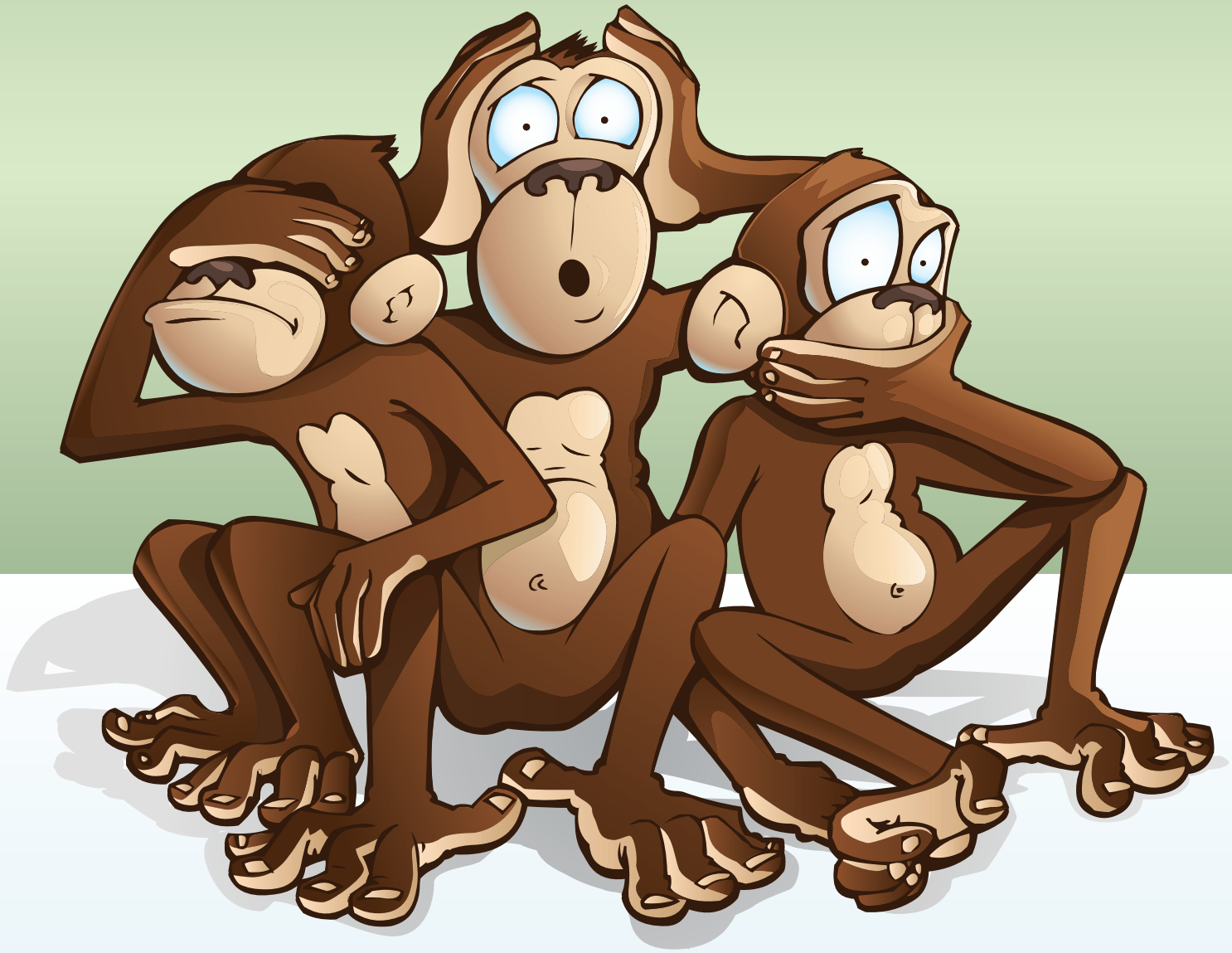
> TICS E VIOLÊNCIA contra as mulheres

> REDES E ESTADOS-NAÇÃO no século 21

> ENTENDA O QUE é o WHOIS

poliTICs

Uma publicação do Instituto Nupef • maio / 2012 • www.politics.org.br



Empresas, governos e Internet: o imperativo ético da defesa de direitos

poliTICs nº 12

Índice

Editorial

Não é raro surgirem notícias sobre as relações comerciais entre empresas provedoras de tecnologias – em sua grande maioria, baseadas em países da Europa e América do Norte - e governos repressivos que violam direitos humanos e perseguem seus cidadãos. Casos em que grandes corporações como a Narus (subsidiária da Boeing), McAfee/Intel e Cisco Systems vendem produtos para governos vigiarem e interceptarem comunicações, censurarem conteúdos e perseguirem pessoas têm gerado intenso debate. A proposta da Electronic Frontier Foundation (EFF) para um compromisso ético das empresas - de adotarem políticas internas de respeito aos direitos humanos - abre esta edição da poliTICs. A EFF apresenta princípios e recomendações relevantes e válidos para empresas em qualquer país do mundo que optem por reconhecer sua corresponsabilidade no uso que será feito das tecnologias que desenvolvem e comercializam.

Um explicação detalhada sobre o WHOIS – que inclui o histórico da criação desta enorme base de dados – é apresentada no artigo de Demi Getschko e Frederico Neves, do NIC.br. Os autores descrevem as diversas tentativas de reformular ou aprimorar o serviço – que identifica o indivíduo ou organização detentora de um nome de domínio (e responsável por ele) – , e mostram por que é importante saber o que é o WHOIS e como ele funciona, quando se debate sobre direitos e deveres na Internet.

Continuamos a edição com um interessante texto da hacker e ativista Eleanor Saitta, que faz considerações contundentes sobre o papel do Estado, do setor privado e dos cidadãos no desenho de um modelo de sociedade centrada em redes. Eleanor também conta sobre os projetos nas quais está envolvida e convida para um diálogo sobre caminhos rumo a um futuro no qual, ela garante, as redes vão vencer. Em seguida, apresentamos um texto adaptado a partir do estudo de caso sobre o Gabinete Digital do Governo do Estado do Rio Grande do Sul, realizado no âmbito do projeto Impacto 2.0, da Fundación Comunica, que analisou políticas de uso de ferramentas Web 2.0 pela admnistração pública em cinco países da América Latina.

O tema da violência contra a mulher através das tecnologias – que ainda tem pouca visibilidade, apesar de o número de crimes praticados através da Internet e do uso de telefones móveis ser crescente – fecha esta edição. O texto é parte dos resultados de um abrangente estudo feito pela Associação para o Progresso das Comunicações (APC) e, além de retratar as formas de violação dos direitos das mulheres, também aponta para caminhos possíveis para responder com eficácia a este tipo de violência. ●

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

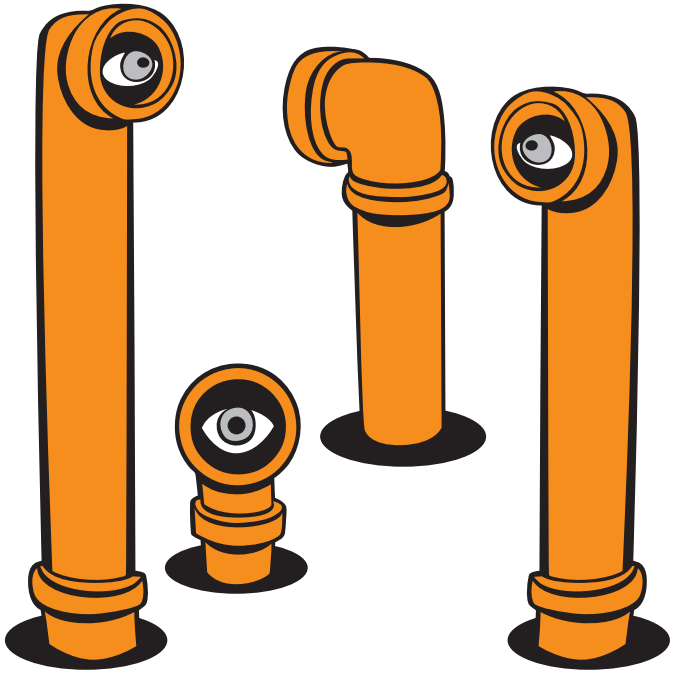
Um abraço,

Graciela Selaimen – *Editora da poliTICs*

> **Cindy Cohn** diretora da Electronic Frontier Foundation

> **Trevor Timm** colaborador ativista da Electronic Frontier Foundation

> **Jillian C.York** diretora da Electronic Frontier Foundation



Direitos Humanos e o comércio de tecnologias:

como as corporações podem evitar colaborar com regimes repressivos

Já há anos é possível encontrar provas suficientes de que governos autoritários ao redor do mundo têm contado com tecnologias produzidas por empresas americanas, canadenses e europeias para facilitar violações de direitos humanos – e hoje tudo indica que esta tendência é crescente. De softwares que permitem filtramento e bloqueio de conteúdo online a ferramentas que ajudam governos a espionarem seus cidadãos, muitas de tais empresas estão servindo ativamente a governos autocráticos, como "pequenos ajudantes da repressão".

O alcance destas tecnologias é incrivelmente amplo: governos podem fazer escutas em chamadas de telefones celulares[1], usar reconhecimento de voz para fazer varreduras em redes móveis, usar reconhecimento facial para fazer buscas em fotografias online e offline, ler mensagens de e-mail e texto, rastrear todos os movimentos de

1. Ben Elgin e Vernon Silver, "The Surveillance Market and Its Victims," Bloomberg, 20 de dezembro de 2011 - http://www.bloomberg.com/data-visualization/wired-for-repression/.

um cidadão utilizando GPS e até mesmo conseguem *mudar* os conteúdos de e-mails durante sua rota rumo ao destinatário[2]. Algumas ferramentas são instaladas usando o mesmo tipo de *malware* e *spyware* perniciosos usados por criminosos online para roubar informações bancárias e de cartões de crédito[3]. Eles podem secretamente ligar webcams embutidas em laptops pessoais e microfones em telefones celulares que não estão sendo usados[4]. Outras ferramentas e serviços permitem que governos bloqueiem categorias inteiras de sítios Web, impedindo que cidadãos acessem informações essenciais. Estas ferramentas têm sido implementadas em uma escala tão massiva em determinados locais, que podem ser utilizadas para rastrear e espionar cada pessoa num país inteiro.

Este é um fenômeno que se espalha pelo planeta e que implica dúzias de corporações. Ao longo do ano passado – e em parte em resposta às insurgências que varreram o mundo árabe – , preocupações sobre este tipo de exportação foram amplificadas em reportagens na mídia e por organizações de defesa de direitos digitais, provocando um debate sobre os cursos de ação mais apropriados.

- Por exemplo, foi revelado que a Narus, uma subsidiária da Boeing, vendeu ao Egito sofisticados equipamentos utilizados para vigilância[5]. É notável que a tecnologia da Narus também tenha sido descoberta em uso para conduzir a vigilância massiva e ilegal de norte-americanos, como parte dos programas de vigilância sem garantias contra os quais a EFF vem tomando medidas legais desde 2006[6].

- Descobriu-se que equipamentos da California BlueCoat Systems, Inc. estão em uso na Síria[7].

- A empresa alemã Trovicor supostamente vendeu tecnologia a uma dúzia de países no Oriente Médio e norte da África, incluindo Bahrein, onde dúzias de ativistas foram torturados antes e depois de serem mostradas transcrições de suas mensagens de texto e conversas por telefone, capturadas com esta tecnologia[8].

- Produtos da empresa canadense Netsweeper são usados pelos governos da Arábia Saudita, Qatar, Emirados Árabes e Iêmen para censurar uma série de conteúdos, inclusive sítios Web políticos.

2. Vernon Silver, "Post-Revolt Tunisia Can Alter E-mail With 'Big Brother' Software," Bloomberg, 12 de dezembro de 2011 - http://www.bloomberg.com/news/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.html. 3. Jennifer Valentino-DeVries, "Surveillance Company Says It Sent Fake iTunes, Flash Updates," Wall Street Journal, 21 de novembro de 2011 - http://blogs.wsj.com/digits/2011/11/21/surveillance-company-says-it-sent-fake-itunes--flash-updates-documents-show/. 4. Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid with U.S.-Europe Spy Gear," Bloomberg, novembro de 2011- http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html. 5. Timothy Karr, "One U.S. Corporation's Role in Egypt's Brutal Crackdown," Huffington Post, 28 de janeiro de 2011 - www.huffingtonpost.com/timothy-karr/one-us-corporations--role_b_815281.html. 6. Para mais informações sobre os casos da EFF, ver: https://www.eff.org/issues/nsa-spying 7. Jillian C. York, "Government Internet Surveillance Starts With Eyes Built in the West," Electronic Frontier Foundation, 2 de setembro de 2011, https://www.eff.org/deeplinks/2011/09/government-internet-surveillance-starts-eyes-built. 8. Vernon Silver e Ben Elgin, "Torture in Bahrain Becomes Routine With Help From Nokia Siemens," Bloomberg, 22 de agosto de 2011 - http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html.

A empresa recusou-se a discutir o assunto, afirmando: "Não há nenhuma boa conversa que possamos ter"[9].

• O SmartFilter, produto da McAfee/Intel, vendeu software para filtragem de conteúdos na Web para diversos países, incluindo Bahrain, Emirados Árabes, Omã e Tunisia. Em todos os casos, o software foi utilizado para censura política[10].

• A Cisco Systems enfrenta litigâncias em Maryland e na Califórnia baseadas em sua suposta venda de equipamentos de vigilância para os chineses – para rastrear, monitorar e desta forma facilitar a prisão ou o desaparecimento de ativistas de direitos humanos e minorias religiosas que têm sido sujeitadas a enormes violações de direitos humanos.[11]

E a lista segue[12]....

