www.nupef.org.br

instituto nupef

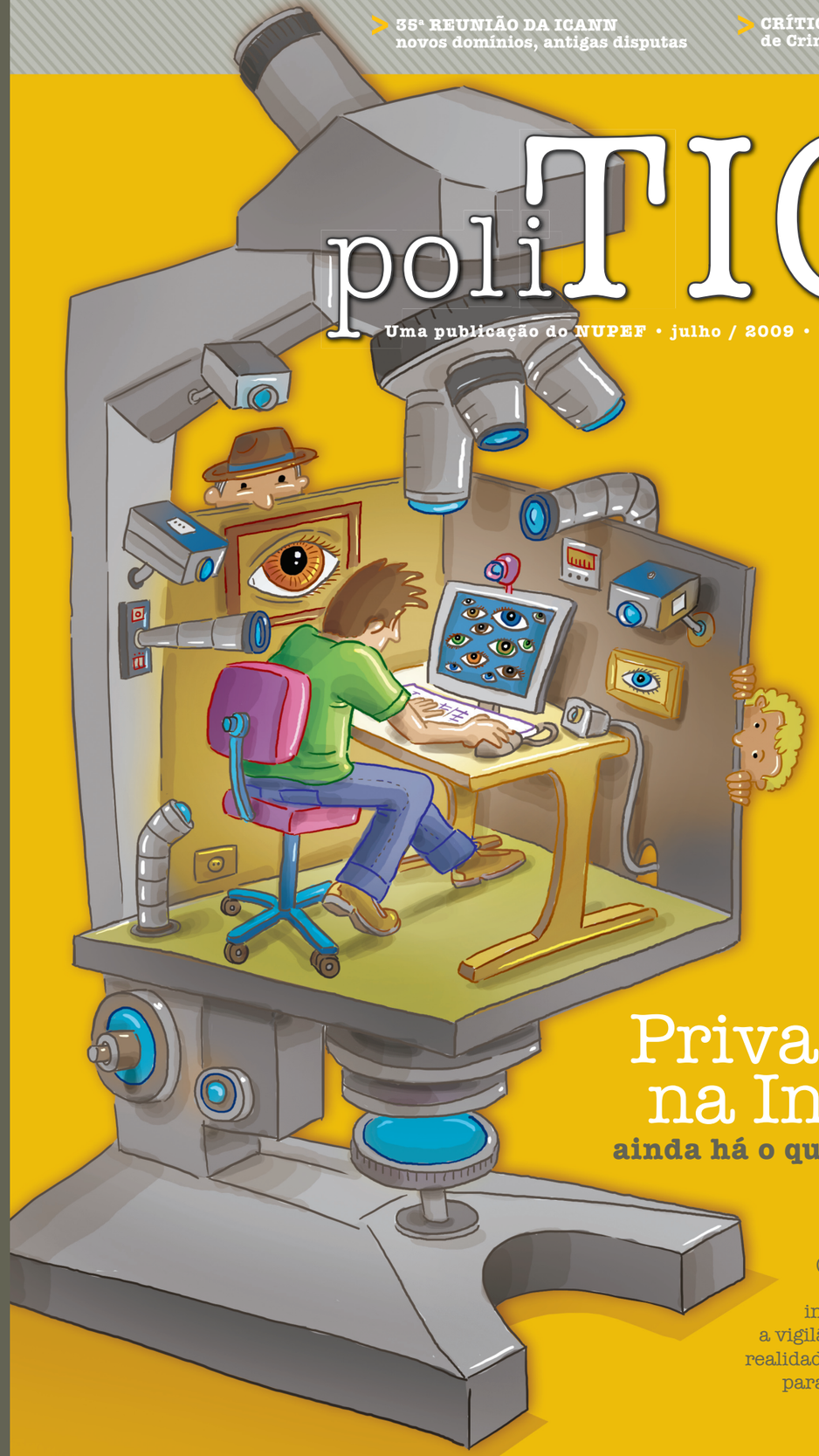
Rua do Ouvidor, 90 | 903 | Centro | 20040-030 | Rio de Janeiro RJ Brasil | telefone +55 21 3553-6809

> 35ª REUNIÃO DA ICANN
novos domínios, antigas disputas

> CRÍTICAS AO PROJETO DE LEI
de Crimes Informáticos

poliTICs

Uma publicação do NUPEF • julho / 2009 • www.politics.org.br



:: DO PANÓPTICO
AO BIG BROTHER
as políticas públicas
que faltam no Brasil

:: REGISTRO DE LOGS,
PROVEDORES
e os equívocos do
"Projeto Azeredo".

:: PRIVACIDADE NA
ERA DA PERSISTÊNCIA
a sociedade que
nossos netos herdarão

Privacidade na Internet

ainda há o que resguardar?

Entre iniciativas de governos, práticas (algumas controversas) de mercado e a falta de informação dos cidadãos, a vigilância na Internet é uma realidade - opaca, mas presente para todos que usam a Web.

poliTICs nº4

Índice

poliTICs

COORDENAÇÃO DO PROJETO GRACIELA SELAIMEN
EDITORES GRACIELA SELAIMEN, CARLOS A. AFONSO
CAPA, PROJETO GRÁFICO E DIAGRAMAÇÃO MONTE DESIGN
ILUSTRAÇÕES DE CAPA E PÁGINA 2 AXEL SANDE
SÍTIO WEB PAULO DUARTE
DISTRIBUIÇÃO SIMONE HUMEL

Esta é uma publicação do Instituto Nupef – Núcleo de Pesquisa, Estudos e Formação.
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@rits.org.br

instituto nupef
Rua do Ouvidor, 90 | 903 | Centro | 20040-030
Rio de Janeiro RJ Brasil | telefone +55 21 3553-6809

Apoio:
FORD FOUNDATION
Strengthen democratic values, reduce poverty and injustice, promote international cooperation and advance human achievement

Os originais foram compostos com OpenOffice 2.0 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 é em grande parte motivada pela intensa mobilização – que envolve principalmente ativistas, técnicos, acadêmicos e especialistas em Direito e Internet – em torno do Projeto de Lei de Crimes Informáticos, também conhecido como projeto Azeredo. Este projeto de lei é uma das iniciativas em curso no Brasil que defende o vigilantismo na Internet em nome de uma almejada "segurança" - uma argumentação que não é exclusividade dos legisladores brasileiros, mas sim repetição de uma retórica largamente utilizada em muitos países do mundo em nome da luta contra o terror, contra o cibercrime, contra a pirataria... e a favor de quem?

O texto de Bruce Schneier que abre esta edição desenha, de maneira contundente, que tipo de sociedade estamos construindo com a produção desenfreada de dados e com sua coleta, uso e armazenamento aparentemente ilimitados. Ariel Foina, por sua vez, instiga-nos a pensar de forma crítica sobre como o sistema legal brasileiro trata o tema do direito à privacidade e as práticas cada vez mais comuns de retenção e processamento de dados pessoais.

O artigo de Túlio Vianna analisa três artigos do projeto Azeredo que o autor considera mais polêmicos e oferece soluções à redação do legislador – equivocada, na visão do articulista. Carlos Afonso e Demi Getschko apresentam uma perspectiva importante, muitas vezes não explorada em profundidade nos debates sobre o projeto Azeredo: a questão da retenção de dados por parte de provedores de conteúdo e de acesso à Internet em função dos aspectos técnicos e comerciais da operação deste tipo de serviço.

As disputas políticas na ICANN – que também envolvem o direito à privacidade, mas abrangem, além disso, outros temas críticos para a defesa de uma Internet livre, com espaços de governança transparentes e democráticos – é o tema do artigo de Flávio Rech Wagner. Por fim, fechando este número da poliTICs, um artigo de minha autoria tenta mostrar como as práticas de vigilância e invasão da privacidade não são exclusividade de governos ou de legisladores – inúmeras empresas e prestadores de serviço na Web usufruem da coleta sistemática dos dados pessoais de seus usuários – que, em sua maioria, consentem inadvertidamente com estas práticas, em troca de facilidade, rapidez, relacionamentos online ou de uns gigabytes a mais para suas mensagens de correio.

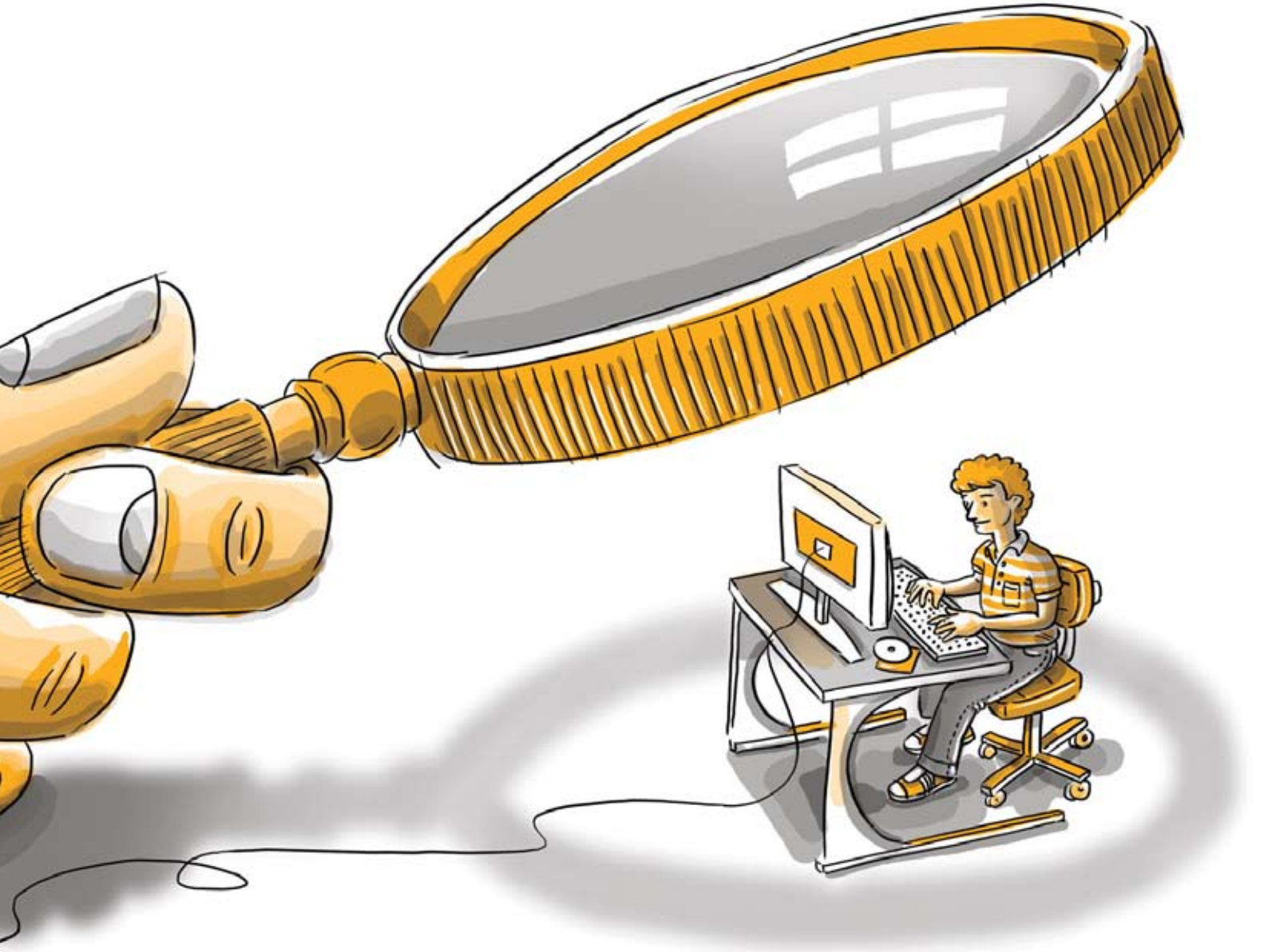
▶ Esperamos que você aprecie a leitura, escreva, comente! – o espaço está aberto em **www.politics.org.br**

Um abraço,

Graciela Selaimen – *Editora da poliTICs*

Bruce Schneier
diretor de Tecnologia da Segurança, British Telecom (BT)

Privacidade na Era da Persistência



Sejam bem vindos ao futuro, onde tudo que existe a seu respeito é "salvo". Um futuro onde suas ações são registradas, seus movimentos rastreados e suas conversas deixam de ser efêmeras. Um futuro trazido a você não por alguma distopia ao estilo 1984, mas pelas tendências naturais dos computadores para a produção de dados.

