Alguém observa enquanto você está on-line: as experiências da Coreia do Sul

*Por **Carlos Afonso** - Diretor Executivo do Instituto Nupef*

Data da publicação:

Fevereiro de 2013

A luta pelo Marco Civil da Internet no Brasil não terminou - pelo contrário, será acirrada nos próximos meses e no momento a vantagem pende para as operadoras de telecomunicações (contra a neutralidade da rede), apoiadas por alguns setores do governo federal, e para as empresas de midia (que defendem a responsabilização de intermediários e a retirada arbitrária de conteúdo da rede sem o devido processo legal).

O experimento conhecido como “verme de Morris”, no final de 1988, revelou a extrema vulnerabilidade da rede originalmente concebida, e desencadeou uma infinidade de processos para estabelecer mecanismos de proteção[1]. Podemos dizer que Robert Morris, hoje professor do MIT, “expulsou a Internet do Paraíso”. Surgiram então as firewalls em servidores e em computadores caseiros, as técnicas de monitoramento e controle, e uma gigantesca indústria de antivírus. Inevitavelmente descobriu-se que esse monitoramento poderia também permitir uso comercial ou político da bisbilhotagem, levando aos sistemas atualmente existentes de monitoramento e manipulação do tráfego de rede.

A neutralidade da rede tem sido rotineiramente violada na chamada “camada de enlace” da Internet - através da qual qualquer computador é conectado à Internet. A conexão é um serviço dominado pelas operadoras de telecomunicações, seja via cabo da TV por assinatura, ou através da linha telefônica, ou ainda por rádio digital (celulares, tablets, conexões via provedores wi-fi, conexões via satélite e outros). O texto de Heesob Nam sobre a bisbilhotagem do tráfego Internet na Coreia do Sul é revelador de uma situação rotineira em todo o mundo - o emprego de técnicas de inspeção profunda de datagramas (deep packet inspection ou DPI) para fins de controle, censura e eventual monetização do perfil de navegação dos usuários.

A violação de direitos na camada de enlace por parte das operadoras e grandes provedores vem de longe. Lembremos do caso AT&T denunciado pela Electronic Frontier Foundation (EFF) em 2006, de espionagem massiva de dados dos usuários a serviço da National Security Agency (NSA) dos EUA[2]. Nesse mesmo período surgiam denúncias de bloqueio do tráfego do Skype na rede da Brasil Telecom[3]. Coincidentemente, a BR Telecom utilizava o mesmo software que a AT&T usava para a bisbilhotagem de datagramas.

Em julho de 2012 o cientista-chefe da APNIC, Geoff Huston, denunciou a Telstra (principal operadora de telecomunicações da Austrália) exatamente por isso: praticar DPI sobre o tráfego de dados de seus usuários, catalogar os perfis de navegação e repassar esse cadastro a uma empresa canadense especializada em mineração de dados e monetização de perfis, a Netsweeper[4]. Essa escandalosa violação de privacidade (que pode até colocar em risco a segurança pessoal de milhares de usuários) foi reconhecida pela Telstra, que afirma não ter feito nada ilegal - o que indica que continuará a violar a privacidade de seus usuários e a adotar outras formas arbitrárias de controle sobre os dados trafegados por sua rede.

Em dezembro de 2012 a União Internacional das Telecomunicações (UIT/ITU), através de seu organismo que define padrões (ITU-T), aprovou em sessões fechadas uma norma para a bisbilhotagem dos dados que trafegam na camada de enlace. A norma Y.2770 sacramenta a DPI, estabelecendo um conjunto detalhado de regras para monitorar, inspecionar e manipular cada datagrama que passa por essa camada. Destina-se especialmente às empresas que produzem equipamentos e software de bisbilhotagem utilizados pelas operadoras e provedores.

Ao mesmo tempo, na Conferência Mundial sobre Telecomunicações Internacionais (WCIT), 89 países (entre os quais o Brasil) assinaram um novo tratado para regulação das telecomunicações (ITR), que requer a aderência aos padrões aprovados pelo ITU-T. Consultados sobre esse padrão de bisbilhotagem, membros da Anatel insistem que o Brasil assinou o tratado mas não está obrigado a cumpri-lo em sua totalidade e tampouco a seguir sem ressalvas a normatização respectiva. Isso é estranho - tratados internacionais são vinculativos. Que partes, que normas, que determinações o Brasil seguirá ou deixará de seguir?

Mesmo que a aprovação dos novos ITRs tenha sido na prática um fracasso (dos 193 Estados membros da UIT, uma maioria de 104 países não assinou ou absteve-se, entre estes os EUA, a Europa e Japão), qualquer país filiado ou não à UIT acaba seguindo os padrões desta, muitos dos quais têm crucial relevância para a operação da rede - exemplos são os padrões da série G.X para codificação da comunicação digital via ADSL ou via rádio digital, os codecs para transmissão de voz e vídeo, e muitos outros. Afinal, a Internet está “montada” em uma estrutura de telecomunicações normatizada por essa agência da ONU. A norma Y.2770 pertence à série Y.27X, dedicada à segurança das redes.