A Electronic Frontier Foundation acredita que é hora de as empresas de tecnologia, especialmente aquelas que vendem equipamentos de vigilância e filtragem, tomarem providências e garantirem que não estão ajudando governos de outros países a cometerem violações de direitos humanos contra seus cidadãos.

A questão é complicada porque a maioria destas tecnologias é "*dual use*." Isso significa que juntamente com a possibilidade de facilitar abusos de direitos humanos, quase todas estas tecnologias podem ser usadas para propósitos legítimos, tanto para os governos quanto para usuários não governamentais. Os usos não governamentais incluem investigação sobre segurança de redes e computadores, pesquisa e proteção, que podem ajudar bastante os usuários a proteger seus direitos e aumentar sua segurança. Os usos governamentais incluem aplicação da lei e segurança nacional sob circunstâncias justificadas, o que também pode ajudar a proteger os usuários. Frequentemente as funcionalidades técnicas para usos legítimos e ilegítimos são as mesmas. Isto torna difícil – se não impossível – usar o design ou descrição técnica, ou o uso potencial de uma ferramenta ou serviço, como a única base para determinar se estas foram usadas para violar direitos humanos. Por esta razão a EFF acredita que qualquer esforço para abordar a facilitação de violações de direitos humanos por tecnologias e serviços deve focar-se nos usos e nos usuários, não em descrições tecnológicas – e não deve ir além dos casos de vendas em que governos e entidades governamentais são os usuários finais.

9. Nicki Thomas and Amy Dempsey, "Guelph-based software censors the Internet in the Middle East," Toronto Star, 12 de junho de 2011 - http://www.thestar.com/news/article/1007399-guelph-based-software-censors-the-internet-in-the-middle-east. 10. Paul Sonne and Steve Stecklow, "U.S. Products Help Block Mideast Web," Wall Street Journal, March 27, 2011, http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html. 11. Rainey Reitman, "Cisco and Abuses of Human Rights in China: Part 1," Electronic Frontier Foundation, August 22, 2011, https://www.eff.org/deeplinks/2011/08/cisco and abuses human rights china part 1. 12. A EFF continua a monitorar casos de venda de tecnologias de vigilância a regimes autoritários. Ver em https://www.eff.org/issues/mass-surveillance-technologies.

Caso contrário, é muito grande o risco de prejudicar usuários legítimos, e no final das contas fragilizar sua segurança e a proteção de seus direitos humanos[13].

Como resultado, a EFF propõe que as empresas transitem por estes temas difíceis adotando um robusto programa "Conheça seu Cliente[14]", similar àquele delineado nos atuais mecanismos de controle de exportação dos EUA, ou um programa similar ao que é requerido, para outros propósitos, pelo *Foreign Corrupt Practices Act*[15]. Manter o foco no usuário e no potencial (ou real) uso da tecnologia para violações de direitos humanos por governos – mais do que nas capacidades das tecnologias, por si só – representa um caminho mais direto para dar fim às violações de direitos humanos, gerando menos riscos colaterais.

A seguir, nós esboçamos uma proposta básica para que as empresas auditem seus clientes governamentais atuais e potenciais, num esforço para evitar que suas tecnologias e serviços sejam usados para abusos de direitos humanos. Há dois componentes-chave: transparência e padrões de "conheça seu cliente". A mesma proposta básica poderia ser implementada através de ação voluntária, governamental, ou através de outros incentivos ou marcos regulatórios.

A despeito de como seja implementado, nós acreditamos que este arcabouço pode ajudar tanto às empresas quanto ao público a alcançar uma visão mais clara de quem está usando estas tecnologias e como elas estão sendo usadas – e depois dar alguns passos básicos para evitar consequências terríveis como as que já testemunhamos[16].

> A Electronic Frontier Foundation acredita que é hora de as empresas de tecnologia, especialmente aquelas que vendem equipamentos de vigilância e filtragem, tomarem providências e garantirem que não estão ajudando governos de outros países a cometerem violações de direitos humanos

13. Falando claramente, com base na experiência da EFF – desde os anos 90, quando atuou para liberar de restrições às exportações tecnologias de encriptação,e mais recentemente, no seu trabalho para libertar as tecnologias de comunicação do efeito combinado de medidas restritivas à exportação e regimes de sanção, nós temos graves preocupações sobre este tema, e provavelmente nos oporíamos à extensão ou implementação de uma abordagem regulatória baseada unicamente em aspectos tecnológicos, no contexto das tecnologias de vigilância e/ou filtragem de conteúdos. 14. Na realidade, diferente de alguns dos outros lugares onde é usado, o "know your customer" é uma ideia razoável, no contexto específico das vendas de tecnologias sofisticadas para governos, em que podem ser usadas para facilitar violações de direitos humanos em países onde a repressão é uma possibilidade concreta. 15. Ver : United States Department of Justice, Foreign Corrupt Practices Act, http://www.justice.gov/criminal/fraud/fcpa/ 16. A Global Network Initiative - uma iniciativa multissetorial que trabalha com empresas buscando evitar ou minimizar censura - já começou a implementar um programa que contém alguns destes mesmos elementos no contexto das tecnologias de vigilância e filtragem.

:: TRANSPARÊNCIA

O primeiro passo é transparência. A indústria de vigilância e censura massivas como um todo tem sido notoriamente silenciosa e opaca, o que, por sua vez, permitiu sua proliferação sem maiores cuidados. Este caráter de opacidade e segredo chegou até mesmo a restringir, no passado, tentativas de fazer estar empresas prestarem contas sobre suas atividades. Por exemplo, o *Government Accountability Office* dos EUA não foi capaz de identificar quaisquer empresas fornecedoras destas tecnologias ao Irã, em parte porque os negócios são velados, segundo reportagens[17].

Entretanto, como aprendemos recentemente, somente o fato de esta informação estar acessível ao escrutínio público já ajuda a promover mudanças.

Por exemplo, em agosto de 2011, depois de uma reportagem da Bloomberg sobre a empresa italiana Area SpA – que estava construindo um imenso centro de vigilância na Síria – irromperam protestos do lado de fora do escritório italiano e a Area SpA suspendeu a construção[18]. Fato parecido ocorreu em 2009, quando protestos sobre o envolvimento da Nokia Siemens Networks em venda de equipamentos para o Irã fizeram com que a empresa vendesse sua subsidiária, agora chamada Trovicor, que constroi centros de vigilância massiva. Também em 2009 a Websense, empresa baseada na Califórnia que vende software de filtragem, adotou a política de não vender para governos estrangeiros depois que descobriu-se que seus produtos eram usados pelo governo do Iêmen[19]. Mais recentemente, em resposta a uma chamada de propostas publicada pelas autoridades paquistanesas, diversas empresas – incluindo a McAfee SmartFilter, que opera em vários países do Oriente Médio – responderam afirmando sua recusa em vender para o governo[20].

A atenção da mídia aos mercados destas tecnologias também tem sido crucial. A cobertura midiática do chamado "*Wiretapper's Ball*," uma série de convenções organizadas pela Intelligence Support Systems (ISS), levou a diretora global de programas da ISS, Tatiana Lucas, a admitir que investigações como as que faz o *Wall Street Journal* "[fazem] as indústrias de armas norte-americanas intimidarem-se ante a perspectiva de desenvolver, e depois exportar, qualquer coisa que possa de alguma forma ser usada para apoiar a vigilância governamental[21]."

17. Ver Ben Elgin, Vernon Silver, e Alan Katz, "Iranian Police Seizing Dissidents Get Aid of Western Companies," 30 de outubro de 2011, Bloomberg, http://www.bloomberg.com/news/2011 10 31/iranian police seizing dissidents get aid of western companies.html 18. Vernon Silver e Ben Elgin, "Torture in Bahrain Becomes Routine With Help From Nokia Siemens," Bloomberg, Augusto de 2011, http://www.bloomberg.com/news/2011 08 22/torture in bahrain becomes routine with help from nokia siemens networking.html. 19. Blog da Websense, "Websense Issues Statement on Use of its URL Filtering Technology by ISPs in Yemen," 17 de agosto de 2009, http://community.websense.com/blogs/websense features/archive/2009/08/17/websense issues statement on use of its url filtering technology by isps in yemen.aspx. 20. Maira Sutton, "Companies Respond to Pakistan's Internet Censorship Proposal," Electronic Frontier Foundation, março de 2012, https://www.eff.org/deeplinks/2012/03/companies respond pakistans national censorship proposal. 21. Jennifer Baker, "Surveillance companies should not sell to despots says EU," IDG, 10 de dezembro de 2011, http://www.pcworld.idg.com.au/article/409841/surveillance_tech_companies_should_sell_despots_says_eu/

Entretanto, não há muito mais que a imprensa possa fazer. A vasta maioria destas empresas recusa-se a sequer comentar sobre publicações de notícias. E o que é pior, as vendas destes perigosos sistemas são canalizadas através de subsidiárias e terceiras partes, deixando os jornalistas no escuro e as empresas prontas para negações plausíveis.

A EFF acredita que muito mais poderia ser feito diretamente pelas empresas para aumentar a transparência nestes mercados nebulosos[22]. As empresas podem começar imediatamente a oferecer informações voluntariamente, como parte de um processo mais amplo de transparência, tais como os que a Global Network Initiative (GNI) já põe em prática com relação a determinados temas, ou como uma iniciativa independente. Mais ainda, no caso de empresas recusarem-se a prestar contas, nós encorajamos o congresso norte-americano, países na União Europeia e autoridades locais a usar seus incentivos (nas contratação de serviços pelos governos, ou de outras formas), bem como seus poderes de investigação, para buscar respostas sobre potenciais cumplicidades em casos de abusos de direitos humanos que possam estar disponíveis em registros públicos. Várias entidades governamentais têm o poder de convocar audiências, emitir petições para obter documentos ou testemunhos e até mesmo conduzir investigações completas. Outras entidades governamentais deveriam considerar requerer transparência em temas de direitos humanos como condição para contratação pelo governo. Por conta de um trabalho importante feito pelas organizações de comunicação e mídia, já existe uma longa lista de empresas que merecem um questionamento mais profundo, embora nós suspeitemos que estas são apenas a ponta do iceberg[23].

:: O ARCABOUÇO DA EFF PARA A ANÁLISE DE CLIENTES

[Nota: este esquema usa termos-chave —Tecnologias, Transação, Empresa e Governo — que estão definidos mais adiante e sempre aparecerão no texto iniciados com letras maiúsculas]

O arcabouço da EFF para a política "conheça seu cliente" tem dois componentes básicos:

1. Empresas que vendem Tecnologias de vigilância ou filtragem para Governos devem investigar proativamente e "conhecer seu cliente" antes e durante uma Transação. Isso inclui, como ressaltamos abaixo, o uso que o cliente faz - ou que parece provável que fará - das Tecnologias. Nós sugerimos que se coloque o foco nos direitos humanos, de maneira similar à que já é requerida

22. Governos repressivos também podem demandar que as empresas entreguem as informações de seus clientes obtidas na prestação de seus serviços e nas relações com os usuários. Isto também pode ajudar governos repressivos a cometer violações de direitos humanos, mas não é um fato abordado neste artigo. Aqui nos focamos unicamente na venda de tecnologias aos governos para fins de vigilância e censura. 23. A lista da Privacy International de provedores de tecnologias de vigilância é o documento mais elucidativo até o momento: https://www.privacyinternational.org/big-brother-incorporated/countries.

da maioria destas empresas sob o *Foreign Corrupt Practices Act*[24] para evitar suborno, e sob a regulação de exportação para evitar transferências de armas, assim como para outros propósitos[25];

2. As Empresas devem abster-se de participar de Transações nas quais sua pesquisa para "conhecer seu cliente" revelar provas objetivas ou gerar preocupações plausíveis de que as Tecnologias providas pela Empresa a um Governo serão usadas para facilitar a violação de direitos humanos.

Este arcabouço básico seria mais eficaz se as empresas o implementassem de forma voluntária, assegurando desta forma a abordagem mais flexível possível, conforme as tecnologias mudam e conforme transformam-se as situações ao redor do mundo. A Nokia Siemens Networks já adotou uma Política de Direitos Humanos que incorpora algumas destas orientações[26]. A Websense adotou uma política anti-censura em 2009 e desde então tornou-se membro da Global Network Initiative, um grupo multissetorial cuja tarefa é proteger a liberdade de expressão e a privacidade, que já lida com algumas destas questões[27].

Se as empresas não agirem por sua própria conta, e não o fizerem logo, com um compromisso convincente, então uma abordagem regulatória provavelmente será necessária. Em 2011, o Parlamento da União Europeia deu um passo rumo

Se as empresas não agirem por sua própria conta, e não o fizerem logo, com um compromisso convincente, então uma abordagem regulatória provavelmente será necessária.

24. N.E.: legislação anti-corrupção implementada pelo governo dos EUA em 1977. Ver em http://www.justice.gov/criminal/fraud/fcpa/
25. Electronic Code of Federal Regulations, Title 15: Commerce and Foreign Trade, http://ecfr.gpoaccess.gov/cgi/t/text/textidxc=ecfr&sid=b59804210 3e95c10c396b0140e0620b7&rgn=div9&view=text&node=15:2.1.3.4.21.0.1.7.22&idno=15 (acessado em 9 de fevereiro de 2012). 26. A Nokia Siemens Networks adotou uma política de direitos humanos em agosto de 2010. Ver: http://ecfr.gpoaccess.gov/cgi/t/text/text- idxc=ecfr&sid=b59804210 3e95c10c396b0140e0620b7&rgn=div9 &view=text&node=15:2.1.3.4.21. 0.1.7.22&idno=15. 27. Política anti-censura da Websense: https://www.websense.com/content/censorship-policy.aspx; e Global Network Initiative: http://globalnetworkinitiative.org/.

