado por grandes linhas de atuação sem que tenha apresentado grandes rupturas de um governo a outro, mas apenas ajustes de rumos. Por um lado, a estabilidade de posições do país concede previsibilidade de ações e confiança dos seus pares. Por outro, nem sempre consegue responder a novos desafios de uma agenda internacional cada vez mais dinâmica, complexa e de interesses multifacetados. O setor de Tecnologias de Informação e Comunicação é um dos temas da agenda internacional que vem oferecendo novos desafios à atuação diplomática brasileira.

O objetivo desse artigo é dar continuidade à discussão sobre a Conferência Mundial de Telecomunicações Internacionais (CMTI)[1] realizada em dezembro de 2012 em Dubai, nos Emirados Árabes Unidos, sob os auspícios da União Internacional de Telecomunicações (UIT)[2]. O texto abordará o processo preparatório e os resultados da Conferência sob a ótica da política externa brasileira e das políticas públicas e regulatórias de telecomunicações. Longe de querer esgotar as possibilidades de análise, é preciso inicialmente traçar um perfil atual da política externa brasileira que possa servir de balizamento para o entendimento

1. Ver http://www.itu.int/en/wcit-12/Pages/default.aspx 2. Ver http://www.itu.int/en/Pages/default.aspx

com relação à CMTI. Em seguida, busca-se delinear os principais objetivos da delegação brasileira liderada pela Agência Nacional de Telecomunicações (Anatel). Por fim, o texto envereda por algumas percepções acerca da dinâmica das negociações e seus possíveis resultados.

:: A POLÍTICA EXTERNA BRASILEIRA E O SETOR DE TELECOMUNICAÇÕES

Às linhas tradicionais de atuação da política externa brasileira - como a defesa do princípio da não intervenção e da solução pacífica de controvérsias; a preferência pelo diálogo e pelo multilateralismo –, pode-se somar a busca por uma governança internacional mais legítima e eficaz; a inequívoca prioridade à integração sul-americana, assim como a intensificação das relações com os países da América Latina; o fortalecimento das relações com os países em desenvolvimento – principalmente no âmbito dos grupos Brasil, Rússia, Índia, China e África do Sul (BRICS)[3] e Índia, Brasil e África do Sul (IBAS)[4]. Todos estes critérios estão aliados à atuação que prima pela não indiferença com relação a países que mais necessitam de ajuda humanitária, assolados pela pobreza, conflitos armados ou desastres naturais.

Uma característica adicional do Brasil nos foros internacionais é que o país não se intimida na exposição de suas convicções nem se esconde diante da relutância dos demais países em expor-se na cena internacional, seja por temer a reprovação de pares mais poderosos ou por fragilidades de legitimidade interna. A firmeza das posições externas do Brasil está expressa tanto pelo crescimento recente da economia brasileira e pela estabilidade de suas instituições, quanto pela certeza de esmerados processos internos de preparação substantiva, ampliados a diversos atores da sociedade. É nesse sentido que trabalha a Anatel[5] nos foros internacionais de telecomunicações, principalmente nas conferências e assembleias da UIT e da Comissão Interamericana de Telecomunicações (Citel)[6]. As posições adotadas pela Anatel estão sempre consubstanciadas pela política externa brasileira, refletindo posicionamento autônomo, vocacionado ao diálogo e ciente de que assuntos de natureza estratégica devem ser amplamente debatidos no plano interno a fim de externar reflexos mais próximos dos anseios nacionais.

Pode-se afirmar que o Brasil alterou seu status de participação nos foros internacionais ao longo dos últimos anos. Conquistando espaço no cenário internacional pelo vigor de suas instituições democráticas, pela estabilidade econômica e força de suas convicções diplomáticas, o Brasil pôde passar de ator refratário às mudanças a proponente das mudanças; de potência de veto a parceiro estratégico nas organizações internacionais. Como resultado desse capital político e de longos

3. Ver http://pt.wikipedia.org/wiki/BRICS 4. Ver http://www.itamaraty.gov.br/temas/mecanismos-inter-regionais/forum-ibas
5. Ver http://www.anatel.gov.br 6. Ver https://www.citel.oas.org/en/Pages/default.aspx

anos de participação nos foros internacionais de telecomunicações, a Anatel oferece contribuições de relevo nas organizações internacionais em que participa, sempre na busca de soluções construtivas e pragmáticas para problemas reais que afetam a comunidade internacional das telecomunicações.