Dados são a poluição da era da informação. Trata-se de um subproduto natural de cada interação mediada por computadores. Eles ficam por aí para sempre, a menos que sejam descartados. São valiosos quando reutilizados, o que deve ser feito com cuidado. Caso contrário, seus efeitos posteriores são tóxicos.

E assim como há cem anos as pessoas ignoravam a poluição, na azáfama de construírem a Era Industrial, hoje ignoramos os dados na azáfama de construirmos a Era da Informação.

Deixamos cada vez mais rastros de pegadas digitais em nosso cotidiano. Antigamente, você entrava numa livraria e comprava um livro pagando em dinheiro vivo. Agora você visita o sítio web da Amazon e todas as suas compras ficam gravadas, inclusive o histórico da navegação. Você comprava o bilhete do trem com moedinhas; agora o cartão eletrônico de ingresso é vinculado à sua conta bancária. Os cartões de fidelidade das lojas lhe dão descontos; os comerciantes usam os detalhes ali registrados para formular seu perfil de compras e consumo.

Dados a seu respeito são coletados sempre que você dá um telefonema, envia uma mensagem de email, usa um cartão de crédito, ou visita um sítio na Internet. Os documentos de identidade digitalizados só exacerbam tudo isso.

Há cada vez mais sistemas computadorizados nos vigiando. As câmeras chegam a ser ubíquas em algumas cidades e há de chegar o dia em que as tecnologias de identificação facial serão capazes de identificar todo e qualquer indivíduo. Aparelhos para varredura de placas de veículos já rastreiam automóveis em alguns estacionamentos e cidades. Impressoras a cores, câmeras digitais e algumas fotocopiadoras trazem embutidos códigos de identificação. Sistemas de vigilância aérea são usados para evitar infrações no acesso a certos prédios e também para informar, com vistas a atividades de marketing, o tamanho dos jardins e das casas. À medida em que forem se tornando mais comuns, os chips de identificação por rádiofrequência (RFID) também serão rastreados. Trata-se de uma vigilância por atacado; não é mais a situação de "siga aquele carro" mas sim de "siga todos os carros".

Os computadores também andam mediando conversas. Face a face, elas são efêmeras. Há alguns anos, as companhias telefônicas talvez já pudessem dizer para quem você telefonou ou quanto tempo durou a conversa, mas não o que foi dito. Hoje você bate um papo por email, através de mensagens de texto, ou em sítios web de redes sociais, faz o seu blog ou interage pelo Twitter. Essas conversas com colegas, amigos e familiares, também podem ser gravadas e armazenadas.

Antigamente era caro demais gravar e guardar ("salvar") todos esses dados, mas a memória do computador hoje é mais barata.

> A privacidade não é só uma questão de ter algo a esconder; trata-se de um direito básico com um valor enorme para a democracia, a liberdade e nossa humanidade

A capacidade de processamento também; cada vez mais dados têm referência cruzada e são correlacionados para uso posterior com propósitos secundários. O que era efêmero agora é permanente.

Quem vai coletar e usar esses dados é algo que depende das leis de cada lugar. Nos EUA, as empresas coletam, depois compram e vendem muitas dessas informações para usar em ações de marketing. Na Europa, os governos coletam mais que as empresas. Em ambos os continentes, as autoridades encarregadas do cumprimento das leis querem acesso à quantidade máxima possível de informações, com vistas a investigações e mineração de dados *(data mining)*.

Em qualquer que seja o país, cada vez mais organizações coletam, armazenam e compartilham dados em volumes crescentes.

E vem mais por aí. Programas e dispositivos de registro da digitação em teclados (*keyboard logging*) já podem guardar todas as sequências das teclas que você aciona; daí a gravar tudo que você diz no telefone celular é uma questão de poucos anos.

O *life recorder*, aparelho que se prende à lapela para gravar tudo que você vê e ouve na sua vida, não fica muito atrás. Será vendido como dispositivo de segurança para que ninguém possa atacá-lo sem que isso fique registrado. Quando isso acontecer, deixar de usar um "gravador da vida" poderá ser considerado evidência de que a pessoa não estava para bons amigos, assim como os promotores já usam o fato de alguém ter deixado o telefone celular em casa como evidência de que não queria ser rastreado?

Estamos vivendo tempos únicos na história: a tecnologia está aí, mas ainda não é impecável. Verificações da nossa identidade são coisas comuns, mas ainda precisamos apresentar a cédula. Em breve, isso vai acontecer automaticamente, tanto pela averiguação remota de um chip na carteira ou pelo reconhecimento do rosto capturado por uma câmera. E todas essas câmeras, agora visíveis, vão encolher ao ponto de não serem mais visíveis. As conversas efêmeras vão praticamente desaparecer e vamos achar isso a coisa mais normal do mundo. Nossos filhos já vivem a vida muito mais em público do que nós. Seu futuro não tem privacidade, não por uma tendência dos governos funcionarem como estado-polícia ou por prevaricação de alguma empresa, mas sim porque os computadores naturalmente produzem dados.

Como bem disse o Cardeal Richelieu: "Se me dessem seis

linhas escritas pelo mais honesto dos homens, eu ali encontraria algo que o levasse à forca." Quando todas as suas palavras e ações podem ser guardadas para um exame posterior, as regras a se aplicar devem ser diferentes.

A sociedade funciona exatamente por ser a conversa algo efêmero; pois as pessoas se esquecem, e não precisam justificar cada palavra que proferem.

Conversa não é a mesma coisa que correspondência. Palavras ditas com pressa ao café da manhã, sejam elas faladas numa lanchonete ou digitadas no minúsculo teclado de um BlackBerry, não são correspondência oficial. Um padrão de dados que indique "tendências terroristas" não pode substituir uma investigação de verdade. O escrutínio constante da vida das pessoas acaba minando as normas sociais; além do que, é de arrepiar.A privacidade não é só uma questão de ter algo a esconder; trata-se de um direito básico com um valor enorme para a democracia, a liberdade e nossa humanidade.

Não vamos parar a marcha da tecnologia, assim como não podemos desinventar o automóvel ou o forno a carvão. Passamos a era industrial nos aproveitando dos combustíveis fósseis, que poluíram o ar e transformaram o clima. Agora tratamos de lidar com as consequências (enquanto ainda usamos os ditos combustíveis fósseis, é claro). Desta feita, talvez consigamos ser um pouco mais proativos.

Assim como olhamos para o início do século anterior e balançamos a cabeça ante a ignorância geral sobre o que a poluição causava, as gerações futuras olharão para nós que vivemos as primeiras décadas da era da informação e julgarão as soluções que demos para a proliferação de dados.

Precisamos, todos juntos, começar a discutir essa grande mudança da sociedade e seu significado. E precisamos dar um jeito de criar um futuro do qual nossos netos sintam orgulho. ●

//PARA SABER MAIS

- Este ensaio foi publicado originalmente no site BBC.com. http://news.bbc.co.uk/1/hi/technology/7897892.stm
- Recursos adicionais: National ID cards ("Cédulas de identidade nacionais"): http://www.schneier.com/essay-160.html
- Surveillance cameras ("Câmeras de vigilância"): http://www.schneier.com/essay-225.html
- RFID chips ("Identificação por rádio-freqüência"): http://epic.org/privacy/rfid/
- Cell phone surveillance ("Vigilância dos telefones celulares"): http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127462 or http://tinyurl.com/au2f4n
- Wholesale surveillance ("Vigilância por atacado"): http://www.schneier.com/essay-147.html
- Data mining ("Mineração de dados): http://www.schneier.com/essay-108.html
- The future of surveillance ("O future da vigilância"): http://www.schneier.com/essay-109.html
- Face recognition ("Reconhecimento facial"): http://epic.org/privacy/facerecognition/
- Privacy and the younger generation ("Privacidade e a geração mais jovem"): http://nymag.com/news/features/27341/
- Ill effects of constant surveillance ("Efeitos maléficos da vigilância constant"): http://news.bbc.co.uk/1/hi/uk_politics/7872425.stm
- The value of privacy ("O valor da privacidade"): http://www.schneier.com/essay-114.html

Ariel G. Foina Advogado
e diretor de Projetos da ONG
Universidade Cidadã, Brasí lia

Do panóptico ao "Big Brother"

por uma política pública para a privacidade de dados no Brasil

Em 1785 Jeremy Bentham concebeu uma estrutura arquitetônica voltada para a edificação de penitenciárias com fins a reduzir os custos do controle dos prisioneiros, denominada panóptico. Nesta nova forma de prédio, havia um centro de onde os detentos poderiam ser vigiados de tal forma que eles mesmos não pudessem ver quem os vigiava (ou saber se quem deveria vigiá-los estava efetivamente lá). Jeremy Bentham não era arquiteto, era um filósofo utilitarista e seu trabalho decorria de uma reflexão sobre a eficiência do controle. O sucesso do panóptico provinha do fato de que ali, naquele modelo, havia um controle simbólico imposto 24 horas por dia – afinal, pelo fato de os detentos não conseguirem ver quem os vigiava

> devemos considerar a hipótese de violação cotidiana da privacidade como fato dado e praticado pelos mais diferentes meios

no centro da estrutura, sentiam-se vigiados o tempo todo, estando presente o vigilante ou não.

Alguns séculos depois, em 1975, Michel Foucault publicou "Vigiar e Punir", onde aborda o debate filosófico sobre a punição em nossa sociedade, correlacionando, por um lado, escolas, presídios e hospitais, e por outro, a vigilância e a punição como forma de adestramento/ educação e controle social.

É inegável que alguns aspectos sociais mudaram desde a concepção destas estruturas/idéias até os dias de hoje. Em algum ponto da transição da modernidade[1] para a "sociedade pós-moderna"[2], o pesadelo de Foucault tornou-se o sonho do consumidor médio de bens de entretenimento, viabilizando-se os assim denominados "*reality shows*".

Não é incomum encontrar indivíduos, nos dias de hoje, dispostos a expor sua privacidade cotidiana, a colocar-se em verdadeiros aquários humanos integralmente vigiados - os *reality shows* no estilo "Big Brother", em troca de uma chance de obter alguma quantia em dinheiro. Mesmo que o prêmio financeiro não seja conquistado, a participação nestes espetáculos é, inegavelmente, associada à possibilidade da "fama" e à consequente exposição pública deste indivíduo, mesmo após o fim do *reality show* – um processo que redunda numa sucessiva e crescente renúncia à privacidade e à intimidade.

1. Termo aqui entendido de forma similar ao que outros autores denominam como "sociedade industrial", "modernidade sólida" e se refere ao período histórico cujo fim se identifica entre as décadas de 60 e 80 do século passado. 2. Sem entrar no debate quanto à existência ou não de uma pós-modernidade, aqui nos referimos à Sociedade Pós como sendo o mesmo período também denominado como "Sociedade pós-industrial", "pós-moderna", "modernidade tardia", "modernidade líquida" ou qualquer conceito que denomine uma nova configuração social historicamente delimitada após a década de 60, seja no entendimento de que se trata de um novo modelo, ou de mera fase de transição.

