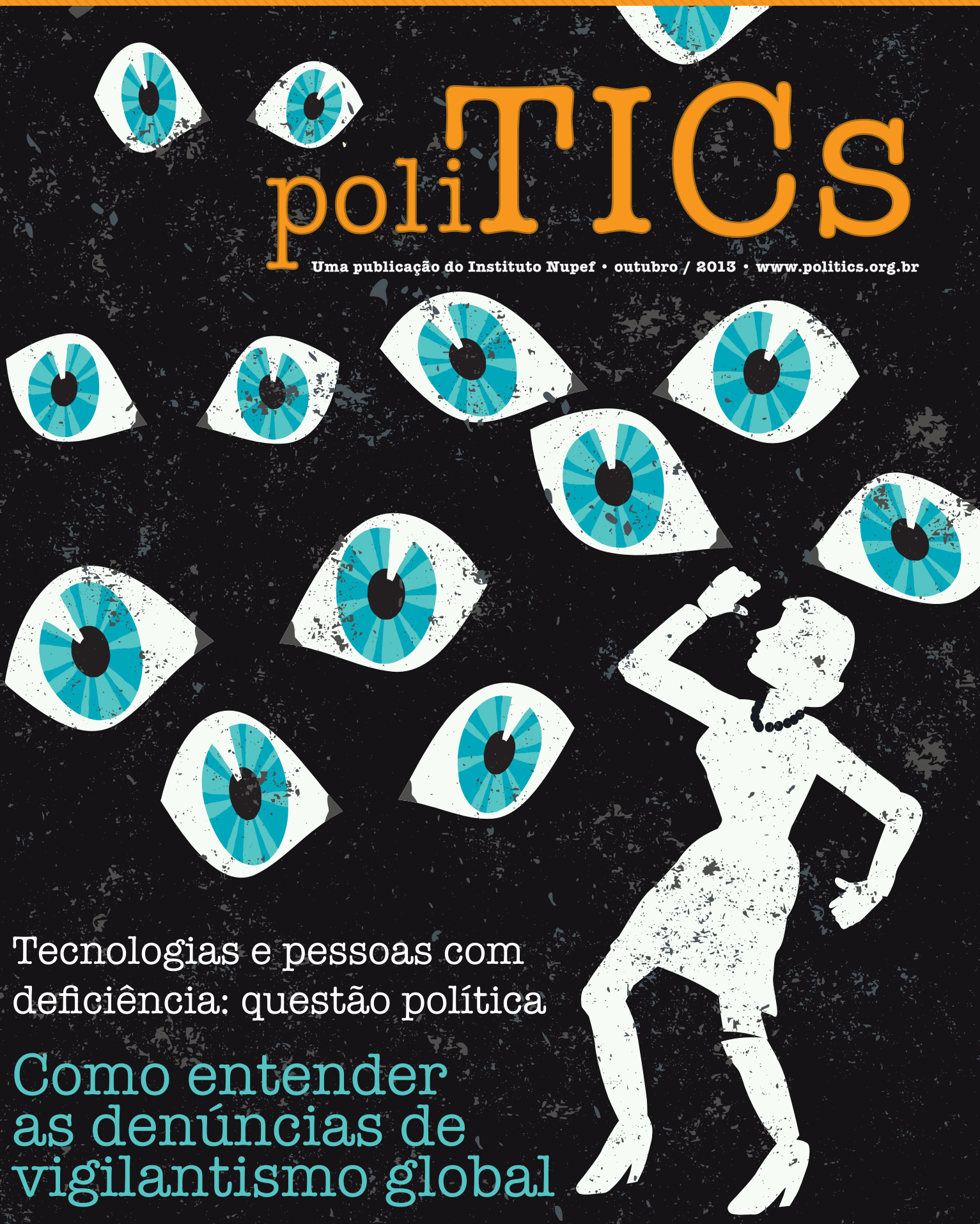
> PROTEÇÃO DE DADOS na União Europeia

> A BITCOIN pode derrubar os EUA

> e-SAÚDE e privacidade no Brasil

poliTICs

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



Tecnologias e pessoas com deficiência: questão política

Como entender as denúncias de vigilantismo global

poliTICs nº16

Índice

poliTICs

EDITOR CARLOS A. AFONSO

CAPA, PROJETO GRÁFICO E DIAGRAMAÇÃO MONTE DESIGN

DISTRIBUIÇÃO VIVIANE GOMES

TRADUÇÕES RICARDO SILVEIRA

Esta é uma publicação do Instituto Nupef.
Versão digitalizada disponível em www.politics.org.br e no sítio do Nupef - www.nupef.org.br
Para enviar sugestões, críticas ou outros comentários: graciela@nupef.org.br

instituto nupef

Rua Sorocaba, 219 | 501 - parte | Botafogo | 22271-110
Rio de Janeiro RJ Brasil | telefone +55 21 2527-0294

Apoio:

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

Google

nic.br
Núcleo de Informação e Coordenação do Ponto BR

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

ISSN: 1984-8803

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

Editorial

Esta edição da poliTICs trata dos inúmeros desafios do emprego de tecnologias de informação e comunicação que afetam a privacidade, a segurança e a acessibilidade, em um contexto de crise econômica mundial e de revelações de espionagem maciça por parte de governos dos países desenvolvidos, em especial os EUA e a Inglaterra.

Pedro Rezende sintetiza com clareza as vulnerabilidades a que estamos todos submetidos no uso da Internet, descrevendo os mecanismos utilizados para invadir redes e equipamentos e os limites das técnicas de proteção na ponta do usuário.

Fernando Botelho faz uma crítica detalhada das políticas públicas brasileiras relativas a tecnologias assistivas para pessoas com deficiência visual e apresenta uma lista bem fundamentada de sugestões envolvendo tecnologias apropriadas e democratização de conteúdos, baseado em sua extensa e qualificada experiência no tema.

A publicação do texto de Rick Falkvinge coincide com o aprofundamento sem precedentes da crise política dos EUA, que pode levar a um calote propagado para o sistema financeiro mundial, dependente de uma moeda sem lastro. O artigo descreve a extensão dos riscos e analisa o surgimento de sistemas alternativos de troca de valores, com o exemplo da bitcoin.

Enquanto debatemos no Brasil o projeto de lei de proteção de dados pessoais, Cory Doctorow mostra os desafios enfrentados pela Europa no processo de discussão sobre as novas regras de proteção de dados. Tal como ocorre no caso do nosso Marco Civil, Cory descreve o "frenesi do lobby" em Bruxelas para aprovar emendas e propostas, e analisa os desafios da anonimização ou pseudonimização de conteúdos.

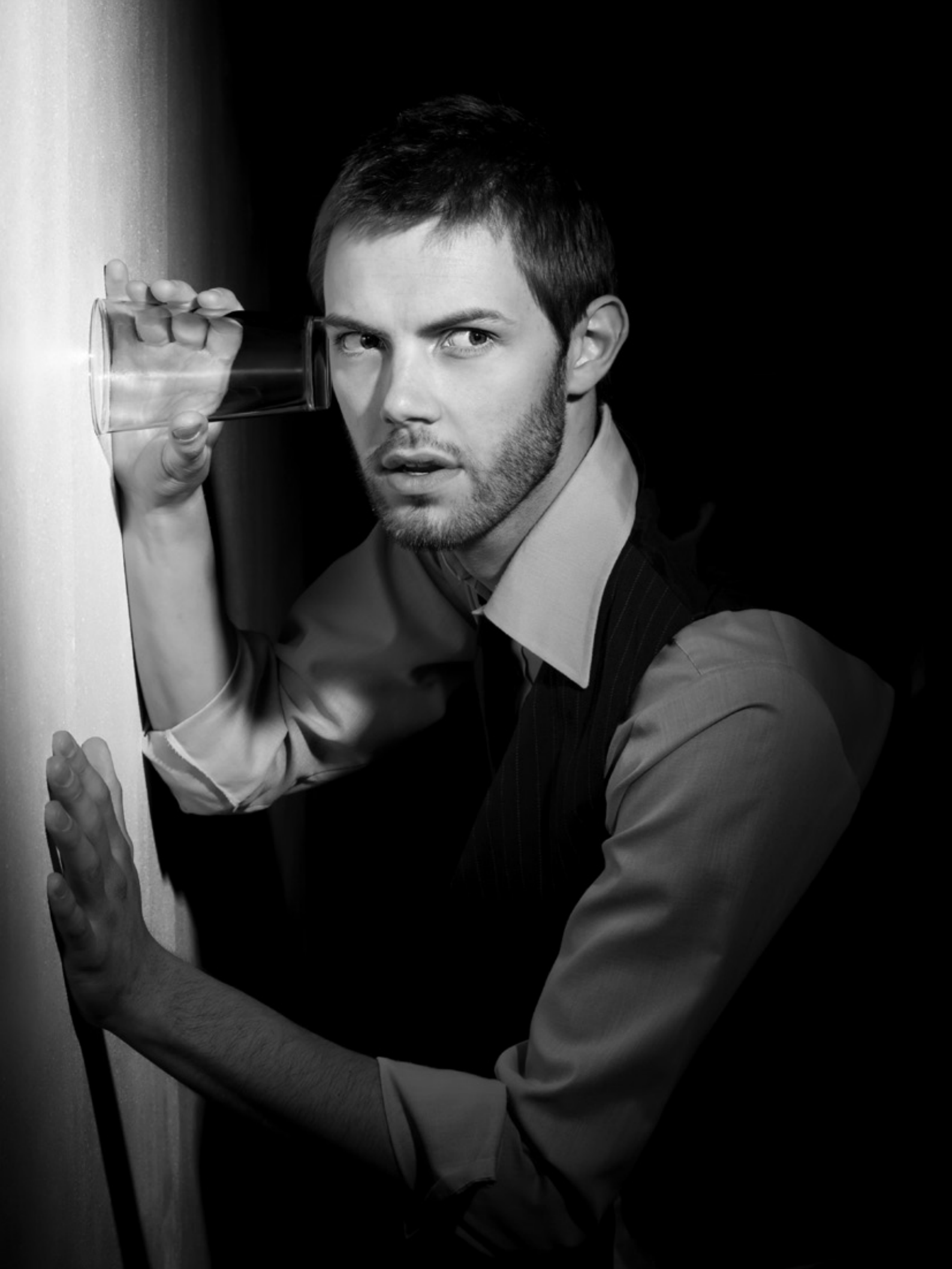
Fechamos a edição com o texto dos pesquisadores do Instituto Nupef, Koichi Kameda e Magaly Pazello, que descrevem a situação atual do uso de tecnologias de informação e comunicação em serviços de saúde no Brasil e os limites quanto a salvaguardas legais e normativas para a proteção da privacidade dos usuários desses serviços.

Boa leitura! ●

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

Um abraço,

Carlos Alberto Afonso – *Editor da poliTICs*



Pedro Antonio Dourado de Rezende
professor do Departamento de Ciências da Computação, Universidade de Brasília.

Como entender as denúncias de vigilantismo global

A divulgação de documentos obtidos pelo ex-funcionário de empresa contratada pela NSA, Edward Snowden, surpreendem mais pela conduta dele e pelas reações que essa conduta provocou. Snowden está soprando em um castelo de cartas que quanto mais cedo cair menos mal fará, ao menos para as vítimas mais indefesas do consequente caos. Caos que de um jeito ou de outro virá, e que está sendo gerado não por ele, mas pela alquimia financeira das treze casas bancárias que controlam a economia no mundo. Elas estão criando dinheiro sem lastro, via malabarismos eletrônicos contábeis, que furtam da moeda circulante sua função de reserva de valor enquanto a mesma é ainda mais rapidamente acumulada em contas de poucos.

Em entrevista ao portal RT o analista financeiro Max Keiser[1], experiente inovador em táticas especulativas para pregões eletrônicos, aponta para o cenário dessas revelações como ele o vê: a compania onde Snowden trabalhava, Booz Allen, junto com algumas outras parceiras são mentoras da manipulação que ocorre em importantes mercados globais de juros e de câmbio, como o LIBOR e o

1. Ver http://rt.com/op-edge/keiser-international-confidence-crumbling-snowden-182

FOREX, e essa manipulação é o combustível que mantém o "império militar" funcionando, supondo eu que Keiser se refere aí à OTAN.

A economia dos EUA por si só não consegue mais manter suas ambições militares, e para isso essas ambições precisam manipular mercados. O tipo de inteligência que Snowden pode mostrar como se agrega, é fundamental para essas manipulações. Elas podem instrumentar a Booz Allen e suas parceiras a canalizar bilhões de dólares para irrigar campanhas militares norte-americanas. Então, essa fúria contra Snowden na verdade seria por causa de dinheiro, e não de segurança. Keiser prossegue nos lembrando que a Casa Branca é refém de Wall Street, dos fundos hedge, de banqueiros corruptos e também da Booz Allen, e que as empresas parceiras no PRISM[2] têm incentivos financeiros para participar desse programa, além dos possíveis pedágios para acesso a dados pessoais dos seus clientes.

Os índices cobiçados são sensíveis a dados econômicos. Se a Booz Allen e certas parceiras podem manipular esses dados, podem com isso manobrar os índices que guiam os mercados – incluindo preços de ações em pregões voláteis, inclusive das suas próprias. Se a Booz Alen e certas parceiras coletam informações privilegiadas, outras parceiras podem, com tais informações, ganhar bilhões e bilhões de dólares para o esquema através de operações algorítmicas em pregões automatizados, que são efetuadas por software em altíssima velocidade, com enormes volumes e quase sempre disparadas por diminutas variações de preços, uma novidade tecnológica ainda infiscalizável e sujeita a sérias falhas[3]. É claro – para Keiser – que os grandes bancos de Wall Street e de Londres estão fazendo isso.