O rápido passo das tecnologias nos obriga a buscar reformas constantes nas instituições de concertação técnica internacional, sob o risco de a obsolescência e o vagar dos entes multilaterais, (muitas vezes centenários), arrefecer o ritmo de cooperação e o fluxo de informações tão almejado entre reguladores. Compreendendo esses novos desafios, a Anatel vem apresentando propostas que visam a garantir maior abertura e transparência dos processos decisórios na UIT, como as de acesso gratuito às Recomendações e demais documentos online, e ainda em prol da abertura dos relatórios financeiros.

No que diz respeito à atuação em foros multilaterais, compreende-se hoje que nossas vozes serão mais ouvidas quanto mais estivermos coordenados no plano multilateral. Longe de aceitação irrestrita de teses destoantes dos objetivos nacionais, o que se deseja é a busca coordenada pelo consenso de forma estratégica. Assim, a Anatel atua para ampliar o relacionamento frutífero que tem com diversos países, aproveitando as bases de diálogo estabelecidas em alto nível pelos condutores da política externa brasileira, especialmente com os países da América Latina, Estados Unidos, Índia, China, Rússia, África do Sul, Japão - com vistas à consecução de interesses comuns.

Num mundo cada vez mais plural, também as decisões de política externa não se restringem ao nível burocrático estatal, incorporando visões de diversos atores da sociedade. Ao passo que democratiza o processo por ampliar a capacidade de articulação com a sociedade, o governo busca chegar aos foros internacionais com uma visão ampla e coesa em defesa de seus interesses nacionais. Nesse escopo, a Anatel, por meio das Comissões Brasileiras de Comunicações (CBCs)[7] incentiva e estimula o engajamento de diversos atores a contribuir para a projeção do país no cenário internacional e, por meio dela, desenvolver o mercado nacional de telecomunicações. As reuniões de preparação para as Conferências de Dubai realizadas pela Anatel reiteram e renovam a disposição de trabalhar de forma aberta e transparente.

As contribuições levadas pelo Brasil, coordenadas pela Anatel, não apenas são fruto de um amplo processo de discussão com a sociedade, como são um reflexo de maturidade do país nos foros internacionais de telecomunicações.
A experiência confirma a tese de que ambições exageradas na construção de posicionamentos externos são geralmente rechaçadas em negociações multilaterais. A construção de novos consensos é tarefa que demanda tempo e uma gama de argumentos poderosos.

7. Na Anatel, as Comissões Brasileiras de Comunicações (CBCs) são responsáveis por coordenar a atuação dos delegados brasileiros nos foros internacionais de telecomunicações. Mais informações no site www.anatel.gov.br

:: A CMTI 2012

Alardeada como a conferência que permitiria aos governos controlarem a Internet, a Conferência Mundial de Telecomunicações Internacionais 2012 de fato passou ao largo das projeções alarmistas sobre o futuro da rede mundial de computadores. Embora para grande parte da mídia, analistas e países não signatários a presença de uma resolução sobre Internet ao final tenha efetivamente trazido tais receios para o texto dos Regulamentos de Telecomunicações Internacionais (RTIs ou, em inglês, ITRs) e comprometido todos os artigos do Tratado intensamente negociados em Dubai, os Atos Finais da Conferência demonstram que a Internet como a conhecemos não sofreu qualquer arranhão em função dos resultados de Dubai.

O Brasil sempre entendeu que a realização dessa Conferência, assim como de outras Conferências da agenda internacional, somente valeria a pena se seu escopo englobasse questões relevantes do setor de telecomunicações, em que fosse possível atacar problemas reais que demandem atuação, gestão e solução globais. Dessa forma, assuntos como segurança, spam, fraude, interconexão, *roaming* internacional, tributos, precisariam ser abordados e profundamente discutidos, sob pena de chegarmos, vinte e cinco anos depois dos ITRs de 1988, com um tratado semelhante a uma declaração de princípios já consagrados.

Os resultados alcançados, no entanto, não são motivo de pleno regozijo nem para a UIT nem para os signatários. Para o Brasil idem, embora o país tenha conseguido incluir nos ITRs suas visões estratégicas e principais questões práticas - como *roaming* internacional, pontos de troca de tráfego e o princípio da rejeição à bitributação nos pagamentos internacionais de tráfego. Restou a todos o sentimento de que a intransigência venceu o consenso em pontos importantes da agenda internacional de telecomunicações e que se foram os contornos antes exclusivamente técnicos da UIT. Dubai deixou claro também que a agenda internacional de telecomunicações se submete a complexidades das agendas de política interna e externa dos países. Tal afirmação parece óbvia, mas nunca na UIT tais agendas haviam ficado tão explícitas quanto nessa Conferência.