A assinatura do tratado por parte do Brasil, especialmente no momento delicado e muito difícil em que tentamos aprovar o Marco Civil com forte oposição de lobbies poderosos, deu a impressão que o Brasil disse ao mundo: ainda não aprovamos o Marco Civil, mas por coerência (ou por vinculação ao tratado) agora pelo menos a neutralidade da rede desaparecerá dele.

Mas não nos iludamos: a Coreia do Sul, a Austrália e os EUA não assinaram o tratado e são exemplos marcantes de violação da neutralidade da rede desde bem antes da normatização da ITU-T. Isso fica bem claro no artigo de Heesob. Vamos a ele.

INTRODUÇÃO

A Inspeção Profunda de Pacotes (conhecida como DPI, sigla em inglês de Deep Packet Inspection) é uma tecnologia que permite a um observador saber quem você é e o que você está fazendo online. Esta tecnologia não é neutra - no sentido de que tem sido desenvolvida e adotada por aqueles que tiram proveitos da possibilidade de vigiar em função de seu próprios interesses. Um destes interesses é ganhar o controle sobre os usuários da Internet; outro é o lucro comercial. O Estado, normalmente os órgãos do Executivo, beneficia-se da DPI, pois através dela obtém uma quantidade inimaginável de informações sobre as pessoas, o que é essencial para controlá-las. O propósito dos interesses comerciais ao usar a tecnologia DPI é simples: ganhar mais dinheiro. Com a DPI as empresas podem fazer mais dinheiro, expulsando concorrentes do mercado ou tirando melhor proveito de oportunidades para atrair mais clientes.

Durante os últimos quatro ou cinco anos, nós, sul-coreanos, testemunhamos inúmeras histórias de adoção da tecnologia DPI, utilizada tanto para a vigilância do Estado como também para a vigilância por parte de empresas. Este artigo tem como objetivo compartilhar as nossas experiências e lições. A história apresentada aqui não é uma história de sucesso. Ao contrário, mostra que o debate em curso sobre tecnologias de vigilância e seu resultado dependem em grande medida da reação dos defensores de uma Internet livre e aberta.

Para efeitos de contextualização sobre a indústria de telecomunicações da Coreia, é importante assinalar que para prestar serviços de telecomunicações ou ser provedor de serviços de acesso à Internet é preciso antes obter uma aprovação da autoridade reguladora. Em setembro de 2012, havia 119 provedores de acesso no país.

Entretanto, o mercado é dominado por três grandes provedores: Korea Telecom (KT), SK Telecom e LG U + . São estes os principais atores quando se fala na implantação das tecnologias DPI.

VIGILÂNCIA DO ESTADO: AS ESCUTAS NA INTERNET

Na Coreia a prática de escuta é estritamente proibida por lei. Conforme a Lei de Proteção da Privacidade das Comunicações (CPPA, por sua sigla em inglês), promulgada em 1993, escutas referemse a qualquer ato de conhecer ou gravar o conteúdo das comunicações eletrônicas de outros usando-se dispositivos mecânicos ou eletrônicos[5]. A definição de "comunicações eletrônicas" é ampla: cobre qualquer transmissão ou recebimento de qualquer tipo de som, texto, vídeo ou sinal por meio de fio, por redes sem fio, por fibra óptica ou qualquer outro meio eletrônico. Qualquer pessoa que efetua escuta telefônica sem autorização judicial e sem o devido processo legal pode ser condenada a pena de prisão de até dez anos ou a suspensão de qualificação de até cinco anos. Não é permitida a pena pecuniária no lugar da prisão. Autoridades como promotores de justiça, oficiais da polícia e de agências de informação não são exceção.

No entanto, a proibição estrita de escutas telefônicas não garante a total proteção da privacidade das comunicações. Para escutas telefônicas legais, a CPPA exige que as autoridades executoras da lei obtenham uma permissão judicial (ou uma aprovação do presidente, nos casos em que estrangeiros estão envolvidos), especificando como inspecionar, o que será inspecionado, por quanto tempo e em que medida a inspeção deve ser feita. No entanto, as autoridades policiais têm encontrado facilidade para obter dos tribunais a permissão de inspeção.