Assim, toda esta fúria persecutória contra Snowden pode ter causa em manobras virtuais que só darão lucro – fraudulento – enquanto houver confiança coletiva em moedas sem lastro. Não é por causa do vazamento de segredos de Estado em si, já que isso ocorre a toda hora sem que os delatores sejam importunados, inclusive a respeito deste caso[4], ou mesmo mentindo[5], se o efeito pretendido na grande mídia for o de maquiar a imagem do governo. Infelizmente, os EUA não têm mais dinheiro para financiar suas guerras e aí o governo precisa recorrer à manipulação de mercados via bisbilhotagem. Esta realidade é última coisa que aquele país quer ver vindo à tona de forma crível[6], por atos de um "insider" em fuga candidato a mártir. Pois o filão secreto de ouro (de tolo) que Keiser aponta seria, na lógica do capital, assim "roubado."

Um despiste que circula, no argumento de que ele é traidor e por isso não merece crédito, tenta tapar o sol com peneira. Se não merece crédito, por que tanta fúria persecutória contra o

2.Ver http://rt.com/op-edge/nsa-network-global-fascism-167/. Sobre o PRISM, ver http://pt.wikipedia.org/wiki/PRISM_%28programa_de_vigil%C3%A2ncia%29 3.Ver http://www.cnbc.com/id/48443271 4.Ver http://www.reuters.com/article/2013/06/26/us-usa-security-tactics-idUSBRE95P00R20130626 5.Ver http://nymag.com/nymetro/news/media/features/9226 6.Ver http://br.reuters.com/article/topNews/idBRSPE96C02B20130713

jovem supostamente desequilibrado e delirante, produzindo crises diplomáticas mais parecidas com tiros no pé? A humilhação aérea ao mais digno índio aimara, o presidente Evo Morales, por exemplo, aparentemente instigada pelo embaixador americano na Áustria William Eacho[7], esbarrou no fiel de uma balança delicada do xadrez diplomático, cuja sacudida legitimou a acolhida de Snowden pelo governo da Rússia. Esse quebra-cabeças portanto ainda tem mais peças a encaixar.

Entre os mecanismos utilizados pelos EUA para interceptar comunicações, as *backdoors* de programas e sistemas operacionais proprietários são apenas uma das vulnerabilidades exploradas. Desde 2001 é sabido que o programa Echelon[8] interceptava sinais de satélite, mas hoje sabemos mais: que as *backdoors* agora exigidas por lei americana (CALEA)[9] nos roteadores de grande porte homologados nos EUA estendem esse vigilantismo também para quase todas as rotas de fibra óptica, centralizadas na arquitetura atual das espinhas dorsais (*backbones*) transcontinentais, que por decisões empresariais bordeiam os pontos de troca de tráfego nacionais. O que cobre praticamente todos os meios de transmissão digital a longa distância hoje em uso.

Mas hoje sabemos também, por revelações de Snowden[10], o que em 2001 apenas suspeitávamos (com o caso NSAKEY)[11]: que a vigilância se

Edward Snowden

estende também, em capilaridade, a quase toda plataforma individual e computador pessoal, àquelas e àqueles que usam sistema operacional proprietário Microsoft Windows, neutralizando nelas e neles a única possível defesa restante, que seria a criptográfica; e capilarmente estendido também a quase todo serviço global agregado, via programa PRISM.

Uma *backdoor* funciona como uma porta virtual secreta, embutida em software, acionável remotamente por quem a conhece para dar passagem sorrateira a dados. Isso funciona tanto para dados copiados de dentro do sistema e enviados para quem controla remotamente a *backdoor*, como também para dados enviados por quem controla remotamente a *backdoor* para dentro

7. Ver http://www.correntewire.com/obamas_austrian_ambassador_was_source_of_bad_intel_that_snowden_was_on_the_morales_plane 8. Ver http://pt.wikipedia.org/wiki/Echelon 9. Sobre a CALEA, ver http://pt.wikipedia.org/wiki/CALEA 10. Ver http://revistaforum.com.br/blog/2013/07/snowden-microsoft-colabora-ativamente-com-a-nsa-e-o-fbi 11. Sobre a *backdoor* NSAKEY no sistema Windows, ver http://en.wikipedia.org/wiki/NSAKEY

do sistema, visando alterá-lo ou manipulá-lo à sorrelfa (inclusive, se for o caso, para apagar ou alterar dados de algum usuário do sistema).

Em um roteador destinado a distribuir o tráfego de dados entre rotas de saída, por satélite ou por fibra óptica, por exemplo, uma *backdoor* pode ser programada para grampear por atacado o fluxo que por ali passe, em todo ou em partes selecionáveis por áreas de origem ou de destino, com a cópia do fluxo enviada para repositórios de agências como a NSA, que para recebê-los inaugura o maior centro de dados jamais construído para esse fim[12].

É impossível impedir a interceptação, mesmo empregando criptografia (por mais robusta que seja), se o sistema operacional rodando no computador de um dos interlocutores for fornecido por uma parceira do PRISM. E é justamente uma empresa que proíbe em contrato a engenharia reversa dos seus sistemas proprietários, blindando-se de admitir publicamente que os mesmos embutem *backdoors*, e que implode os mais recentes diante de qualquer tentativa de sanitizá-los contra *backdoors* embutidos, que fornece mais de 90% desses sistemas.

Por outro lado, sem empregar criptografia é impossível impedir a interceptação, seja com sistema operacional livre ou proprietário, se a rota entre os interlocutores tiver algum ponto de passagem obrigatória por um roteador que tenha *backdoor*. Seja *backdoor* embutida pelo fabricante, o que é obrigatório nesse tipo de equipamento se o fabricante quiser que seja homologado nos EUA, seja instalado por empresa de telecomunicação que os opera, situação previsível onde tais empresas sejam parceiras de algum dos inúmeros programas de espionagem global ou de vigilantismo militar.

É possível impedir a interceptação apenas entre plataformas auditáveis, portanto com sistemas livres e de código aberto, que sendo livres não requerem cadastramento para serem habilitadas, sanitizadas contra *backdoors* nas duas pontas da comunicação, combinada com o uso correto de criptografia robusta. Mas isso é relativamente possível apenas, pois tais condições são difíceis de serem garantidas, já que são relativas à competência técnica de potenciais adversários com interesse em interceptar no varejo, haja vista as ferramentas virtuais de ataque conhecidas como "*zero-day exploits*"[13], que proliferam num comércio cinzento aquecido pelas verbas ocultas que sustentam esses esquemas[14].

Não é por acaso que o braço brasileiro do cartel das grandes empresas de software proprietário demoniza tanto o software livre[15], que é a única alternativa para se usar a Internet de forma efetivamente protegível contra interceptação de varejo, quando devidamente sanitizada nas pontas de uma comunicação corretamente criptografada.

12. Ver https://www.youtube.com/watch?v=xLTXRF4w-Cc 13. Ver http://en.wikipedia.org/wiki/Zero-day_attack 14. Ver http://mobile.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html 15. Ver http://www.dignow.org/post/associa%C3%A7%C3%A3o-brasileira-das-empresas-de-software-diz-que-brasil-perdeu-dez-anos-discutindo-software-livre-5725569-67902.html

Não é de hoje que os braços legais dos agentes deste esquema incitam todos à devassidão digital auto-consentida, enquanto seus lobbies pressionam legislativos contra o uso autônomo da criptografia, com os quatro cavaleiros do ciberapocalipse – pornografia infantil, terrorismo, pirataria e cibercrime – servindo sempre de espantalhos.

Medidas de infraestrutura anunciadas pelo governo brasileiro (lançamento de satélite nacional, construção de cabos submarinos próprios aos EUA, Europa e África) não são suficientes para impedir a espionagem do tráfego de dados envolvendo serviços globais oferecidos por parceiros privados do programa PRISM. Em casos envolvendo o uso de serviços globais, não há medida neutralizadora possível a não ser a do usuário optar por serviços alternativos ou semelhantes instalados e operados com tecnologia livre e adequadamente implementada e gerenciada.

Mesmo assim, o efeito de proteção será aí relativo ao poder de fogo disponível ao vigilantismo global, modulado pelo interesse nele despertável pelo perfil rastreável de quem queira se proteger. No caso de redes sociais, essa adequação requer redes federadas colaborativas[16] e ferramentas criptográficas próprias para anonimização, como aquelas oferecidas por softwares e serviços do projeto Tor[17]. Satélite nacional e cabos submarinos controlados pelo país só agregariam efeito neutralizador da espionagem e do vigilantismo global quando as duas pontas de uma comunicação internacional estiverem operando com computadores protegidos contra interceptação de varejo, ou seja, com software livre sanitizado de *backdoors* para conexões corretamente criptografadas.

Sem criptografia, ou com ela fraca ou incorretamente usada, o efeito neutralizador dessas medidas, no caso de comunicação doméstica, só pode ser efetivo se combinado à sanitização dos roteadores na rota do tráfego dos dados. E isso ainda não é possível aqui, devido à privatização total da infraestrutura de telecomunicações que o Brasil sofreu e à forma atual com que os equipamentos, tais como centrais comutadoras e roteadores, são homologados pela Anatel – que só checa as especificações de funcionalidade declaradas pelo fabricante. Portanto, as medidas anunciadas têm grande chance de serem, sozinhas, na prática inócuas ou irrisórias, no máximo apenas encarecendo um pouco a bisbilhotagem desbragada.

Com a arquitetura propositadamente devassa das telecomunicações no Brasil, hoje totalmente privatizada e muito mal fiscalizada, perante o alcance e o escopo do esquema de espionagem e vigilantismo denunciado por Snowden, o que se revela é um cenário de grave vulnerabilidade para o país. Um cenário cujo efeito prático nessa área é o de facilitar e baratear a bisbilhotagem, e cuja

16. Ver http://iaesjournal.com/online/index.php/IJ-CLOSER/article/download/Cairo,%20Mesir/pdf 17. Ver https://www.torproject.org/index.html.en

gravidade se deve a muito desleixo e descaso – não só quando somos repetidamente tungados no pré-sal[18], mas também em relação a princípios constitucionais pétreos.

Ainda, as várias ferramentas de coleta e processamento empregados nesse esquema instrumentam não só a espionagem militar clássica, a industrial e a comercial em favor das empresas do esquema e suas parceiras, mas também aplicações militares até então inéditas, como por exemplo a mineração de dados para os *signature strikes*, em que aeronaves remotamente controlada (VANTs ou *drones*) matam suspeitos rastreando-os por padrões digitais de comportamento[19], sem identificação positiva do alvo. Testados no Afeganistão e no Paquistão em mais de mil civis, esses métodos de ataque estão em amplo desenvolvimento e generalização, com mais de 40 países buscando lançar tecnologias similares[20].

Em tempos ainda de paz, propostas recentes do Ministério das Comunicações podem parecer motivo para pilhérias em audiências legislativas, do tipo "marido traído", mas mesmo assim tal conduta não parece prudente para membros do governo de um pais já tão espoliado como o Brasil. Se já havia no governo brasileiro quem soubesse do esquema em 2008, como indicam matérias na imprensa, sobre quem advogava e advoga terceirização frouxa para tudo tecnológico, e debocha de estratégias para defesa da soberania via autonomia tecnológica, cabe perguntar a quem interessa manter o atual ministro das Comunicações.

Cabe perguntar por que esse ministro sabotou o Programa Nacional de Banda Larga, o que fez com a infraestrutura nele erguida, e por que demitiu o mentor e gestor desse programa, um dos mais tarimbados estrategistas brasileiros com bagagem técnica para negociações internacionais. Por que enterrou esse programa, cuja importância estratégica para neutralizar a exposição de toda a comunicação digital brasileira ao esquema denunciado está muito bem explicada, em matéria de Luiz Grossman no portal *Convergência Digital* por exemplo[22].

Se traição à pátria no Brasil não é assunto de interesse jornalístico para a mídia corporativa, se não for mais crime, ou se é crime só para certa cor ideológica do suposto beneficiado inimigo, então podemos ao menos dizer que tal conduta de um servidor público revela vassalagem neocolonial, como denunciada em recente audiência pública no Senado sobre o tema[23], para usar um termo recém-empregado em declaração conjunta dos chefes de Estado na cúpula do Mercosul[24]. ●

Este texto é adaptado de uma entrevista a Tadeu Breda publicada em julho de 2003 no portal de notícias Rede Brasil Atual[25].

18. Ver http://www.fazenda.gov.br/resenhaeletronica/MostraMateria.asp?cod=441160 19. Ver http://rt.com/usa/cia-drone-strikes-unknown-targets-293 20. Ver http://www.wired.com/dangerroom/2012/06/drones-south-america. Sobre o futuro da guerra baseada em "drones", ver Nick Turse e Tom Engelhardt, Terminator Planet: The First History of Drone Warfare 2001-2050, e-book. 21. Ver http://www1.folha.uol.com.br/mundo/2013/07/1309366-brasil-sabe-desde-2001-que-os-eua-espionam-internet.shtml e também http://www.youtube.com/watch?v=aPV0kebN804 22. Ver http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34223&sid=8#.Ud7A8KwQMZY 23. Ver http://www.youtube.com/watch?v=wfPGArGoxcg 24. Ver http://www.secretariageral.gov.br/noticias/ultimas_noticias/2013/07/12-07-2013-cupula-social-do-mercosul-de-montevideu-divulga-sua-declaracao 25. Ver http://www.redebrasilatual.com.br

Medidas de infraestrutura anunciadas pelo governo brasileiro (lançamento de satélite nacional, construção de cabos submarinos próprios aos EUA, Europa e África) não são suficientes para impedir a espionagem do tráfego de dados

Sugestões relativas às políticas públicas brasileiras sobre tecnologias assistivas para pessoas com

deficiência visual

Fernando H. F. Botelho fundador da F123, iniciativa voltada para o acesso à educação e ao emprego para pessoas com deficiência visual.