à prevenção de vendas de equipamento de vigilância a regimes autoritários. Membros do Congresso dos EUA também estão observando a questão de perto[28]. Na data em que publicamos este artigo, um projeto de lei foi apresentado pelo Congressista Chris Smith chamado "*Global Online Freedom Act of 2012*" contendo várias provisões positivas, incluindo requerimentos de transparência como parte de um devido processo de auditoria de direitos humanos, analisado de maneira independente por uma terceira parte e reportado publicamente[29].

Em seguida elencamos as orientações básicas para assegurar que as empresas norte-americanas não sejam cúmplices de violações de direitos humanos ao redor do mundo, quer sejam seus esforços voluntários ou impostos por regulação.

:: RECOMENDAÇÕES: O PROCESSO DE DIREITOS HUMANOS "CONHEÇA SEU CLIENTE"

Investigar Afirmativamente: a Empresa deve ter um processo, liderado por uma pessoa especificamente designada para isso, para dedicar-se a uma avaliação permanente sobre a possibilidade ou o fato de que as Tecnologias ou Transação sejam — ou estejam sendo — usadas para ajudar, facilitar ou encobrir abusos de direitos humanos, conforme estes são definidos pelos principais instrumentos internacionais das Nações Unidas. Um bom modelo para isso pode ser a atual tendência entre as empresas de designar Diretores de Privacidade, que geralmente são funcionários de alto nível, em posições de poder, que asseguram que a empresa respeita a privacidade de seus clientes e de outras pessoas. Diretores de Direitos Humanos poderiam desempenhar papel similar com respeito aos impactos das atividades da empresa nesta área[30].

A despeito da forma como é implementado, este processo deve ser muito mais do que simplesmente palavras ditas da boca para fora e precisa ser verificável (e verificado) por pessoas de fora da empresa. Este deve ser um compromisso institucional, com mecanismos reais implementados, incluindo-se aí ferramentas, treinamento e formação de pessoal, bem como a previsão de consequências para os funcionários quando o processo não for cumprido. Ele deve ser incluído na política e nos procedimentos operacionais de toda a empresa e comunicado aos parceiros comerciais, às instituições contratantes e ao público. Além disso, para construir transparência e consolidar uma comunidade mais

28. Vernon Silver, "EU Curbs Export of Surveillance Systems," Bloomberg, 27 de setembro de 2011, http://www.bloomberg.com/news/2011 09 27/eu curbs export of surveillance systems.html. Ver também o comentário da EFF: https://www.eff.org/deeplinks/2011/10/eu parliament takes first step bans sales.
29. H.R. 3605: Global Online Freedom Act of 2011, http://www.govtrack.us/congress/bills/112/hr3605. 30. Kenneth A. Bamberger e Deirdre K. Mulligan, "New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States," Law and Policy (2011), papers.ssrn.com/sol3/papers.cfm?abstract_id=1701087.

> a Empresa deve ter um processo, liderado por uma pessoa especificamente designada para isso, para dedicar-se a uma avaliação permanente sobre a possibilidade ou o fato de que as Tecnologias ou Transação sejam - ou estejam sendo - usadas para ajudar, facilitar ou encobrir abusos de direitos humanos

ampla de empresas agindo para proteger os direitos humanos, uma Empresa que decida recusar (ou dar continuidade a) serviços com base nestes padrões deve, quando possível, tornar sua decisão pública, de modo que outras empresas beneficiem-se desta avaliação.

O PROCESSO DEVE INCLUIR, NO MÍNIMO:

1. REPRESENTAÇÕES. Revisão do que afirma o Governo que faz a compra e do que os agentes de Governo e os funcionários da Empresa estão dizendo sobre o uso das Tecnologias, tanto antes quanto durante qualquer Transação. Isto inclui, entre outras coisas, revisão de materiais de vendas e marketing, discussões e questões técnicas, apresentações, especificações técnicas e contratuais, discussões sobre customização e treinamento, bem como discussões e requisições sobre suporte técnico e atualizações. Algumas das provas mais problemáticas no caso da Cisco são as apresentações que foram feitas pelos funcionários da empresa, que inegavelmente fazem marketing sobre a Tecnologia e o suporte oferecidos ao Governo da China na repressão aos praticantes do Falun Gong[31].

2. POSSIBILIDADES E MITIGAÇÃO. Revisão das possibilidades oferecidas pela Tecnologia para a violação de direitos humanos e consideração de possíveis medidas de mitigação, tanto técnicas quanto contratuais.

3. CUSTOMIZAÇÃO E SERVIÇOS A LONGO PRAZO. Revisão de quaisquer requisições (ou demandas) de customização, bem como de serviços de mais longo prazo, atualizações e outros arranjos.

31. Sarah Lai Stirland, "Cisco Leak: 'Great Firewall' of China Was a Chance to Sell More Routers," Wired, May 20, 2008, http://www.wired.com/threatlevel/2008/05/leaked cisco do/.

4. PROTEÇÕES LEGAIS. Revisão das leis, regulação e práticas do Governo relativas a vigilância e filtragem, incluindo-se interceptação de comunicação, acesso a comunicações arquivadas, requerimentos quanto ao devido processo legal e outros processos legais relevantes, como parte da análise de risco sobre como as Tecnologias podem ser usadas – para o bem e para o mal. Por exemplo, em sua política de direitos humanos a Nokia Siemens diz que só proverá capacidades para a interceptação legal da rede (i.e. vigilância) que forem requeridas legalmente e "baseadas em padrões claros e em fundamentos transparentes na lei e na prática".

5. INFORMAÇÃO EXTERNA. Revisão dos relatórios de direitos humanos do Departamento de Estado dos EUA[32], de relatórios relevantes das Nações Unidas, e de outros relatórios plausíveis sobre o Governo, incluindo notícias ou outros relatos de fontes não governamentais ou de fontes locais que indiquem se o Governo utiliza recursos de vigilância para conduzir violações de direitos humanos.
Onde for possível, isso deve incluir a criação de um processo através do qual os indivíduos impactados pela Tecnologia e aqueles que fazem denúncias possam prover informação direta à empresa –, garantindo assim segurança àqueles que reportarem questões e um caminho para que a informação possa ser revisada e ações possam ser tomadas.

Abster-se de Participação: a Empresa não deve participar – ou continuar sua participação – em uma Transação, ou prover a Tecnologia, se for razoavelmente previsível que a Transação ou Tecnologia vai facilitar a violação de direitos humanos pelo Governo direta ou indiretamente, incluindo-se:

1. USO. A parte da Transação na qual a Empresa está envolvida ou a Tecnologia específica a ser provida inclui construção, customização, configuração ou integração em um sistema que é sabidamente usado para violações de direitos humanos, ou quando este uso for razoavelmente previsível .

2. USUÁRIO ESPECÍFICO. O setor do Governo que está envolvido na Transação ou que esteja supervisionando as Tecnologias tenha sido identificado como violador de direitos humanos usando ou baseando-se em Tecnologias similares, direta ou indiretamente.

3. HISTÓRICO GERAL DO GOVERNO.
O histórico geral do Governo na área de direitos humanos gera preocupações legítimas de que a Tecnologia ou Transação será utilizada para facilitar violações de direitos humanos.

4. AÇÕES DO GOVERNO. O Governo recusa-se a incorporar termos contratuais confirmando o uso

32. U.S. Department of State, Human Rights Reports, http://www.state.gov/j/drl/rls/hrrpt/ (acessado em 9 de fevereiro de 2012).

pretendido das Tecnologias, recusa-se a permitir a inspeção suficiente sobre seu uso ou dá sinais sobre a utilização – pretendida ou em curso – das Tecnologias para a violação de direitos humanos.

Definições-chave e escopo do processo: quem deve seguir estes passos? O escopo é, de fato, bem estreito – Empresas envolvidas em Transações para vender, alugar ou prover de qualquer outra forma Tecnologias a Governos, definidos como segue:

1. "Transação" inclui todas as vendas, *leasings*, aluguéis ou outros tipos de arranjo onde uma Empresa, em troca de qualquer tipo de pagamento ou outra recompensa, incluindo-se a possibilidade de operar naquele país, provê ou assiste no provimento de Tecnologias, recursos humanos ou apoio não tecnológico a um Governo. Isto também inclui o provimento de qualquer tipo de suporte tais como atualizações de software ou hardware, consultoria ou serviços similares.

2. "Tecnologias" inclui todos os sistemas, serviços, hardware, software, consultoria e suporte passíveis de serem utilizados para vigiar terceiros ou fazer filtragem, incluindo-se, mas não limitando-se, a tecnologias que interceptam comunicações, registram atividades do usuário e suas informações, farejam pacotes ou fazem inspeção profunda de pacotes, aparatos e sistemas de biometria, sistemas de votação e medidores de uso. "Tecnologias" inclui especificamente qualquer serviço, customização, apoio ao cliente e *paths* ou componentes para atualizações.

3. "Empresa" inclui subsidiárias, *joint ventures* (incluindo-se *joint ventures* diretamente com entidades governamentais), e outras estruturas corporativas nas quais a Empresa tem partes significativas ou controle operacional.

4. "Governo" inclui governos formais, reconhecidos, englobando também Estados membros das Nações Unidas. Também inclui entidades governantes ou com status de governo, como o Partido Comunista da China ou o Talibã – e outras entidades não governamentais que efetivamente exercem poderes de governo sobre um país ou parte de um país. Para estes propósitos, "Governo" inclui vendas indiretas através de um agente, contratante ou outro intermediário (ou múltiplos intermediários) se a Empresa está ciente ou devesse saber que o receptador final, usuário ou beneficiário da Tecnologia é um Governo. A *Export Administration Regulations*[33] (EAR) e a FCPA[34] podem prover orientação mais específica sobre estas determinações.

33. Bureau of Industry and Security U.S. Department of Commerce, Export Administration Regulations, http://www.bis.doc.gov/policiesandregulations/index.htm#ear. 34. Electronic Code of Federal Regulations, Title 15: Commerce and Foreign Trade, http://ecfr.gpoaccess.gov/cgi/t/text/text idx?c=ecfr&sid=b598042103e95c10c396b0140e0620b7&rgn=div9&view=text&node=15:2.1.3.4.21.0.1.7.22&idno=15

> Nenhuma empresa razoável, e certamente nenhuma no Vale do Silício, quer ser conhecida como uma empresa que ajuda a facilitar violações de direitos humanos.

Este arcabouço, evidentemente, não é a única opção razoável para abordar o problema. Se levarmos em conta os passos que estas grandes empresas que competem nestes mercados já precisam dar – sob leis de exportação, o *Foreign Corrupt Practices Act*, entre outras – esta é uma inclusão relativamente pequena. Mesmo que algumas pessoas possam argumentar que pressionar empresas tecnológicas norte-americanas e as multinacionais sobre as quais os EUA têm jurisdição para que tenham sólidos programas de direitos humanos dará uma vantagem competitiva a empresas que não têm tal programa, o mesmo é verdade no que diz respeito às leis anti-suborno. Se podemos esperar que estas grandes empresas não façam negócios através de subornos – mesmo que algumas de suas concorrentes o façam – , também é razoável pedir que elas não façam negócios que resultem no favorecimento da repressão.

:: CONCLUSÃO

Nenhuma empresa razoável, e certamente nenhuma no Vale do Silício, quer ser conhecida como uma empresa que ajuda a facilitar violações de direitos humanos. Há numerosas maneiras pelas quais as empresas podem assegurar que as ramificações dos direitos humanos sejam consideradas em suas decisões de negócios. Enquanto a EFF defende a adoção de um marco que primeiramente garanta transparência e depois coloque o foco da tomada de decisões na abordagem "conheça seu cliente", pode haver outras formas de assegurar que empresas assumam responsabilidade pelos usos que governos fazem de suas tecnologias. Quaisquer que sejam os passos que elas deem, com ou sem a pressão de legisladores e reguladores, é hora de as empresas de tecnologia adotarem medidas reais para assegurar que não sirvam como "pequenos ajudantes da repressão". ●

Este artigo foi originalmente publicado pela EFF em: https://www.eff.org/node/70462

> **Demi Getschko** Diretor Presidente do NIC.br

> **Frederico A.C. Neves** Diretor de Serviços e de Tecnologia do NIC.br

WHOIS, Conceitos e perspectivas

:: PREÂMBULO

Quando é contratado um nome de domínio qualquer, seja sob um domínio de país (".br", ".de" etc) ou sob um domínio genérico (".com", ".info" etc), a entidade registradora insere informações cadastrais do contratante do domínio em uma base de dados pública na Internet, conhecida como WHOIS.

Por exemplo, uma consulta à base de dados WHOIS do nome de domínio "bb.b.br" apresenta o seguinte resultado:

- domain: bb.b.br
- owner: BANCO DO BRASIL S.A.
- ownerid: 000.000.000/0001-91
- responsible: Larissa da Silva Novais Vieira
- country: BR
- owner-c: BABRA22
- admin-c: BABRA22
- tech-c: JOGOM30
- billing-c: BABRA22

- nserver: dns1.bb.com.br
- nsstat: 20120512 AA
- nslastaa: 20120512
- nserver: dns2.bb.com.br
- nsstat: 20120512 AA
- nslastaa: 20120512
- dsrecord: 37018 RSA/SHA-1 E1CFDEF1AE C5235D6AD9F0AF731535FB4D2F555D
- dsstatus: 20120510 DSOK
- dslastok: 20120510
- created: 20090107 #5165498
- expires: 20140107
- changed: 20111125
- status: published

- nic-hdl-br: BABRA22
- person: Banco do Brasil
- e-mail: webmaster@bb.com.br
- created: 20110915
- changed: 20120207

- nic-hdl-br: JOGOM30
- person: Joaquin Gomide
- e-mail: jgomide@bb.com.br
- created: 20090616
- changed: 20090616

A consulta pode ser feita, para qualquer nome de domínio, através de um simples programa de consulta disponível para qualquer sistema (Windows, MacOS, Linux, Android, iOS etc), ou através de serviços de consulta na Internet[1].