Essa renúncia à privacidade parece ser impulsionada por estímulos financeiros, em maior ou menor grau, o que resulta no fato de que este bem denominado "privacidade" – que até pouco tempo atrás parecia tão precioso – hoje está disponível para ser negociado, a maior ou menor preço, pela grande maioria dos indivíduos que compõem nossas sociedades ocidentais contemporâneas. É como reduzir o debate do "se a ex-brother vai posar para a revista de conteúdo erótico" a uma questão apenas de "por quanto".

O exemplo anterior é retórico, o usuário médio da Internet não vai posar para revista[3], mas sua renúncia à privacidade parece seguir no mesmo curso do exemplo que demos no parágrafo anterior. As pessoas não parecem estar muito preocupadas com o "a que custo", desde que em troca da renúncia à privacidade lhe sejam oferecidos, por exemplo, vários gigabytes gratuitos de espaço para sua caixa de correio eletrônico.

:: URBANIZAÇÃO E PRIVACIDADE

A sociologia clássica, se lida como forma de entendimento de contextos históricos anteriores ao nosso, parece poder elucidar algo da possível causa deste "barateamento" da privacidade. A partir da leitura de vários trabalhos sociológicos fica a impressão de que a perda da privacidade está relacionada com o processo de urbanização.

Mais do que o aspecto óbvio – de que uma casa isolada em uma área rural remota é capaz de oferecer mais privacidade do que uma casa em uma cidade; de que esta pode oferecer mais privacidade do que um apartamento, e este pode oferecer mais privacidade do que um quarto em uma república universitária –, existe algo do urbano que é introjetado pelo indivíduo e que o impulsiona a flexibilizar seus critérios de limite na intromissão externa à sua esfera de intimidade e, conseqüentemente, à sua privacidade.

Mais do que isto, no meio urbano existe o chamado comportamento *blasé*, onde o indivíduo urbano precisa ignorar outros indivíduos urbanos, dada a impossibilidade de se estabelecer com todos sucessivos processos de socialização - sendo tal comportamento recíproco entre os demais indivíduos urbanos (na prática significa dizer que uma pessoa não pode cumprimentar todos os estranhos que passam por ela numa rua movimentada, aprendendo a ignorá-las. Isso a sociologia urbana do início do século passado chamou de comportamento *blasé*).

Sem aprofundar-nos na teoria, cabe destacar apenas que, se por um lado existe uma gradativa renúncia à privacidade, por outro lado existe uma certa expectativa de que aquilo de privado que se expõe seja parcialmente ignorado sempre que esteja de acordo com o comportamento médio.

3. Esta frase também é em boa parte retórica, considerando-se fenômenos como o "*sexting*" e a possibilidade deste tipo de comportamento extrapolar as faixas etárias mais jovens. O fato é que não é possível afirmar de forma categórica qual será (ou se haverá) um limite à renúncia à privacidade e que aspectos da privacidade tal limite (ou a falta dele) pode vir a afetar.

Não se tem certeza sobre qual variável influenciaria o indivíduo a flexibilizar sua exigência de privacidade - mas, seja pelo contato mais intenso com outros indivíduos, seja pela redução do espaço, seja pelo aumento na organização do tempo e sua consequente escassez, ou então, seja pelo mero "agravamento" do processo de urbanização[4], o fato é que todas estas variáveis parecem suscetíveis aos impactos das novas Tecnologias de Comunicação e Informação.

Com a globalização e, mais recentemente, com a intensificação do uso da Internet, a construção social de conceitos como tempo e espaço se modificaram para se adequar a novos sítios e ritmos de interação. Conceitos sociais como o de distância (construído tendo como referência o tempo que se leva para percorrer um espaço), parecem ter sofrido modificações drásticas[5], que podem ser comumente percebidas, por exemplo, pelos critérios com que os indivíduos utilizam expressões como "aqui" e "ali", ou pela proximidade que se estabelece entre pessoas em relações mediadas por computadores.

:: PRIVACIDADE E O SISTEMA JURÍDICO BRASILEIRO

Assim sendo, a questão da privacidade de dados no Brasil, especialmente quando se fala de privacidade na Internet ou em sistemas eletrônicos – excetuada a transmissão de dados[6] – costuma ser reduzida a dois aspectos fundamentais: as relações de consumo, com o consequente direito à informação, e a correção das informações armazenadas em bancos de dados.

Tal redução geralmente decorre de uma situação jurídica brasileira muito singular, se observados outros países: o fato de que as únicas ferramentas legais que tratam de privacidade de informações no Brasil serem o Código de Defesa do Consumidor e a Constituição Federal quando trata das garantias e da via do hábeas-data. Desta míngua de normas, resulta a frequente posição, comum entre juristas e operadores do direito, de que há a necessidade de se

4. Desenvolvemos um ensaio teórico sobre este tema: Foina, A. G. O urbano na rede: Como a Teoria Sociológica Urbana Pode Ler as Cidades do Ciberespaço, Urbanidades, 2002 <http://www.unb.br /ics/sol/urbanidades/arielfoina.htm> 5. Ver Bauman, Z . Globalização: as conseqüências humanas, no capítulo denominado "Tempo e Espaço", Jorge Zahar Ed., 1999.

estabelecer critérios e leis que ditem como, para que e quais as informações relativas ao comportamento do indivíduo e seus dados pessoais podem ser armazenadas.

Denúncias de que uma ou outra empresa rastreia o comportamento de seus clientes ou de usuários de Internet para lhes oferecer determinados produtos ou publicidade, ou, simplesmente, para vender os dados a terceiros (tudo sem o conhecimento dos usuários), são muito comuns e normalmente recaem na discussão sobre o que está ou não está previsto nos Termos de Uso do Serviço - ou se houve ou não houve informação clara ou anuência prévia do consumidor quanto a tal conduta.

Este debate é necessário e relevante, mas não deve ser o único. Como apontamos anteriormente, existem indícios de que a questão da privacidade vem sendo relegada a uma posição de menor relevância pelos próprios usuários de redes digitais, fruto de um processo social que vem traçando seu curso histórico desde muito antes da existência dos computadores, e cuja tendência nos parece ser de agravamento.

Esta crescente renúncia à proteção da própria privacidade, se por um lado é motivada por um benefício imediado ao indivíduo frente a uma enxurrada de serviços gratuitos, e intensificada pelo descaso na atenção à maioria dos Termos de Uso de Serviço – extensos, complexos, mal traduzidos, e pouco inteligíveis – por outro lado implica em custos sociais ainda pouco experimentados no Brasil.

existem indícios de que a questão da privacidade vem sendo relegada a uma posição de menor relevância pelos próprios usuários de redes digitais

:: POR UMA POLÍTICA PÚBLICA DE PRIVACIDADE

Violações de grandes bancos de dados já foram realizadas para os mais variados fins - desde perturbações meramente comerciais, mediante oferta de serviços por concorrentes que deliberadamente copiaram bases de dados de clientes, passando por esquemas de chantagem e extorsão operados pela máfia do Leste Europeu decorrentes da obtenção da base de clientes de sítios web pornográficos, chegando ao crime de

6. A privacidade da transmissão de dados tem proteção constitucional, e existe uma expectativa entre a maioria dos cidadãos de que tal proteção é efetiva - tendo em vista, inclusive, a legislação específica para regular as hipóteses e os meios de quebra de tal proteção mediante ordem judicial. Mesmo assim, este debate possui nuances complexas que não vamos abordar aqui - a questão da transmissão de dados não é objeto deste trabalho.

"roubo de identidade", ainda pouco falado no Brasil mas já famoso em países onde o número de bancos de dados com informações de consumidores é muito maior do que em nosso país.

Não é razoável se esperar do usuário médio uma leitura atenta de todos os Termos de Uso de Serviço, nem se esperar de todos os prestadores de serviço um cuidado exacerbado com a privacidade da informação do usuário - uma vez que isso implica em custos muitas vezes maiores do que aqueles incorridos com as consequências da divulgação não autorizada dos dados armazenados.

Assim sendo, mais do que definir leis que estabeleçam formas aceitáveis de aquisição de dados, com prévia autorização dos usuários, é necessário que o país acorde para uma questão mais ampla – devemos pensar não apenas em entregar aos cidadãos um acervo de recursos para a proteção da privacidade (que, por desinteresse, pressa ou desinformação, poderia não ser utilizado); mas também em criar, nas esferas jurídica e administrativa, formas de controle e regras que permitam a redução dos danos nos casos de vazamento e comprometimento de bancos de dados com informações privadas.

> é certo que deveria haver uma preocupação pública quanto aos motivos que levam ao crescente armazenamento de dados

É hora de nos perguntarmos se é correto que um sítio web comercial armazene dados como número de RG, data de nascimento, nome, endereço, telefone, sexo, etc. - quando seria necessário, para fins fiscais, apenas o nome e o C.P.F. de seus usuários. Da mesma forma, deveríamos nos perguntar para que um orgão público deveria compor bases de dados que incluem, numa mesma ficha de registro, o nome do indivíduo, o nome dos pais, a data de nascimento, o número de diversos documentos (entre eles, passaporte ou identidade, C.P.F.), o endereço residencial, o número da CNH - apenas para

nos outorgar uma habilitação para condução de veículos automotivos.

Independente da resposta, é certo que deveria haver uma preocupação pública quanto aos motivos que levam ao crescente armazenamento dos dados, a real necessidade deste armazenamento, a finalidade para a qual foram compostos os bancos, os níveis de segurança adequados a cada tipo de cadastro e a possibilidade e forma de sua negociação, se for o caso.

Outros países como o Canadá, os Estados Unidos, a Inglaterra e a França [7], entre outros, já têm legislações que visam delimitar as práticas de retenção e armazenamento de dados, relevando-se aí muitas diferenças culturais. Em alguns casos, existem até comissões ou órgãos da administração pública especialmente dedicados à fiscalização, padronização e estudo de bancos de dados com informações de cidadãos e consumidores.

No Brasil não se escuta muito falar sobre este tema. Talvez por uma questão de cultura, não estamos acostumados a questionar a real necessidade do registro de uma extensa quantidade de informações sobre nós em diversos e redundantes cadastros nacionais. Especialmente num país como o nosso - onde dados inquestionavelmente sigilosos e privados, como os da Declaração de Imposto de Renda de Pessoa Física, até pouco tempo atrás, encontravam-se à venda no mercado informal - o debate sobre a forma de funcionamento, os limites de uso, o armazenamento e a segurança dos bancos de dados com informações de cidadãos, consumidores e usuários parece uma preocupação cada vez mais urgente. Este debate deve ser promovido, não só com fins acadêmicos, mas também com vistas à necessária regulação estatal[8].

Por fim, devemos considerar a hipótese de violação cotidiana da privacidade como fato dado e praticado pelos mais diferentes meios, com perspectivas de agravamento. Portanto, cabe ao Estado e à sociedade civil se preocupar em definir de forma clara e urgente um número de questões que não foram apreciadas pelo nosso sistema legal, tampouco por outras esferas da sociedade, como por exemplo: o que se tem feito efetivamente com os dados coletados? Por quem são manipulados? O que é registrado? O que deve ser registrado? Por quanto tempo? A quem se deve prestar contas? Qual nível de segurança adequado a cada tipo de dado? O que é comercializado? O que pode ser comercializado? Para que fim?

A lista não se esgota aí. Há várias outras questões ainda em aberto. Esta é uma discussão que não pode mais ser adiada. ●

7. Entre várias normas e instituições que podem ser citadas, temos na União Europeia: Diretiva 2002/58/EC e Diretiva 95/46/EC de Privacidade Eletrônica e Proteção Geral de Dados, respectivamente; no Reino Unido: Data Protection Act 1998; na França, desde 1978 há a Commission Nationale de l'Informatique et des Libertés.
8. Mesmo motivado pelos bancos de dados eletrônicos, o debate é (e deve ser) estendido aos dados coletados ambientalmente, como no caso de informações decorrentes de RFIDs (Radio-Frequency Identification ou Identificação por Rádio Frequência), dados biométricos e leitores de imagem e faciais, bem como o armazenamento de dados de DNA e informações genéticas, restando ainda muito o que ser debatido e, eventualmente, regulado.