Um dos principais problemas enfrentados por pessoas com deficiência visual hoje no Brasil é o alto preço de leitores e ampliadores de tela com vozes de alta qualidade, apoio técnico, e habilidade de acessar arquivos e serviços Web de grande popularidade. Mesmo no caso da minoria da população que tem acesso a softwares de alto custo por meio de doações, os obstáculos são enormes[1]. No momento em que aquele jovem privilegiado, que teve acesso a tecnologia de alto custo em alguma organização tenta obter um estágio, o alto custo volta a ser a maior barreira. Um estágio é a forma mais efetiva para possibilitar que alguém com deficiência consiga um emprego, pois justamente isto permite que um empregador dê uma oportunidade, sem assumir grandes riscos. No entanto, um estágio que tenha um gasto adicional, para o empresário, equivalente a dois computadores, deixa de ser uma oportunidade na grande maioria dos casos[2].

Uma solução verdadeiramente efetiva requer que o baixo custo seja permanente, ou estrutural de um ponto de vista econômico e não dependa da caridade ou de estratégias temporárias de expansão de mercado de uma empresa. Por isso o foco do governo federal não pode se limitar a tecnologias específicas e deve também considerar a estrutura do mercado e os incentivos ali presentes.

Além da importância do nível de competição entre provedores de software, é também essencial olhar o ecossistema digital disponível a pessoas com deficiência como um todo, porque a produtividade e inclusão social desta comunidade hoje não depende mais somente do software instalado no computador de cada indivíduo. Tanto tecnologias assistivas de alto custo quanto aquelas acessíveis a todos os brasileiros hoje apresentam dificuldade em acessar uma grande variedade de serviços Web pela forma com que estes serviços estão desenhados. Em sua grande maioria, estes são obstáculos perfeitamente corrigíveis sem grandes modificações técnicas[3].

Finalmente, não podemos deixar de enfatizar a falta de capacitação para professores em escolas públicas e outras entidades e a falta de materiais e conteúdos de capacitação com licenças

1. Ver em Botelho, Fernando H. F.; "Export Capacity Building Among Service Exporters with Disabilities: overview and analysis of Latin American service exporters with disabilities"; Internal Phase I Report; International Trade Centre UNCTAD/WTO; Março de 2005. 2. Diagnóstico confirmado por Fernando Botelho em palestras, debates e apresentações feitas entre 2007 e 2010 na Latinoware (Brasil, 2007); Rotary and UTFPR (Brasil, 2008); WSIS (Suíça, 2008); Dialogue in the Dark (Alemanha, 2008); IGF (Índia, 2008); e-STAS (Espanha, 2009); Digital World Forum (Bélgica, 2009); ITU Accessibility Workshop (Mali, 2009); Hands On Europe (França, 2009); IGF, Nile TV e International, Egyptian TV (Egito, 2009); Conferencia da Secretaria dos Direitos da Pesoa com Deficiência do Estado de São Paulo (Brasil, 2009); Karlsruher Institut für Technologie, SightCity (Alemanha, 2010); Conferencia da Secretaria dos Direitos da Pesoa com Deficiência do Estado de São Paulo, LaraMara, Reatec, Rotary, FISL, Congresso Muito Especial da Paraíba, Reatiba FIEP (Brasil, 2010); IGF (Lituânia, 2010); Oficina F123 (Equador, Peru, Costa Rica e El Salvador, 2010). 3. Ver IGF 2009, Egito, Novembro 2009. http://igf09.eg/homeeng.html http://www.intgovforum.org/cms/index.php/the-meeting

Creative Commons, que permitem a cópia e reutilização dos mesmos. Dada a importância destes profissionais para a correta utilização de tecnologias assistivas, e por consequência, o desenvolvimento acadêmico e profissional de crianças e jovens com deficiência, é essencial melhorar o apoio dado a professores e demais especialistas ligados a esta comunidade.

:: NOSSAS SUGESTÕES

A estratégia do governo brasileiro para promover melhorias no acesso a tecnologia assistiva deve garantir um alto nível de competição entre provedores de soluções para esse mercado.
A intensificação na competição entre provedores nacionais e estrangeiros de software assistivo resultará num aumento na qualidade dos produtos e serviços disponíveis a este setor e uma diminuição nos preços. Igualmente importante é o foco na produtividade e inclusão social de pessoas com deficiência, ou seja, manter o foco de nossas políticas públicas no ecossistema digital no qual esta comunidade deve agir em seu dia-a-dia e não apenas no software que é instalado diretamente em computadores. Para garantir esses resultados a estratégia deve incluir os seguintes elementos: interoperabilidade entre serviços Web, apoio federal a entidades e indivíduos que melhoram tecnologias assistivas baseadas em software livre, e a priorização em compras do governo de tecnologias baseadas inteiramente em software livre.

> O impacto do uso de protocolos e formatos de arquivos abertos em serviços Web é extremamente positivo para a acessibilidade de pessoas com deficiências

:: INTEROPERABILIDADE ENTRE SERVIÇOS WEB

A produtividade e inclusão social de pessoas com deficiência na Internet depende cada vez mais de decisões tomadas por empresas provedoras de serviços Web como o compartilhamento de fotos, comentários e notícias por redes sociais, e-mail, mensagens instantâneas, editores de texto, e muitos outros. Embora a regulamentação das interfaces usadas nestes serviços não seria sempre prática de um ponto de vista de complexidade técnica, imprevisibilidade de inovações e a própria lentitude do processo legislativo, existe uma alternativa legal que é compatível com a velocidade da evolução tecnológica que vivemos hoje.

O governo pode exigir que todo serviço digital tenha seus protocolos de comunicação e formatos de arquivos baseados em padrões abertos, ou minimamente, que proporcionem conectividade para redes ou softwares que sim atendem a esta exigência caso prefiram usar padrões fechados dentro de seus serviços.

O impacto do uso de protocolos e formatos de arquivos abertos em serviços Web é extremamente positivo para a acessibilidade de pessoas com deficiências a estes serviços[4]. O exemplo clássico desta dinâmica é o contraste entre o serviço de correio eletrônico usado globalmente e o mensageiro instantâneo usado pela empresa americana AOL. Neste *case* de acessibilidade eletrônica, pode se observar que embora o mensageiro instantâneo da empresa AOL tenha demorado anos para ficar acessível aos cegos, e requerido enormes gastos e um processo legal pela Federação Nacional dos Cegos dos Estados Unidos (NFB), o mesmo problema nunca se observou no acesso a e-mail. No caso do protocolo de correio eletrônico, conhecido como SMTP, qualquer empresa desenvolvedora de clientes de e-mail inacessíveis por falta de conhecimento, recursos, ou sabedoria, não impedia os cegos de usarem e-mail normalmente.

Devido ao fato de o protocolo usado em e-mail ser aberto, sempre existiu uma grande competição entre diferentes softwares para o acesso a e-mail, e cegos sempre tiveram várias alternativas entre as quais encontraram opções acessíveis a leitores de tela. O mesmo não se observou no caso da empresa AOL, onde o protocolo de comunicação usado em sua rede de mensagens instantâneas era fechado e com isso, limitava única e exclusivamente o acesso ao software feito pela própria empresa. Era o equivalente a uma empresa de telecomunicações que só proporcionasse acesso a sua rede a quem comprasse o celular oferecido pela própria empresa, sem que o aparelho vendido pela empresa fosse acessível a pessoas com deficiência.

Se a empresa AOL tivesse uma exigência legal de usar um protocolo de mensagens instantâneas aberto (como o XMPP), qualquer erro seu no desenho da interface de seu software cliente de mensagens, não impediria que alguém cego acessasse a rede AOL por meio de um dos diversos softwares compatíveis com o protocolo aberto. O próprio protocolo XMPP pode ser interpretado por diversos clientes acessíveis a tecnologias assistivas, e estão disponíveis para instalação em diversos sistemas operacionais, desde Android até Linux, MacOS e Windows, e em diversos dispositivos desde computadores até tablets e smart phones.

Alternativamente, uma empresa com situação equivalente pode ser obrigada a disponibilizar um serviço de conversão de seu protocolo fechado a outro aberto, permitindo assim a interoperabilidade

4. Ver em Botelho, Fernando H. F.; "R&D and Public-Private Partnerships for Low and No-Cost Assistive Technologies"; artigo apresentado à União Internacional de Telecomunicações; 2009. http://www.itu.int/dms_pub/itu-t/oth/06/27/T06270000060042PDFE.pdf

entre diversas redes e garantindo a acessibilidade a quem tem deficiência visual. Uma empresa que se nega a permitir que uma pessoa com deficiência tenha acesso a seus direitos pela forma que desenha seu serviço e software, deve minimamente permitir por meio de protocolos e arquivos abertos, que a pessoa acesse os serviços por meio de meios e softwares alternativos.

:: APOIO FEDERAL A ENTIDADES E INDIVÍDUOS QUE MELHORAM TECNOLOGIAS ASSISTIVAS BASEADAS EM SOFTWARE LIVRE

As empresas de software proprietário mais conhecidas do mundo da tecnologia assistiva, que hoje dominam o mercado brasileiro assim como o mundial, estão todas baseadas em países desenvolvidos e seguem um modelo de negócios que depende de altos preços. Este modelo de negócios não causa problemas sociais em países onde governos tem recursos abundantes para comprar a tecnologia assistiva requerida por seus cidadãos com deficiência. No entanto, no contexto brasileiro, o mesmo modelo contribui de forma significativa aos enormes obstáculos enfrentados por pessoas com deficiência em acessar seus direitos. Em paralelo, softwares desenvolvidos com recursos governamentais brasileiros[5] não chegaram a ter o impacto social desejado, e certamente tiveram o seu efeito reduzido ainda mais pela ausência de um requerimento universal de disponibilizar todo o código fonte do software desenvolvido com dinheiro público de forma aberta e livre.

É importante enfatizar que utilizamos aqui a definição correta, embora menos conhecida de software livre. Isto é, chamamos de software livre não aquele que é gratuito, e sim todo software que tem licença GPL (sigla em inglês para Licença Pública Geral) ou equivalente[6]. Neste modelo de desenvolvimento tecnológico a receita, ou seja, o código fonte do software, pode ser estudado, modificado, melhorado e redistribuído sem nenhum pré-requisito, pagamento, ou autorização. É um modelo que permitiu o rápido desenvolvimento da Internet e muitas histórias de sucesso – desde empresas como Google e Facebook, até softwares como Firefox e LibreOffice. No setor da tecnologia assistiva, o mesmo sucesso (apesar de escassos recursos) se observa também em projetos Dasher[7] e eSpeak[8], NVDA[9], F123[10] e EviaCam[11].

5. Leitor de tela desenvolvido pelo Ministério das Telecomunicações - http://www.mc.gov.br/acoes-e-programas/redes-digitais-da-cidadania/170-sem-categoria/22727-leitor-de- telas#conteudo 6. Licença Pública Geral, conhecida por sua cicgla em inglês GPL (General Public License). http://www.gnu.org/licenses/gpl.html 7. Dasher: sistema de entrada de dados para múltiplos idiomas, baseado em software livre, que funciona em uma ampla variedade de sistemas operacionais e plataformas, incluindo computadores, tablets e celulares. http://www.inference.phy.cam.ac.uk/dasher/ 8. eSpeak: sintetizador de voz, com múltiplos idiomas, baseado em software livre que funciona em uma ampla variedade de sistemas operacionais e plataformas, incluindo computadores, tablets e celulares. http://espeak.sourceforge.net/ 9. NVDA: Leitor de tela baseado em software livre para sistema operacional proprietário Windows. http://www.nvaccess.org/ 10. F123: Software que contém sistema operacional, aplicativos e leitor e ampliador de tela, e materiais de capacitação para pessoas com deficiência visual total ou parcial. http://F123.org/ 11. EViaCam: software para o controle do mouse por meio de rastreio de movimento pela imagem de uma Webcam. http://eviacam.sourceforge.net/index.php

A criatividade, competitividade e baixo preço que caracterizam os softwares livres para pessoas com deficiência podem inspirar políticas públicas de apoio a tecnologias que são chave para pessoas com deficiência visual e que podem ser melhoradas de forma rápida e eficiente seguindo este modelo. Por exemplo, sintetizadores de voz, software OCR para o reconhecimento de textos digitalizados, teclados virtuais e melhorias à acessibilidade de aplicativos livres chave como o LibreOffice[12] são algumas das muitas tecnologias que podem ter um enorme e positivo impacto social, se seu desenvolvimento receber apoio do governo em espírito de parcerias público-privadas.