Em dezembro de 2011 a equipe de revisão do serviço WHOIS da ICANN[2] publicou um relatório[3] mostrando que uma porcentagem significativa de pessoas ou organizações que registram nomes de domínio não conhecem o serviço WHOIS ou não sabem quais dados são divulgados publicamente. O serviço, assim, é parte relevante das discussões sobre direitos e deveres na rede, preservação da autonomia e abrangência da Internet, bem como formas de proteger a liberdade e a privacidade dos internautas. Tanto a qualidade necessária dos dados, quanto as caracteristicas e as informações que devem constar dele e a forma de tornar disponíveis essas informações são tópicos dessa discussão.

:: BREVE HISTÓRICO

A primeira especificação técnica do WHOIS é anterior à disseminação maciça do protocolo TCP/IP que caracteriza a Internet. Seu objetivo, desde o início, foi servir como uma base de dados muito simples para identificar os responsáveis por cada um dos "nós" ligados à rede, "nós" que podiam enviar

1. Exemplo de um serviço gratuito de consulta WHOIS: http://ipduh.com 2. A ICANN (Internet Corporation for Assigned Names and Numbers) coordena mundialmente a designação de nomes de domínio de primeiro nível: http://www.icann.org 3. Ver: http://www.icann.org/en/reviews/affirmation/whois-rt-draft-final-report-05dec11-en.pdf 4. Ver: http://tools.ietf.org/html/rfc812 5. SRI-NIC Stanford Research International - Network Information Center. Nesta época o SRI prestava o serviço de centro de informações da ARPANET para a DCA (Defense Communications Agency).

e receber informações. Saber quem opera algum nó e como se poderia entrar em contato com este operador era vital para que uma rede em intensa fase de crescimento mantivesse estabilidade. Quando alguém indentificava algum problema relacionado a algum computador ligado à rede, era pelo WHOIS que poderia localizar o responsável e, assim, fazer com que a situação eventual de erro se normalizasse.

O que este primeiro documento de especificação, a RFC 812 (março de 1982)[4], descrevia era um serviço de "diretório", então fornecido pelo SRI-NIC[5], e que continha dados de contato. A RFC sugeria que as consultas a esse diretório utilizassem programa de computador fornecido pelo próprio SRI-NIC.

Lembremos que à época não havia ainda a estrutura hierárquica de nomes, que o DNS[6] implementou em 1983. A tabela de "nós" da rede era uma listagem simples, um rol de nomes de máquinas. Certamente essa relação não suportaria o crescimento vertiginoso da rede anos depois e teria que ser substituída.
Com a implantação do DNS hierárquico em novembro de 1983[7], na forma que conhecemos hoje, com a formalização da estrutura de nomes de domínio e a definição do processo em outubro de 1984[8], o SRI-NIC estendeu o serviço WHOIS – que também passou a fornecer informações sobre os dados de contato dos que registravam nomes de domínio no novo sistema de DNS. Afinal um nome de domínio registrado pressupunha que uma nova máquina, com suas idiossincrasias, estaria entrando na rede.

Entre 1992 e 1996 um grupo de trabalho da *Internet Engineering Task Force* (IETF[9]), motivado em boa parte pelos resultados obtidos pelos criadores do protocolo de indexação de servidores FTP (Archie)[10], trabalhou para tentar melhorar o serviço de WHOIS propondo extensões ao protocolo original (WHOIS++). Infelizmente o escopo muito amplo e a complexidade acabaram por prejudicar sua adoção.

Nos já quase vinte anos da Internet comercial outras duas tentativas na IETF tentaram aperfeiçoar o WHOIS, visando incluir características desejáveis – como suporte a descoberta de servidores, internacionalização dos dados armazenados (originalmente apenas em caracteres latinos sem diacríticos, formato conhecido como ASCII) e a codificação de perguntas e respostas de maneira padrão.

Entre 1997 e 1998 houve uma nova tentativa na IETF[11] de retrabalho da especificação do protocolo RWHOIS[12] que lançava mão do modelo hierárquico usado no sistema de nomes de domínios, adicionado aos conceitos do serviço padrão de diretório OSI/ISO X.500[13], e com a semântica largamente influenciada pelo protocolo de envio de mensagens de e-mail

6. Sistema de Nomes de Domínio, que permite localizar máquinas e serviços na Internet a partir de nomes em vez dos números IP. Ver: http://pt.wikipedia.org/wiki/Domain_Name_System 7. Ver: http://tools.ietf.org/html/rfc882 8.Ver: http://tools.ietf.org/html/rfc920 9.Internet Engineering Task Force. Ver: http://www.ietf.org/wg/concluded/wnils.html 10. File Transfer Protocol, protocolo de cópia de arquivos entre computadores em rede. Ver: http://en.wikipedia.org/wiki/Archie_search_engine 11.Ver: http://www.ietf.org/wg/concluded/rwhois.html 12. Ver: http://tools.ietf.org/html/rfc2167

> apesar da idade e do histórico de tentativas de substituição, este serviço, essencial para a operação e segurança da rede, continuará a ser prestado pelo nosso velho e remendado WHOIS por alguns bons anos

SMTP[14]. Apesar de toda sua arquitetura distribuída, sua implementação e uso acabou sendo limitada a quem, na época, operava o serviço comercial de diretório para o InterNIC[15]: a empresa Network Solutions.

Outro grupo de trabalho na IETF[16] especificou uma linguagem para políticas de roteamento, RPSL[17], que era ampla o suficiente para também cobrir serviços de registros de nomes. Esta linguagem acabou sendo adotada como extensão para o serviço WHOIS na representação dos dados por vários dos registros de endereços e registros de nomes de domínio. O ".br" foi um dos que adotou o RPSL em 1998.

Com a falta de um padrão amplamente adotado, extensões específicas e de fabricantes acabaram por proliferar em outros registros, complicando o cenário global.

Entre 2001 e 2008 a IETF, com o grupo de trabalho CRISP[18], produziu uma especificação que pretendia unificar o serviço. Apesar de melhor e mais completo, sua complexidade e as dificuldades que surgiram pela necessidade da distribuição de novos programas de consulta para a comunidade de usuários acabaram por protelar sua disseminação. Entretanto, suas ideias progrediram[19], apoiadas em um trabalho dos registros regionais de endereços[20], que procuraram consolidar os requisitos do CRISP, mas com um foco em uma implementação mais simples e que não requeresse a distribuição de novos programas para a utilização do serviço.

Assim, apesar da idade e do histórico de tentativas de substituição, este serviço, essencial para a operação e segurança da rede, continuará a ser prestado pelo nosso velho e remendado WHOIS por

13. Ver: http://pt.wikipedia.org/wiki/X.500 14. Ver: http://pt.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol 15. Ver: http://pt.wikipedia.org/wiki/InterNIC
16. Ver: http://www.ietf.org/wg/concluded/rps.html 17. Ver: http://tools.ietf.org/html/rfc2280 18. Ver: http://www.ietf.org/wg/concluded/crisp.html
19. Ver: http://www.ietf.org/mail-archive/web/weirds/current/msg00884.html 20. Ver: http://tools.ietf.org/html/draft-newton-weirds-arin-whoisrws-00

alguns bons anos, antes de ser substituído por um protocolo que atenda às demandas de tão diversos usos que hoje são esperados dele.

:: A DISCUSSÃO

Não se pretende aqui esgotar o tema, mas apenas levantar os pontos principais que, a nosso ver, deveriam balizar este debate. O primeiro ponto a se observar é que a Internet sempre tratou seus partícipes como dignos de crédito. Na Internet a maioria das informações são "declarativas". Ou seja, eu informo o que quero sobre mim e, *a priori*, essa informação é aceita como verdadeira até que alguém duvide dela. A presunção é, sempre, de boa fé.

A extensão disso ao WHOIS é que, pelos costumes da rede, o que o detentor do domínio declara é o que deve ser considerado verdadeiro até prova em contrário. O WHOIS representaria a "melhor tentativa" de catalogar os operadores de domínios na Internet. Querer dele mais que isso é avançar em terreno desconhecido e possivelmente hostil à rede.

A segunda observação, decorrente da anterior, é que os dados mínimos de identificação unívoca do responsável pelo nome de domínio registrado devem ser visíveis a toda a rede. É a forma de fazer valer a "boa fé" do primeiro ponto. Ou seja, a rede se protege contra fraudes e falsidades expondo a todos o que se sabe dos detentores de cada domínio. Se a declaração de um deles for obviamente falsa, alguém poderá pedir a correção. Este também é o argumento fundamental para que o acesso seja universal e uniforme. A criação de "privilégios" de acesso à base apenas coloca em risco e torna vulneráveis os usuários da rede, criando categorias "especiais" que podem "ver" mais que outras.

É claro que a maneira uniforme e transparente com que a rede funciona sempre gera oportunidades para aqueles que desejam aproveitar-se disso para o mal. Um exemplo claro é usar a base do WHOIS para simplesmente colecionar endereços de correio eletrônico, visando à formação de listas para spam. No entanto, um mau uso de um serviço nunca deve tolher seu uso adequado (*abusus non tollit usum*...). Assim, trata-se de impedir, por exemplo, excesso de acessos partindo de uma única origem, e impedir o acesso maciço às informações (*bulk acess*) a quem quer que seja.

Finalmente, resta destacar que o uso de WHOIS em registros de país[21] e seu uso em registros genéricos pode ter grandes disparidades. É muito difícil estabelecer um identificador unívoco global, e é razoavelmente simples identificar unicamente pessoas físicas ou jurídicas dentro de um país. Por outro lado, a diversidade linguística coloca barreiras bastante difíceis de transpor quando falamos de uma base de dados que terá informações sobre detentores de domínios de todas as partes do mundo e em diversos alfabetos. ●

21. Conhecidos como *ccTLDs* (Country Code Top Level Domains).

> **Eleanor Saitta** é hacker e designer, co-fundadora do projeto Trike, e do Constitutional Analysis Support Team (CAST)

Redes e estados-nação

O século 20 foi um século de instituições e de centralização do poder. Esta centralização foi impulsionada inicialmente pelo capital industrial e, em seguida, pelo capital financeiro e da indústria cultural. Agora nós estamos assistindo à mudança para um capitalismo da sociabilidade, que ao mesmo tempo é ativado por e requer novas estruturas de organização para a sua exploração. Como sempre, a agonia do velho é mais visível do que os passos hesitantes do novo; a crise do capital financeirizado do qual nós viemos a depender tem prioridade nos meios de comunicação - que também estão morrendo.

Neste buraco, novas estruturas estão nascendo. Muitas delas se parecem com empresas tradicionais – como o Facebook, tentando afetar o capitalismo da sociabilidade inteiramente dentro do modelo de uma estrutura corporativa tradicional, tentando criar capital de rede e ao mesmo tempo mantendo o controle institucional. Este controle institucional é endêmico na governança do Estado contemporâneo, onde nos deparamos com uma paisagem de quase total captura regulatória. O Estado, é claro, está tentando tanto adaptar-se às mudanças, quanto usá-las para consolidar o seu controle – enquanto

> se algo que nós reconheceríamos como "civilização" sobreviver a este século, será necessária uma redistribuição dramática de riqueza, uma igualdade social radical e global. Este não será um século lucrativo.

lida com as rupturas do sistema financeiro do qual também vem dependendo. Os ricos que foram bem sucedidos em capturar o Estado estão usando este momento para tentar garantir que aqueles que estão melhor colocados na velha economia sejam mais capazes de operar a nova economia, taticamente devolvendo ao Estado a responsabilidade pelas necessidades básicas, sem devolver recursos ou autoridade.

Isso tudo está acontecendo numa tentativa de moldar o que será uma futura rede estruturada, de forma a criar lugar para o controle nestas redes, para assegurar que nem todos ali sejam iguais.

Esta, no entanto, não é a história do século 21. Este será um detalhe considerável, mas ainda assim apenas uma detalhe, daquilo que só podemos descrever como um genocídio evitável.

Todas estas estruturas organizacionais, os estados, capitais, redes, consumo etc., são construídos sobre uma base de recursos fundamentalmente insustentável. Entendemos os problemas e a magnitude dos problemas, e temos feito isso, em termos cada vez mais refinados, pelo menos há 40 anos.

Nós não agimos - e é claro que, enquanto os sistemas existentes de controle forem incapazes de agir, nós também não o faremos.

Os remanescentes do Estado existem apenas para ratificar os desejos das corporações e para exercer o controle social; este Estado que está aí não vai agir. Nós precisamos de uma mudança fundamental na sociedade rumo à simplicidade - e ao mesmo tempo em que haverá muitas novas oportunidades técnicas, muitos novos desafios ao

1. Ver sobre o CAST – Constitutional Analysis Support Team em http://const.is/

longo do caminho, se algo que nós reconheceríamos como "civilização" sobreviver a este século, será necessária uma redistribuição dramática de riqueza, uma igualdade social radical e global. Este não será um século lucrativo.

Em algum momento esta verdade será inevitável, mesmo para as atuais estruturas de controle - mas aí já será tarde demais. Com a mudança de uma sociedade centrada em instituições para uma sociedade centrada em redes, temos um momento em que podemos ser capazes de tomar uma decisão diferente, tomar um caminho diferente, pois as ferramentas de controle foram momentaneamente pegas com as calças na mão.

Dois projetos nos quais estou envolvida estão operando, em níveis muito diferentes, para ajudar a afetar essa mudança.