Por exemplo, em 2011, o Serviço de Inteligência Nacional (SIN) fez escutas telefônicas em 6.840 números de telefone. Isso equivale a 95,4% do total de inspeções feitas no país por autoridades encarregadas da aplicação das leis[6]. Este número reflete apenas a vigilância realizada por intermédio de provedores de Internet, a pedido do SIN - o que significa que a inspeção realizada pelo SIN sem passar pelos provedores não é contabilizada (note-se que o SIN possui mais de 30 equipamentos de inspeção, conforme foi revelado em 2010 por uma investigação do Congresso). De acordo com Della, um dos ativistas de privacidade mais proeminentes na Coreia do Sul, as autoridades que fazem investigação estão utilizando cada vez mais a Internet como alvo de suas escutas. Em 2011, o percentual de escutas na Internet foi superior a 60% do total de escutas realizada em serviços de telecomunicações. As autoridades investigadoras observaram os e-mails dos suspeitos e toda a sua navegação na Web. As ações de inspeção na comunicação móvel vão além de nossa imaginação. Quando algo suspeito acontece em uma determinada área, as autoridades policiais inspecionam todas as estações móveis dentro daquela área. Somente no ano de 2010, cerca de 39 milhões de números de telefones móveis foram inspecionados na Coreia.

Durante muito tempo após a promulgação da CPPA, em 1993, não sabíamos se a inspeção autorizada pelos tribunais (que é chamada de "medidas restritivas sobre a comunicação", nos termos da lei) incluía inspeção profunda de pacotes. Entretanto, durante um julgamento criminal em 2009, foi revelado que o SIN havia inspecionado cada mensagem de e-mail, toda a navegação na Internet e todas as conversas telefônicas do suspeito. Em outro caso, ficou provado que o SIN realizou inspeção profunda de pacotes por cerca de seis anos - de julho de 2003 a junho de 2009. Nesta situação, o SIN conseguiu obter a permissão da corte 36 vezes para inspecionar a mesma pessoa sob a mesma suspeita, que estava relacionada à Coreia do Norte. Surpreendentemente, o tribunal permitiu a inspeção da linha de Internet instalada na casa do suspeito, de duas contas de e-mail do suspeito, e da linha de conexão à Internet do local de trabalho do suspeito. Isso significa que o SIN pode capturar todos os pacotes que fluem através das conexões e assistir remotamente e em tempo real tudo o que está sendo exibido na tela do computador da pessoa.

Este caso causou polêmica sobre a legalidade da inspeção de pacotes. Em 2010, os membros da Assembleia Nacional organizaram uma discussão aberta, demonstrando como a inspeção de pacotes funciona. Os participantes da discussão podiam ver cada mensagem de e-mail e até mesmo a senha que um usuário digitou para entrar num programa de mensagens instantâneas – estes dados foram capturados e exibidos na tela do sistema de DPI. Alguns legisladores apresentaram projetos de lei para limitar a inspeção legal de pacotes. Uma proposta foi a de permitir a inspeção de pacotes somente quando um observador autorizado estiver presente.

Todavia os esforços legislativos não se concretizaram. Por isso, em 29 de março de 2011, defensores dos direitos humanos levaram o caso para o Tribunal Constitucional argumentando que a inspeção profunda de pacotes é inconstitucional porque a autorização judicial permitindo a inspeção de pacotes é equivalente ao mandado genérico de busca e apreensão, que é proibido[7]. Note-se que o argumento deles não era o de limitar o âmbito do

que é admissível em se tratando de DPI. Também não se tratava de aprimorar a vigilância judicial sobre o governo em questões envolvendo DPI. O argumento era simples e claro: a permissão para uso de DPI, por si só, é inconstitucional.

De acordo com a nossa constituição, um mandado judicial deve ser de alcance limitado, ou seja, deve especificar qual pessoa será inspecionada. No entanto, a inspeção profunda de pacotes em uma conexão de Internet permite a inspeção da comunicação de outras pessoas que compartilham a conexão, o que é comum em se tratando de conexão à Internet. Além disso, o controle deve ser limitado a certas comunicações - aquelas que são relevantes para o crime sendo investigado. Todavia esta relevância não pode ser determinada até que os investigadores olhem para o conjunto das comunicações feitas através daquela conexão e decidam que parte da comunicação é relevante. Portanto, o mandado que permite a DPI equivale a um mandado "genérico", que é inconstitucional - os freios e contrapesos judiciais não podem ser postos em prática, quando se trata de DPI.

MARKETING E DPI - O PHORM E A PUBLICIDADE DIRECIONADA

O uso de DPI para fins comerciais é outra ameaça à privacidade. Um exemplo que merece atenção é o uso de DPI para publicidade direcionada, que foi chamado em 2009 pela Korea Telecom de "QOOK SmartWeb[8]." A KT desenvolveu este sistema com base no sistema Webwise do Phorm[9], e tornou público o fato de que a KT já colocou em prática um serviço experimental desta tecnologia tendo como alvo milhares de clientes que vivem em Seul.