Além das conhecidas melhores práticas para o gerenciamento de iniciativas públicas, como é por exemplo a transparência total do processo, podemos sugerir também critérios específicos a políticas públicas ligadas ao software. São importantes, por exemplo, os seguintes parâmetros:

• **Multiplicidade de atores** - todos os setores da sociedade, desde o público, até o privado e o terceiro setor podem fazer importantes contribuições ao processo de desenvolvimento de softwares livres. É essencial que projetos sejam estruturados de forma que diversas universidades públicas e privadas, empresas grandes e pequenas, e até mesmo indivíduos possam participar em cada um dos projetos apoiados. Essa participação não implica necessariamente que todos os participantes receberão pagamentos, mas sim implica que todos terão acesso sem restrição alguma ao código fonte produzido em cada iniciativa. O importante é o acesso democrático por meio da Web, sem empecilhos burocráticos ou legais, ao código fonte para o uso destas tecnologias em serviços, produtos, experimentos, inovações e atividades educacionais. Hoje o acesso a esta tecnologia é tão importante quanto o acesso ao conhecimento sobre matemática, e como no caso

> As empresas de software proprietário mais conhecidas do mundo da tecnologia assistiva, que hoje dominam o mercado brasileiro assim como o mundial, estão todas baseadas em países desenvolvidos e seguem um modelo de negócios que depende de altos preços.

12. LibreOffice: Aplicativos de escritório, compatíveis com múltiplas plataformas, baseados em software livre. http://www.libreoffice.org/

> De um ponto de vista de política pública, qualquer investimento em tecnologia assistiva que seja mantido com seu código fechado, sem permitir e facilitar contribuições do público e de instituições do setor privado, perde o enorme potencial tecnológico que é possível graças ao modelo do software livre.

da matemática, o seu impacto na qualidade de vida dos cidadãos brasileiros depende do acesso democrático à mesma.

• **Preferência por tecnologias de base** - tecnologias de base são aquelas tecnologias como sintetizadores de voz ou reconhecedores OCR de textos digitalizados, que são tecnologicamente complexos mas necessários em uma grande variedade de aplicativos assistivos. Por exemplo, software OCR pode ser usado em um aplicativo tradicional de computador ou em celulares, tablets, ou até mesmo dentro de um navegador Web. O mesmo se observa em sintetizadores de voz que podem ajudar a pessoas cegas em uma enorme variedade de situações, mas também a pessoas com deficiências que dificultem a comunicação e até mesmo pessoas com deficiências intelectuais no âmbito educacional. Estas tecnologias têm importância estratégica, não só por sua grande utilidade, mas também porque são o principal obstáculo para permitir que organizações e pequenas empresas brasileiras possam competir com provedores estrangeiros. Programas de apoio do governo federal onde universidades, empresas e até indivíduos possam participar e acessar todo o código fonte, teriam um enorme impacto no aumento na variedade, utilidade e baixo preço de alternativas nacionais.

• **Preferência por projetos livres já existentes com comunidades ativas** - os enormes ganhos em eficiência e baixo custo que são possíveis quando projetos públicos e privados usam tecnologias baseadas em software livre são consequência do fato que softwares livres de sucesso têm comunidades de especialistas, fundações, organizações, empresas e governos já apoiando o seu desenvolvimento. É importante não reinventar a roda duplicando esforços já existentes, e sim apoiar a participação brasileira em projetos estabelecidos como o sintetizador de voz eSpeak, o leitor de tela Orca, o software de reconhecimento de textos SpeedyOCR, o sistema de entrada de dados Dasher, o rastreador de movimento para controle de mouse eViaCam e muitos outros.

É também essencial que a acessibilidade de projetos mais genéricos como o navegador Firefox[13] e os aplicativos de escritório LibreOffice[14], tenham apoio para garantir a sua compatibilidade com tecnologias assistivas.

• Total aderência aos princípios do software livre - de um ponto de vista de política pública, qualquer investimento em tecnologia assistiva que seja mantido com seu código fechado, sem permitir e facilitar contribuições do público e de instituições do setor privado, perde o enorme potencial tecnológico que é possível graças ao modelo do software livre. O potencial não se limita ao aproveitamento de contribuições técnicas de terceiros, mas também facilita a divulgação e utilização de ferramentas e produtos de software desenvolvidos com recursos públicos por toda a sociedade. O modelo de desenvolvimento do software livre é efetivamente um método de parceria massiva que já demonstrou a sua efetividade repetidas vezes no Brasil e em todo o mundo. Por esses benefícios chave, em termos de políticas públicas é essencial que somente sejam apoiados projetos que seguem os princípios e usam a Licença Geral Pública (GPL), a primeira e mais reconhecida licença de software livre do mundo.

• Apoio ao desenvolvimento de materiais de capacitação com licenças livres - professores e outros profissionais que são essenciais para o desenvolvimento pessoal, acadêmico e profissional de crianças com deficiência precisam ter acesso a materiais de capacitação e apoio com a mesma qualidade que os softwares livres disponíveis para seu trabalho do dia-a-dia. O apoio do governo a iniciativas que popularizem o acesso a materiais de capacitação de alta qualidade com licenças Creative Commons, que permitem a livre distribuição e reutilização desses materiais, vai garantir que o material de apoio evolua junto ao software que ele tem como foco. Igualmente ao software,

> O incrível impacto social que tecnologias assistivas baseadas em software livre podem ter, é em grande parte devido ao fato que neste modelo de desenvolvimento a existência de empresas e outras entidades especializadas em dar apoio técnico e capacitação a preços extremamente baixos é perfeitamente viável.

13. Mozilla Foundation: fundação baseada nos Estados Unidos que apoia o desenvolvimento, incluindo aspectos de compatibilidade com tecnologias assistivas, de diversos softwares incluindo o navegador Firefox e o cliente de e-mail Thunderbird, compatíveis com uma grande variedade de sistemas operacionais livres e proprietários. http://www.mozilla.org/foundation/ 14. The Document Foundation: fundação baseada na Alemanha que apoia o desenvolvimento, inclusive a acessibilidade para tecnologias assistivas, dos aplicativos de escritório LibreOffice. http://www.documentfoundation.org/

a licença livre Creative Commons permite um custo de desenvolvimento muito mais acessível graças ao fato que indivíduos, organizações, fundações, empresas e governos sabem que não precisarão desenvolver sozinhos o material e sempre terão direito de usar aquilo que é criado conjuntamente[15].

:: PRIORIZAÇÃO EM COMPRAS DO GOVERNO DE TECNOLOGIAS BASEADAS INTEIRAMENTE EM SOFTWARE LIVRE

O incrível impacto social que tecnologias assistivas baseadas em software livre podem ter é, em grande parte, devido ao fato que neste modelo de desenvolvimento a existência de empresas e outras entidades especializadas em dar apoio técnico e capacitação a preços extremamente baixos é perfeitamente viável[16]. Isto se dá em grande parte porque a reprodução de materiais digitais, sejam estes softwares ou conteúdos, é um processo extremamente barato depois que o investimento para desenvolver os mesmos já foi feito pela comunidade dedicada a essas soluções livres. No entanto, uma grande parte desse beneficio à sociedade é perdido se a tecnologia assistiva baseada em software livre depende de outros softwares que não são livres, e que em alguns casos, são extremamente caros para o contexto brasileiro.

Por este motivo, o governo deve evitar investimentos em tecnologias assistivas que funcionem exclusivamente em ambientes digitais que não sejam livres. Em outras palavras, o governo não deve usar seus escassos recursos para melhorar a acessibilidade de produtos de empresas privadas quando essas empresas não disponibilizam esses produtos com licença GPL. Um software proprietário não dá ao governo nenhum dos direitos de estudo, modificação e redistribuição que são tão importantes para o baixo custo e a longevidade dessas tecnologias, impedindo assim que a sociedade tenha todo o beneficio do investimento em acessibilidade que venha a ser feito[17].

Investimentos em tecnologias como o sintetizador eSpeak ou o sistema de entrada de dados Dasher podem beneficiar usuários de sistemas operacionais totalmente livres, o que deve ser o foco primário do governo, e também daqueles que usam sistemas operacionais proprietários. Estas tecnologias também oferecem portabilidade em termos de plataformas, permitindo seu uso em computadores convencionais e também em tablets e smart phones.

15. WikiMedia Foundation: fundação dedicada à divulgação gratuita do conhecimento humano por meio da participação do público e de diversas instituições públicas e privadas e a utilização de licenças Creative Commons, que permitem a redistribuição e modificação de conteúdos de forma gratuita e livre. http://wikimediafoundation.org/wiki/Home 16. Ver Botelho, Fernando H. F.; "Open Source Software-Based Assistive Technologies"; ITU-G3ict e-Accessibility Policy Toolkit for Persons with Disabilities; Global Initiative for Inclusive Information and Communication Technologies (G3ICT); 7 de julho de 2010. http://www.e-accessibilitytoolkit.org/toolkit/promoting_assistive_technologies/open-source 17. Existem exemplos de tecnologias assistivas proprietárias e de alto custo, como o leitor de tela Slimware Window Bridge da empresa canadense Syntha Voice Computers, que saíram do mercado por problemas na liderança da empresa. Neste caso, todo o investimento feito pelo governo americano e canadense na compra de licenças e capacitação de pessoas cegas, foi perdido.

> Investimentos em tecnologias como o sintetizador eSpeak ou o sistema de entrada de dados Dasher podem beneficiar usuários de sistemas operacionais totalmente livres, o que deve ser o foco primário do governo, e também daqueles que usam sistemas operacionais proprietários.

:: NOSSA EXPERIÊNCIA

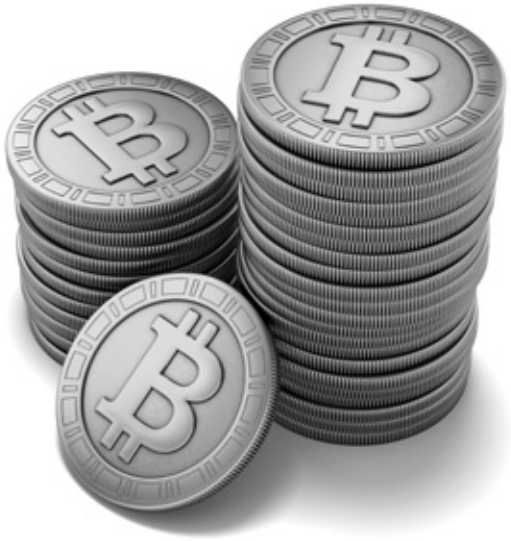
Observamos estabilidade por muitos anos no mercado brasileiro de softwares para pessoas com deficiência visual. Tínhamos sempre softwares proprietários de altíssimo custo e performance competitiva, ajudando a uma pequena minoria; softwares gratuitos de limitada utilidade, ajudando pouco a muita gente; e softwares livres de performance competitiva mas difícil instalação, ajudando a poucos. Foi somente nos últimos três anos, que o lançamento do F123 (pronunciado F 1 2 3) mostrou a viabilidade técnica e econômica de disponibilizar versões gratuitas e pagas de softwares livres de grande utilidade e competitividade para pessoas com deficiência visual.

A iniciativa F123, responsabilidade deste autor e alguns parceiros, se diferencia por usar e apoiar o desenvolvimento de softwares livres, facilitar a portabilidade e facilidade de uso destas tecnologias e manter seu foco no impacto social – que é seu real objetivo – e não apenas na tecnologia. Este foco no impacto social é o que faz com que a iniciativa ofereça serviço de apoio técnico, materiais de capacitação e até mesmo uma versão que pode ser instalada em pendrives, para viabilizar o uso por parte de quem não tem recursos para comprar seu próprio computador. Enfim, esta tecnologia assistiva se caracteriza por ser uma solução completa, incluindo desde sistema operacional até aplicativos e leitor e ampliador de tela; por incluir materiais de capacitação e apoio técnico; por sua compatibilidade com os meios de comunicação e formatos de arquivos mais usados; e por levar em consideração as necessidades de uma variedade de usuários, desde aqueles que exigem sintetizador de voz de alta qualidade até aqueles que não têm computador próprio.

Mesmo sendo uma alternativa bastante recente, o F123 já está disponível em português, espanhol[18] e inglês – e já está sendo usado ou testado em mais de 20 países tão variados quanto Brasil, Uruguai e Zâmbia. Este software é desenvolvido por uma empresa social, que se caracteriza por reinvestir todo lucro em sua causa, que no caso da F123 é o aumento das oportunidades educacionais e de emprego para pessoas com deficiência visual em todo o mundo. Entre pessoas beneficiadas por serem usuários do F123 e aquelas que aproveitam contribuições técnicas feitas pela iniciativa, estima-se que já foram beneficiadas aproximadamente 504.000 pessoas em todo o mundo[19]. ●

18. Ver Arroyo, Guillermo Oscar; Pagliaroli, Adriana; Botelho, Fernando H. F.; "Soluciones para la Baja Visión"; Editora Paratexto libros, Buenos Aires, Argentina; maio de 2011. 19. Estimativa feita com base na porcentagem mundial de pessoas com baixa visão, de acordo com a Organização Mundial da Saúde, aplicada ao total de 14 milhões de usuários da interface gráfica Gnome, à qual a equipe F123 contribuiu. O estudo foi feito pela empresa de consultoria Neary Consulting e pode ser encontrado no seguinte endereço: http://www.neary-consulting.com/index.php/services/gnome-census/

> **Rick Falkvinge** fundador e primeiro lider do Partido Pirata sueco.



Como a bitcoin pode derrubar os Estados Unidos

A bitcoin[1] representa uma ameaça significativa ao domínio da moeda norte-americana, que é a única coisa a sustentar o status dos EUA enquanto superpotência mundial. Depois da inadimplência dos Estados Unidos diante de todos os empréstimos internacionais em 15 de agosto de 1971,[2] a balança comercial do país vem se mantendo através de uma combinação de ameaças militares com ordens de compra de dólares americanos apenas para financiar a continuidade do consumo nacional. Enquanto outras moedas não conseguiram desafiar o dólar norte-americano, e por conseguinte esse mecanismo de manutenção do domínio econômico do país, a bitcoin pode conseguir.