A Equipe de Apoio à Análise Constitucional (CAST, na sigla em inglês[1]) é uma organização que surgiu na Islândia em outubro de 2010, num momento em que o processo constitucional naquele país começou a ganhar força. Smari McCarthy e eu, que somos a equipe central da CAST, trabalhamos com países que estão se reinventando - seja após um momento de reforma fundamental, ou depois de uma revolução. Existem dois grandes eixos no nosso trabalho. Primeiro, tomamos a afirmação de Lessig de que o "código é lei" e a levamos um passo adiante, tratando a lei como código. Uma Constituição, como um corpo autônomo de normas legais, pode ser analisada em busca de falhas exatamente da mesma maneira que pode ser feito com um sistema de computador. Embora a lei, constituída pela complexa semiótica humana, seja mais do que apenas um código, muitas questões como decidibilidade, complexidade Booleana, variáveis indefinidas, e lógica predicativa podem ser tratadas de forma idêntica a qualquer pedaço de código. Nós damos um passo adiante e executamos tanto a modelagem de ameaças formais e a análise situacional informal do documento, interagindo (idealmente) com a Assembleia Constituinte ao longo de todo o processo e registrando falhas conforme as encontramos.

O outro eixo do nosso trabalho envolve a interação direta do público com o processo constitucional. Na Islândia, o Facebook (junto com uma ferramenta de fórum online) foi usado para que todos os islandeses e islandesas pudessem comentar sobre o esboço do novo texto constitucional. Milhares de observações foram recebidas e respondidas, e na maioria dos casos, foram abordadas diretamente pela Assembleia Constituinte.

Temos acompanhado e contribuído para a discussão sobre Democracia Líquida durante algum tempo, e estamos ansiosas para trazer soluções mais abertas e um engajamento mais profundo em processos constitucionais no futuro e, ao mesmo tempo, preencher a lacuna entre os mais fortemente conectados e os menos conectados.

Este processo, que poderíamos chamar, em sua implementação plena, de um *crowdsourcing* do Direito (que, apresso-me a acrescentar, não é exatamente como eu chamaria o que aconteceu na Islândia), tem o potencial de minar dramaticamente a estrutura hierárquica de controle que o Estado impõe sobre a governança de uma nação, na sua ponta da negociação social que é a criação do Estado de Direito. Embora eu não esteja recomendando que apenas tentemos fazer essa transição em nível constitucional, este é um nível que permite uma dimensão de engajamento muito fundamental.

O outro projeto que eu quero abordar fala muito mais diretamente ao controle social no dia a dia. O Sukey é uma ferramenta de nivelamento para ativistas que interagem com forças policiais globais cada vez mais militarizadas. Sukey veio dos protestos estudantis em Londres, após o cerco policial à manifestação da ponte Westminster. Sua primeira implementação foi um simples *mashup* de mapas do Google, mais tarde substituída por uma instância Ushahidi[2]. O Sukey permite que indivíduos num determinado território geográfico enviem relatórios sobre o local onde os policiais estão, onde estão sendo formadas manifestações e onde ações de brutalidade policial estão acontecendo. Os relatórios são analisados por uma equipe que correlaciona e geolocaliza as informações, disseminando as principais notícias através de um canal geral e colocando informações táticas mais detalhadas em um mapa que pode ser visualizado por qualquer pessoa.

Obviamente, a polícia é capaz de ver essas informações, mas como ela, em teoria, já sabe o que está fazendo, isso não lhe diz muito. Tanto a abertura quanto as limitações de ter uma única equipe de análise - que pode ser infiltrada - e um único conjunto de servidores centrais - que podem ser apreendidos - são obviamente problemas estruturais e estratégicos do sistema. O Sukey versão dois vai ser construído em cima de Briar[3], e passará a ser um sistema completamente descentralizado, com a possibilidade de anonimização mais segura, podendo contar com tantas equipes de análise quantas desejarem fazer este trabalho (que podem ser confiáveis sem serem totalmente conhecidas), e sem nenhum servidor, onde quer que seja, para ser apreendido.

Embora a tecnologia seja inútil na ausência de pessoas que a usem, as estruturas de controle do Estado também são tão tecnológicas quanto são performativas. O Sukey pretende desenvolver-se como o equivalente funcional do "*Future Combat System Common Operating Picture*" do Departamento de Defesa dos EUA, mas funcionando da maneira como nós fazemos, no formato de rede.

No final, se realmente mantivermos viva a civilização, as redes vão vencer. Ilegíveis entidades meméticas em forma de rede como o Anonymous

2. Ushahidi é uma plataforma em software livre usada para coletar informações de múltiplos canais e apresentá-la visualmente, especialmente em mapas. Ver http://www.ushahidi.com 3. Briar é um sistema para comunicações seguras: http://briar.sourceforge.net/

desafiarão o poder de qualquer nação do planeta, embora talvez tenhamos que travar uma guerra contra o fascismo global em rede para chegar lá.

Embora este seja, de certa forma, um cenário esperançoso, ele também deve ser algo aterrorizante. Nenhum de nós é tão cruel quanto todos nós.

Além disso, onde é que vão parar a misericórdia humana, a discrição e a decência, em um futuro executado por um protocolotariado? Quando construímos redes sociais, cidades inteligentes, e os aplicativos da vida quotidiana, estamos construindo as regras que determinam como nós permitimos que as pessoas vivam. Os computadores são muito ruins em entender outra coisa senão uma visão muito rígida da "justiça"; são muito ruins em entender um estado de graça. Computadores, apesar dos nossos esforços, são horríveis em compreender a complexidade das relações humanas - a maioria das redes sociais que foram bem sucedidas utilizam definições muito simples de conectividade, adequadas à sua comunidade, e nós nos adaptamos elas, porque as nossas máquinas são estúpidas demais para nos conhecer realmente.

Se construímos uma rede, as nossas máquinas podem não precisar nos conhecer, mas, se o futuro tiver que ser humano, as regras dos negócios que construirmos devem ser humanas. Como podemos programar com clemência, sem simplesmente digitalizar o nepotismo? Apelo àqueles de vocês que desenvolvem sistemas como este para que respondam a este chamado.

Quando construímos redes sociais, cidades inteligentes, e os aplicativos da vida quotidiana, estamos construindo as regras que determinam como nós permitimos que as pessoas vivam.

Se a humanidade das aplicações fala aos meios de vida, como respondemos à outra função do Estado contemporâneo, o controle social? Se entidades como o Anonymous tornarem-se os atores dominantes do próximo século, capazes de desafiar o Estado à vontade (se este ainda existir), para onde vai a jurisprudência? Os direitos fundamentais? Como é que uma entidade como o Anonymous decide como sanções sociais podem e devem ser aplicadas?

Eu não tenho todas as respostas aqui, mas estou muito interessada em continuar o diálogo sobre o assunto. ●

Este texto foi traduzido a partir da transcrição da palestra de Eleanor Saitta proferida na conferência Unlike Us #2 em março de 2012. O vídeo da palestra está em http://vimeo.com/39258895

Políticas de uso de ferramentas Web 2.0 pela Administração Pública na América Latina

o caso do Brasil: Gabinete Digital do Governo do Rio Grande do Sul[1]

A iniciativa do Gabinete Digital do Governo do Estado do Rio Grande do Sul é recente. Foi lançada em 24 de maio de 2011, sob a coordenação direta do gabinete do governador Tarso Genro, gerando um espaço digital[2] "dedicado à comunicação direta do governador com a população" onde são feitas perguntas que são submetidas a uma votação; a pergunta mais votada é respondida por Genro em um vídeo. Além disso, nesse espaço incentiva-se a divulgação, nas redes sociais, de consultas feitas pela população.

Nesse sentido, seu objetivo é "estimular uma nova cultura de gestão pública por meio do estabelecimento de canais de diálogo e de colaboração com a sociedade a partir da utilização de ferramentas digitais". Dessa forma, o projeto é definido como um organismo articulador da cultura e governança digitais[3].

1. Este texto é uma versão editada e adaptada pelo Instituto Nupef a partir do estudo *Políticas de uso de ferramentas Web 2.0 pela Admnistração Pública na América Latina - o caso do Brasil: Gabinete Digital do Governo do Rio Grande do Sul*. O estudo de caso sobre o Brasil é uma parte de uma pesquisa regional realizada no âmbito do projeto Impacto 2.0 da Fundación Comunica, patrocinado pelo Centro Internacional de Pesquisas para o Desenvolvimento (IDRC), com a participação da Associação para o Progresso das Comunicações (APC). Veja mais sobre este projeto em http://impacto2.comunica.org/ 2. http://www.gabinetedigital.rs.gov.br/ 3. Informação obtida da seção "O que é o Gabinete Digital", disponível em http://www.gabinetedigital.rs.gov.br/conteudo.php?cod_menu=57. Acessada em 6 de outubro de 2011.

O projeto tem três componentes:

1. **O Governador Responde**, onde os usuários registrados no sítio Web podem enviar perguntas para a autoridade máxima do Governo do Rio Grande do Sul e votar em perguntas submetidas por outros internautas. Uma vez por mês, o governador Genro responde àquela que obteve mais votos a seu favor.

2. **O Governador Escuta**, que são audiências públicas presenciais nas quais o governador ouve os cidadãos e cidadãs a respeito de determinadas questões. As audiências são também transmitidas pela Internet e os internautas podem enviar perguntas, que são analisadas pelo governador.

3. **Agenda Colaborativa**, que visa ajudar na elaboração da agenda do governador e de seus secretários. As pessoas podem enviar sugestões de lugares onde o governo deveria estar presente para ouvir as demandas locais. Existe particularmente o objetivo de priorizar as cidades e regiões povoadas do interior do estado.

Essa é uma iniciativa de formato pioneiro no Brasil. Embora outras iniciativas de participação da população por meio da Internet e de ferramentas interativas - como consultas populares e reuniões participativas digitais - tenham sido implementadas

no país para permitir o encaminhamento direto de demandas populares que exigem resposta do Poder Executivo, no caso do Gabinete Digital o Governo do Rio Grande do Sul apresenta suas propostas para avaliação e aprovação da população por meio de ferramentas Web 2.0.

Ao mesmo tempo, abre-se um amplo espaço para o envio de sugestões e perguntas não limitadas a uma lista fixa de opções. De fato, nas audiências de "O Governador Escuta", qualquer cidadão pode encaminhar perguntas de qualquer natureza.

Todos os conteúdos do sítio Web do Gabinete Digital do Governo do Rio Grande do Sul estão licenciados na forma de *Creative Commons* e toda a tecnologia utilizada é baseada em software livre.

No portal do Governo Digital, os cidadãos podem participar, comentar e compartilhar informações em três redes sociais: Twitter (com 1.642 seguidores em 10 de outubro de 2011), Facebook (726 seguidores em 10 de outubro de 2011) e Identi.ca. Essa última é uma rede social e um microblog desenvolvido em software livre. Além disso, há um canal RSS para quem quer receber notícias sobre o projeto.

:: DIAGNÓSTICO DO USO DAS TICS NA ENTIDADE [4]

As ferramentas Web 2.0 (Twitter, Facebook e Identi.ca) do Gabinete Digital do Governo do Rio Grande do Sul são importantes para a interiorização do governo do estado, que está contemplada no componente "Agenda Colaborativa". Antes de o governador Genro partir de Porto Alegre, capital do estado, para um município do interior - onde irá divulgar as políticas para esse local e receber as opiniões da população -, a equipe do projeto entra em contato com os cidadãos por meio das contas de redes sociais, explica Everton Rodrigues, do setor de Gestão de Mobilização do Gabinete Digital do Governo do Rio Grande do Sul: "Procuramos pessoas no Facebook, no Twitter. Iniciamos um diálogo usando as redes sociais e começamos a informar as pessoas da região em questão. Isso tudo é feito por nós. As pessoas então começam a enviar propostas - e nós vamos avaliando estas propostas à medida que vão chegando. Em geral não levamos mais que cinco horas para aprovar uma proposta."

Quem são estas pessoas e de que maneira usam estas contas de redes sociais? O acesso às redes sociais dentro desta entidade pública é universal ou restrito? Estas são algumas das 22 perguntas que compuseram a pesquisa realizada para esta investigação, respondidas por 15 funcionários do Governo do Rio Grande do Sul.

Ao serem indagados sobre o conhecimento de ferramentas web 2.0, todos os entrevistados identificaram tanto a Internet como a intranet como espaços de interação. Esse resultado homogêneo pode ser devido ao fato de que faz parte da estratégia da administração à frente do Governo do Rio Grande do Sul desenvolver ferramentas próprias e conectá-las às redes sociais existentes[5].

Um exemplo de ferramenta desenvolvida pela nova administração é a "Audiência Pública Digital", parte do componente "O Governador Escuta" - na qual o governador conversa com as pessoas presentes e ouve especialistas num determinado assunto, e pessoas de qualquer parte do estado podem acompanhar e fazer comentários pela Internet.

Outra ferramenta própria é o componente "O Governador Responde", por meio do qual a autoridade máxima do Governo do Rio Grande

4. Para a elaboração deste relatório foram utilizadas informações obtidas atravésde 15 pesquisas e quatro entrevistas. As entrevistas foram realizadas com representantes do governo, da sociedade civil e do meio acadêmico. 5. Entrevista com Everton Rodrigues, do setor de Gestão de Mobilização do Gabinete Digital do Governo do Rio Grande do Sul.

do Sul responde mensalmente à pergunta mais votada entre as questões enviadas pelos cidadãos, como mencionado anteriormente. Nesse processo, há uma campanha em torno da votação digital[6].

Sobre as atividades em torno das ferramentas próprias, Everton Rodrigues explica que a entidade pública pretende guardar o histórico desse processo entre o governo estadual e os cidadãos. Para isso, as ferramentas que foram desenvolvidas armazenam as conversas realizadas através dos aplicativos Web 2.0 "para que o próprio cidadão possa fiscalizar este diálogo (...). Temos a preocupação de ter as ferramentas sob nosso controle, para que essa memória seja guardada".