.aero
.travel
.mobi
.asia
.eu
.mil
.org
.int
.com
.edu
.info
.gov
.pro
.net
.biz
.jobs

Flávio Rech Wagner representante
da comunidade científica e tecnológica
no Comitê Gestor da Internet no Brasil (CGI.br)

ICANN

novos domínios, antigas disputas

Este artigo oferece um relato parcial sobre a 35a reunião da ICANN (realizada de 20 a 26 de junho em Sidney, Austrália). É parcial no sentido em que descreve mais detalhadamente algumas das discussões que ocorreram durante a reunião da NCUC (*Non-Commercial Users Constituency*) - uma das muitas instâncias dentro da ICANN -, e no Fórum Público da ICANN, com um foco mais específico na discussão sobre a criação de novos nomes de domínio genéricos – os gTLDs (.com, .org, .edu, .gov, .net, etc.) e suas implicações políticas, econômicas, técnicas e sociais.

A organização da ICANN[1] contém múltiplas instâncias administrativas e de atuação dos seus diversos *stakeholders*, ou grupos de interesse. Entre estas, está a GNSO (*Generic Names Supporting Organization*)[2], que reúne os grupos interessados na gestão dos gTLDs (*generic Top Level Domains*).

1. A organização da ICANN pode ser vista em http://www.icann.org/en/about. 2. http://gnso.icann.org.

Na sua estrutura atual, a GNSO possui seis *constituencies* (que são grupos que têm direito a voto), cada uma delas reunindo representantes dos diversos grupos de interesse[3]. Uma destas é a NCUC (*Non-Commercial Users Constituency*)[4], de cuja reunião participei no dia 23 de junho. A GNSO é conduzida por um Conselho, formado por 21 pessoas, sendo 18 delas eleitas pelas *constituencies* (três de cada *constituency*) e três outras indicadas por um Comitê de Nomeações.

A NCUC possui como membros tanto organizações como indivíduos[5]. A associação à NCUC está aberta a todos que atenderem a um determinado conjunto de critérios. Nota-se uma grande maioria de organizações envolvidas com os interesses dos usuários individuais, especialmente aquelas que defendem direitos de usuários e consumidores. A atual coordenadora da NCUC é a advogada norteamericana Robin Gross. Os três representantes eleitos pela NCUC para o Conselho do GNSO são William Drake, pela América da Norte, Mary Wong, pela Ásia, e Carlos Affonso Pereira de Souza, da Fundação Getúlio Vargas, pela América Latina e Caribe.

Como representante da comunidade científica e tecnológica, a NCUC é a *constituency* que corresponde à minha atuação no CGI.br. No entanto, nota-se na NCUC uma grande ausência de acadêmicos (indivíduos e organizações) relacionados com a parte técnica da Internet. Em troca, há forte participação de acadêmicos com atuação em ciências sociais e direito.

A agenda da reunião da NCUC realizada em Sidney incluía um grande número de itens[6], mas apenas dois assuntos foram de fato discutidos, cada um deles em grande detalhe, suscitando posições bastante fortes dos presentes. Estes temas – reorganização da GNSO e mecanismos de proteção a marcas globais na criação de novos gTLDs – correspondem, por um lado a questões de organização e de poder dentro da ICANN e, por outro lado, a questões técnicas, ambos ilustrando claramente as disputas que ocorrem entre os

3. As constituencies são: *Commercial and Business Users*; gTLD Registries; Internet Service and Connection Providers; Non-Commercial Users; Registrars; e Intellectual Property. Registries são as entidades responsáveis pela gestão dos TLDs - sejam gTLDs (.com, .org, .net, etc) ou ccTLDs – country code TLDs (.br, .ar, .uk, etc.). Registrars são as entidades responsáveis pela gestão de nomes de domínio de segundo nível. 4. http://gnso.icann.org/non-commercial. 5. Uma relação não atualizada de membros da NCUC se encontra em http://ncuc.syr.edu/members.htm. Vê-se a participação de três organizações brasileiras: Fundação Getúlio Vargas, RITS – Rede de Informações para o Terceiro Setor e Comitê para a Democratização da Informática de Pernambuco. 6. A agenda originalmente prevista para a reunião está em http://syd.icann.org/node/3764

diferentes grupos de interesse em todas as atividades da ICANN.

:: A REORGANIZAÇÃO DA GNSO[7]

Em sua organização atual, a GNSO tem seis *constituencies* e cada uma destas elege três representantes para o Conselho da GNSO.
Estão sendo propostas diversas modificações que deveriam aperfeiçoar o funcionamento da GNSO[8]. Entre estas, uma de grande impacto é o aperfeiçoamento das *constituencies* e a consequente reorganização do Conselho da GNSO. Segundo proposta que está sendo elaborada pelo *Structural Improvements Committee* (SIC), indicado pelo Conselho Diretor da ICANN, e que deveria ser aprovada até a próxima reunião desta entidade (em Seul, em outubro de 2009), a GNSO passaria a ser organizada em duas "Casas", uma delas representando os *contractual stakeholders* (basicamente *registries* e *registrars*) e outra representando os *non-contractual stakeholders* (correspondendo às demais constituencies atuais). Cada uma destas casas passaria a ter 12 assentos no Conselho da GNSO.
Em cada casa existiriam dois Grupos de Interesse, cada um deles com um certo número de *constituencies* e cada um elegendo seis representantes para o Conselho.

No caso dos *non-contractual stakeholders*, os grupos corresponderiam a grupos com interesses comerciais (reunindo três das atuais *constituencies* – Usuários Comerciais e Empresariais; Provedores de Conexão e Serviços; e Propriedade Intelectual), e a grupos com interesses não-comerciais, cuja sigla seria NCSG (*Non-Commercial Stakeholders Group*). Este grupo, no momento, é composto apenas pela NCUC.

É expectativa do SIC e da GNSO que novas *constituencies* surjam dentro do NCSG, correspondendo a outras comunidades hoje mal representadas na NCUC, tal como a comunidade acadêmica técnica[9].

Em relação à organização atual da GNSO, o grupo *non-contractual* com interesses comerciais estaria perdendo três vagas no Conselho da GNSO, enquanto o grupo *non-contractual* sem interesses comerciais estaria ganhando três vagas. Como resultado desta alteração do balanço de poder dentro do Conselho do GNSO, o grupo com interesses comerciais estaria tentando negociar a indicação dos três nomes adicionais que irão representar os não comerciais.

Esta é uma discussão bastante relevante em termos da representatividade dos membros da NCUC no Conselho da GNSO e da própria evolução da NCUC, que se transformará em NCSG e deve

7. N.E.: Um maior detalhamento da discussão sobre a reorganização da GNSO e das discussões do Fórum Público pode ser lida na versão completa deste texto, em www.politics.org.br. 8. Uma visão geral dos diversos aperfeiçoamentos propostos pode ser encontrada em http://gnso.icann.org/en/improvements. 9. Esta expressão "comunidade acadêmica técnica" foi utilizada por Roberto Gaetano, coordenador do SIC, para identificar a comunidade de especialistas em questões técnicas da internet, em oposição a acadêmicos de áreas das ciências sociais.

incluir novas *constituencies*, de outros segmentos da sociedade hoje pouco representados na NCUC.

:: NOVOS GTLDS E A PROTEÇÃO A MARCAS GLOBAIS

Existem atualmente apenas 20 gTLDs[10]. Com a intenção de estimular a competição e beneficiar os usuários, a ICANN pretende liberar a partir de 2010 a criação de um número muito maior de gTLDs[11]. Este programa traz consigo muitas questões que precisam ser adequadamente resolvidas antes que os novos gTLDs possam ser introduzidos. Elas estão organizadas em torno de quatro grandes eixos: questões econômicas, questões de segurança e estabilidade da rede, questões de proteção de propriedade intelectual e questões derivadas de comportamento malicioso na rede.

Em particular, a ICANN designou em março de 2009 um Grupo de Implementação de Recomendações (IRT) para elaborar uma proposta de proteção a propriedade intelectual[12] em função da introdução de novos gTLDs. Esta proposta (um relatório com 69 páginas) foi divulgada em maio de 2009 e submetida publicamente a comentários até 6 de julho.

Entre diversas medidas, o relatório do IRT fez algumas propostas que motivaram fortes críticas de membros da NCUC. O IRT propõe a proteção automática a marcas globais nos domínios de primeiro e segundo nível, através de mecanismos ligeiramente distintos em cada um destes casos. Estas marcas globais seriam incluídas numa lista denominada GPML (*Globally Protected Marks List*) a partir de sua aderência a um certo conjunto de critérios quanto a seu caráter "global" (i.e. amplamente reconhecidas em todo o mundo).

A GPML estaria baseada na suposição de que o proprietário de uma marca detém uma determinada cadeia de caracteres (tal como "apple", "ibm", "nike", "mcdonalds", etc.), de modo que esta lista administrada pela ICANN permitiria que:
(a) os detentores destas marcas sejam avisados quando houvesse uma tentativa de registro de um domínio de primeiro ou segundo nível usando a mesma linha de caracteres; e
(b) os registros de domínios utilizando estas linhas sejam automaticamente bloqueados.

Dois membros da NCUC – Kathryn Kleiman e Konstantinos Komaitis – elaboraram pareceres, distribuídos durante a reunião[13], com uma avaliação técnica (na realidade principalmente abordando aspectos jurídicos e de procedimentos) a respeito do relatório do IRT. Basicamente, a crítica se centra em três conjuntos de argumentos[14]:

10. Além dos sete gTLDs originais (.com, .org, .edu, .gov, .net, .mil e .int), outros foram criados sucessivamente, a partir de 2001, tais como .biz, .info, .asia, .mobi e .travel. Ver mais em http://www.icann.org/en/tlds 11. http://www.icann.org/en/topics/new-gtld-program.htm 12. Ver o relatório final com a proposta do IRT em http://www.icann.org/en/topics/new-gtlds/irt-final-report-trademark-protection-29may09-en.pdf. 13. Infelizmente, recebi apenas versões impressas destes pareceres. Não tive ainda acesso a versões eletrônicas que possam ser referenciadas aqui.

1. a proposta do IRT extrapolaria o escopo de leis nacionais e internacionais de proteção de propriedade intelectual, atribuindo à ICANN uma competência que se sobreporia a leis existentes;
2 a proposta do IRT extrapolaria o escopo da missão as funções da ICANN, criando para ela uma atribuição (de proteção a marcas) que ela não deveria ter;
3 .a proposta do IRT extrapolaria as diretrizes e critérios estabelecidos pelo próprio IRT.

Houve críticas também à composição do IRT, no qual não estariam devidamente representadas muitas das *constituencies*, resultando num predomínio da *Constituency* de Propriedade Intelectual e críticas à forma de trabalho do IRT, que não teria tido a devida transparência.

São princípios do funcionamento da ICANN a transparência de todas as suas ações e decisões e a *accountability* perante os seus grupos de interesse

Outro tema que provocou protestos por parte de membros da NCUC foi a proposta de criação de um WHOIS[15] global, armazenado na própria ICANN, pelo risco de violação de direitos de privacidade.

:: NOVOS GTLDS – O FOCO DO FÓRUM PÚBLICO [16]

São princípios do funcionamento da ICANN a transparência[17] de todas as suas ações e decisões e a *accountability* [18] perante os seus grupos de interesse.