Para compreender essa hipótese, precisamos primeiro compreender o grau de falência dos Estados Unidos da América. Por alguma razão, o destaque do momento vai para o fracasso do euro; talvez pelo fato de que o dólar norte-americano falhou há muito e vem sendo mantido vivo por uma bolha que expande-se a cada dia. Em suma, os EUA deram calote nos seus empréstimos internacionais depois da Guerra do Vietnã, e continuam a contrair empréstimos para financiar seu consumo extravagante desde então.[3]

1. Para uma introdução aos conceitos da moeda digital bitcoin, ver http://falkvinge.net/2013/04/03/why-bitcoin-is-poised-to-change-society-much-more-than--the-internet-did. Ver também http://pt.wikipedia.org/wiki/bitcoin 2. Ver https://en.wikipedia.org/wiki/Nixon_Shock e https://en.wikipedia.org/wiki/Bretton_Woods_system 3. Para uma descrição simplificada desse processo, ver http://falkvinge.net/2011/06/17/the-imminent-dollar-collaps-explained-to-an-8-year-old/

Rick Falkvinge

> a bitcoin supera em muito o dólar americano, em todos os aspectos, como um vale para o comércio internacional. Seu uso é mais barato, mais fácil, e é muito mais rápido

Há muito que só se toma dinheiro emprestado para pagar os juros dos empréstimos anteriores. Ano passado, o déficit orçamentário do país impressionou bastante, chegando a 50%, ou seja, para cada dólar de receita *dois eram gastos*. Note-se que isso não é muito debatido – imagino se fosse: a capacidade do país pagar seus empréstimos seria trazida à baila, algo que seria o equivalente a derrubar o castelo de cartas com uma tonelada de tijolos, e ninguém parece estar muito interessado em balançar o barco a ponto de fazer essa água toda. Afinal, todos estão sentados em cima de reservas de dólares norte-americanos, que perderiam totalmente o valor da noite para o dia se uma coisa dessas acontecesse.

Os Estados Unidos começaram a imprimir mais moeda no dia 15 de agosto de 1971, e não pararam desde então. Só em 2011 foram 16 trilhões de dólares – estamos falando de trilhões, com "t" – impressos para segurar a economia dos EUA[4]. A que corresponde esse valor? Um pouco mais do que o produto interno bruto norte-americano[5]. *Para cada dólar produzido em valor, foi impresso outro do nada, na esperança de que alguém o compre*. E as pessoas compram! É isso: existe um mecanismo chave aqui que força as pessoas a continuar comprando os dólares norte-americanos.

Os Estados Unidos mantêm-se vivos enquanto país pelo fato de que as pessoas que querem comprar bens de outro país, da China, por exemplo, primeiro têm de comprar dólares norte-americanos e depois trocá-los pelos bens que querem adquirir da China. É isso, além do fato de que isso leva todos os países a comprar toneladas de dólares norte-americanos como divisas.

O fato de que as pessoas *precisam* continuar comprando dólares norte-americanos para conseguir o que querem de qualquer *outro* país do mundo é o mecanismo que sustenta toda a economia dos EUA e, o mais importante, alimenta o seu poderio militar que, por sua vez, põe esse mecanismo em prática (ver Iraque, Líbia, Irã etc)[6]. Trata-se de um ciclo de dominância econômica exercida através da violência que leva a gastos extravagantes, gastos *conquistados*, por parte dos Estados Unidos, quase todos com o poderio militar para manter tal dominância.

(Uma nota à parte: já se questiona o quanto a classe média nos EUA ainda se beneficia disso. Há uma década esse ciclo de retroalimentação tornava o padrão de vida normal nos EUA marcantemente mais alto do que em outras partes do mundo ocidental; hoje em dia, os EUA chegam bem atrás em todas as categorias de padrão de vida.)

Como as preconizações de "fim do mundo" costumam ser descartadas como baboseira, eu quis começar este artigo colocando logo na mesa alguns fatos econômicos. Os EUA estão na falência e a única coisa que evita o colapso são as suas forças armadas e o fato de que todo o mundo tem

4. Ver http://www.businessinsider.com/feds-16-trillion-dollar-secret-slush-fund-props-up-our-way-of-life-2011-7 5. Ver https://en.wikipedia.org/wiki/List_of_countries_by_GDP_(nominal) 6. Sobre a invasão do Iraque, ver http://falkvinge.net/2012/10/06/the-us-invaded-iraq-because-it-wouldnt-have-survived-otherwise. Sobre a Líbia, ver http://www.thenewamerican.com/economy/markets/item/4630-gadhafi-s-gold-money-plan-would-have-devastated-dollar. Sobre o Irã, ver http://www.telegraph.co.uk/finance/commodities/9077600/Iran-presses-ahead-with-dollar-attack.html

investimentos tão pesados no país que nenhum governo quer que a falência ocorra no seu turno. Assim é que os empréstimos e os gastos excessivos seguem por mais um dia... até que acabem.

O que aconteceria se os EUA tivessem de passar um dia sem esses gastos todos? Haveria uma queda colossal da economia global, porém – o que é mais importante – os EUA cairiam ao estilo soviético, só que pior, por causa das diferenças estruturais. (Para compreender essas diferenças, considere o fato de que o transporte público continuou funcionando durante o colapsto soviético e que muitas famílias estavam bem preparadas para a escassez de alimentos. Nos EUA seria diferente, haveria pessoas isoladas nos subúrbios, sem combustível, alimento ou remédios – só com um monte de armas e munição. Veja os argumentos de Dmitry Orlov para saber um pouco mais sobre essa diferença estrutural.[7])

:: ENTRA A BITCOIN, CAPAZ DE ROMPER O CICLO DE EMPRÉSTIMOS E GASTOS.

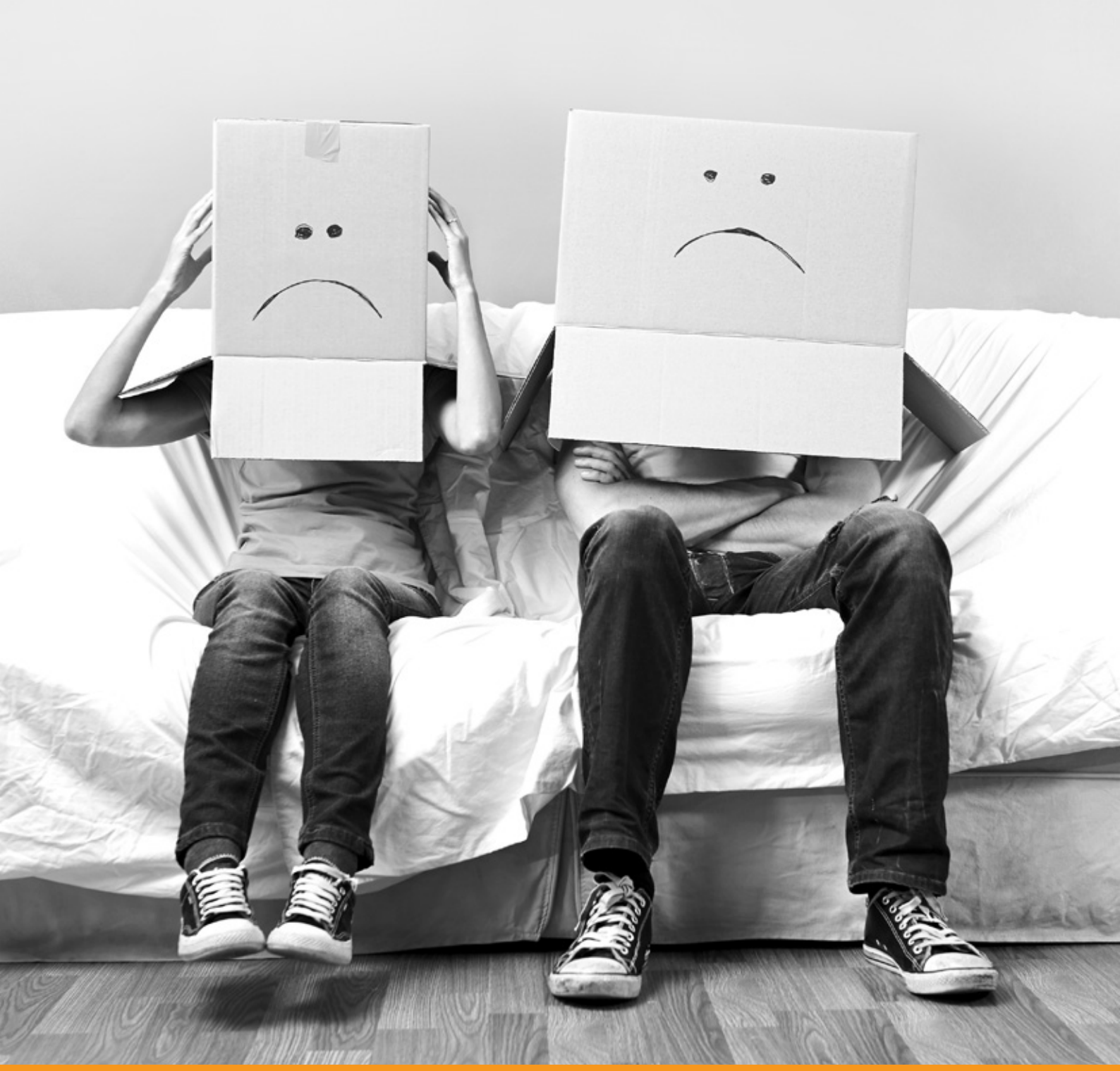
Conforme observamos, a razão chave para as pessoas verem-se forçadas a comprar dólares norte-americanos é que esse é o mecanismo internacional de trocas de valores. Quem quiser comprar uma buginganga qualquer da China ou da Índia vai ter de primeiro comprar dólares norte-americanos para depois trocá-los pela buginganga. Mas, conforme já vimos, a bitcoin supera em muito o dólar americano, em todos

os aspectos, como um vale para o comércio internacional[8]. Seu uso é mais barato, mais fácil, e é muito mais rápido do que os sistemas internacionais de hoje para a transferência de valores.

Praticamente todas as pessoas com quem conversei que estão envolvidas com o comércio internacional passariam para um sistema semelhante ao da bitcoin num piscar de olhos se pudessem, dando vazão a anos de frustração acumulada com o legado do sistema bancário (que usa o dólar norte-americano). Se isso acontecer, os EUA não serão capazes de encontrar compradores para o dinheiro recém-impresso que sustenta a sua economia (e financia as suas forças armadas).

Se for rompido o lacre do ciclo do dólar, os Estados Unidos vão desabar. Uma queda e tanto! Já parece inevitável a esta altura, e a bitcoin pode ser o mecanismo capaz de romper esse ciclo.●

7. Ver http://www.resilience.org/stories/2006-12-04/closing-collapse-gap-ussr-was-better-prepared-collapse-us 8. Ver http://falkvinge.net/2011/06/18/bitcoins-four-drivers-part-two-international-trade



Proteção de dados na UE: a certeza da incerteza

Cory Doctorow escritor, ativista, jornalista e blogueiro, coeditor do portal Boing Boing, ex-diretor da Electronic Frontier Foundation e cofundador do Open Rights Group da Inglaterra.

Quando uma regulamentação afirma que algum dado é "anônimo", ela está desconectada das melhores teorias da ciência computacional. No momento em que escrevo, o Parlamento Europeu está envolvido numa acirradíssima disputa mundial sobre a nova Regulamentação Geral para a Proteção de Dados[1]. Estão em jogo as futuras regras para privacidade online, mineração de dados, *big data*[2], publicidade dirigida, ciências sociais guiada por dados (*data-driven social sciences*), espionagem governamental (via *proxy*) e milhares de outras atividades que se encontram no cerne de muitas das maiores empresas da internet, e das ambições mais obscuras e descontroladas de nossos políticos.

Os lobistas estão a todo vapor. Os ativistas que conheço e sei que vão a Bruxelas dizem que nunca viram algo assim: é o verdadeiro frenesi do lobby. Há na mesa centenas de emendas e propostas, algumas boas, outras ruins, e só para tomar pé de todas elas já exige trabalho em tempo integral.

Por mais complicadas que sejam as propostas, existe uma regrinha básica que devemos ter sempre em mente quando há na mesa alguma proposta para proteção de dados: sempre que alguém fala em relaxar as regras sobre compartilhamento de dados que tenham sido "anonimizados" (dos quais foram retiradas as informações de identificação) ou "pseudonimizados" (cujos identificadores foram substituídos por pseudônimos), devemos assumir, enquanto não houver provas, que esse alguém está dizendo besteira.

Trata-se de uma "lei férrea da privacidade", que pode ser usada para descartar rapidamente as ideias sem sentido. O que sobra podem ser boas ou más ideias, porém, pelo menos não estarão baseadas em uma quase-impossibilidade.

Anonimizar dados é um negócio bastante difícil. Nesse quesito, há três falhas notórias que são muito citadas: o lançamento que a AOL fez em 2006 de pesquisa anônima na internet (*anonymous search data*); o lançamento feito pela Comissão de Seguros em Grupo do Estado de Massachusetts de cadastros de saúde anonimizados (*anonymised health records*); e o lançamento do acervo de 100 mil vídeos para aluguel que a Netflix fez em 2006.