Ao mesmo tempo, EUA e Europa, principais defensores da não adoção do Tratado, também saíram vitoriosos, uma vez que seus principais itens de interesse não foram substancialmente tratados ou alterados: o respeito aos direitos humanos foi incluído; há parágrafo assegurando que o tratado não se refere a conteúdo; segurança e spam possuem artigos próprios, mas suas redações estão longe de modificarem o status quo internacional; a palavra "Internet" não é mencionada em nenhum artigo; na definição de *Operating Agency* (OA) – motivo de grande obstrução por parte da delegação norte americana - restou claro que tais entidades não se confundem com as empresas de conteúdo da Internet, em geral não reguladas pelos Estados-membros e, portanto, afastadas do âmbito de aplicação do Tratado.

A divisão entre países signatários e não signatários durante a revisão dos ITRs era esperada, tendo em vista a não disposição de EUA e países europeus de negociarem qualquer revisão substancial do tratado, já exposta na Conferência de Plenipotenciários da UIT de 2010.

O fato de ter havido em Dubai uma nítida fragmentação dos países em dois grandes blocos é ainda mais relevante no ambiente da UIT – acostumado às decisões por consenso e razoável nível de acomodação de interesses. Os negociadores enfrentaram diversos momentos de impasse - sendo que em duas ocasiões as divergências só foram resolvidas por voto. Apesar de ser o voto um mecanismo legítimo e usual em qualquer reunião plenária, o fato de se ter utilizado desse mecanismo para solucionar impasse com relação à Resolução 3 sobre Internet e sobre o artigo 5º (segurança e spam) aflorou as divisões que já se faziam perceptíveis. Transpondo tais textos para ambiente de negociação de recomendações, opiniões ou resoluções - *soft law* – e não em nível de tratado como os ITRs, tais textos teriam sido aprovados com relativa facilidade. Vale lembrar ainda que a não adesão de governos a tratados negociados em âmbito multilateral é prática rotineira e que reflete, no mais das vezes, não apenas clivagens ideológicas, mas também importantes divisões econômicas.

Apesar de os signatários somarem 89 países, aqueles que não assinaram o tratado respondem por grande parte do mercado internacional de telecomunicações - o que compromete a efetividade do documento. No momento observa-se movimentação diplomática em dois sentidos opostos. Um lado, o dos signatários, tenta convencer os países que ainda não assinaram a completarem suas consultas internas e acederem ao tratado. Os países contrários aos ITRs por sua vez buscam disseminar suas razões da recusa aos que estão em consultas - e mesmo sobre aqueles que já assinaram, mas que demandam processo de ratificação, como é o caso do Brasil.

A multiplicação dos motivos de impasse alegados por alguns blocos foram sendo compreendidos como estratégia deliberada de recomposição ao objetivo inicial de não assinar o tratado, quaisquer que fossem seus resultados finais. Sob essa ótica, EUA e Europa teriam cumprido melhor papel se tivessem obstado a realização da CMTI já em 2010, ou nem participado das reuniões preparatórias. Mas, o que ficou demonstrado em diversas reuniões preparatórias foi que ambos trabalhariam para que a conferência chegasse a bom termo. Durante a Conferência, no entanto, causou surpresa o posicionamento de que a simples menção a determinados termos colocaria em risco toda a Conferência, inclusive termos de telecomunicações habitualmente usados nas reuniões da UIT.

A polarização ficou mais explícita em Dubai em função das discussões globais sobre a governança da Internet num momento em que tais temas voltam à cena internacional com a proximidade da revisão da Cúpula Mundial da Sociedade da Informação (CMSI).

É sabido que a UIT, com a ascensão inequívoca e irrevogável da Internet, vem buscando se afirmar como um dos foros relevantes na definição de padrões relacionados à Internet ou nas discussões políticas sobre Internet. Se nos temas relacionados à coordenação de frequências e órbitas a UIT é a organização líder no mundo, nos temas relacionados à Internet – e também em diversos assuntos mesmo de telecomunicações, como tecnologias móveis – tal liderança não acontece, estando os principais foros disseminados em diversos grupos e entidades privadas especializadas como a ICANN, o IETF, W3C, 3GPP.