Entre os vários mecanismos previstos para assegurar o respeito a estes princípios estão: a realização de reuniões abertas de todas as instâncias decisórias; a transcrição e registro de todas as sessões; a colocação de todos os documentos em consulta pública para recebimento de comentários antes de sua aprovação; e a possibilidade

14. Faço aqui um esclarecimento: repito a essência dos argumentos contidos nestes pareceres de membros da NCUC, sem emitir juízo de valor sobre a correção dos mesmos, especialmente por não ser um especialista em questão de proteção a marcas e não ter experiência suficiente com os procedimentos da ICANN. 15. WHOIS é uma base de dados contendo informações que identificam os detentores de domínios, que deve ser mantida por registries (neste caso denominada Thick Whois) e registrars (neste caso Thin Whois). 16. O Fórum Público é uma das diversas sessões plenárias que ocorrem durante a reunião da ICANN. 17. IVer as formas de transparência previstas nos Estatutos em http://www.icann.org/en/general/bylaws.htm#III 18. O termo accountability indica que a ICANN deve ser responsável perante todos os seus grupos de interesse em termos de uma atuação consistente com sua missão e Estatutos. Ver mais em http://www.icann.org/en/general/accountability_review.html.

de participação remota nas reuniões. O Fórum Público é mais um dos mecanismos de transparência, aberto à participação de todos os interessados.

O Fórum Público é uma sessão plenária da qual participam todos os grupos de interesse da ICANN. Como não é programada nenhuma outra atividade em paralelo, esta sessão atrai a maioria dos participantes da reunião.

Dos cinco temas previstos na agenda do Fórum Público desta 35a reunião da ICANN, quatro deles estavam relacionados à criação de novos gTLDs (generic Top Level Domains):

- Relatório do IRT *(Implementation Reccomendation Team)* e proteção a marcas;
- Separação vertical entre *registries* e *registrars*;
- IDNs (*Internationalized Domain Names*);
- Outros temas relacionados a gTLDs.

Além destes, também constava da agenda o tema do JPA (*Joint Project Agreement*[19]) e o aumento da confiança institucional.

Algumas das críticas da NCUC à proposta de criação de novos gTLDs foram repetidas durante o Fórum Público.

Entre as posições manifestadas pelo público estavam:

- A crítica ao prazo para avaliação do relatório do IRT (que teria sido curto) e a sugestão de que seria necessário mais tempo para a discussão com a comunidade.

O Presidente do Conselho Diretor da ICANN, Peter Thrush[20], afirmou que o assunto ainda está em aberto e haverá novas rodadas de discussão.

- A percepção de que o IRT teria sido controlado principalmente pela *Intellectual Property Constituency*[21]. Seria necessário procurar um consenso maior entre os diversos grupos de interesse da ICANN, reunidos em outras *constituencies*.
- A observação de que teria faltado, no trabalho do IRT, a transparência que é tão cara à ICANN em todos os seus procedimentos.
- A crítica à proposta do IRT, pois esta não obedeceria a regras do direito internacional (p.ex. da OECD).
- A percepção de que o *thick whois*[22] no *registry* é um mecanismo que põe em risco a privacidade dos usuários. A proposta deveria obedecer a normas internacionais de privacidade de dados.

:: OUTROS TEMAS RELACIONADOS AOS NOVOS GTLDS

Além do tema da propriedade intelectual, outras questões foram levantadas pelos participantes do Fórum Público. Uma delas

19. O JPA é o documento firmado entre a ICANN e o Departamento de Comércio dos EUA em setembro de 2006, em substituição a acordos anteriores, que prevê o desenvolvimento conjunto de mecanismos, métodos e procedimentos necessários para efetuar a transição da gerência do DNS para o setor privado.
20. http://www.icann.org/en/biog/thrush.htm
21. A IPC (Intellectual Property Constituency) é uma das constituencies que compõem a GNSO. Ver mais em http://gnso.icann.org/intellectual-property
22. Thick whois , conforme proposta do IRT, será um banco de dados, armazenado no registry, com informações sobre todos os detentores de domínios dentro do TLD gerido pelo registry. Ver mais em http://www.icann.org/en/topics/new-gtlds/thick-thin-whois-30may09-en.pdf

> O *thick whois* é um mecanismo que põe em risco a privacidade dos usuários

ressaltou o fato de que, no contexto do programa de novos gTLDs, está sendo proposta uma política de objeção baseada em conceitos de moralidade e ordem pública[23]. Estaria sendo introduzido também o conceito de *independent objector*[24], que seria uma entidade externa que poderia atuar em nome de interesses difusos da comunidade. A questão que se impõe, neste caso, é: qual é a relação entre ambos os mecanismos? Neste sentido, um representante da NCUC expressou a preocupação de organizações que defendem a liberdade de expressão, participantes desta *constituency*, quanto à proposta de que qualquer pessoa ou organização possa objetar à criação de um domínio em função de questões de moralidade e ordem pública. Para este membro da NCUC, este não é um padrão razoável a ser estabelecido pela ICANN.

A criação de novos gTLDs dá margem também a outras discussões complexas, além daquelas motivadas pelos temas da propriedade intelectual e do controle em prol da moralidade e da ordem pública. Uma das questões que parecem suscitar polêmica foi levantada pelo GAC[25], que expressou a posição de que a ICANN não pode negar a um governo o direito de manter os ccTLDs[26] que correspondem a seu país e/ou territórios. Imagine-se, num exemplo extremo, que a ICANN aprovasse a criação de um gTLD chamado "brasil", atribuindo a um *registrar* a sua gerência. Assim, o GAC quer garantir a reserva de nomes geográficos não apenas no primeiro nível como também no segundo nível.

Na reunião do Conselho Diretor da ICANN, no dia seguinte ao Fórum Público, foi decidido que a equipe da ICANN irá preparar até o final de agosto de 2009 um documento, a ser aberto para comentários públicos, com opções para continuação do trabalho do IRT. Assim, a discussão continua – e a participação neste debate é possível para qualquer pessoa interessada, através das consultas públicas online e da participação na NCUC – em http://www.ncdnhc.org. ●

23. http://www.icann.org/en/topics/new-gtlds/morality-public-order-30may09-en.pdf 24. http://www.icann.org/en/topics/new-gtlds/independent-objector-18feb09-en.pdf 25. O GAC (Governmental Advisory Committee) é uma das organizações que fazem parte da ICANN, composta por representantes de governos. Ver em http://gac.icann.org 26. Ver explicação sobre os ccTLDs na nota de rodapé no. 3

> **Carlos A. Afonso** é diretor executivo do Instituto NUPEF e conselheiro do Comitê Gestor da Internet no Brasil (CGI.br), eleito como um dos representantes do terceiro setor.

> **Demi Getschko** é diretor presidente do Núcleo de Informação e Comunicação do Comitê Gestor da Internet no Brasil (NIC.br), Conselheiro do Comitê Gestor da Internet no Brasil (CGI.br), eleito como representante de notório saber em assunto da Internet.

Eu registro, você filma, ele vai preso...

"A iniciativa de se regular a Internet do ponto de vista criminal é louvável, especialmente para coibir condutas graves. No entanto, ela traz em si riscos consideráveis. O caminho natural de regulamentação da rede, seguido por todos os países desenvolvidos, é primeiramente estabelecer um marco regulatório civil, que defina claramente as regras e responsabilidades com relação a usuários, empresas e demais instituições acessando a rede, para a partir daí definir regras criminais. O direito criminal deve ser visto como ultima ratio, isto é, o último recurso, que é adotado quando todas as demais formas de regulação falham. Nesse sentido, o caminho correto seria a partir do estabelecimento do marco civil, verificar o que teve efeito ou não de então adotar legislação criminal para regular a rede com base na experiência adquirida."

Ronaldo Lemos, Carlos Affonso Pereira de Souza, Sérgio Branco, Pedro Mizukami, Luiz Moncau, Bruno Magrani, Proposta de Alteração do PLC 84/99 / PLC 89/03 (Crimes Digitais) e Estudo sobre História Legislativa e Marco Regulatório da Internet no Brasil, Rio de Janeiro: Centro de Tecnologia e Sociedade, Escola de Direito, Fundação Getúlio Vargas, junho de 2009, p.4.

Um de nós acaba de receber em casa um suposto boleto a pagar, enviado por um banco. O destinatário não tem conta nesse banco, e trata-se de um boleto de um certo "fundo de capitalização". Averiguação detalhada mostra que é mesmo do tal banco e no boleto consta o nome completo da pessoa e o seu CPF, bem como o endereço exato e o valor a pagar de R$20. Uma forma malandra de buscar aderentes ao seu "plano de capitalização" (capitalização dele, banco, é claro). Como é um boleto bancário, basta que um de nós dois (autores deste texto) seja um pouco mais distraído (o que não é difícil), para simplesmente pagar primeiro e depois perceber do que se trata a "cobrança" – afinal, são só R$20. Mas a pergunta que nos interessa agora é: como o banco obteve esses dados?

No universo do crédito e das contas bancárias, nossa privacidade já está violada – as operadoras de cartões de crédito pesquisam os dados de seus clientes para canalizar propaganda ou gerar listas de risco[1], e revendem ou repassam essas informações a outras empresas (como a Experian/Serasa e outras de análise de risco ou "marketing").

Nestes casos, há uma justificativa para as empresas solicitarem informações pessoais: trata-se de um contrato de serviços envolvendo crédito e ambos os lados têm o direito de saber com quem estão lidando. Não se justifica, de nenhum modo, no entanto, a violação de confidencialidade dessas informações para proveito próprio (de bancos e operadoras de cartões) ou de terceiros.

O cadastramento é feito também por empresas que fornecem acesso à Internet (via linha telefônica, ADSL, rádio digital, satélite, cabo de TV etc). Trata-se de um contrato de serviços em que obrigatoriamente há um acordo assinado entre as partes (com cláusulas nem sempre cumpridas pela operadora – mas essa é outra história), com os dados necessários registrados em cadastro. Do mesmo modo, não se justifica o uso desse cadastro para nenhum outro fim que não seja diretamente relacionado ao contrato de serviços.

Uma empresa operadora fará o registro de utilização do serviço oferecido para poder comprovar que, em qualquer período do contrato em vigência, o sistema estava funcionando, ou deixou de funcionar por problema identificável. Portanto, é natural esperar que uma fornecedora de conectividade e transporte de dados de Internet (conhecida como "provedor de acesso") mantenha os registros de conexão de seus clientes com a precisão devida. É surpreendente constatar que, mesmo no caso de grandes operadoras, isso muitas vezes não ocorre. Em caso recente de crime de pedofilia relatado pela ONG Safernet - em que houve necessidade legal de comprovação de acesso por parte dos autores dos crimes -, as operadoras não conseguiram apresentar dados com data e hora corretas[2].
Ou seja, esses dados não servem para dirimir dúvidas no cumprimento do contrato de acesso ou para apuração

1. Por exemplo, listas de possíveis mau pagadores. 2. Conforme o relato da Safernet sobre a chamada Operação Turko: "Foram aproveitadas, por exemplo, apenas 34% das informações fornecidas pela NET, 43% dos dados da Brasil Telecom e 51% da Oi/Telemar. Somente os dados da Telefônica e da GVT atingiram 80% de utilização." Ver http://www.safernet.org.br/site/noticias/opera%C3%A7-turko-%C3%A9-deflagrada-partir-das-den%C3%BAncias-safernet

de eventuais crimes. Para que então registrar?

Um dos argumentos utilizados pelos provedores de acesso contra o registro de dados de acesso é o custo envolvido. A prática do registro vem do início da Internet comercial, quando a cobrança era feita em função do tempo de conexão telefônica ao provedor de acesso (conexão via chamada telefônica ou "linha discada"). Desde essa época os provedores aperfeiçoaram os métodos de registro, e eles estão embutidos em praticamente todos os sistemas comerciais de cobrança desse tipo de serviço.

No caso das conexões via linha telefônica em que o sinal de transporte de dados e o enlace lógico ficam ativos continuamente, independente do telefone estar em uso ou não (serviços que usam a tecnologia ADSL da chamada "banda larga", conhecidos no Brasil por marcas como Speedy, Velox e outros), ou seja, em que o usuário pode manter seu computador conectado à Internet o tempo todo, independente da conta do serviço de telefonia, por um preço fixo mensal, ainda assim é praxe manter o registro de acesso para eventuais comprovações contratuais.
O mesmo ocorre no caso de qualquer outro serviço de acesso similar em que a conexão pode ficar ativa permanentemente a um preço fixo mensal (via rádio digital, via TV a cabo ou via satélite).