Em cada um desses casos, os pesquisadores mostraram como se pode usar algumas técnicas relativamente simples para re-identificar os dados nesses conjuntos, normalmente escolhendo em cada registro os elementos que os tornam únicos. Há vários fumantes nos registros de saúde, mas quando se restringe a busca a um anônimo fumante negro que nasceu em 1965 e se apresentou na

1. Ver http://www.guardian.co.uk/technology/data-protection 2. Ver http://www.guardian.co.uk/technology/big-data

> Só porque uma coisa parece anônima num primeiro olhar, não quer dizer que de fato seja; tanto por causa da matemática da distinção individual quanto por causa da quantidade imensa de bancos de dados que estão se tornando disponíveis.

ala de emergência com dor nas articulações, na verdade é bastante simples fazer uma fusão do registro "anônimo" com outro banco de dados "anonimizado", de onde surgirá a identidade quase certeira do paciente.

:: DESANONIMIZAÇÃO

Desde meados da década de 2000, a desanonimização se tornou algo como um esporte de contato para os cientistas da informática, que vivem tirando da cartola esquemas de anonimização com espertos truques de reidentificação. Um artigo publicado recentemente na *Nature Scientific Reports*[3] mostrou como os dados "anonimizados" da empresa telefônica europeia (provavelmente uma na Bélgica) poderiam ser re-identificados com 95% de precisão, a partir de apenas quatro itens sobre cada pessoa (com apenas duas informações, mais da metade dos usuários do conjunto de dados poderiam ser re-identificados).

Há quem diga que isso não importa. Para essas pessoas, a privacidade morreu, ou é irrelevante, algo sem importância. Se você concorda com elas, lembre-se: a razão pela qual a anonimização e pseudonimização estão sendo contempladas na Regulamentação Geral para Proteção de Dados é que os próprios autores dizem que a privacidade é importante, e que vale a pena preservá-la. Falam sobre anonimização de conjuntos de dados porque acreditam que ela seja capaz de proteger a privacidade – e isso significa que estão dizendo, implicitamente, que vale a pena preservar a privacidade. Se for essa a meta das políticas públicas, então essas políticas devem procurá-la de maneira conforme à realidade que compreendemos.

De fato, toda a premissa básica dos *big data* está em risco com a ideia de que os dados podem ser anonimizados. Afinal, os *big data* prometem que, com os grandes conjuntos de dados, relacionamentos sutis podem ser destrinchados. No mundo da reidentificação, fala-se de abordagens de "dados esparsos" (*sparse data*) para a desanonimização. Embora a maior parte dos seus traços pessoais seja compartilhada com

3. Ver http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html

muitos outros, há certas coisas a seu respeito que se encontram menos comumente representados no conjunto – talvez a confluência dos seus hábitos de leitura com o seu endereço; talvez a sua cidade natal em combinação com as suas opções de carros. Essas raridades praticamente saltam dos dados e apontam diretamente para você, assim como se prontificam a fazer as demais conclusões dos *big data*. Se os *big data* conseguem encontrar a combinação de fatores ambientais sutis em comum para todas as vítimas de uma doença rara, eles também devem ser capazes de encontrar a combinação de identificadores sutis compartilhados com todos os diferentes conjuntos de dados nos quais você está presente, de fundi-los e de trazer a público a sua identidade.

:: FRENESI LOBISTA

A UE está sofrendo um lobby como nunca se viu igual. A Comissária Viviane Reding, da UE, diz: "Nunca vi na minha vida uma operação de lobby tão pesada!"[4] E está funcionando!

Uma quantidade imensa de textos escritos por lobistas está chegando até as emendas dos MPEs[5]. Os lobistas se tornaram legisladores de fato, só que recebem mais e não precisam comparecer a todas aquelas enfadonhas reuniões.

A cláusula quatro da Regulamentação Geral para Proteção de Dados contém definições usadas no documento, e trata-se de um dos principais campos de batalha. Ela estabelece a ideia de que existem dados "anônimos" e os isenta de regulamentação, e cria uma segunda categoria de informações "pseudônima" que pode ser tratada com menos restrições do que impostas às "informações de identificação pessoal".

Fui a dois dos meus cientistas da computação favoritos e lhes perguntei o que achavam da plausibilidade da anonimização ou pseudonimização de conjuntos de dados. Seth David Schoen (tecnólogo da Electronic Frontier Foundation) disse-me: "Os pesquisadores já mostraram que a anonimização é muito mais difícil do que parece. Só porque uma coisa parece anônima num primeiro olhar, não quer dizer que de fato seja; tanto por causa da matemática da distinção individual quanto por causa da quantidade imensa de bancos de dados que estão se tornando disponíveis. Isso significa que devemos ser extremamente cautelosos quanto ao anonimato das coisas; não devemos nos fiar somente na nossa intuição."

Ed Felten, que saiu da Comissão Federal dos EUA para o Comércio e agora está em Princeton, disse: "Uma década inteira de pesquisas da ciência da computação mostra que muitos conjuntos de dados podem ser re-identificados. Não basta remover os identificadores óbvious para evitar a reidentificação. Pode ser que não baste remover

4. Ver http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html
5. Ver http://www.motherjones.com/politics/2013/03/google-facebook-sopa-privacy

todos os dados sobre indivíduos. Até os conjuntos de dados totalmente compostos de informações agregadas podem ser usados, em alguns casos realísticos, para inferir informações sobre indivíduos específicos.

"Mas dizer que não existe a menor esperança para a reidentificação é ir um pouco longe demais. Existe uma ciência emergente da análise de dados que preservam a privacidade, que pode ser aplicada em alguns ambientes. Via de regra, dados oriundos das características dos indivíduos, inclusive os comportamentais, provavelmente irão passar informações sobre esses indivíduos, na ausência de uma rígida base técnica para se crer que não.

"A tendência é no sentido de tratar o assunto como criptografia, onde não vale o argumento de que 'misturei os dados um bocado' nem o de que 'não consigo nem pensar num ataque' – é preciso um argumento tecnicamente rigoroso de que um ataque é uma coisa impossível."

Como se pode ver, ambos tomaram o cuidado de não eliminar a possibilidade de que alguém possa um dia apresentar um esquema de anonimização, mas tampouco se lançaram a criar uma categoria regulatória de dados "anônimos" que possa ser tratada como se não apresentasse riscos para as pessoas das quais eles foram coletados.

Pedi que ambos me indicassem uma leitura mais profunda sobre o assunto. Felten sugeriu "*Privacy and Security Myths and Fallacies of 'Personally*

> Quando uma regulamentação vem faceiramente determinar que alguns dados são "anônimos" ou mesmo "pseudônimos", essa regulamentação está gritantemente desconectada das melhores teorias de que dispõe a ciência da computação

Identifiable Information", de Arvind Narayanan e Vitaly Shmatikov[6], excelente iniciação sobre as questões técnicas tiradas das *Communications of the Association for Computing Machinery* de junho de 2010. Shoen recomendou "*Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*"[7], de Paul Ohm, uma abrangente resenha jurídica sobre a ideia de anonimização na regulamentação publicada numa edição da *UCLA Law Review* de 2010.

Da minha parte, recomendo "*On the Feasibility of User De-Anonymization from Shared Mobile Sensor Data*"[8], um olhar fantástico (ainda que um tanto técnico) sobre as inferências de reidentificação que podem ser tiradas dos aparentemente inócuos dados de sensoriamento (*sensor-data*) que saem dos nossos telefones móveis, da Ata da *Terceira Oficina Internacional sobre Aplicações de Sensoriamento nos Telefones Móveis*, de 2012.

:: PRIVACIDADE DIFERENCIAL

A Microsoft tem feito pressão no sentido de uma abordagem que chamam de "privacidade diferencial", e parece que podem cumprir com o prometido. Conforme Schoen descreve: "Os pesquisadores fazem as perguntas de suas pesquisas ao controlador original de dados, que devolve respostas intencionalmente distorcidas/corrompidas, e pode-se dizer que dá para quantificar matematicamente o mal causado à privacidade no processo, discutindo depois se valeu a pena diante dos benefícios da pesquisa."

Mas tudo isso são conjeturas: embora a quantidade de "distorção" dos dados seja uma questão quantitativa, o grau de proteção propiciada à sua privacidade pela distorção é, em última análise, uma questão pessoal, voltando-se à maneira como você se sente diante da divulgação e das suas consequências. Como costuma ser o caso, essa solução técnica incorpora um monte de premissas sobre questões que são sociais, em última instância, e calorosamente contestadas. Não se pode calar o argumento de que sua privacidade está sendo ou deixando de ser violada só com matemática.

É fascinante pensar nisso tudo, mas a maior dimensão é a seguinte: quando uma regulamentação vem faceiramente determinar que alguns dados são "anônimos" ou mesmo "pseudônimos", essa regulamentação está gritantemente desconectada das melhores teorias de que dispõe a ciência da computação. Quando se encontra algo assim numa regulamentação, sabe-se logo que o autor não tratava a proteção da privacidade com seriedade ou não era qualificado para redigir uma regulamentação. De qualquer forma, é causa para alarme.●

6. Ver http://www.cs.utexas.edu/users/shmat/shmat_cacm10.pdf 7. Ver https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006
8. Ver http://niclane.org/pubs/lane_phonesense.pdf

> **Koichi Kameda** Pesquisador do Instituto Nupef

> **Magaly Pazello** Pesquisadora do Instituto Nupef

e-Saúde

e desafios à proteção da privacidade no Brasil

O uso de tecnologias de informação e comunicação (TICs) para o oferecimento e entrega de serviços de saúde é hoje visto como estratégico em todo mundo, incluindo o Brasil. Grandes promessas (algumas antigas e custosas) alimentam a introdução de prontuários eletrônicos nas unidades de saúde e a criação de registro eletrônico de saúde dos usuários do Sistema Único de Saúde (SUS), assim como o uso de redes colaborativas para auxiliar a prestação de serviços, entre os quais o telediagnóstico, a teleconsultoria etc.

Esses sistemas envolvem a intensa manipulação de informações pessoais de saúde, consideradas informações sensíveis em razão do potencial discriminatório que guardam caso sejam reveladas em determinadas situações e sem o consentimento de seu titular. Assim, preocupações com a proteção da privacidade dos pacientes nesses ambientes inevitavelmente emergem.

Este artigo tem o propósito de apresentar um breve panorama da e-Saúde no Brasil, identificando as principais iniciativas já implementadas ou em vias de implementação, e a presença (ou ausência) de salvaguardas legais e normativas para a proteção da privacidade dos usuários dos sistemas de saúde.

:: INICIATIVAS DE E-SAÚDE NO BRASIL

O uso de tecnologias de informação e comunicação para mediar a atenção à saúde é denominado de e-Saúde (*eHealth*). A terminologia[1], adotada pela Organização Mundial da Saúde para abarcar o campo, inclui a assistência a paciente, pesquisa, educação e capacitação da força de trabalho e monitoração e avaliação em saúde.[2] De mais específico, processos de e-Saúde incluem: teleconsultorias, telediagnóstico, segunda opinião formativa, telecirurgia, telemonitoramento (televigilância), educação permanente, teleducação e prontuário eletrônico.[3]

Alguns exemplos de iniciativas de e-Saúde são a rede RUTE, considerada bem-sucedida; o Cartão Nacional de Saúde; e a adoção de prontuário eletrônico.

A RUTE - Rede Universitária de Telemedicina (www.rute.rnp.br) -, é um projeto do Ministério da Ciência, Tecnologia e Inovação, criado em 2005 com o propósito de conectar hospitais universitários e instituições de ensino via infraestrutura de comunicação nacional da Rede Nacional de Ensino e Pesquisa, possibilitando, de modo colaborativo, a realização de videoconferências para o intercâmbio de informação, discussões, estudo de casos, educação continuada, segunda opinião formativa, teleconsultoria, entre outros usos.[4] Outra rede é a Telessaúde Brasil Redes, capitaneada pelo Ministério da Saúde, e inicialmente instituída sob o nome Programa Nacional de Telessaúde em 2007.[5]

O Cartão Nacional de Saúde, também conhecido como Cartão SUS, é um documento de identificação do usuário do SUS. Instituído em 1996, possui mais de 144 milhões de usuários cadastrados. Entre os objetivos do Cartão, que passa por reformulação, estão facilitar a marcação de consultas e exames pelos pacientes e permitir a consulta ao histórico clínico dos usuários a partir de uma base de dados.[6] O projeto é alvo de críticas, tendo a falta de transparência sido apontada como uma das explicações para a sua não finalização. Com a promessa da integração digital do SUS com interoperabilidade, mais de duzentos milhões de dólares foram gastos pelos governos entre 2000 e 2011, sem o acompanhamento do controle social.[7]

Recentemente a Secretaria de Estado da Saúde de São Paulo lançou um modelo de prontuário eletrônico unificado com o histórico de atendimentos dos pacientes nas unidades estaduais de saúde. O programa "S4SP" (Saúde para São Paulo), com

