Eu registro, você filma, ele vai preso…

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

Demi Getschko, diretor presidente do Núcleo de Informação e Comunicação do Comitê Gestor da Internet no Brasil, Conselheiro do Comitê Gestor da Internet no Brasil, eleito representante de notório saber em assunto da Internet

Data da publicação: Julho de 2009 (*)

> *"A iniciativa de se regular a Internet do ponto de vista criminal é louvável, especialmente para coibir condutas graves. No entanto, ela traz em si riscos consideráveis. O caminho natural de regulamentação da rede, seguido por todos os países desenvolvidos, é primeiramente estabelecer um marco regulatório civil, que defina claramente as regras e responsabilidades com relação a usuários, empresas e demais instituições acessando a rede, para a partir daí definir regras criminais. O direito criminal deve ser visto como ultima ratio, isto é, o último recurso, que é adotado quando todas as demais formas de regulação falham. Nesse sentido, o caminho correto seria a partir do estabelecimento do marco civil, verificar o que teve efeito ou não de então adotar legislação criminal para regular a rede com base na experiência adquirida."*
>
> – Ronaldo Lemos, Carlos Affonso Pereira de Souza, Sérgio Branco, Pedro Mizukami, Luiz Moncau, Bruno Magrani, *Proposta de Alteração do PLC 84/99 / PLC 89/03* (Crimes Digitais) e *Estudo sobre História Legislativa e Marco Regulatório da Internet no Brasil*, Rio de Janeiro: Centro de Tecnologia e Sociedade, Escola de Direito, Fundação Getúlio Vargas, junho de 2009, p.4.

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

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

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

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

1 Por exemplo, listas de possíveis mau pagadores.

desse cadastro para nenhum outro fim que não seja diretamente relacionado ao contrato de serviços.

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

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

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

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

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

2 Conforme o relato da Safernet sobre a chamada Operação Turko: "Foram aproveitadas, por exemplo, apenas 34% das informações fornecidas pela NET, 43% dos dados da Brasil Telecom e 51% da Oi/Telemar. Somente os dados da Telefônica e da GVT atingiram 80% de utilização." Ver *https://pt.wikipedia.org/wiki/Opera%C3%A7%C3%A3o_Turko*

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

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

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

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

No primeiro caso, o registro ou "log" contém um identificador da conta do usuário (ou do contrato do usuário com o provedor de acesso), data, hora de início e hora de término da conexão a um serviço de acesso à Internet. Esse registro contém também o número IP designado ao modem do usuário no período. Notem que a designação do IP é ao modem do usuário, não ao computador ou aos computadores do usuário. A partir do modem, um roteador local pode redistribuir a conexão a vários computadores, e não há como atribuir a um computador específico que serviço está sendo utilizado a partir do registro de acesso.

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

Este registro de visitas contém em geral o número IP de origem, os dados de tempo, as páginas e serviços visitados, e através de cruzamento com bases de dados de nomes e números (automaticamente feito pelos programas de registro), este número IP revela o país de origem. É o mesmo número IP cadastrado em algum lugar do planeta por um provedor de acesso desse usuário. Ou seja, em tese, é possível associar os dois registros

entre si, mas não necessariamente associá-los à pessoa que realmente está fazendo a visita. E mais: esse visitante pode ser um "robô" automático de sistemas indexadores, como o Google ou o Yahoo. Pergunta a certos autores de projetos de lei: esses "robôs" deveriam cadastrar-se com identidade e CPF?

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

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

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

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

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

Se os provedores de conteúdo preservam os registros de visitas, se só preservam o suficiente para identificar origem geográfica ou qualquer outro critério de interesse, e por quanto tempo, é assunto para um bom debate. Mas se você entrar agora em um sítio Web da Transilvânia, o provedor de conteúdo da Transilvânia poderá registrar

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

automaticamente o IP de origem de sua conexão ao seu provedor de acesso e, se quiser, registrar quais as páginas ou diretórios do servidor você consultou. E um zeloso procurador de lá poderá solicitar ao provedor de acesso daqui o cadastro da pessoa física ou jurídica relacionado àquele número IP durante aquele período de conexão. Mas ele pode chegar ao provedor de acesso se este for uma "lan-house" à beira da rodovia Dutra? Ou se for um provedor de um hotel que fornece Internet gratuita nos apartamentos? Ou uma rede municipal que tem wi-fi aberto? Daí a chegar à pessoa real que visitou o sítio Web é um caminho quase impossível – lembrando que esses registros, se existirem, não são legalmente auditados.

O "log" de visitas, tal como é feito hoje, não deixa de ser uma violação de privacidade, se for possível associar o registro da visita a uma pessoa. O que você vê, onde você vai na Internet, é informação de natureza privada. A analogia, de novo, é que ninguém deve poder monitorar que revistas você folheia numa banca de jornais, ou que livros você consulta numa biblioteca.A pergunta a responder: quem é imputável por conteúdo supostamente ilegal, ou por uso ilegal de dados armazenados e, uma vez consensuado esse "quem" e assegurada a efetiva ilegalidade do conteúdo ou de seu uso indevido, como chegar inequivocamente ao indivíduo de origem, o "verdadeiro culpado"? O culpado, nesses casos, não é quem deu passagem (acesso) à Internet ou quem sediou conteúdo alheio. Não se processa a concessionária de uma rodovia por ter deixado passar um carro carregado de cocaína ou com milhares de DVDs contendo pornografia infantil.

Nem será processado o dono do estacionamento em que o carro assim carregado ficou por algum tempo. Se o conteúdo é ilegal ou foi obtido ilegalmente, cabe à justiça buscar o "dono" do conteúdo, ou o responsável pela obtenção dos dados, qualquer que seja o meio. Se há ilegalidade, cabe ao sediador cumprir a determinação da justiça de impedir que o conteúdo continue exposto, ou ceder informações sobre o acesso que possam estar registradas. Mas não cabe aos provedores – em nenhum ponto da cadeia de uso – exercer a censura prévia.

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

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

(*) Publicado em poliTICs nº 4, julho de 2009 – *https://politics.org.br/edicoes/eu-registro-voc%C3%AA-filma-ele-vai-preso*