Nestes casos, o registro do acesso é ainda mais fácil por duas razões. Em primeiro lugar, é comum que a conexão fique ativa (o usuário desliga o computador mas deixa o modem ligado, por exemplo). Neste caso, o número de registros na base de dados é muito menor que no caso do antigo sistema de conexão via linha discada, já que não há "bilhetagem" por contagem de tempo, exceto em casos especiais de serviços cruzados (um exemplo destes é o acesso a um serviço wi-fi de aeroporto utilizando a conta de usuário de um provedor de acesso – caso em que este provedor cobrará do usuário pelo tempo de uso da rede da outra empresa e a esta repassará uma porcentagem do valor cobrado). Portanto, é contraditória uma das razões alegadas pelas operadoras para a dificuldade da obrigatoriedade de manter o registro: que o custo do serviço de registro é alto pelo número elevado de acessos.

Em segundo lugar, apesar de os contratos de "banda larga" não garantirem ao usuário um número IP fixo, este na prática fica fixo pelo menos enquanto o modem de um dos lados da conexão não for reiniciado – se nunca houver desligamento ou reinício em qualquer dos lados, o número IP em geral não muda. Mas, mesmo quando há reinício, nota-se

> a função de um provedor de acesso é dar os meios a alguém, que apenas tem um canal de comunicação de dados, para que possa chegar à Internet e nela navegar

na grande maioria dos casos que o número IP permanece o mesmo. Isso é conveniente para as operadoras, uma vez que a cada mudança de IP um novo registro dessa conexão teria que ser criado na base de dados – e talvez seja a razão pela qual nos serviços de "banda larga", o IP do usuário, na prática, é fixo por longos períodos de tempo. Isso também confirma que o número de registros na base de dados é muito menor do que se esperaria, quando as operadoras lamentam os "altos custos" de preservar as bases de dados desses registros. Por outro lado, mostra a arbitrariedade das operadoras na oferta de endereços IP fixos, uma vez que solicitar formalmente a adição da garantia de IP fixo encarece em muito os contratos de "banda larga", enquanto o custo marginal de um IP fixo nestes casos é na prática zero para as operadoras - afinal, é óbvio que elas têm que garantir permanentemente um número IP real para cada enlace.

No entanto, em nenhum dos casos acima, o registro é obrigatório. Ele é apenas necessário para responder a questionamentos contratuais, mas um provedor gratuito (uma rede aberta wi-fi, um serviço gratuito de acesso em um hotel ou conferência, ou o serviço de acesso em um telecentro comunitário ou em uma rede municipal gratuita) não precisa disso, exceto para avaliar o seu mérito enquanto serviço comunitário ou social. Mesmo no caso da necessidade de comprovações contratuais, esse registro teria que ser auditado ou certificado por entidade independente, o que nenhuma operadora no Brasil faz.

Lembremos que a função de um provedor de acesso é dar os meios a alguém, que apenas tem um canal de comunicação de dados, para que possa chegar à Internet e nela navegar. Ele registra dados dessa operação de acesso.

Mas o que exatamente se registra? Há dois tipos de registro: o de acesso, já comentado, e o de visitas (consulta ou interação com aplicativos e conteúdos na rede).

No primeiro caso, o registro ou "log" contém um identificador da conta do usuário (ou do contrato do usuário com o provedor de acesso), data, hora de início e hora de término da conexão a um serviço de acesso à Internet. Esse registro

contém também o número IP designado ao modem do usuário no período. Notem que a designação do IP é ao modem do usuário, não ao computador ou aos computadores do usuário. A partir do modem, um roteador local pode redistribuir a conexão a vários computadores, e não há como atribuir a um computador específico que serviço está sendo utilizado a partir do registro de acesso.

No segundo caso, trata-se do registro de visitas a serviços de conteúdo via Internet (essencialmente páginas Web de sítios, blogs, serviços de email etc etc). Neste caso, o registro é feito pelos provedores de conteúdo por razões de mercado (ou para avaliar impacto). Por exemplo, o sítio do Fórum Social Mundial tem um registro de visitas para estimar seu impacto, a partir da obtenção de informações quanto a países de origem das visitas, número de visitas, que páginas são mais vistas etc. O mesmo fazem os sítios de provedores de conteúdo comerciais, já que o perfil e volume de visitas permite a "monetização" das páginas através de anúncios e patrocínios.

Este registro de visitas contém em geral o número IP de origem, os dados de tempo, as páginas e serviços visitados, e através de cruzamento com bases de dados de nomes e números (automaticamente feito pelos programas de registro), este número IP revela o país de origem. É o mesmo número IP cadastrado em algum lugar do planeta por um provedor de acesso desse usuário. Ou seja, em tese, é possível associar os dois registros entre si, mas não necessariamente associá-los à pessoa que realmente está fazendo a visita. E mais: esse visitante pode ser um "robô" automático de sistemas indexadores, como o Google ou o Yahoo. Pergunta a certos autores de projetos de lei: esses "robôs" deveriam cadastrar-se com identidade e CPF?

Notemos que o IP de origem da visita não é informação pessoal como seria o número de uma carteira de identidade, por exemplo. Apenas identifica uma máquina na Internet (um modem conectado a um provedor, um roteador etc) através da qual o usuário fez a visita a um sítio na Internet. Se fosse possível associar esse IP inequivocamente a uma pessoa durante o período da visita, poderia ser considerado um identificador pessoal e portanto sujeito, naquele período, aos direitos de proteção à privacidade dessa pessoa. Mas em geral é quase impossível caracterizar o IP de origem de uma visita como "IP pessoal" nesse sentido.

Esses registros são feitos hoje independente da chamada "azeredização" ou não da Internet brasileira (referência feita ao projeto de lei liderado pelo senador Azeredo, que procura impor a todos os provedores de acesso e de conteúdo a identificação e o registro de usuários). Legalmente vai ser impossível impedir que esses registros, tal como descritos, continuem – no primeiro caso, por razões jurídicas (contratuais), além de ser de interesse do usuário que esse registro exista no caso de ações contra o provedor, por exemplo – e no segundo caso porque sem esses dados simplesmente se mata a "monetização" dos conteúdos na Web - adeus Google e negócios similares.

Por quanto tempo são preservados esses registros? Há alguns anos o Comitê Gestor da Internet no Brasil (CGI.br) emitiu uma resolução recomendando que os registros de acesso fossem preservados por até três anos, justamente para proteger ambos os lados do contrato de provimento de acesso em disputas jurídicas. Uma recomendação apenas, até porque o CGI.br não tem mandato para regular práticas como essa. Não há no Brasil legislação que obrigue o provedor a fazer os registros – até porque essa obrigação legal teria que ser acompanhada de critérios rigorosos e obrigatórios de auditagem ou certificação (necessidade que o caso das operadoras já citado demonstra). Como fazer isso? Todavia, há múltiplas tentativas em curso para criar este tipo de obrigação via projetos de lei, inclusive o do senador Azeredo (quase todas revelando ignorância sobre como funciona a Internet).

Um caso recente, envolvendo o serviço de redes sociais Facebook e o governo do Canadá, revela que em alguns países o tempo de armazenagem de dados cadastrais ou registros de acesso ou visitas pode violar leis de privacidade. A lei canadense permite que qualquer organização retenha dados de clientes ou usuários somente pelo período necessário para determinados propósitos (como, por exemplo, durante a vigência de um contrato de prestação de serviços). No entanto o governo canadense constatou que esses dados são retidos pelo Facebook mesmo depois que a conta do usuário é desativada.

Cerca de 12 milhões de canadenses estão cadastrados no Facebook (mais de um em cada três da população do país)[3].

Se os provedores de conteúdo preservam os registros de visitas, se só preservam o suficiente para identificar origem geográfica ou qualquer outro critério de interesse, e por quanto tempo, é assunto para um bom debate. Mas se você entrar agora em um sítio Web da Transilvânia, o provedor de conteúdo da Transilvânia poderá registrar automaticamente o IP de origem de sua conexão ao seu provedor de acesso e, se quiser, registrar quais as páginas ou diretórios do servidor você consultou. E um zeloso procurador de lá poderá solicitar ao provedor de acesso daqui o cadastro da pessoa física ou jurídica relacionado àquele número IP durante aquele período de conexão. Mas ele pode chegar ao provedor de acesso se este for uma "lan-house" à beira da rodovia Dutra? Ou se for um provedor de um hotel que fornece Internet gratuita nos apartamentos? Ou uma rede municipal que tem wi-fi aberto? Daí a chegar à pessoa real que visitou o sítio Web é um caminho quase impossível – lembrando que esses registros, se existirem, não são legalmente auditados.

O "log" de visitas, tal como é feito hoje, não deixa de ser uma violação de privacidade, se for possível associar o registro da visita a uma pessoa. O que você vê, onde você vai na Internet, é informação de natureza privada. A analogia, de novo, é que ninguém deve poder

3. BBC News, "Facebook 'breaches Canadian law'", http://news.bbc.co.uk/2/hi/americas/8155367.stm, 17-7-2009

monitorar que revistas você folheia numa banca de jornais, ou que livros você consulta numa biblioteca. A pergunta a responder: quem é imputável por conteúdo supostamente ilegal, ou por uso ilegal de dados armazenados e, uma vez consensuado esse "quem" e assegurada a efetiva ilegalidade do conteúdo ou de seu uso indevido, como chegar inequivocamente ao indivíduo de origem, o "verdadeiro culpado"? O culpado, nesses casos, não é quem deu passagem (acesso) à Internet ou quem sediou conteúdo alheio. Não se processa a concessionária de uma rodovia por ter deixado passar um carro carregado de cocaína ou com milhares de DVDs contendo pornografia infantil. Nem será processado o dono do estacionamento em que o carro assim carregado ficou por algum tempo. Se o conteúdo é ilegal ou foi obtido ilegalmente, cabe à justiça buscar o "dono" do conteúdo, ou o responsável pela obtenção dos dados, qualquer que seja o meio. Se há ilegalidade, cabe ao sediador cumprir a determinação da justiça de impedir que o conteúdo continue exposto, ou ceder informações sobre o acesso que possam estar registradas. Mas não cabe aos provedores – em nenhum ponto da cadeia de uso – exercer a censura prévia.

Infelizmente, tanto o espírito quanto a letra dos projetos de lei sendo considerados no país sobre o tema podem ser resumidos no título deste artigo: eu registro, você filma, ele vai preso. Ou seja, na perseguição a autores de crimes na Internet provavelmente acabará sendo castigada a pessoa ou entidade errada e os eventuais criminosos continuarão a agir. Até pode ser que, se aprovados estes projetos, um deputado ou outro ficará feliz porque prestou os serviços de seu "lobby" - mas a lei será inaplicável.

Qualquer legislação que se proponha nesta área deverá ser muito bem informada sobre como funcionam as diferentes camadas da Internet, o alcance transfronteiras da rede (tanto do lado dos usuários como da infraestrutura de rede, dos provedores e dos conteúdos), em que medida ilegalidades cometidas já estão cobertas pelos códigos civil ou criminal (e na maioria dos casos conhecidos já estão) e quais exatamente são as cadeias de responsabilidade. Feito esse filtro, é provável que quase todos os projetos de "leis para a Internet" em trâmite no momento no nosso Congresso sejam tramitados pelo caminho merecido: o da lata de lixo.

> Não cabe aos provedores – em nenhum ponto da cadeia de uso – exercer a censura prévia

Túlio Vianna Professor
de Direito Penal da PUC Minas.

