ComCiência n.158 Campinas May 2014

O que os dados podem dizer sobre nós

Juliana Passos

Reportagem

Um garoto pisou na bola ao terminar com a namorada pelo Instagram. Expôs a menina e a si mesmo em uma situação que virou notícia no mundo inteiro, com direito a lições de moral em diversas línguas. Uma moça perdeu a chance de concorrer a um posto de trabalho, porque seu possível empregador descobriu que ela estava processando a antiga empresa – do mesmo setor – no banco de dados online disponibilizado pelo judiciário. Uma bebê foi acordada por uma voz estranha durante a madrugada. Um hacker entrara no sistema de sua babá eletrônica e pedira que acordasse, algo de proporção bem menor do que a espionagem da Agência Nacional de Segurança (NSA) dos Estados Unidos feita a milhares de usuários do Yahoo que conversavam via webcam. Esses são alguns exemplos chocantes, revoltantes ou engraçados de situações às quais estamos expostos em um mundo cibermediado.

"As pessoas ainda estão aprendendo a lidar com a exposição de dados na rede. A internet é muito nova e (muitos usuários) não viram até agora nenhum problema acontecer, mas a partir do momento em que você coloca várias informações suas na rede, pode sofrer invasão", diz o ativista Silvio Rhatto, um dos sócios da empresa de segurança Oblivia. Ele aponta que as violações de privacidade podem ser feitas tanto por um plano de saúde que consegue acessar suas informações a partir de prontuários eletrônicos quanto pela Serasa, com sua construção de banco de dados feita com informações repassadas pelo Tribunal Superior Eleitoral, além das recorrentes invasões de conta bancária por estelionatários.

Em entrevista ao jornal *Folha de S. Paulo*, o consultor Andreas Weigend, que foi cientista-chefe da Amazon e hoje dá aulas na Universidade Stanford, coloca a exposição de dados como algo irreversível, mas vê a necessidade de regulamentação do destino desses dados. "A questão não é mais se queremos revelar ou compartilhar algo, já que informações que a KGB (agência russa de espionagem) não conseguia arrancar das pessoas sob tortura estão agora disponíveis na internet. A questão é o que a sociedade vai fazer com essas informações. Se um empregador descobre pelo Facebook que eu sou gay e ele não quer contratar homossexuais, o que a sociedade vai fazer com isso?".

Ele compara a quantidade de dados disponíveis na rede, o "big data", com o petróleo bruto. "Do mesmo modo, no caso do 'big data', as grandes companhias, aquelas que vão ganhar muito dinheiro, serão aquelas que transformarem essas informações em produtos que permitam que nós tomemos decisões melhores". Weigend se refere ao poder de mineração dos dados, o *data mining*. Um exemplo de mineração dos dados foi apresentado em uma matéria do jornal *The New York Times* em 2012, ao explicar que usuários que visualizavam uma certa quantidade de itens para bebês tinham alta probabilidade de estarem próximos de ganhar um filho e, partir disso, os sites visitados passaram a enviar pelo correio cupons promocionais desses produtos. Dentro das redes

sociais, a mineração de dados é intensa para mapear as principais conexões entre indivíduos e seus gostos ou hábitos de consumo.

O coordenador do Pimenta Lab – Laboratório de Tecnologia, Política e Conhecimento da Universidade Federal de São Paulo (Unifesp), Henrique Parra, lembra do potencial de rastreabilidade inerente às tecnologias digitais, não necessariamente ligadas a redes de relacionamento ou email. Em uma simples compra, ao utilizar o cartão de crédito e solicitar a nota fiscal eletrônica, suas informações são enviadas ao seu banco, à operadora do cartão, à Receita Federal e à prefeitura do município onde a compra foi realizada. Também é possível pagar o transporte público com seu bilhete com cadastro do CPF e entrar no escritório de trabalho passando por uma catraca eletrônica ao introduzir seu crachá. Para o pesquisador, a facilidade das novas tecnologias cria um paradoxo. "Ao mesmo tempo em que oferece uma facilidade, ela, de alguma maneira, tem implícita uma racionalidade política para o seu funcionamento. E essa técnica é tão mais eficiente quanto mais facilidade ela apresenta no seu uso e quanto mais indireta for a forma que ela instala uma racionalidade política no seu funcionamento. É a possibilidade de relações plenamente transparentes com um mecanismo de controle implícito". Ele lembra que as possibilidades de registro atuais não são sinônimos de monitoramento, pois isso depende da forma de armazenamento de dados. “Uma coisa é a difusão das tecnologias de registro, outra coisa é a integração desses bancos de dados, que é uma coisa que está acontecendo mais facilmente à medida que cresce a convergência digital”.