1. Outros termos comumente utilizados como sinônimos de eSaúde são telessaúde e telemedicina, embora tenham sido utilizados em momentos mais iniciais (Rezende et al., 2010). Hoje a preferência é pela terminologia "eSaúde". (PNIIS, 2012). 2. http://www.who.int/topics/ehealth/en/ 3. REZENDE, E. J. C. et al. Ética e telessaúde: reflexões para uma prática segura. Rev Panam Salud Publica, v. 28, n. 1, p. 58–65, 2010. 4. A nível operacional, cada membro da rede formaliza o seu Núcleo de Telemedicina e Telessaúde, com espaço físico e equipe dedicada; são organizados workshops para compreensão do trabalho colaborativo visando à integração nacional em ensino, pesquisa e melhoria do atendimento de saúde da população; e grupos de interesse especial formados pelas instituições são criados para o desenvolvimento de atividades colaborativas de pesquisa, ensino e assistência em temas específicos da Telemedicina e Telessaúde. (Coury et al, 2010). Para mais informações sobre a RUTE ver Coury et al, 2010; Silva e Moraes, 2012. 5. SILVA, A. B.; MORAES, I. H. S. DE. O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira; The case of Telemedicine University Network: analysis of telehealth entry in the Brazilian political agenda. Physis (Rio J.), v. 22, n. 3, p. 1211–1235, 2012. 6. "Ceensp debate novos rumos para o Cartão SUS". Disponível em Disponível em http://www.ensp.fiocruz.br/portal-ensp/informe/site/materia/detalhe/24947 7. SILVA, A. B.; MORAES, I. H. S. DE. O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira; The case of Telemedicine University Network: analysis of telehealth entry in the Brazilian political agenda. Physis (Rio J.), v. 22, n. 3, p. 1211–1235, 2012.

investimentos de R$ 56 milhões do governo do Estado, foi desenvolvido no Instituto do Coração (InCor) do Hospital das Clínicas da Faculdade de Medicina da USP, numa parceria com a Companhia de Processamento de Dados de São Paulo (Prodesp). O sistema permitirá o armazenamento padronizado e o compartilhamento dos registros de saúde do paciente coletados em hospitais, ambulatórios, laboratórios ou farmácias da Secretaria. Segundo notícia da página eletrônica oficial da Secretaria da Saúde do Governo do Estado de São Paulo, "o grande diferencial do novo sistema é operar em 'nuvem', o que resultou em custo zero em hardwares, softwares e equipamentos, como microcomputadores, ou mesmo a montagem de uma rede física de servidores e sistema de segurança e manutenção."[8] A Prodesp ficará responsável pela garantia do sigilo das informações dos cerca de vinte milhões de pacientes do SUS no Estado.[9]

É preciso observar que o campo da e-Saúde está diretamente relacionado às políticas de informação, informática e comunicação em saúde no Brasil. Essa afirmação é importante num contexto em que se constata a inseparabilidade cada vez maior entre informação e as tecnologias que lhe dão suporte, o que tem contribuído para a progressiva substituição da denominação "informação, informática e comunicação" por "tecnologia da informação e comunicação".[10]

O uso de informação para gestão do sistema de saúde não é de hoje entendida como relevante, tendo a lei 8.080/1990 incluído entre as atribuições das unidades federativas a organização e coordenação do sistema de informação em saúde (art. 15, inciso IV, CF). A despeito dos diversos sistemas de informação em saúde existentes, Vasconcellos e Moraes (2005, p. 97) identificam o potencial, ainda pouco explorado, do uso da informação no processo decisório de saúde, incluindo a formulação de políticas, gestão, vigilâncias, clínica e também no controle social a fim de enfrentar a desigualdade de acesso aos benefícios do avanço tecnológico.

A necessidade de se estabelecer o propósito e as diretrizes de um Sistema Nacional de Informação em Saúde levou à elaboração de uma Política Nacional de Informação e Informática em Saúde, finalizada em 2004. Embora a PNIIS não tenha tido seu conteúdo regulamentado nem institucionalizado, acredita-se que tenha servido de inspiração para ações e normatizações no âmbito do SUS e do MS, bem como fundamento para o processo de construção da PNIIS 2012, em fase final de elaboração.[11]

O documento de 2012, que ainda resta ser aprovado, reconhece "e-Saúde" como a terminologia mais utilizada no mundo para descrever as políticas nacionais na área de TI em

8. "Paciente ganha prontuário unificado na rede do SUS paulista". Disponível em http://www.saude.sp.gov.br/ses/noticias/2013/agosto/paciente-ganha-prontuario-unificado-na-rede-do-sus-paulista 9. "Entidades médicas de SP temem quebra de sigilo em novo modelo de prontuário digital". Disponível em http://veja.abril.com.br/noticia/saude/entidades-medicas-de-sp-temem-quebra-de-sigilo-em-novo-modelo-de-prontuario-digital 10. MORAES, I. H. S. DE; VASCONCELLOS, M. M. Política Nacional de Informação, Informática e Comunicação em Saúde: um pacto a ser construído. Revista Saúde em Debate, v. 29, n. 69, p. 86–98, 2005. 11. BRASIL. Política Nacional de Informação e Informática em Saúde. Brasília: Ministério da Saúde, 2012. Disponível em: http://www.isc.ufba.br/arquivos/2012/Politica_ Nacional_de_Informacao_e_Informatica_em_Saude.pdf

saúde e propõe a mudança da nomenclatura para "Política Nacional de e-Saúde".[12] Nesse contexto, o documento afirma que a nova PNIIS deve ter como foco o usuário e registro eletrônico de saúde (RES), defendendo para isso o estabelecimento de padrões para representação e compartilhamento da informação em saúde, de infraestrutura de conectividade, a capacitação de recursos humanos na área de informação e informação em saúde, e, principalmente, a garantia da privacidade e confidencialidade da informação de saúde pessoal.[13]

Em paralelo aos debates para revisão da PNIIS, a constatação da necessidade de uma política estratégica de e-Saúde levou à elaboração de uma proposta de "Visão Estratégica de e-Saúde para o Brasil", conduzida pela Secretaria de Gestão Estratégica e Participativa (SGEP) do Ministério da Saúde, por meio do Departamento de Informática do SUS (DATASUS). A construção desse documento se deu em oficinas com a participação de profissionais representativos do Ministério da Saúde e de outros órgãos do governo federal, estadual e municipal, bem como do setor privado e de organizações não governamentais. Essas oficinas de e-Saúde, realizadas desde maio de 2012, tiveram como foco a construção do RES, que integrado ao Sistema de Informação de Saúde (E-SUS), compõe o Sistema Cartão Nacional de Saúde. O grupo de trabalho é composto por especialistas e técnicos do Poder Executivo Federal, de conselhos de classe, das operadoras de planos de saúde e profissionais de saúde dos Estados e Municípios.[14]

:: DESAFIOS À PROTEÇÃO DA PRIVACIDADE NO ÂMBITO DOS SISTEMAS DE E-SAÚDE E A NECESSIDADE DE UM MARCO REGULATÓRIO DO TRATAMENTO DE DADOS PESSOAIS

Os sistemas de e-Saúde, por envolverem o processamento de informações, que varia da simples comunicação entre pacientes e funcionários ao compartilhamento mais complexo de dados entre instituições de atenção à saúde[15], exigem cautela quanto ao seu emprego e ambiente tecnológico e, ao mesmo tempo, garantias com relação a proteção da privacidade e dos dados pessoais dos pacientes e usuários dos serviços de saúde. Ademais, esses sistemas, em razão de sua diversidade, envolvem o tratamento de diferentes tipos de informação pessoal para propósitos distintos.[16]

Antes de avançar, é preciso fazer alguns esclarecimentos.

Ainda que corriqueiramente utilizados como sinônimos, existe distinção entre "dado" e "informação". "Dado" possui uma conotação mais primitiva, estando ligado a uma espécie de "pré-informação", anterior à interpretação

12. Para mais detalhes sobre o documento da PNIIS 2012, consultar: http://www.isc.ufba.br/arquivos/2012/Politica_ Nacional_de_Informacao_e_Informatica_em_Saude.pdf 13. BRASIL. Política Nacional de Informação e Informática em Saúde. Brasília: Ministério da Saúde, 2012. Disponível em:http://www.isc.ufba.br/arquivos/2012/Politica_ Nacional_de_Informacao_e_Informatica_em_Saude.pdf 14. "Especialistas se reúnem em Brasília para a VI Oficina da E-Saúde". Disponível em http://portal.saude.gov.br/portal/saude/profissional/visualizar_texto.cfm?idtxt=42509 15. Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations. The London School of Economics and Political Science, 2010. 16. Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations. The London School of Economics and Political Science, 2010.

e ao processo de elaboração da informação. "Informação", por sua vez, pressupõe a depuração de seu conteúdo.[17]

Quando se fala em dados ou informações pessoais, refere-se a qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, como o seu nome, número de identidade, etc.

Dentre os dados pessoais, uma subcategoria especial é a dos dados sensíveis, assim compreendidos aqueles tipos de informação que se conhecidos e processados podem ter utilização potencialmente discriminatória ou particularmente lesiva, apresentando maiores riscos que a média, para o indivíduo e até mesmo para a coletividade.[18]

Os dados de saúde são considerados dados sensíveis, assim como aqueles dados que revelem a origem racial ou étnica de uma pessoa, sua convicção religiosa, filosófica ou moral, sua opinião política, sua filiação partidária, sindical ou a organizações de caráter religioso, filosófico ou político. Também são incluídos entre os dados sensíveis os dados referentes à vida sexual e os dados genéticos e biométricos de uma pessoa.[19] [20]

Considerados esses esclarecimentos, num contexto atual em que as novas tecnologias possibilitam o registro e o tratamento de informações em grande volume, incluindo informações sensíveis, surgem alguns desafios à proteção da privacidade dos usuários do sistema de saúde, como aqueles relacionados ao "vazamento" e ao acesso indevido de dados pessoais. A ausência de uma política de administração dessas informações permite que a sua manipulação ocorra de modo descuidado e em quantidades excessivas, facilitando a sua difusão pública, acidental ou intencional.[21]

Os casos de vazamento de dados pessoais, ao se tornarem públicos, acabam provocando uma sensação de desconfiança por parte dos cidadãos e dos consumidores em relação à instituição que permitiu a difusão das informações. E ainda que não se torne pública, a difusão indevida dos dados é capaz de provocar danos concretos em diversas situações, com potencial de discriminação no caso de dados sensíveis.[22]

Outro risco envolve a transferência de dados pessoais sem consentimento do seu titular ou utilização dos dados para fins distintos dos que legitimaram a sua coleta. Denúncia recente causou grande polêmica ao revelar convênio firmado pelo Tribunal Superior Eleitoral para entrega de dados pessoais de eleitores para o Serasa, empresa privada que se ocupa da comercialização de informações.[23]

Essas preocupações fazem total sentido no âmbito das iniciativas de e-Saúde, que têm o potencial

17. DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar Rio de Janeiro, 2006. 18. DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar Rio de Janeiro, 2006. 19. DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar Rio de Janeiro, 2006. 20. Ministério da Justiça. Anteprojeto de proteção a dados pessoais. Disponível em http://culturadigital.br/dadospessoais/files/2011/03/PL-Protecao-de-Dados_.pdf 21. MAGRANI, Bruno et al. Relatório de Políticas Digitais http://www.cgi.br/publicacoes/ livros/pdf/relatorio-politicas-internet-pt.pdf 22. MAGRANI, Bruno et al. Relatório de Políticas Digitais http://www.cgi.br/publicacoes/ livros/pdf/relatorio-politicas-internet-pt.pdf 23. "Lavits critica convênio TSE-Serasa e pede mais rigor no trato de dados pessoais". Disponível em http://www.rets.org.br/?q=node/2313

de identificar o usuário dos serviços de saúde a partir da expansão e do aprimoramento de bases nominais e da integração entre os bancos de dados. Exemplos são os já citados Cartão Nacional de Saúde, que promove o cadastramento da população, e as aplicações da telemedicina e da telessaúde, que poderão fornecer informações de percurso do paciente pelos serviços de saúde e seu atendimento sem a necessidade de presença física do médico.[24]

É, portanto, importante que existam regras claras sobre o tratamento dos dados pessoais por essas iniciativas, sobretudo num contexto de tensão entre interesses públicos, coletivos e da indústria privada no âmbito do uso das TICs no SUS.[25] Moraes[26] adverte sobre a importância de se adotar um processo democrático emancipador em relação à implantação das tecnologias de informação para a saúde, o que inclui o estabelecimento de limites ao tratamento de informações pessoais dos pacientes, sob pena de os pobres terem os seus corpos esquadrinhados, de os indivíduos serem regulados e controlados em nome da garantia das suas qualidades de vida.[27]

Por tais razões, o tratamento de dados pessoais vêm sendo alvo de crescente regulação no exterior. Contudo, o Brasil ainda não possui uma lei de proteção de dados pessoais, a exemplo dos demais integrantes do G20[28].

A proteção da privacidade no país tem como base a Constituição Federal, que a inclui entre os direitos fundamentais, nos dispositivos que tratam da tutela da intimidade e da vida privada (art. 5o, inciso X) e da inviolabilidade da correspondência, do domicílio e das comunicações (art. 5o, incisos XI e XII).[29]

No âmbito infraconstitucional, o Código Civil (lei 10.406/2002) garante a proteção da vida privada do indivíduo (art. 21) e o Código de Defesa do Consumidor (lei 8.078/1990) regula a manutenção de bancos de dados e cadastros de consumidores, estabelecendo uma série de garantias a estes últimos.

O sigilo profissional também é tratado pela legislação. O Código Penal trata da divulgação de informações obtidas no exercício de atividade profissional, incluindo entre os tipos penais a revelação, sem justa causa, de segredo do qual se teve conhecimento em razão de função, ministério, ofício ou profissão, e cuja revelação possa causar dano a alguém (art. 154). Também é proibida ou desobrigada de depor a pessoa a respeito de fato que deva guardar sigilo profissional (Código de Processo Penal, Código de Processo Civil e Código Civil).