3 críticas

ao Projeto de Lei de Crimes Informáticos[1]

Há 10 anos tramita no Congresso Nacional o projeto de lei nº 84/1999 que visa tipificar os crimes informáticos em nosso ordenamento jurídico. Aprovado na Câmara em novembro de 2003, o projeto foi enviado para apreciação no Senado onde tramitou sob o nº 89/2003 e recebeu substitutivos dos senadores Eduardo Azeredo e Aloizio Mercadante que acabaram culminando com a aprovação da sua redação final em 9 de julho de 2008. O projeto, então, retornou à Câmara dos Deputados, onde tramita atualmente.

Nossa proposta aqui é analisar os três artigos mais polêmicos do projeto e propor algumas soluções para seu aperfeiçoamento.

:: TÉCNICA LEGISLATIVA

Logo de início se percebe a péssima técnica legislativa do projeto que criou um novo capítulo no Código Penal completamente dissociado dos critérios que regem nosso código:

"CAPÍTULO IV
DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS"

É um consenso entre os penalistas brasileiros que os tipos penais são classificados de acordo com o bem jurídico protegido, ou seja, com o direito fundamental da pessoa humana que fundamenta a criminalização da conduta. Assim, temos crimes contra o direito à vida, contra o direito ao

1. A pedido do autor, este artigo não foi revisado e editado pela equipe da poliTICs – está publicado exatamente conforme o texto original por ele enviado.

patrimônio, contra o direito à honra, contra o direito à liberdade sexual, etc.

Os direitos que se procuram resguardar com a criação destes crimes informáticos são o direito à propriedade dos dados informáticos (não se pode apagá-los ou modificá-los sem a permissão do dono) e o direito à privacidade destes dados (não se pode acessá-los sem a permissão do dono). Em um único conceito: inviolabilidade dos dados informáticos, entendida como a tutela simultânea da propriedade e da privacidade destes dados, tal como, na inviolabilidade de correspondência.

Destarte, os novos tipos deveriam constar nos arts.154-a e seguintes, logo após os crimes contra a inviolabilidade de correspondência (arts.151 e 152) e inviolabilidade de segredos (arts. 153 e 154).

O legislador, porém, demonstrando sua pouca intimidade com regras básicas da dogmática penal, optou por posicionar os tipos logo após os crimes contra a saúde pública (art.267-285).

SOLUÇÃO PROPOSTA:

Criação da Seção V – Dos crimes contra a inviolabilidade dos dados informáticos no Capítulo VI, do Título I da Parte Especial do Código Penal, iniciando os novos tipos penais a partir do art.154-a.

Criminalizações

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

O primeiro equívoco visível no art.285-A é exigir que a conduta seja praticada com violação de segurança, o que implica na ausência de tipicidade da conduta do hacker que invade um computador doméstico não protegido por um firewall ou um antivírus. Seria o equivalente a permitir que um ladrão furte uma casa, tão-somente porque seu proprietário deixou a porta aberta. Um completo absurdo.

Não menos absurda é a necessidade de uma "expressa restrição de acesso". O fato de alguém deixar seu notebook na mesa de um restaurante enquanto vai ao banheiro, não torna lícita a conduta de quem se aproveita desta ausência para acessar os dados. Não é razoável exigir que o proprietário tenha que declarar expressamente que ninguém está autorizado a acessar seus dados. Trata-se de uma restrição tácita elementar, não amparada, porém, pelo projeto Azeredo.

Por outro lado, a mesma lei que contém estas lacunas na proteção do usuário doméstico incauto, permite interpretações bastante rigorosas, já que a redação do tipo é bastante vaga.

Algum juiz poderia entender, por exemplo, que a restrição prevista

neste artigo abarca a conduta de alguém que usa um crack (pequeno software para retirar restrições de acesso em softwares originais que visam a proteção de direitos autorais) para executar um jogo de computador sem a necessidade do uso do DVD.

Ainda que não pareça ser este o intuito do legislador, é preciso lembrar que, após aprovada uma lei, pouco importa qual era a pretensão original do legislativo, pois o juiz a interpretará de acordo com a sua livre convicção. Por fim, ainda em relação a este artigo, o parágrafo único prevê um aumento de pena para a hipótese de o agente se utilizar de nome falso para a prática do crime. Trata-se de mais um grave equívoco do legislador, que parte do pressuposto de que haverá casos em que o autor utilizará de seu nome verdadeiro para a prática do crime, o que é bastante improvável.

As qualificadoras só devem impor incremento de pena se – e somente se – a circunstância a ser utilizada como qualificadora demonstrar um plus de reprovabilidade da conduta do agente, isto é, uma gravidade maior daquela já punida pela pena do caput do artigo.

Em seguida, continua o projeto:

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Trata-se de uma conduta que é desdobramento natural da prevista no art.285-A e, portanto, a boa técnica penal recomenda que seja abordada em parágrafos do artigo anterior e, não, de um novo tipo, pois, caso aprovado o projeto, o agente não poderia ser condenado simultaneamente nas iras do art.285-a e 285-b, já que para obter ou transferir os dados (art.285-b) é condição necessária que num primeiro momento ele os acesse (art.285-a).

SOLUÇÃO PROPOSTA:

Reescrever os arts.285-a e 285-b, em um único artigo, dando-lhes uma redação mais objetiva e prevendo hipóteses privilegiadoras e qualificadoras que, de fato, demonstram uma menor ou uma maior reprovação social da conduta. A título de sugestão:

Acesso não autorizado a sistemas computacionais

Art. 154-A. Acessar, sem utorização, dados ou programas em sistema computacional alheio.

Pena – detenção, de um a seis meses, ou multa.

§ 1º. A pena será reduzida de um a dois terços ou o juiz aplicará somente a pena de multa se o agente não inha intenção de lucro ou de obter vantagem de qualquer espécie para si ou para outrem e foi pequeno o prejuízo para a vítima.

> o artigo imporia uma vigilância constante aos acessos do cidadão comum

§ 2º. Aumenta-se a pena de um terço até metade:

I. se o crime é cometido contra sistema computacional da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II. se o crime é cometido por funcionário público ou por quem exerça a função de administrador de sistemas ou assemelhada, com abuso de poder ou com violação de dever inerente a função;
III. se o agente destrói ou danifica o sistema computacional ou os dados nele armazenados;
IV. se o agente divulga a terceiros as informações obtidas, causando dano material ou moral à vítima.

§ 3º. Somente se procede mediante representação, salvo na hipótese do § 2º, II, em que a ação é pública incondicionada.

Finalmente, cabe analisar o artigo mais polêmico do projeto:

Vigilância

Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:
I. manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;
II. preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;
III. informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.

A idéia de que todo usuário de Internet tenha seus registros de acesso armazenados nos servidores por 3 anos é exageradamente invasiva e fere visivelmente o art.5º, X, da Constituição da República que dispõe:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Além do mais, se aprovado, o dispositivo inviabilizaria a inclusão digital por meio de redes sem fio (Wi-fi) em áreas de difícil acesso, tais como florestas, regiões interioranas com pouca infra-estrutura ou mesmo favelas, criando uma desnecessária e cara burocratização ao se exigir o cadastro prévio dos usuários.

Não bastasse a violação de privacidade dos usuários e a burocratização da redes de Internet sem fio, a proposta mostra-se bastante ingênua, pois criminosos e pessoas mal-intencionadas de uma forma geral, poderiam conseguir acesso à Internet com relativa facilidade em lan-houses, com o uso de documentos falsos ou de terceiros. Também não faltam recursos técnicos que permitam a usuários de computadores camuflarem seus endereços I.P., de modo que, mesmo que acessem de sua casa ou local de trabalho, seus atos não deixem rastros na rede.

Finalmente, o parágrafo terceiro cria ainda a obrigação de delação por parte do provedor de acesso, colocando os responsáveis pelo serviço na difícil condição de vigias dos atos de centenas ou milhares de usuários. Algo como exigir que as operadoras de telefonia delatem seus usuários quando houver indícios da prática de crimes em seus telefonemas. Dispositivo fadado a ser letra morta, portanto.

Em suma, o artigo imporia uma vigilância constante aos acessos do cidadão comum, dificultaria em muito a inclusão digital por meio de redes sem fio e, por outro lado, seria ineficaz no combate aos verdadeiros criminosos da Internet.

SOLUÇÃO PROPOSTA:
a supressão integral deste artigo do projeto de lei.

:: À GUISA DE CONCLUSÃO

Finalmente, é preciso advertir o leitor de que o projeto é composto ao todo por 23 artigos e que só tratamos aqui de 3 deles, pois os consideramos eivados dos maiores equívocos.

Nosso silêncio quanto aos demais não deve ser interpretado, porém, como aprovação do texto, mas tão-somente, como uma estratégia para que não se perca o foco da discussão dos temas mais relevantes.

O conjunto do texto do projeto é muito fraco do ponto de vista técnico-penal e sua adequada reestruturação implicaria praticamente na criação de um novo projeto, razão pela qual, o melhor a se fazer atualmente é arquivar o presente projeto e criar uma comissão formada por professores de Direito Penal, professores de Ciência da Computação e representantes da sociedade civil para que construam democraticamente um novo texto que contemple os interesses dos brasileiros de uma Internet razoavelmente segura, preservando os direitos fundamentais da pessoa humana.

Graciela Selaimen
editora da poliTICs e
diretora do Instituto Nupef

Redes sociais

a quem pertence seu perfil?

Um usuário da rede social Facebook – que hoje reúne mais de 250 milhões de usuários[1] no mundo – passou por momentos tensos, no mês passado, ao entrar no sítio Web da rede e encontrar a foto de sua mulher publicada num anúncio que dizia: "Ei, Peter, uma solteira sexy espera por você". O anúncio era de um serviço que promovia encontros – não exclusivamente virtuais -, e Peter levou mais um susto ao procurar explicações sobre como a foto de sua mulher tinha ido parar ali[2]. O fato é que ela havia autorizado o uso da foto – e o mais incrível é que eu mesma e provavelmente você, leitor ou leitora (se for usuário/a do Facebook) também corremos o mesmo risco de ter nossas fotos ilustrando um anúncio sabe-se lá de que, no sítio dessa rede social, com nossa autorização.

Um dos problemas que leva a este tipo de situação está naquelas páginas chatas de ler, cujo conteúdo a maioria dos usuários ignora, marcando automaticamente uma caixinha que diz "cadastre-se": são os Termos de Uso e a Política de Privacidade, espaços onde o Facebook oferece explicações sobre o que pode e o que não pode fazer com seus dados pessoais. A vontade de criar logo uma conta na rede social e encontrar os amigos, conhecidos, contatos de amigos, possíveis futuros contatos – e saber o que eles andam fazendo e o que estão pensando – faz a maioria de nós, usuários desavisados, aceitar os termos e a política do serviço sem ler. Só que é justamente ali que temos a primeira chance de descobrir como evitar surpresas desagradáveis no futuro, como a do

1. De acordo com a estatísticas do Facebook: http://www.facebook.com/press/info.php?statistics 2. A mulher de Peter, Cheryl Smith, conta esta história em seu blog e ensina como ajustar as configurações na conta do Facebook para evitar transtornos parecidos: http://www.culturesmithconsulting.com/change-your-facebook-settings-or-else/

Peter. O Facebook adota, para estas e outras situações relacionadas à privacidade dos membros da rede, a chamada polí tica do "opt-out" na qual o usuário, depois de cadastrado, pode decidir alguns limites para o usos de seus dados por parte do Facebook e de seus associados. Isso significa que a configuração padrão da rede permite ampla divulgação – além de outras possibilidades de uso - dos dados que os usuários inserem e compartilham em suas contas, ou em seus "perfis". Para limitar esta ampla possibilidade de uso de dados pessoais, o usuário deve optar por termos de uso que são exceções à configuração padrão, o que se chama de "opt-out". A alternativa que seria mais recomendável, nesta e em qualquer outra rede social, seria uma política de privacidade que vai justamente no sentido oposto: a política "opt-in". Neste caso, as configurações padrão e a política de funcionamento da rede seriam mais "amigáveis" em relação à proteção da privacidade do usuário, e as exceções seriam aqueles casos em que o usuário aceita e prefere ter seus dados divulgados, compartilhados com terceiros (geralmente, parceiros comerciais da rede social) e utilizados para diversos fins, com autorização do próprio usuário.