Resistência ao uso

Um dos motivos para o uso da criptografia – método de codificação de mensagens para que apenas o seu destinatário consiga lê-la –, na opinião de Ricardo Dahab, pesquisador do Instituto de Computação da Universidade Estadual de Campinas (Unicamp), vem de uma lógica simples. "Se existe um mercado paralelo para venda de roupas, eletrônicos, existe também um para o comércio de dados". Um dos objetos de pesquisa de Dahab é a produção de segundas formas de verificação para acesso a contas, como envio de códigos para celular e o uso de geradores de senhas – *tolkiens* – para bancos. Atualmente ele trabalha com a produção de transparências capazes de serem visualizadas apenas com uma luz específica com função parecida com a do *tolkien*. Apesar de acreditar na necessidade de proteção, ele considera que há uma certa resistência do usuários em adotar medidas de segurança porque elas, em geral, criam barreiras para o acesso fácil a determinados serviços. “As pessoas também acabam ficando com medo de criar senhas e esquecerem e perder todos os dados que tinham em um computador”, aponta.

O pesquisador avalia que, para a maioria das pessoas, adotar sistemas de segurança ainda é visto como um estorvo. “Quem quer ter 10 cadeados na sua porta? Ficar lidando com cadeado, guardando chave. Não é uma coisa que você quer fazer, nunca, é?” Tanto ele, quanto o presidente da Associação Brasileira de Internet (Abranet), Eduardo Neger, consideram que o interesse por medidas de segurança por parte do usuário comum ainda é pequeno. No caso da Abranet, que representa provedores de conteúdo e pequenos provedores de conexão, Neger relata que diversas empresas que estão investindo em sistemas de segurança não estão recebendo o número de propostas que esperavam.

“Nem mesmo usuários corporativos – empresas de grande e médio porte – têm demonstrado interesse em proteger seus dados”, diz.

O manual do grupo Saravá, coletivo formado para desenvolver instrumentos tecnológicos para movimentos sociais, avisa que não existe segurança sem algum esforço para evitar “paranoia” ou excesso de senhas, e recomenda “estabelecer uma política pessoal de segurança levando em conta qual o nível de privacidade você quer nas suas informações” e sugere que, a partir disso, você “construa seu esquema de segurança informacional”.

O número de projetos para desenvolvimento de comunicação segura é imenso. A maioria, de acordo com Silvio Rhatto e Ricardo Dahab, está focada em boa implementação da criptografia para facilitar a própria atividade dos programadores. Eles apontam usabilidade como um dos desafios para tornar a criptografia como algo de uso das massas. “Assim como existem vários botões que permitem uma série de funções, deveria ter um ‘tranque (criptografe) o meu celular totalmente’, um botãozinho só”, exemplifica Dahab.

Para garantir uma navegação anônima sem coleta de registro de acesso (*logs*), um dos programas mais usados é o Tor – sigla em inglês para The onion router. No entanto, a navegação anônima promovida por esse software livre não significa que seus dados de conteúdo não possam ser coletados. Para isso é necessário usar o programa Tails, queridinho de Edward Snowden e que acaba de sair em sua versão beta, para proteger o conteúdo do seu acesso e criptografar esses dados.

Aos poucos, programas ligados à comunicação segura estão aparecendo, com serviços de e-mail e aplicativos seguros para troca de mensagens instantâneas. Um deles é o TextSecure, embora tenha a necessidade de estar vinculado à *play store* da Google, mas permite a troca de mensagens criptografadas e bate-papo gratuito entre usuários.

Um projeto mais amplo de comunicação segura é o Leap, sediado nos Estados Unidos, com contribuições de diversas partes do mundo, inclusive do Brasil, com a participação da Oblivia. O projeto é desenvolvido totalmente em software livre e tem como objetivo criar sistemas de comunicação segura. Até o final do ano, está previsto o lançamento do serviço de e-mails. Ao falar em software livre, Rhatto lembra que não significa que seja totalmente gratuito, pois os custos de verificação de criptografia são extremamente altos e o ideal seria que houvesse uma rede de financiamento de usuários. Atualmente, boa parte dos trabalhos em software livre como Linux, Tor e o próprio Leap são financiados com dinheiro do Estado americano.

Dahab também pondera que o financiamento coletivo seria o ideal. “Um governo deve trabalhar pelo cidadão, pela população, mas nem sempre se comporta assim. Você tem uma coisa (o software livre) que é pra ser idealmente libertária, que dá autonomia ao cidadão. Então, eu acho que idealmente deveria ser algo independente de financiamento oficial”, diz. Ele acredita que a possibilidade de verificação permitida pelos softwares livres diminua a chance de ingerência por parte dos governos e empresas que eventualmente financiem determinados projetos.

Democracia

Em um *talk show* realizado para a conferência TED (Tecnologia, Entretenimento e Design) em março deste ano, Edward Snowden fez um apelo a empresas de conteúdo para que usem conexões seguras, ao explicar o que é possível recolher com metadados. A sua coleta é prevista pela legislação americana e permite obter todos os registros telefônicos feitos e saber se o telefone está público – nas inúmeras listas telefônicas disponíveis online, é possível saber com quem e quando você está falando e até para onde você viajou. Também é possível saber em quais livros você clicou no banco de dados da Amazon – e a partir deles você recebe novas sugestões de títulos relacionados. "Todas as empresas precisam ter o hábito da navegação criptografada como padrão, para proteger os usuários que não tenham realizado qualquer ação ou escolhido quaisquer métodos especiais por conta própria", disse Snowden.