Assim sendo, vem cabendo à UIT apenas a tentativa de buscar espaço de discussão sobre políticas públicas relacionadas à Internet. E mesmo assim, verifica-se que o caminho a ser trilhado para alcançar esse objetivo ainda é longo e pode nunca se concretizar. A UIT é, no máximo, instância de reverberação dos interesses de governos alijados dos domínios de deliberação da Internet, em níveis técnicos e políticos, assim como diversas outras instâncias, como o Fórum de Governança da Internet (IGF), a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (Unesco), a Comissão de Ciência e Tecnologia para o Desenvolvimento (CSTD) do Conselho Econômico e Social das Nações Unidas (a ECOSOC/ONU).

Os problemas de Dubai não estavam no texto do tratado. Foram diversas as ocasiões em que os representantes manifestaram conforto com artigos alcançados. As votações realizadas, de forma rápida, mas dentro do arcabouço legal da UIT, sobre a Resolução 3, "*Fostering an Enabling Environment for the Internet*" e sobre segurança, não foram o motivo real de descontentamento das delegações que ao final não aceitaram os ITRs. O fato de não ter sido possível discutir tais temas com a profundidade necessária – o que demandaria muito mais tempo – e que acabou levando ao dissenso, pode ser entendido como um dos agravantes. E, ainda que as votações formais tivessem ocorrido, o resultado não seria diferente.

Ademais, a resolução não é parte dos ITRs, não é de caráter vinculante e apenas repete linguagem já adotada nas Cúpulas Mundiais da Sociedade da Informação realizadas em Genebra e Túnis. O que a resolução diz apenas é que os países desejam continuar discutindo os aspectos relacionados às políticas públicas da Internet e que a UIT representa um desses foros de discussão. Caberia analisar, portanto, quais as repercussões negativas sobre a atual gestão da rede que impediriam tantos países de adotarem os ITRs simplesmente por causa de resolução que nada traz de novo a respeito do tema.

É possível analisar a fratura em Dubai também como fruto de uma radicalização de posições diante da recusa inicial dos Estados Unidos de negociarem qualquer assunto que se relacionasse diretamente à Internet, à governança da Internet, segurança ou spam, evitando a qualquer custo que essas palavras aparecessem no texto. À posição norte-americana de excluir qualquer menção a tais temas no Tratado, seguiu-se uma forte reação de Rússia e países árabes, principalmente, em tentar incluir

todos os temas mais sensíveis dessa agenda, como segurança cibernética, controle governamental dos espaços da Internet, gestão estatal das redes de telecomunicações, expressa em contribuição que poderia inclusive ter sido aprovada caso fosse levada a voto. Diante de posições extremadas, a Resolução ora aprovada significou alternativa negociadora razoável, de fácil comprometimento entre os atores e reduzida abrangência. Insuficiente, porém, para atender aos interesses de muitos países.

É importante salientar o papel que vêm desempenhando os grupos de pressão nas sociedades democráticas. Meses antes da realização da Conferência, disseminou-se a partir dos EUA, principalmente nos meios empresariais e na sociedade civil, a ideia de que os ITRs serviriam para que os governos controlassem a Internet. Ledo engano. Imaginar que os ITRs forneceriam sustentação para redirecionar todo o atual sistema de governança da Internet foi um exagero. Acreditar nesse fato é desconhecer o sistema de governança da Internet, o processo de negociação de um organismo do sistema das Nações Unidas e as regras básicas do Direito Internacional Público. Apesar disso, a manobra serviu bem aos que tinham interesse em associar todas as discussões com liberdade de expressão, livre iniciativa e governança da Internet. O que restou, portanto, aos olhos do público em geral, foi a imagem de que aqueles que assinariam o tal tratado representariam a face autoritária no sistema internacional.

O movimento "*please stand for a free and open Internet*", coordenado pela americana Google,[8] talvez tenha ganhado dimensão maior do que o esperado e até mesmo constrangido as delegações norte-americana e europeia, que sentiram ser impossível firmar os Atos Finais. Ao temor das empresas provedoras de conteúdo da Internet se somaram os apoios de inúmeros cidadãos e dos parlamentos desses países, o que reduziu a margem de manobra dos representantes desses governos.