Segundo os acadêmicos ouvidos na pesquisa, o uso de ferramentas Web 2.0 e de ferramentas próprias no Governo do Rio Grande do Sul é considerado positivo em comparação com outros governos estaduais no Brasil, embora a utilização de aplicativos 2.0 seja usada de forma mais informativa do que interativa ou colaborativa - tanto no caso da entidade analisada, quanto nos demais órgãos da administração pública do Brasil. Sobre este cenário, Ana Cláudia Farranha, professora da Universidade de Brasília (UnB), reflete: "Você abre o Twitter e consegue saber tudo o que está acontecendo na administração pública federal brasileira. É possível saber onde está acontecendo um seminário, onde foi lançado um estudo, o que um determinado órgão do governo está pesquisando, ou ainda o que o Ministério do Desenvolvimento Agrário está fazendo na Bahia. Qualquer cidadão acessa o blog da Presidenta, consegue informação. O problema é que o acesso pode significar apenas isso: informação.(...) Isso está muito relacionado à questão da reforma gerencial dos anos 90. Todo o mundo adotou a ideia do portal eletrônico. No portal se mostra o governo; mas é só isso. É muito mais informação que interatividade."

Do ponto de vista de Celso Schröder, diretor da Federação Nacional dos Jornalistas, o uso da Internet é um elemento inovador na administração pública brasileira, cujo potencial ainda não foi totalmente explorado. Nesse sentido, afirma: "[A Internet] aparece como uma grande novidade e como uma ferramenta, digamos, política para os governos. Todos os governos se propuseram a usá-la, mas ainda me parece que ela está longe de ser uma ferramenta cotidiana, efetiva e eficiente, incorporada à rotina dos governos."

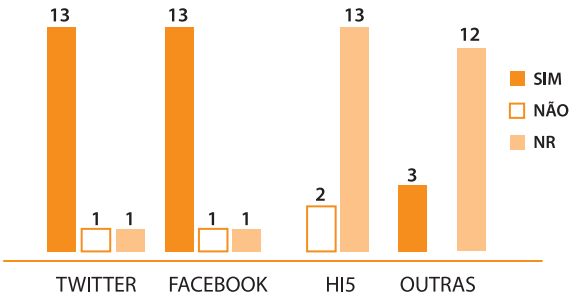
:: ACESSO, USOS E CONTEÚDOS

Como mostrado no gráfico a seguir, as redes sociais são bastante utilizadas pelos funcionários do governo do Rio Grande do Sul. Seu uso é feito para receber conteúdos; 93,3% as utilizam dessa forma. A busca ativa por informações é o objetivo de uso

6. Seguindo o mesmo princípio do componente "O Governador Responde", o Departamento de Planejamento do Gabinete Digital realizou um processo de votação para os projetos de 2012, por meio do qual as pessoas das regiões do Conselho Regional de Desenvolvimento votaram nos 10 projetos mais indicados e selecionados em reuniões presenciais. Mais de um milhão de pessoas votaram em até quatro projetos para a sua região, sendo que 130.000 o fizeram pela Internet.

de cerca de 80% dos funcionários. A produção de conteúdos, a colaboração envolvendo conteúdos e a conexão e colaboração com outras pessoas são realizadas por 86,6% dos entrevistados.

Acesso a contas de rede social no ambiente de trabalho



*Total de 15 pessoas entrevistadas

> o uso da Internet é um elemento inovador na administração pública brasileira, cujo potencial ainda não foi totalmente explorado.

Outra questão apresentada na pesquisa foi em relação aos conteúdos e, especificamente, ao conhecimento da frequência com que estes são atualizados pela equipe do governo. Os resultados mostram que as 100% dos funcionários entrevistados conhecem a frequência com que os conteúdos são renovados e informam que é diária.

Para Celso Schröder, a atualização de conteúdos é uma atividade que gera obrigações para com a população por parte do Governo do Rio Grande do Sul, e também por parte da administração pública brasileira em geral. Nesse sentido, Schröder afirma que "não há dúvida de que o uso de ferramentas tecnológicas oferece uma poderosa capacidade de comunicação com o público, mas, por outro lado, cria uma exigência enorme de respostas imediatas e de compromissos. (...) Acho que isso impõe uma nova realidade para o Estado."

:: POLÍTICAS E NORMAS INTERNAS DO GOVERNO

Após a obtenção de referência quanto a formas de uso, conhecimentos e acesso às ferramentas Web 2.0 pelo Gabinete Digital do Governo do Rio Grande do Sul, perguntou-se sobre normas internas e sobre a existência de disposições institucionais para o uso da Internet e de seus aplicativos interativos e colaborativos.

Neste aspecto, 80% dos funcionários entrevistados disseram que conheciam o assunto.

Nas especificações sobre as políticas adotadas, foram elencadas várias iniciativas - que vão desde a política de participação, de transparência e de democratização da informação implementadas por meio do Gabinete Digital do Governo do Rio Grande do Sul, até o desenvolvimento da política Gestão 2, que busca incentivar os funcionários do governo a utilizar a Internet como ferramenta de gestão.

> a atualização de conteúdos é uma atividade que gera obrigações do Governo do Rio Grande do Sul, e em geral da administração pública brasileira, para com a população.

É muito ilustrativo que os próprios funcionários desejem que estas políticas melhorem as ações do Governo do Rio Grande do Sul por meio da rede, e existe uma expectativa de legislação específica sobre a governança e a cultura digital. Sobre esse propósito institucional, Everton Rodrigues assinala que no Governo do Estado do Rio Grande do Sul "não existe ainda um regulamento, uma carta de princípios", mas "está sendo planejada uma ampla conversa sobre o tema com os funcionários públicos interessados na utilização da Internet" em todos os níveis.

Quanto às restrições a usos identificadas pelos entrevistados, menciona-se a proibição de acesso a conteúdos pornográficos e considerados inadequados – e alguns departamentos ainda limitam o uso das redes sociais. Por outro lado, a entrevista com Rodrigues evidencia que também existem limitações técnicas – o que faz com que um grupo de funcionários do governo estadual ainda não tenha correio eletrônico institucional ou não faça uso do mesmo, o que representa um problema de contato direto entre o Estado e os funcionários públicos.

"Em principio, todo mundo tem [acesso à Internet]. Mas ainda existe uma defasagem no número de equipamentos disponíveis. Então, todos os equipamentos existentes estão sendo utilizados e a maioria dos funcionários tem acesso a um computador, mas sabe-se que 20% deles

não têm uma conta de e-mail institucional ou, às vezes, têm uma conta de e-mail sobre a qual não são informados - e por isso acabam utilizando seu e-mail pessoal."

Na análise das respostas sobre este tema, observa-se que há uma preocupação muito grande com a governança das TICs, especialmente com os ativos de aquisição (hardware e software) e a regulação do uso das redes sociais.

De um modo geral fica claro que para os funcionários do governo a Internet pode ser usada como instrumento para um trabalho mais eficaz e cuja utilização é segura. Também fica clara a percepção de que as políticas internas são necessárias, mas que não se deve limitar a liberdade de expressão ou restringir o acesso de funcionários a conteúdos. A pesquisa mostrou que todos os funcionários ouvidos disseram ter conhecimento sobre alguma política ou disposição institucional que restringe o uso da Internet de alguma forma. Na verdade, 66,7% dos entrevistados afirmaram que estas medidas de fato têm efeitos. Sobre esse assunto, foram registradas opiniões que atribuem algumas restrições de acesso a limitações da largura de banda. Sinaliza-se também que alguns departamentos adotaram esses procedimentos restritivos isoladamente, mas que não se trata de uma política de governo.

Ao discutir os efeitos das restrições a determinados usos e conteúdos, são considerados

há uma preocupação muito grande com a governança das TICs, especialmente com os ativos de aquisição (hardware e software) e a regulamentação do uso das redes sociais.

alguns inconvenientes – para alguns funcionários isso torna mais difícil realizar seu trabalho e a produtividade diminui. Outro inconveniente apontado é a eventual incapacidade de compartilhar conteúdos com colegas de outros setores; assinala-se explicitamente então que esses efeitos são negativos, pois esses espaços de interatividade são importantes no desempenho de suas funções

Ao responder sobre os efeitos positivos, os entrevistados consideraram que alguns dos conteúdos aos quais o acesso é limitado não estão relacionados com o trabalho que fazem, e que podem dispersar as pessoas e comprometer o rendimento das equipes. Outra consequência positiva de determinadas limitações de acesso a conteúdos é a garantia da segurança dos trabalhadores e da rede do governo.

Entre as recomendações e sugestões de políticas institucionais de uso de ferramentas Web 2.0 feitas pelos funcionários do governo do estado do Rio Grande do Sul, ressalta-se a proposta de que se aproveite o conhecimento dos desenvolvedores de software livre para melhorar o sistema da entidade. Considera-se que seja fundamental o aprimoramento da formação e da capacitação dos funcionários no uso de ferramentas, incluindo o uso estratégico das redes sociais e a extensão do uso de videoconferências; também menciona-se como necessária uma política institucional que inclua todas as ferramentas de comunicação e de gestão em uma plataforma Web interoperável, à qual se possa acessar a partir de qualquer lugar.

:: WEB 2.0, POLÍTICAS PÚBLICAS E GOVERNABILIDADE

Do ponto de vista do Governo do Rio Grande do Sul, sustenta-se que é necessária a elaboração de uma política pública nacional de uso de ferramentas Web 2.0, considerando, em especial, as experiências da população.

Para o pesquisador Fabro Steibel, os ministérios, as secretarias e as prefeituras estão implementando políticas de uso de ferramentas de forma fragmentada, com o interesse de promover as administrações de turno. Quanto à legislação sobre Internet no país, Steibel e Everton Rodrigues consideram que o Marco Civil da Internet pode ser um marco regulatório que defina regras claras para as autoridades públicas, para os cidadãos e para as empresas.

Também em termos de políticas públicas surgem recomendações e sugestões por parte dos funcionários do governo relativas à adoção do software livre e aberto, bem como de processos de treinamento para qualificar as pessoas no uso das ferramentas Web 2.0. Além disso, inclui-se o acesso universal à banda larga, com preço acessível, como outro fator que contribuiria para a promoção da transparência e do acesso a informações do governo por parte dos cidadãos.

Na opinião de Everton Rodrigues, políticas que fomentem a apropriação do uso cidadão das

> não basta apenas ter acesso, é preciso ter todo um conjunto: interesses, pessoas articuladas, pessoas provocando um debate, que é um de nossos objetivos: ter uma nova cultura política de participação"

ferramentas tecnológicas são fundamentais: "Já podemos dizer que não basta que as pessoas tenham acesso à Internet ou às tecnologias da informação e comunicação. A questão é um pouco mais complexa que isso, pois, veja, aqui na região, a cidade que mais conseguiu votos para o orçamento foi Pelotas, e a segunda foi Porto Alegre - sendo que Porto Alegre tem uma população maior e muito mais pessoas estão conectadas. Acontece que um grupo de pessoas de Pelotas se interessou mais e fez campanha (...) Por isso, não basta apenas ter acesso, é preciso ter todo um conjunto: interesses, pessoas articuladas, pessoas provocando um debate, que é um de nossos objetivos: ter uma nova cultura política de participação".

Uma maior interação entre o governo estadual e os cidadãos, entre o governo estadual e o governo federal e entre os próprios cidadãos deve modificar as práticas de governabilidade da administração pública em geral. Nesse sentido, Celso Schröder sustenta que a universalização da Internet contribuirá para "a constituição de mecanismos importantes de mobilização, articulação, cobrança e transparência" do Estado frente à população e vice-versa.

Essa nova governabilidade seria o resultado da aplicação das tecnologias a favor da democracia, segundo a acadêmica Farranha. Apesar de seu posicionamento crítico quanto ao uso meramente informativo da Internet, ela sustenta

que "esta é uma ferramenta com potencial para o aprofundamento da democracia, para a democratização das políticas públicas e para a coordenação intergovernamental".

:: ALGUMAS CONCLUSÕES

A experiência do Governo do Rio Grande do Sul com relação ao acesso e o uso de ferramentas Web 2.0 é pioneira no país, e possivelmente na América Latina, devido ao fato de ter sido desenvolvida uma plataforma digital que torna a principal autoridade pública periodicamente disponível aos cidadãos, e também devido à utilização de aplicativos Web 2.0 para convocar as pessoas com relação a temas específicos. A partir dos dados e opiniões registrados, conclui-se que:

1. Apesar de o acesso às TICs não ser universal nessa entidade pública brasileira, seus funcionários possuem amplo conhecimento sobre a Internet e a intranet do governo, bem como sobre os aplicativos da plataforma digital própria, porque o governo de Tarso Genro tem como estratégia de gestão digital a conexão dos novos aplicativos com três ferramentas colaborativas e interativas (Twitter, Identi.ca e Facebook), as quais, conforme mencionado no contexto da Internet na América Latina, são importantes ambientes eletrônicos de contato.

A experiência do Governo do Rio Grande do Sul com relação ao acesso e o uso de ferramentas Web 2.0 é pioneira no país, e possivelmente na América Latina

2. O fato de Genro estar há menos de um ano[7] no cargo de governador não tem sido obstáculo para definir que um dos usos da plataforma digital seja o armazenamento das informações obtidas na relação governo estadual/cidadãos em torno de seus três componentes: O Governador Responde, O Governador Escuta e Agenda Colaborativa. A partir dessa utilização, espera-se uma fiscalização dos debates, propostas e, sobretudo, das ações desse governo por parte da população.

3. Nesse cenário, porém, não há políticas internas explícitas para o uso da plataforma digital e das ferramentas Web 2.0 pelos funcionários públicos. A pesquisa evidencia que, por exemplo, o acesso às redes sociais e profissionais, blogs e outros aplicativos da Internet varia de acordo com o cargo e a função desempenhada dentro do governo; além disso, a partir das entrevistas detalhadas, registrou-se um uso mais informativo do que interativo dessas ferramentas.

> a administração pública brasileira usa os portais Web e os aplicativos 2.0 principalmente para difundir as ações e decisões das autoridades

4. Essa situação não é exclusiva do Gabinete Digital do Governo do Rio Grande do Sul; na verdade, a administração pública brasileira usa os portais Web e os aplicativos 2.0 principalmente para difundir as ações e decisões das autoridades, estabelecendo dessa forma novos canais de informação para a população.