O ex-analista da NSA também comentou sobre a retenção de conteúdo dos internautas, ainda sem regulamentação prevista. "O Prism é um programa do governo que pode obrigar as empresas americanas a fazer trabalho sujo para NSA. E apesar de algumas empresas resistirem, pedindo que isso fosse feito por meios legais – acredito que o Yahoo e o Google sejam algumas delas –, todas contribuíram, porque isso nunca havia sido tentado em um tribunal aberto".

No Brasil, uma brecha legal para monitoramento foi aprovada com o novo Marco Civil em seu artigo 15, com a permissão de guarda de *logs* e acesso a aplicativos e serviços por seis meses a um ano, podendo ser estendidos em caso de pedido judicial. Para Silvio Rhatto, tal determinação respeita menos os limites de privacidade do que os já previstos na Lei do Grampo. Em seu *blog*, ele escreve: "Na balança dos direitos individuais '*versus*' interesses supostamente coletivos, o ganho de agilidade em investigações civis e criminais seria muito baixo em comparação à gravidade da drástica diminuição da privacidade de toda a população do país". Isso porque aqueles que usam a rede para praticar crimes como de pedofilia, lavagem de dinheiro ou roubo de informações realizam essas ações através de operações sofisticadas e utilizam inúmeras formas de segurança de dados.

O diretor presidente da Abranet, Eduardo Neger, acredita que fixar um prazo para guarda de dados foi um avanço da legislação. "Há provedores que guardam *logs* de acesso há muito tempo, até por tempos maiores do que foi determinado pelo Marco Civil. O que é importante é que a legislação determinou o que cada um pode guardar. O provedor de conexão e de telefonia não pode guardar seu histórico de navegação e nenhuma outra informação relativa à sua navegação, somente o *log* de acesso. Você corria o risco de sua operadora guardar tudo o que você fazia na internet. Hoje não pode mais. A operadora só pode guardar a hora que você entrou e quem você é (seu endereço IP), só isso. O grande impacto que ocorreu foi nas operadoras de telecomunicação, que não fazem parte da nossa associação (a Abranet), aquelas que estavam contra a neutralidade da rede".

Em abril, o Tribunal de Justiça Europeu decidiu suspender a Diretiva de Retenção de Dados estabelecida desde 2006, após ataques terroristas em Madri, por considerar que há brechas jurídicas para coleta de dados que violam a privacidade das pessoas, como hábitos da vida cotidiana, locais de residência permanentes ou temporários, os deslocamentos diários, atividades exercidas, relações sociais e meios sociais frequentados.

Após as manifestações de junho de 2013 no Brasil, o governo do estado do Rio de Janeiro criou a Comissão Especial de Investigação de Atos de Vandalismo em Manifestações (CEIV), que previa o repasse de dados por parte das operadoras de telecomunicação em 24 horas e sem mandado judicial. Após pressão da sociedade civil e da Ordem dos Advogados do Brasil (OAB), o texto foi alterado: "As empresas operadoras de telefonia e provedores de internet darão prioridade para o atendimento dos pedidos de informações formulados pela CEIV ou decorrentes de ordem judicial nos casos de sigilo previstos na legislação".

Ao propor uma reflexão sobre a retenção de dados por parte da NSA ou questionar a exposição de dados em sites governamentais sobre pessoas físicas, Henrique Parra faz uma diferenciação entre a divulgação dos documentos secretos realizada pelo Wikileaks e a exposição de dados de pessoas físicas. "O Wikileaks trabalha com uma ideia de transparência aplicada a governos e grandes corporações. Uma diferença fundamental é pensar em uma assimetria das relações de poder. O Wikileaks trabalha com transparência para governos, que têm um dever de publicização. Eles respondem por isso, faz parte da democracia. E as corporações, na medida em que fazem ações que têm impacto sobre a sociedade, também devem prestar contas".

A distinção também é feita pela jornalista Natália Viana, da Pública, uma agência de reportagem e jornalismo investigativo sem fins lucrativos e responsável pelo Wikileaks no Brasil. "A liberação de dados não tem nada a ver com privacidade. Os vazamentos são relatórios oficiais aos quais já tinham acesso 2,5 milhões de pessoas. Os documentos revelaram inúmeros abusos de poder, mostraram espionagens do governo americano a integrantes da ONU, como cartão de crédito e DNA, em nome de empresas e governos. Mostrou como funciona a política a portas fechadas", comenta. Viana também confirmou a tentativa de censura sofrida por Julian Assange em sua participação durante o NetMundial, a qual classificou como "excesso de zelo do governo brasileiro", após ministros receberem ligações do Estado americano de que tal participação seria uma indelicadeza, o que atrasou por alguns minutos o debate do qual Assange participaria.