24. MORAES, I. H. S. DE; VASCONCELLOS, M. M. Política Nacional de Informação, Informática e Comunicação em Saúde: um pacto a ser construído. Revista Saúde em Debate, v. 29, n. 69, p. 86–98, 2005. 25. SILVA, A. B.; MORAES, I. H. S. DE. O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira; The case of Telemedicine University Network: analysis of telehealth entry in the Brazilian political agenda. Physis (Rio J.), v. 22, n. 3, p. 1211–1235, 2012. 26. (Moraes, 2002) 27. SILVA, A. B.; MORAES, I. H. S. DE. O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira; The case of Telemedicine University Network: analysis of telehealth entry in the Brazilian political agenda. Physis (Rio J.), v. 22, n. 3, p. 1211–1235, 2012. 28. "Lei de dados pessoais: Justiça promete reenvio de anteprojeto à Casa Civil.". Disponível em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=32911&sid=97#.UbCQ1qU8hzo 29. A CF também assegura o direito de acesso do indivíduo às informações que lhe digam respeito e constem de registros ou bancos de dados de entidades governamentais ou de caráter público, bem como a possibilidade de retificação desses dados (inciso LXXII). Esse remédio constitucional, chamado de habeas data, é disciplinado pela lei 9.507, de 12 de novembro de 1997. Vale mencionar que também se assegura o sigilo das informações obtidas no exercício da atividade profissional (inciso XIV).

Na área da saúde, a privacidade e o sigilo de informações em saúde são abordadas por algumas normas setoriais e éticas.

O Código de Ética Médica (CEM) elenca, entre os seus princípios, o dever de sigilo profissional, salvo por motivo justo, dever legal ou consentimento do paciente; veda ao médico permitir o manuseio dos prontuários sob sua responsabilidade por pessoas não obrigadas ao sigilo profissional (art. 85); e proíbe também, durante o exercício da docência, a prática da medicina sem o consentimento do paciente e sem zelar por privacidade (art. 110).

A Agência Nacional de Saúde Suplementar (ANS) estabeleceu um padrão obrigatório para a troca de informações em saúde entre operadoras de planos privados de assistência à saúde e prestadores de serviço, que foi denominado Padrão TISS (Troca de Informações na Saúde Suplementar), atualmente estabelecido pela Resolução Normativa 305 (RN 305), de outubro de 2012. Um dos componentes desse padrão é o da segurança e privacidade, que prevê os requisitos para proteção dos dados de atenção à saúde, devendo seguir a legislação vigente.

Cabe mencionar que as normas existentes relacionadas a e-Saúde demonstram preocupação com a segurança e a privacidade das informações, como a portaria 2.073/2011, sobre o uso de padrões de informação em saúde e de interoperabilidade entre os sistemas de informação do SUS e para os sistemas privados e de saúde suplementar, e a Portaria 940/2011, que regulamenta o Sistema Cartão Nacional de Saúde, ambas do Ministério da Saúde. Enquanto a Portaria 2.073/2011 apenas coloca entre seus objetivos a promoção da utilização de uma arquitetura da informação em saúde de modo a permitir o compartilhamento de informações em saúde num meio seguro e com respeito ao direito à privacidade (art 20, II), a Portaria 940/2011 especifica as regras para garantia do sigilo dos dados e das informações dos usuários SUS coletados pelo Sistema.

Também a PNIIS 2012, como mencionado, entende a importância da garantia da confidencialidade, sigilo e privacidade do que chama de "informação de saúde pessoal", identificando a necessidade do estabelecimento de um marco legal, normativo e organizacional relacionado à segurança e confidencialidade da informação.[30]

Tendo em vista a legislação existente sobre privacidade no país, percebe-se a importância de um marco regulatório que estabeleça de modo mais geral os limites para o tratamento de dados pessoais, sobretudo para as informações pessoais sensíveis e de saúde, e os direitos do titular desses dados. Esse seria um primeiro passo para se garantir a proteção da privacidade num momento em que se descobre o potencial das tecnologias da informação para a prestação de serviços, como em iniciativas de e-Saúde.

30. BRASIL. Política Nacional de Informação e Informática em Saúde. Brasília: Ministério da Saúde, 2012. Disponível em: http://www.isc.ufba.br/arquivos/2012/Politica_ Nacional_de_Informacao_e_Informatica_em_Saude.pdf.

Uma iniciativa que merece menção é o anteprojeto de lei (APL) de proteção aos dados pessoais, concebido pelo Ministério da Justiça e levado a discussão pública entre novembro de 2010 e abril de 2011. O anteprojeto regula o tratamento[31] de dados pessoais realizado em território nacional por pessoa física ou jurídica de direito público ou privado, estabelecendo os princípios gerais e requisitos para utilização desses dados.

O APL estabelece que, em regra, o tratamento de dados pessoais somente pode ocorrer mediante prévio consentimento livre e expresso do titular, o qual deve ser informado, entre outras questões, da finalidade da coleta e tratamento de seus dados, da difusão desses dados e de seus direitos como, por exemplo, o de se negar a fornecer tais dados.

O anteprojeto elenca alguns princípios gerais de proteção aos dados pessoais, entre eles:

- Princípio da finalidade: os dados pessoais somente podem ser alvo de tratamento compatível com as finalidades que fundamentaram a sua coleta e foram informadas ao titular.
- Princípio da necessidade: o tratamento dos dados pessoais deve ser limitada ao mínimo necessário, sobretudo quando a finalidade possa ser atingida com a utilização de dados anônimos ou com uso de meios que permitam a identificação do titular somente em caso de necessidade.
- Princípio do livre acesso: o titular deve poder consultar gratuitamente os seus dados pessoais e as modalidades de tratamento dos mesmos.
- Princípio da proporcionalidade: o tratamento de dados pessoais deve ocorrer apenas quando houver relevância e pertinência em relação à finalidade para a qual foram coletados.
- Princípio da qualidade dos dados: exatidão dos dados pessoais alvo de tratamento.
- Princípio da transparência: o titular deve ser informado sobre os tratamentos de seus dados, como finalidade, quais dados foram tratados e tempo de conservação dos mesmos; o anteprojeto também exige o respeito da lealdade e da boa fé objetiva no tratamento das informações (princípio da boa fé objetiva).
- Princípios da segurança e da prevenção: utilização das medidas técnicas e administrativas proporcionais ao atual estado da tecnologia, à natureza dos dados pessoais e às características específicas do tratamento a fim de proteger os dados de destruição, perda, alteração e difusão, tanto acidentais quanto ilícitas, bem como do acesso não autorizado. Ademais, tais medidas, sempre que possível, devem ser capazes de prevenir a ocorrência desses danos.
- Princípio da responsabilidade: deverão ser reparados os danos patrimoniais, morais, individuais ou coletivos causados aos titulares dos dados pessoais.

O anteprojeto possui normas específicas sobre dados sensíveis, categoria que inclui os dados de saúde. Por se tratarem de dados pessoais com potencial de gerar discriminação de seus titulares, os dados sensíveis encontram restrições para a

31. O anteprojeto entende como tratamento "toda operação ou conjunto de operações, realizadas com ou sem o auxílio de meios automatizados, que permita a coleta, armazenamento, ordenamento, conservação, modificação, comparação, avaliação, organização, seleção, extração, utilização, bloqueio e cancelamento de dados pessoais, bem como o seu fornecimento a terceiros por meio de transferência. comunicação ou interconexão".

sua inclusão em bancos de dados. O tratamento seria permitido em alguns casos, mediante prévio consentimento livre, informado e por escrito do titular, quando indispensável para o exercício legítimo das atribuições legais ou estatutárias do responsável pela utilização dos dados; quando for destinado a pesquisa histórica, científica ou estatística; quando for realizado por profissionais da área da saúde e for indispensável para a tutela da saúde do interessado; e quando for necessário para o exercício de funções próprias dos poderes de Estado.

Para a estrita observância das normas do anteprojeto é criada uma autoridade de garantia da proteção de dados pessoais. A autoridade é responsável por propor ações da política nacional de proteção de dados pessoais; receber e analisar consultas, denúncias e sugestões apresentadas por titulares de dados pessoais, entidades representativas ou pessoas jurídicas de direito público ou privado referentes à proteção de dados pessoais; e aplicar sanções, medidas corretivas e preventivas para garantir a observância das normas e princípios do anteprojeto, entre outras medidas.

Os princípios e regras previstos no APL se coadunam com os requisitos legais e regulatórios estabelecidos em legislações dos Estados Unidos, Canadá e Europa a respeito da privacidade em ambientes de alta tecnologia. Segundo estudo da *Policy Engagement Initiative, da London School of Economics*, tais requisitos podem, inclusive, auxiliar na própria prestação dos serviços de saúde e na incorporação de iniciativas de e-Saúde, ajudando a garantir a integridade e acurácia da informação médica presente nesses bancos de dados.[32]

:: CONCLUSÃO

Este artigo procurou apresentar brevemente um panorama das iniciativas de e-Saúde no Brasil, apontando as lacunas da legislação sobre privacidade em termos de proteção aos dados pessoais no âmbito da saúde. Os sistemas de e-Saúde, um campo marcado pela diversidade de tecnologias e aplicações, envolve o tratamento de diferentes tipos de dados pessoais e para finalidades distintas.

Num momento em que se discute a implementação de iniciativas como o Cartão Nacional de Saúde, que inclui o registro eletrônico de saúde dos usuários dos sistemas de saúde, e a adoção de prontuários eletrônicos pelas unidades de saúde, é preciso que sejam acompanhadas de regras claras sobre o tratamento dos dados e informações de saúde. A portaria 940/2011 do MS possui dispositivos específicos sobre o sigilo das informações dos usuários vinculadas ao Cartão Nacional de Saúde, mas outras legislações são exigidas para regular o tratamento de informações pessoais de saúde em outras iniciativas.

É importante que as iniciativas e políticas de e-Saúde, como a PNIIS 2012, que já identificam a importância de um marco legal relacionado à segurança e à confidencialidade da informação, estejam integradas a outras iniciativas do próprio

32. Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations. The London School of Economics and Political Science, 2010.

governo envolvendo a regulação das tecnologias de informação e comunicação e o tratamento de dados pessoais. Um marco normativo para proteção dos dados pessoais beneficiaria sem dúvida o setor da saúde ao prever princípios e regras que assegurem, por exemplo, que apenas as informações relevantes sejam coletadas e sejam armazenadas com o devido cuidado.

É claro, além das medidas legais, outras são igualmente primordiais para se garantir a privacidade dos pacientes no âmbito dos sistemas de e-Saúde. Assim, a adoção de tecnologias baseadas em conceitos como *privacy-enhancing*, *privacy assessment impact e privacy-by-design*, e normas que regulem a nível profissional a confidencialidade e a privacidade das informações dos pacientes e usuários dos sistemas de saúde, inclusive com medidas de educação dos profissionais envolvidos no tratamento dos dados pessoais, podem ser úteis.[33]

Referências bibliográficas

BRASIL. Política Nacional de Informação e Informática em Saúde. Brasília: Ministério da Saúde, 2012. Disponível em:http://www.isc.ufba.br/arquivos/2012/Politica_ Nacional_ de_Informacao_e_Informatica_em_Saude.pdf

Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations. The London School of Economics and Political Science, 2010. http://www.cgi.br/publicacoes/ livros/pdf/relatorio-politicas-internet-pt.pdf

MAGRANI, Bruno et al. Relatório de Políticas Digitais. Disponível em http://www.cgi.br/publicacoes/livros/pdf/relatorio-politicas-internet-pt.pdf

Ministério da Justiça. Anteprojeto de proteção a dados pessoais. Disponível em http://culturadigital.br/dadospessoais/files/2011/03/PL-Protecao-de-Dados_.pdf

MORAES, I. H. S. DE; VASCONCELLOS, M. M. Política Nacional de Informação, Informática e Comunicação em Saúde: um pacto a ser construído. Revista Saúde em Debate, v. 29, n. 69, p. 86–98, 2005.

REZENDE, E. J. C. et al. Ética e telessaúde: reflexões para uma prática segura. Rev Panam Salud Publica, v. 28, n. 1, p. 58–65, 2010.

SILVA, A. B.; MORAES, I. H. S. DE. O caso da Rede Universitária de Telemedicina: análise da entrada da telessaúde na agenda política brasileira; The case of Telemedicine University Network: analysis of telehealth entry in the Brazilian political agenda. Physis (Rio J.), v. 22, n. 3, p. 1211–1235, 2012.

WHO. eHealth. http://www.who.int/topics/ehealth/en/

"Ceensp debate novos rumos para o Cartão SUS". Disponível em http://www.ensp.fiocruz.br/portal-ensp/informe/site/materia/detalhe/24947

"Entidades médicas de SP temem quebra de sigilo em novo modelo de prontuário digital". Disponível em http://veja.abril.com.br/noticia/saude/entidades-medicas-de-sp-temem-quebra-de-sigilo-em-novo-modelo-de-prontuario-digital

"Especialistas se reúnem em Brasília para a VI Oficina da E-Saúde". Disponível em http://portal.saude.gov.br/portal/saude/profissional/visualizar_texto.cfm?idtxt=42509

"Lavits critica convênio TSE-Serasa e pede mais rigor no trato de dados pessoais". Disponível em http://www.rets.org.br/?q=node/2313

"Lei de dados pessoais: Justiça promete reenvio de anteprojeto à Casa Civil." Disponível em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=32911&sid=97#.UbCQ1qU8hzo

"Paciente ganha prontuário unificado na rede do SUS paulista". Disponível em http://www.saude.sp.gov.br/ses/noticias/2013/agosto/paciente-ganha-prontuario-unificado-na-rede-do-sus-paulista

33. Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations. The London School of Economics and Political Science, 2010.

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

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

instituto nupef

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