5. No âmbito do Gabinete Digital, a limitação técnica em torno do número de computadores disponíveis para o pessoal está impactando o contato direto entre Estado e funcionários públicos, uma vez que estes estão usando suas contas pessoais em aplicativos Web para tratar de assuntos públicos. A essa restrição somam-se proibições de acesso a certos conteúdos audiovisuais que, todavia, não respondem a critérios de produtividade ou segurança das informações.

6. Do ponto de vista dessa mesma entidade pública selecionada, é reconhecido que não existe uma cultura estabelecida de uso das

7. N.E.: informação relativa à data de publicação do relatório da pesquisa.

tecnologias de informação e comunicação para a gestão pública. Os funcionários ainda não têm consciência do potencial da Internet e de seus aplicativos e, portanto, seguem publicando informações pessoais por meio dessas tecnologias; o governo estadual, por sua vez, enfrenta desafios para manter um debate político qualificado com a população.

7. Apesar de o Brasil haver iniciado um debate sobre um Marco Civil da Internet, sugere-se que uma política pública nacional de uso de ferramentas Web 2.0 seja necessária porque, até o momento, as entidades públicas têm atuado de maneira fragmentada, sem reconhecer ou aprofundar-se nas expectativas da população em termos de participação e tomada de decisões mediadas pela tecnologia.

8. Quanto ao acesso universal à Internet, sugere-se que essa possibilidade deverá modificar as práticas de governabilidade de toda a administração pública brasileira. Em termos de conceitos de governabilidade, uma mudança giraria em torno da gestão unidirecional de conteúdos. Em termos de práticas, as mudanças se dariam em torno dos serviços, que deixariam de satisfazer prioritariamente às necessidades individuais, passando a satisfazer prioritariamente às necessidades coletivas. ●

sugere-se que uma política pública nacional de uso de ferramentas Web 2.0 seja necessária porque, até o momento, as entidades públicas têm atuado de maneira fragmentada

O informe completo da pesquisa *Políticas de uso de ferramentas Web 2.0 pela Administração Pública na América Latina* - que abrange também estudos sobre o Chile, Equador, Peru e Uruguai - pode ser lido (em espanhol) na versão online da revista poliTICs: www.poliTICs.org.br

Katerina Fialova Coordenadora do projeto GenderIT.org
Flavia Fascendini Editora do portal GenderIT.org

Vozes dos espaços digitais:

violência contra a mulher relacionada à tecnologia[1]

:: O CENÁRIO

As tecnologias de informação e comunicação (TICs) compreendem um conjunto de tecnologias que as pessoas usam para coletar, compartilhar e distribuir informação e para se comunicar. A rápida expansão destas tecnologias mudou a forma com que as pessoas relacionam-se umas com as outras e com o mundo. Graças às TICs, as possibilidades de comunicar e compartilhar informação se multiplicaram e agilizaram.

As TICs podem ser usadas de diferentes maneiras, inclusive para ampliar ou limitar liberdades e direitos. Isto pode ser observado em relação à violência contra as mulheres (VCM) – o dano físico, mental ou sexual que as mulheres sofrem por serem mulheres ou que as afeta de forma desproporcional. Cada vez mais mulheres sofrem violência por conta do uso da Internet e dos telefones móveis. Por outro lado, as TICs podem ser utilizadas para incrementar o acesso das mulheres à informação e aos serviços necessários para proteger e promover seus direitos.

Não obstante, poucas ativistas pelos direitos das mulheres abordam a complexa relação entre VCM e TICs em suas atividades. e na maioria dos países há pouca análise legal e política sobre o tema.

1. Este é o informe síntese do estudo *"Voices from digital spaces: Technology related violence against women"*, realizado pelo Programa de Apoio a Redes de Mulheres da Associação para o Progresso das Comunicações. O relatório completo está disponível no portal GenderIT.org (em inglês): www.genderit.org <http://www.genderit.org> .

Este informe apoia-se nas experiências e achados do projeto ODM3: Dominemos a tecnologia! - da Associação para o Progresso das Comunicações (APC). Este projeto trabalhou com organizações de direitos das mulheres de doze países da África, Ásia e América Latina entre 2009 e 2011 e ofereceu apoio a estas organizações para que investigassem e respondessem à violência relacionada com a tecnologia, e fortalecessem sua capacidade para usar ferramentas TIC em suas respostas à violência.O informe baseia-se também em outros trabalhos do Programa de Apoio às Redes de Mulheres (PARM) da APC na área de VCM, direitos das mulheres, direitos sexuais e TICs.

Não é nosso propósito oferecer um mapa exaustivo da violência relacionada com a tecnologia nem mergulhamos em todos os debates relevantes sobre o tema. Este informe, por sua vez, explora as tendências e padrões emergentes da violência relacionada com a tecnologia vivida por mulheres de todo o mundo e esboça possíveis formas de resposta.

:: O CONTEXTO DE GÊNERO E TICS

Em todo o mundo as mulheres sofrem desigualdades econômicas, políticas, sociais e culturais baseadas em gênero, que incluem o acesso a direitos como educação, saúde e segurança. A VCM manifesta-se de distintas maneiras ao redor do mundo. A violência e desigualdade que as mulheres vivenciam dependem de sua raça, classe social, orientação sexual, nacionalidade e localização geográfica.

Numa perspectiva global, as mulheres têm menos acesso às TICs e menos controle sobre elas que os homens, e as utilizam de maneira diferente. Nos países em desenvolvimento, há menos usuárias de Internet que usuários. Em países de média e baixa renda, as mulheres têm 21% menos probabilidades de ter um telefone móvel[2].Esta desigualdade tem relação com a desigualdade de gênero mais ampla que existe nestas sociedades.

Muitos fatores contribuem para as diferenças de gênero no acesso, uso e controle das TICs, incluindo o acesso à educação, os custos de conexão, a falta de infraestrutura física, a pobreza, a disponibilidade de tempo e atitudes culturais. Para que a sociedade da informação seja mais acessível para as mulheres, estas deveriam poder conectar-se às TICs de onde quer que estejam. Ademais, os conteúdos e espaços online disponíveis teriam que responder às necessidades e interesses das mulheres. Por último, as mulheres e suas organizações devem ter a capacidade de usar e tirar proveito das TICs.

:: COMO AS TICS E A VCM SE CONECTAM?

A violência relacionada à tecnologia é uma forma de VCM que se manifesta no contexto destas novas tecnologias. As TICs podem ser usadas para perpetrar violência de várias formas.

Os perpetradores de violência utilizam telefones móveis e Internet para seguir, molestar e vigiar os movimentos e atividades das mulheres. Em especial, usam os serviços de localização dos telefones

2. Fundo de Desenvolvimento GSMA Women & mobile: A global opportunity (GMSA, 2010) www.mwomen.org/Research/ women-mobile-a-global-opportunity_1

celulares, obtêm senhas e vigiam as mensagens de texto e as chamadas recebidas. Os perpetradores também usam as TICs para obter e distribuir fotos e gravações íntimas e sexuais de mulheres sem sua autorização.

As formas mais frequentes de VCM relacionadas à tecnologia são:

- Perseguição online e cibermolestamento, uma das formas mais visíveis de VCM.
- Violência doméstica, quando a tecnologia é usada em atos de violência e abuso em relações familiares ou conjugais.
- Agressão sexual e estupro, onde a tecnologia é utilizada para seguir os movimentos e atividades das mulheres e para saber onde elas estão. Também, quando a violência continua mediante o registro digital e distribuição da violação. Há casos em que foram utilizados avisos ou mensagens falsas na Internet para atrair as mulheres para as situações nas quais ocorreram as agressões sexuais.
- VCM culturalmente justificada, quando a tecnologia cumpre uma função na criação de uma cultura de VCM ou perpetua o uso da cultura ou da religião para justificar, ignorar ou aceitar atos de VCM.
- Violência dirigida a comunidades, onde determinadas comunidades sofrem ataques e perseguições online por conta de sua identidade sexual ou de gênero ou por sua posição política.

As TICs permitem que os perpetradores cometam atos de violência de forma anônima e distante das mulheres às quais se dirigem, o que torna mais difícil identificá-los e denunciá-los à justiça. Os serviços de rastreamento de telefones e as plataformas para compartilhamento de informações na rede também permitem a vigilância das atividades das mulheres e a reprodução e distribuição de fotos íntimas com muito pouco esforço e baixo custo.

Devido à memória "tudo se registra, nada se esquece" da Internet e à possibilidade de reprodução infinita da informação, as mulheres experimentam as consequências dos textos e imagens da violência dirigida a elas sem poder fazer nada para controlar esta situação.

Em muitos casos de violência, os perpetradores são vários. Por exemplo, na distribuição não autorizada de imagens privadas é frequente haver um único perpetrador principal – a pessoa que publica as imagens. Porém, quem as vê e as faz circular torna-se perpretador adicional. Da mesma maneira, a perseguição online costuma envolver vários abusadores que publicam comentários sexualmente agressivos e ameaças.

Todos estes atos de violência violam um conjunto de direitos das mulheres, que inclui o direito à privacidade e à proteção de informação pessoal e de dados sensíveis.

As pesquisadoras feministas defendem a ideia de que no contexto das TICs, o corpo transcende o físico. Em consequência, a distribuição de

> Os perpetradores de violência utilizam telefones móveis e Internet para seguir, molestar e vigiar os movimentos e atividades das mulheres.

representações íntimas e abusivas de corpos viola o direito das mulheres à integridade e à autonomia corporal.

Além disso, a violência relacionada à tecnologia afeta a liberdade das mulheres para expressarem-se, transitar no ambiente digital com liberdade e desfrutar das comunidades online – portanto viola sua autonomia, liberdade de expressão e acesso à informação.

O dano que as mulheres sofrem por conta desta violência é principalmente psicológico e emocional e inclui medo, nojo, stress e depressão. Ademais, o abuso online, se não é controlado, pode levar ao abuso físico na vida real. Em alguns casos, a violência relacionada à tecnologia desembocou em suicídios, em particular de pessoas jovens. As mulheres que sofrem este tipo de abuso também tendem a retirar-se das redes sociais online e na vida real, e deixam de participar ativamente na vida política, social e econômica.

:: COMO OS MARCOS LEGAIS E AS POLÍTICAS DE TIC RESPONDEM À VCM?

Existem políticas e leis na área de TICs, inclusive em alguns dos países alcançados pelo projeto Dominemos a tecnologia!. Mas, em sua maioria, estas políticas e leis não contemplam a perspectiva de gênero nem levam em conta a VCM relacionada à tecnologia. Ademais, na legislação dirigida a cumprir e proteger os direitos das mulheres, raras vezes as TICs são mencionadas.

O projeto ODM3: Dominemos a tecnologia! documentou a luta das vítimas/sobreviventes de violência relacionada à tecnologia para conseguir que se faça justiça e que sejam respeitados seus direitos. Os mecanismos legais e regulatórios e os organismos executores da lei geralmente carecem de certeza acerca de que leis se aplicam em cada caso. Consultam leis contra a VCM, códigos de delitos informáticos e leis sobre direito à privacidade.

:: ESTUDO DE CASO – VIOLÊNCIA SEXUAL E DISTRIBUIÇÃO NÃO AUTORIZADA DE IMAGENS ÍNTIMAS DE MULHERES

Ainda que não haja estatísticas sobre o volume de fotos e vídeos íntimos de pessoas que são distribuídas sem seu consentimento, os informes da mídia, das pessoas e das organizações que trabalham na área da VCM mostram que as mulheres e as minorias sexuais são objeto frequente destas agressões.

As imagens e gravações distribuídas desta maneira são tomadas com ou sem o consentimento da mulher. Em alguns casos, as imagens e gravações provêm de meios voyeurísticos, como câmeras ocultas. Em outros, as mulheres enviam suas imagens íntimas a seus companheiros sexuais ou consentem em gravar uma relação sexual com seu parceiro, que depois usa este registro de forma abusiva enquanto ainda há a relação afetiva ou depois de seu término.

Os abusadores também podem manipular fotografias de mulheres para convertê-las em imagens pornográficas e distribuí-las com informação pessoal, como número de telefone e endereço.

Também são filmados momentos de violação e agressão sexual, e os espectadores ou perpetradores da violência os distribuem através da Internet e de telefones móveis. Por exemplo, em 2010, uma moça foi drogada e atacada sexualmente por um grupo de homens em uma festa. Espectadores da cena registraram o incidente e o distribuíram amplamente pela Internet.

Os perpetradores deste tipo de violência registram estas imagens por diferentes razões. Em alguns casos, ameaçam distribuí-las para extorquir uma mulher ou forçá-la a permanecer em uma relação abusiva. Também ocorre a distribuição de imagens e filmes para humilhar e difamar mulheres que são figuras públicas. Em outros casos, os abusadores circulam estas imagens e gravações como um "hobby" para ganhar prestígio entre seus pares ou simplesmente para mostrar que podem fazê-lo.

A circulação pública de imagens e gravações conduz à vitimização múltipla das vítimas/sobreviventes. Cada vez que outra pessoa vê uma foto ou gravação íntima de uma mulher ou publica comentários que a culpabilizam ou a agridem, a mulher é novamente vitimizada.

:: ACESSO À JUSTIÇA

As leis sobre pornografia infantil, as leis de proteção da privacidade e as leis contra a VCM oferecem possibilidades de reparação para as vítimas/sobreviventes da distribuição não autorizada de imagens e gravações, mas também têm limitações.

:: LEIS SOBRE PORNOGRAFIA INFANTIL

As leis sobre pornografia infantil criminalizam a criação, exibição e distribuição de imagens sexuais de meninos e meninas, a quem se define como pessoas menores de 18 ou 16 anos de idade, segundo cada país.