Uma análise possível seria entender parte dos resultados como falhas de construção do processo negociador iniciado há anos pela UIT e construído de forma débil até Dubai. Embora a possibilidade de realização da CMTI venha sendo discutida desde os anos noventa e finalmente aprovada sua realização na Conferência de Plenipotenciários de Guadalajara em 2010, o processo de discussão levado a cabo pela UIT padeceu de três falhas cruciais:

- A primeira falha foi não ter realizado uma conferência preparatória aos moldes da Reunião Preparatória da Conferência (CPM) que ocorre um ano antes da Conferência Mundial de Radiocomunicações (CMR). Se uma Conferência preparatória como essa tivesse sido planejada teria sido possível tratar de temas sensíveis e buscar consenso no período subsequente.
- A segunda falha foi ter baseado todo o processo negociador prévio em reuniões de caráter

8. https://www.google.com/takeaction/ Consulta no dia 25/01/2013 informava que 3.122.199 vozes apoiavam o movimento.

meramente informativo em Genebra. Não se aproveitou o tempo dos negociadores para já nas reuniões preparatórias abordar sensibilidades e assim criar consensos mínimos. Dessa forma, doze dias em Dubai não poderiam ser suficientes para lidar com a diversidade de temas e interesses.

· A terceira falha foi não ter dado início a um processo de abertura de documentos em discussão para participação ampla de todos os interesses, principalmente os da sociedade civil. Apesar de ser uma das organizações em que participação ampliada é comum, mormente da indústria de telecomunicações, a UIT ainda carece de mecanismos adequados de participação de atores não estatais e não empresariais. Como consequência, o custo para a UIT e para a Conferência foi excessivo, pois a imagem que foi passada para o público em geral – graças também a uma forte campanha de empresas norte-americanas – foi de que a UIT era uma instituição retrógrada em defesa de uma indústria em decadência.

Para o Brasil, apesar de ganhos substanciais com os ITRs, quando o assunto é governança da Internet há que se buscar aprimoramento das estratégias:

· Primeiro, o governo brasileiro, em conjunto com a sociedade, precisa urgentemente definir seus interesses relativos à Internet e estabelecer uma estratégia clara de atuação nos foros internacionais que levem em consideração as possibilidades reais de ganhos políticos, econômicos e tecnológicos.

· Segundo, a UIT pode e deve ser parte integrante de qualquer uma das opções que se queira redesenhar quanto ao futuro das negociações sobre Internet, tendo em vista que se constitui como o foro mais especializado da ONU para as TICs, por contemplar participação multissetorial e apresentar processo negociador com regras claras e conhecidas.

· Terceiro, o Brasil deve usar seu vigor diplomático para disseminar suas teses e construir parcerias que abranjam uma ampla gama de países. Verifica-se atualmente que poucos são os países que realmente conhecem os temas relacionados à Governança da Internet e que fazem valer suas opiniões nos foros internacionais. Ainda, alguns desses países que buscam as mudanças em determinados aspectos da governança da Internet não são compreendidos como democracias reconhecidas, o que dificulta o diálogo do governo brasileiro com seus pares e mesmo no plano interno.

À guisa de conclusão, podemos considerar que os ITRs representam avanços significativos para o ambiente internacional das telecomunicações, mas que seu sucesso está obviamente atrelado à possibilidade de ampliação do universo de signatários. Para os países em desenvolvimento, como o Brasil, a ausência de consenso nos pontos aqui levantados e os erros do processo de construção do Tratado levaram à perda de um momento histórico e de possibilidades de ganhos mais efetivos. Assuntos relevantes foram mastigados intensamente com vistas à construção de um consenso que, ao final, foi trocado por formulações insustentáveis sobre governança da Internet e temores infundados sobre segurança e proteção do conteúdo online. ●

O Instituto Nupef é uma organização sem fins de lucro dedicada à reflexão, análise, produção de conhecimento e formação, principalmente centradas em questões relacionadas às Tecnologias da Informação e Comunicação (TICs) e suas relações políticas com os direitos humanos, a democracia, o desenvolvimento sustentável e a justiça social.

Além de realizar cursos, eventos, desenvolver pesquisas e estudos de caso, o Nupef edita a poliTICs, a Rets (Revista do Terceiro Setor) e mantém o projeto Tiwa – provedor de serviços internet voltado exclusivamente para instituições sem fins lucrativos – resultado de um trabalho iniciado há 21 anos, com a criação do Alternex (o primeiro provedor de serviços internet aberto ao público no Brasil). O Tiwa é um provedor comprometido prioritariamente com a privacidade e a segurança dos dados das entidades associadas; com a garantia de sua liberdade de expressão; com o uso de software livre e de plataformas abertas não-proprietárias.

instituto nupef

Rua Sorocaba 219, 501 | parte | Botafogo | CEP 22271-110 | Rio de Janeiro | RJ | Brasil
Telefone/fax +55 (21) 3259-0370 | www.nupef.org.br