No caso específico de anúncios, por exemplo, isso fica bem claro nos Termos de Uso do Facebook, onde a empresa afirma:

1. *You can use your privacy settings to limit how your name and profile picture may be associated with commercial or sponsored content. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.*

A citação está em inglês porque o Facebook não oferece uma versão em Português de seus Termos de Uso. Uma introdução ao documento "*Statement of Rights and Responsibilities*[3]" afirma que "a versão em língua inglesa deste documento será a única versão juridicamente válida e passível de reger a sua conduta no Facebook". Portanto, além de ler cuidadosamente os Termos de Uso (de preferência em inglês, mas também pode ser em espanhol, italiano, francês ou alemão[4]), a Política de Privacidade (esta, felizmente, em português), o usuário precisa entender tudo direitinho e fazer suas opções sobre o que pode e o que não pode ser feito com seus dados pessoais.

Este não é o primeiro caso em que o uso indevido de dados pessoais pelo Facebook repercute na mídia e na "blogosfera". Na verdade, episódios desse tipo fazem parte da história desta rede social: desde 2006 – ano em que a rede foi aberta para usuários de qualquer parte do mundo[5] -, acontecem mobilizações em função de novas funcionalidades incorporadas ao serviço ou de mudanças nos termos de uso e nas políticas da rede. Um bom exemplo disso foi a celeuma causada pela introdução da News Feed[6] – funcionalidade que entrou no ar no dia cinco de setembro de 2006, e oferecia a possibilidade aos usuários de acompanharem em tempo

3. Disponível em http://www.facebook.com/terms.php?ref=pf 4. Em 27 de agosto de 2009, estas eram as línguas nas quais havia versões do documento. 5. O Facebook foi criado por Mark Zuckerberg em 2004 – inicialmente concebido como um site de rede social para alunos da Universidade de Harvard. Em fevereiro de 2006, o Facebook foi aberto para alunos de escolas secundárias e funcionários de algumas grandes empresas, incorporando outras redes sociais já existentes nestas instituições. Em setembro do mesmo ano, esta já robusta rede social passou a aceitar qualquer usuário de qualquer parte do mundo.

real quaisquer mudanças de perfil e atividades de seus contatos na rede. Assim, se um usuário atualizasse em seu perfil seu status – por exemplo, de "casado" para "namorando" -, todos os seus contatos eram imediatamente notificados. A introdução desta funcionalidade não incluiu nenhuma consulta prévia aos usuários do Facebook e causou mal estar entre um número significativo deles: mais de 700 mil assinaram uma petição online demandando a retirada da funcionalidade, alegando que sua privacidade estava comprometida pelo serviço.

Outro caso – este, mais recente – deu-se em fevereiro de 2009, quando foram revisados os Termos de Uso da rede social. A versão original do documento garantia que, mediante o fechamento da conta do usuário na Facebook, este deixava de ter quaisquer direitos sobre o conteúdo divulgado por aquele usuário durante o período de existência daquela conta. Na nova versão dos Termos de Uso divulgados no início de fevereiro passado, qualquer conteúdo que um usuário tenha publicado em sua área pessoal na rede social poderia ser utilizado pelo Facebook sem nenhum tipo de restrição, mesmo após o encerramento da conta – garantindo ao Facebook direitos permanentes e retroativos de propriedade sobre dados pessoais do usuário.

Mais uma vez, ONGs e usuários se levantaram contra uma política daquela rede social: encabeçadas pela EPIC[7], mais de uma dúzia de organizações que defendem direitos de privacidade e direitos do consumidor deram início a mobilizações contra a medida do Facebook. Além das entidades civis, grupos de usuários se organizaram e levaram adiante inúmeras manifestações e protestos – a maior delas feita pelo grupo People Against the New Terms of Service[8], que reuniu mais de 130 mil usuários. Dezenas de blogs e sítios Web serviram de plataforma para protestos, e, assim que a revista PCWorld[9] publicou a decisão da EPIC de levar uma reclamação formal à FCC (Comissão Federal de Comunicações dos Estados Unidos), Mark Zuckeberg, criador e diretor executivo da rede, manifestou-se em defesa da privacidade dos usuários do Facebook, no texto "*On Facebook, People Own and Control Their Information*":

Estamos vivendo um momento interessante no desenvolvimento do mundo online onde problemas deste tipo estão sendo elaborados e resolvidos. Este é um terreno difícil e nós vamos dar passos em falso, mas, sendo hoje o principal serviço para compartilhamento de informações, nós assumimos estas questões e assumimos nossa responsabilidade em colaborar para resolvê-las, com muita seriedade[10].

Poucos dias depois, o Facebook voltava atrás e restaurava os Termos de Uso originais. No dia 26 de fevereiro era anunciada a nova política de governança do Facebook[11], que "oferece aos seus usuários ao redor do mundo o papel de determinar as futuras políticas de governança do serviço", numa ação "sem precedentes".

Evidentemente, o Facebook não é o único serviço de rede social que adota

6. Bruce Schneier publicou artigo interessante sobre este episódio, que pode ser lido em http://www.schneier.com/blog/archives/2006/09/facebook_and_da.html
7. A Electronic Privacy Information Center – em http://www.epic.org 8. Em http://www.facebook.com/group.php?gid=7706910743 2 9. A notícia está publicada em http://www.pcworld.com/article/159703/facebook.html?tk=rel_news 10. Texto completo (em inglês) em http://blog.facebook.com/blog.php?post=54434097130. Este trecho foi traduzido por mim.

medidas controversas em relação à privacidade de seus usuários.

O tema da proteção da privacidade em redes sociais tem ganho cada vez mais espaço de destaque em eventos e fóruns internacionais onde são discutidas políticas de Internet, direitos humanos, governança da rede mundial. Um dos documentos mais elucidativos sobre este tema é o relatório[12] do Grupo de Trabalho Internacional sobre Proteção de Dados nas Telecomunicações divulgado em março de 2008 – também chamado de "Memorandum de Roma". Este documento explica que, em termos da defesa da privacidade na Internet, as redes sociais representam um enorme desafio – principalmente pelo fato de as informações divulgadas nestas redes serem publicadas ali pelos próprios usuários e utilizadas com seu consentimento. A maioria dos marcos regulatórios de proteção à privacidade tem a função de definir regras para proteger as pessoas do uso indevido de dados pessoais por parte da administração pública (inclusive por parte da polícia e de outras autoridades) e por parte de empresas privadas – mas ainda há poucas experiências de regulação que abranjam a proteção a dados publicados voluntariamente por usuários de serviços online - este é um desafio recente, que ganha importância à medida em que cresce exponencialmente o número de pessoas que compartilham informações em redes sociais, blogs, microblogs, etc.

O Memorandum de Roma afirma, em sua introdução, que "legisladores, autoridades de proteção de dados e provedores de serviços de redes sociais enfrentam hoje uma situação inédita. Enquanto as redes sociais oferecem uma nova gama de oportunidades para a comunicação e o intercâmbio de qualquer tipo de informação em tempo real, o uso de tais serviços também pode pôr em risco a privacidade de seus usuários (e mesmo a de outras pessoas que não são sequer registradas em nenhuma rede social)". Entre alguns dos riscos apontados, estão:

- a perenidade dos dados retidos pelas redes sociais. Algumas redes se recusam a deletar os dados recolhidos dos usuários, mesmo após a extinção dos seus perfis; outras deletam os dados, mas não têm controle sobre a manutenção destas informações nas bases de dados de terceiros - outras empresas associadas ou mesmo poderosas ferramentas de busca;
- a negociação de dados pessoais e perfis com empresas de marketing direcionado;
- o roubo de identidade - por exemplo, qualquer pessoa pode copiar os dados de um perfil na rede social (inclusive as fotos) e utilizar este perfil em outros sítios web, para outras finalidades;
- o uso indevido de dados pessoais por terceiros - por exemplo, para a vigilância de empregadores sobre os hábitos e relacionamentos de funcionários, ou mesmo por serviços de agências estatais de segurança, especialmente em países onde há perseguições políticas.

Há várias recomendações apresentadas no relatório – para reguladores, para provedores de serviços de redes sociais e para usuários.

11. Facebook Opens Governance of Service and Policy Process to Users Releases Draft Principles and Statement of Rights and Responsibilities For User Review, Comment and Vote - http://www.facebook.com/press/releases.php?p=85587 12. Publicado em www.datenschutz-berlin.de/.../WP_social_network_services.pdf

Como ainda não existe no Brasil um marco regulatório para a proteção da privacidade (e este é um vácuo especialmente crítico no que diz respeito à privacidade nas redes digitais de comunicação), consideramos importante reproduzir aqui algumas das recomendações dirigidas aos reguladores:

1. Criar a opção do direito ao uso de pseudônimo[13] em marcos regulatórios em que este direito não esteja previsto;
2. Assegurar que os provedores de serviços de redes sociais sejam honestos e transparentes sobre quais informações são realmente necessárias à oferta dos serviços básicos, de modo que os usuários façam escolhas conscientes sobre a adesão à rede social e de modo que possam recusar quaisquer possibilidades de usos secundários (especialmente para anúncios direcionados), pelo menos através de política de "opt-out". Note-se que há problemas específicos nos casos de obtenção de consentimento por parte de pessoas menores de idade[14].
3. Introduzir a obrigatoriedade de aviso sobre falhas de segurança na proteção dos dados registrados. Os usuários somente serão capazes de lidar com os crescentes riscos do roubo de identidade se eles forem notificados de falhas na proteção de suas informações pessoais. Ao mesmo tempo, esta medida ajudaria a obter um panorama sobre o quanto as empresas são capazes de oferecer a segurança dos dados recolhidos em seus serviços, e estimularia mais a adoção e a otimização de medidas de segurança.
4. Reavaliar os existentes marcos regulatórios no que diz respeito às possibilidades de controle (especialmente por terceiros) de dados pessoais publicados nos sítios de redes sociais, com vistas à possibilidade de atribuir aos provedores de serviços de redes sociais mais responsabilidade em relação a estes conteúdos.
5. Aprimorar a abordagem de temas ligados à proteção da privacidade no sistema educacional. Como a oferta de dados pessoais tornou-se parte do dia-a-dia – especialmente de jovens -, a proteção da privacidade e as ferramentas para a autodefesa devem fazer parte do currículo escolar.

Aos usuários de redes sociais o relatório recomenda principalmente cuidado, informação, atenção, e adoção de medidas simples, tais como variar o nome e a senha em diferentes serviços, bem como eleger opções de serviço que sejam restritivas à ampla divulgação dos dados compartilhados nas redes. Este tipo de cautela não custa muito – mudar as configurações de privacidade no Facebook, por exemplo, dá trabalho mas não é tarefa impossível, principalmente quando se tem um passo a passo como o que a Cheryl Smith generosamente oferece em seu blog. Dá para fazer isso entre um quiz e outro. E por falar em quiz, que tal tentar este aqui: *What Do Facebook Quizzes Know About You ?*[15]

13. O uso do pseudônimo neste contexto significa o direito de estar numa rede social sem ter que revelar sua "verdadeira identidade" aos outros usuários do serviço, ou ao publico em geral – isso não exclui a necessidade de se revelar a identidade e fornecer dados pessoais verificáveis ao provedor do serviço da rede social no momento do registro do usuário. 14. Conforme o documento "Children's' Privacy On Line: The Role of Parental Consent", adotado na 31a. Reunião, Auckland (Nova Zelândia), 26/27 de março 2002; http://www.datenschutz-berlin.de/attachments/205/child_en.pdf?1200656702 15. Em http://blog.aclu.org/2009/06/11/quiz-what-do-facebook-quizzes-know-about-you/