Para este tipo de delito, as leis sobre pornografia infantil dispõem sanções penais mais severas do que, por exemplo, as leis de privacidade. Hoje existe uma forte vontade entre os estados de investigar e perseguir os delitos de pornografia infantil nacional e internacionalmente. Isto permite a necessária cooperação internacional que faculta à policia atuar frente a delitos que transcendem as fronteiras dos países.

De todas as maneiras, as leis sobre pornografia infantil não diferenciam entre gravação e distribuição autorizada ou não autorizada das imagens. Portanto, uma menina pode ser acusada de delito quando expõe uma imagem de si mesma com um companheiro afetivo. As leis devem reconhecer o direito da juventude à autodeterminação e à integridade corporal e distinguir entre atos consentidos e não consentidos. Enquanto se discute até que grau a juventude consente com estas ações com base em decisões informadas, a ênfase deveria estar na prevenção, mais que na criminalização. Por exemplo, os programas educativos para a juventude poderiam ajudar a negociar os espaços online e as interações sexuais com segurança.

As leis sobre pornografia infantil tampouco reconhecem a natureza de gênero destes abusos. Isto é necessário para uma resposta holística e adequada às necessidades das mulheres vítimas/sobreviventes deste tipo de violência.

:: LEIS DE PROTEÇÃO À PRIVACIDADE

As leis de privacidade protegem o direito de respeito à vida privada e regulam a coleta, armazenamento e uso da informação. Muitos estados têm legislação inadequada para proteger o direito à privacidade e de fato delegam este dever aos indivíduos e ao mercado.

Além disso, a violação da privacidade costuma ser equiparada à intrusão do estado ou das empresas na vida das pessoas e não se leva em conta as violações cometidas por indivíduos, incluindo companheiros, pais ou irmãos.

Nos debates sobre privacidade predominam as perspectivas dos homens de classe média. Devido a este fato, as preocupações quanto à privacidade das mulheres e a VCM relacionada à tecnologia – as quais são definidas pela posição social das mulheres e que costumam implicar violações da privacidade cometidas por indivíduos, incluindo companheiros, pais e irmãos - não recebem atenção.

A isso soma-se o fato de que o discurso público e político sobre a privacidade frequentemente demarca-se dentro das mesmas perspectivas culturais e morais usadas para controlar o corpo das mulheres. Por isso, em muitos contextos, os casos de distribuição não autorizada de imagens íntimas de mulheres são considerados uma corrupção das normas sociais e familiares em vez de violações ao direito das mulheres à integridade e autonomia corporal. Em consequência, muitas vezes acaba-se questionando a moralidade da vítima/ sobrevivente e a violação se converte em uma vergonha para ela.

Outro nível deste debate é como equilibrar o direito de uma pessoa à privacidade com o direito público à informação, em particular em relação a figuras públicas. Na Malásia, por exemplo, circulou publicamente um vídeo sexual de uma mulher em cargo político. As apelações por uma proteção mais forte da privacidade que se seguiram a este incidente foram diluídas em debates sobre a moral das figuras públicas e as expectativas da opinião pública.

Nas Filipinas, a lei contra o voyeurismo de fotos e vídeos sancionada em 2009 é uma lei inovadora que penaliza o ato de tirar, copiar e distribuir fotos ou vídeos de atos sexuais ou de partes íntimas sem o consentimento da pessoa ou das pessoas envolvidas. Esta lei dispõe penas mais severas que outras leis de privacidade e inclui a possibilidade de prisão.

De todas as formas, esta lei não reconhece que estes atos podem ser uma forma de VCM e não especifica o que significa consentimento. Se a implementação da lei faz recair o ônus da prova do consentimento sobre as vítimas/sobreviventes, pode desalentar as mulheres a denunciar delitos e procurar reparação, como costuma acontecer com as leis sobre agressão sexual.

:: LEIS CONTRA A VCM

Nos casos de distribuição não autorizada de imagens íntimas de mulheres podem ser aplicadas três classes de leis contra a VCM: leis contra a pornografia, leis contra delitos sexuais e leis sobre perseguição sexual.

As três classes de leis reconhecem estes delitos contra as mulheres como uma forma de VCM. Portanto, asseguram uma investigação e ação judicial sensível a gênero. Entretanto, provar o dano psicológico e emocional e, portanto, demonstrar que foi cometido um ato de violência é tão difícil no marco destas leis como é, por exemplo, no marco das leis de privacidade.

Estas leis necessitam ser ampliadas para incluir definições de violência com base no dano emocional e psicológico, de modo que possam contemplar as violações que as mulheres sofrem online e o impacto da violência relacionada à tecnologia. Também é preciso que reflitam a fronteira nebulosa entre violência online e na vida real, em especial devido ao fato de que uma destas forma de violência pode ganhar escala e converter-se na outra, ou estarem relacionadas entre si. Por exemplo, a gravação e distribuição da agressão sexual conduz a uma vitimização ulterior da mulher.

:: O EQUILÍBRIO ENTRE LIBERDADE E "PROTEÇÃO" NO TRATAMENTO DA VCM

Ainda que seja necessário desenvolver medidas novas e inovadoras para combater a VCM, também necessitamos prestar atenção à forma com que estas soluções são adotadas. Por exemplo, as medidas que assumem uma concepção protecionista da segurança online das mulheres podem incrementar a censura por parte de atores governamentais ou privados, o que por sua vez pode limitar as liberdades das mulheres.

Um caso que exemplifica esta situação é o de algumas diretivas recentes para combater a pornografia infantil, que fazem com que os serviços de busca filtrem conteúdos sexuais e terminologia relacionada às comunidades lésbica, gay, bissexual e transsexual (LGBT) nas regiões árabes. Isso pode restringir o direito à expressão e o acesso à informação das mulheres e das minorias sexuais.

Recomendações para formuladores/as de políticas, intermediários de TICs, mídia, usuários/as de TICs e organizações que trabalham com VCM

Responder com eficácia à VCM relacionada à tecnologia requer a ação de todas as pessoas que incidem na configuração das TICs e de todas as pessoas responsáveis por abordar a VCM. Isto inclui usuários e usuárias de TICs, provedores de serviços de Internet, o estado, organizações que trabalham na área da VCM e os meios de comunicação.
A ação deve ter lugar em diferentes níveis: atacar as raízes da VCM e transformar as relações de poder assimétricas; limitar as consequências da VCM para as vítimas/ sobreviventes assegurando imediata resposta e apoio; e oferecer assistência e apoio de longo prazo às vítimas/sobreviventes.

A necessidade de envolver os intermediários de Internet que desenvolvem e operam plataformas de Internet e de telefonia móvel é cada vez mais evidente. Estes intermediários são atores com muito poder no desenho das políticas de TIC e incidem nos debates e medidas regulatórias. Não obstante, costumam subestimar seu papel crucial e sua responsabilidade quanto à proteção de suas usuárias frente à possibilidade de VCM.

:: LEIS E POLÍTICAS

Os estados precisam criar, implementar e observar leis e políticas que respondam à VCM relacionada à tecnologia. É necessário ampliar as leis anti-VCM para que contemplem a natureza da violência relacionada à tecnologia. As leis que tratam de delitos de TICs devem considerar as diferenças e desigualdades de gênero.

O desenvolvimento destas leis requer uma perspectiva holística que avalie e equilibre todos os direitos das mulheres, de modo que nenhum deles sofra efeitos adversos, como por exemplo mediante medidas que impliquem censura. Também é necessário envolver diferentes atores e assegurar a participação das mulheres. Os espaços multissetoriais e transnacionais, como o Fórum de Governança da Internet, constituem boas plataformas para o diálogo.

:: ASSEGURAR A PARTICIPAÇÃO DAS MULHERES

As organizações da sociedade civil devem estimular que os/as formuladores/as de políticas tomem em conta a VCM relacionada à tecnologia e que as mulheres participem nos espaços de formulação de políticas.

Os quadros e informes do setor de TICs que supervisem e avaliem a inclusão das mulheres nos fóruns e organismos do setor podem ser úteis para desafiar a baixa representação das mulheres. O projeto ODM3: Dominemos a tecnologia! apoiou

a presença de representantes de organizações locais de direitos das mulheres para que participem em espaços regionais e internacionais de formulação de políticas. O projeto também apoiou diálogos nacionais entre formuladores/ as de políticas do setor das TICs e governamentais e organizações de direitos das mulheres nos 12 países para desenvolver planos estratégicos sobre VCM relacionada à tecnologia.

:: PRODUÇÃO DE PROVAS

São necessárias observações e informes sistemáticos da VCM relacionada à tecnologia para apoiar os esforços de incidência e contribuir para o desenho de políticas baseado em evidências. Estes estudos deveriam incluir a participação e perspectivas de mulheres de diferentes contextos, raças, classes, sexualidades e nacionalidades.

A APC, em colaboração com as participantes da campanha ODM3: Dominemos a tecnologia! desenvolveu uma plataforma de mapeamento online[3] para que as mulheres compartilhem histórias, notícias e experiências sobre VCM relacionada à tecnologia. A plataforma registra e ordena por categorias a violência denunciada.

:: INTERMEDIÁRIOS DE INTERNET

Os provedores de serviços de Internet e telefonia móvel deveriam garantir que as mulheres usuárias de seus serviços entendam que comportamentos põem em risco sua segurança e como prevenir e deter a violência.

Nos processos de disposição de normas deveriam participar especialistas em políticas contra a VCM. Os serviços também deveriam incluir mecanismos eficientes de denúncia ou queixa para denunciar abusos e para obter ajuda para detê-los.

Os intermediários de TICs também podem contribuir para a segurança contra a violência mediante o desenho de serviços de TIC mais seguros. Por exemplo, os perfis das redes sociais podem ser configurados como "privados" por padrão, a fim de restringir a possibilidade de que estranhos acessem, vejam e comentem sobre um perfil de usuária.

Iniciativas como os 'Princípios para redes sociais mais seguras', da União Europeia – resultado de processos multissetoriais – podem orientar os intermediários quanto às melhores práticas para promover a segurança.

:: CAPACITAÇÃO EM MÍDIAS E EMPODERAMENTO DE USUÁRIAS

A prevenção da VCM requer que se trabalhe com usuárias de TIC e vítimas potenciais para mudar atitudes e comportamentos. As iniciativas de capacitação em mídia buscam que as usuárias sejam mais conscientes das implicações de seus atos. Por exemplo, iniciativas de educação de jovens para jovens nos Estados Unidos orientam a juventude sobre as consequências legais e sociais de compartilhar informação sexual. A campanha mundial Dominemos a tecnologia! convida a todas as

3. www.apc.org/ushahidi

usuárias de TICs a tomar o controle da tecnologia para acabar com a VCM, inclusive mediante ações diárias como o compromisso "eu não reenvio violência".

Outras iniciativas trabalham com mulheres e meninas para aumentar seu controle sobre as TICs e capacitá-las para que as utilizem de forma eficaz e segura. Por exemplo, a APC aporta na formação das mulheres defensoras dos direitos humanos capacitando-as para a comunicação online de forma segura e encorajando-as a trabalhar em rede.

:: MEIOS DE COMUNICAÇÃO

As pessoas que trabalham em mídias virtuais e impressas têm a responsabilidade de não distribuir informação delicada sobre vítimas/sobreviventes de VCM relacionada à tecnologia. Na África do Sul, assim que a gravação de uma presumida violação grupal circulou através de TICs, alguns jornais publicaram relatos detalhados do conteúdo da gravação e publicaram imagens da casa da vítima/sobrevivente. Informação como esta viola os direitos da vítima/sobrevivente e pode desembocar em vitimizações ulteriores. Os meios de comunicação podem cumprir uma função positiva se analisam e dão nome a este tipo de violência.

:: APOIO PARA AS VÍTIMAS/ SOBREVIVENTES DE VIOLÊNCIA

Também há necessidade de dar assistência às organizações que trabalham na área da VCM para que possam ajudar melhor às vítimas/sobreviventes de VCM relacionada à tecnologia. As organizações que estão na linha de frente de ações de assistência necessitam capacitação e ferramentas práticas sobre como comunicar-se, denunciar e responder online e de forma segura em casos de VCM relacionada à tecnologia.

As TICs também podem facilitar a assistência e apoio às vítimas/sobreviventes através de redes sociais e comunidades online. Ademais, as TICs podem ser utilizadas em campanhas civis de solidariedade com as vítimas/sobreviventes de violência. Por exemplo, na Malásia, logo após terem vazado na Internet fotos íntimas de uma mulher política, uma campanha solidária utilizou o Facebook para mobilizar apoio à vítima. Esta campanha impediu que a mulher renunciasse a seu posto após o incidente.

:: CONCLUSÃO

Este informe demonstra que os casos que envolvem VCM relacionada à tecnologia estão em crescimento e causam sérios danos às mulheres. As vítimas/sobreviventes de VCM relacionada à tecnologia correm maior risco de vitimização ulterior por múltiplos perpetradores. As tendências, vazios e estratégias que apresentamos neste estudo constituem pontos de partida cruciais para as organizações que trabalham em políticas de TIC e/ou direitos das mulheres para deter a violência. O mais importante agora é promover estratégias e políticas que empoderem as mulheres e lhes permitam controlar suas situações, opostas à adoção de abordagens protecionistas. Este deveria ser o eixo central do trabalho para acabar com a VCM. ●

poliTICs

COORDENAÇÃO DO PROJETO GRACIELA SELAIMEN

EDITORES GRACIELA SELAIMEN, CARLOS A. AFONSO

CAPA, PROJETO GRÁFICO E DIAGRAMAÇÃO MONTE DESIGN

DISTRIBUIÇÃO VIVIANE GOMES

TRADUÇÕES JULIA GUIMARÃES

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

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 +55 (21) 2527-0294 | fax +55 (21) 3259-0370 | www.nupef.org.br