Muitas organizações da sociedade civil e especialistas expressaram suas preocupações sobre a potencial violação do direito à privacidade dos usuários porque a publicidade direcionada da KT baseava-se na inspeção e análise de termos de busca e comportamentos online dos usuários. Enquanto a KT, o Phorm e seus advogados argumentaram que não havia ameaça à privacidade porque o serviço foi aplicado apenas àqueles que consentiram ser alvo de seu uso, as organizações da sociedade civil obtiveram sucesso em mostrar que a publicidade direcionada viola a CPPA, que proíbe qualquer ato que busque conhecer e gravar a comunicação eletrônica alheia.

USO DE DPI EM BENEFÍCIO DO PROVEDOR DE SERVIÇOS INTERNET: O CASO DA SMART TV

Provedores de acesso à Internet usam a tecnologia DPI para seu próprio benefício. Eles anseiam por garantir suas vantagens de mercado da maneira que for possível, mesmo que isso signifique sufocar a concorrência.

Em 10 de fevereiro de 2012, a Korea Telecom bloqueou uma conexão à Internet feita através da smart TV da Samsung. De acordo com a KT, seu bloqueio foi legítimo, porque era muito provável que a smart TV gerasse tráfego excessivo (diz-se que a smart TV gera tráfego de 5 a 15 vezes maior do que a IPTV). Mas este argumento não foi razoável, porque a KT não bloqueou a smart TV da LG Electronics[10]. A Korea Telecom argumentou que tentou negociar com a Samsung sobre a taxa de uso de sua rede, mas a Samsung não quis negociar. Em 2010 e 2011, a Samsung vendeu cerca de 750.000 aparelhos de smart TV na Coreia e, para o serviço de smart TV, tinha 77 servidores alocados nos EUA e linhas alugadas da AT&T.

A KT pôde bloquear o tráfego de smart TV, simplesmente capturando pacotes com endereço de destino dirigidos para os servidores da Samsung e derrubando-os em seus quatro roteadores centrais localizados em Seul[11]. No dia seguinte, a Samsung foi à justiça e pediu uma liminar para proibir a KT de fazer este bloqueio - e o governo coreano, ou seja, a Korea Communications Commission (KCC) interveio no caso. Além disso, a opinião pública estava contra a KT.

Finalmente, em 14 de fevereiro de 2012, a KT suspendeu sua sanção à smart TV da Samsung, e a KCC decidiu em 4 de maio que o bloqueio da KT violara a Lei de Empresas de Telecomunicações, pelo fato de ter sido feito apenas ao tráfego da smart TV da Samsung e não ao tráfego da LG. Além disso, o bloqueio foi feito sem aviso prévio aos assinantes.

USO DE DPI E SERVIÇOS DE VOIP MÓVEL

O debate sobre serviços de voz sobre IP móvel (VoIP móvel) em 2012 mostrou como o DPI foi usado para o benefício das operadoras de telefonia, solapando o princípio da neutralidade da rede. O serviço KakaoTalk, que foi lançado em 2010 e tinha, em janeiro de 2013, cerca de 70 milhões de assinantes (sendo que 35 milhões só na Coreia), é uma aplicação de software para dispositivos móveis que permite aos usuários enviar e receber

mensagens, incluindo textos, fotos e vídeos. No ano passado, a KakaoTalk começou a oferecer também o serviço de chamadas gratuitas através de voz sobre IP. Mas as principais operadoras de telecom – a SK Telecom, a Korea Telecom e a LG U + - todas prestadoras de serviços de telefonia e de VoIP móvel, não perderam um minuto sequer. No dia seguinte ao lançamento do serviço de chamada gratuita da KakaoTalk , as três empresas estrangularam o tráfego de mVoIP da Kakao.

Segundo pesquisa da KakaoTalk, a taxa de perda de qualidade do serviço no primeiro dia de funcionamento do VoIPmóvel foi de aproximadamente um por cento – o que significa pouca dificuldade nas ligações. No entanto, a partir do segundo dia, a taxa de perda disparou para 20 por cento no caso da SK Telecom – e 54 por cento no caso da LG U + – , tornando a qualidade das ligações via Kakao demasiado pobre, impossibilitando a comunicação.

Ao contrário do caso da smart TV, a autoridade reguladora (KCC) apenas assistiu inerte, dizendo que a situação deveria ser resolvida de acordo com os mecanismos de autorregulação do mercado. Mas aos olhos dos defensores da neutralidade da rede, o bloqueio arbitrário de tráfego VoIP por parte dos grandes provedores de acesso à Internet é anti-competitivo e viola a Lei de Negócios de Telecomunicações, assim como ocorreu no caso da smart TV da Samsung.

Aproveitando a oportunidade, várias organizações da sociedade civil, especialistas e ativistas lançaram o Fórum dos Usuários para a Neutralidade da Rede (chamado de nnForum) e tomaram diversas medidas. Por exemplo, o nnForum pediu ao Conselho Nacional de Auditoria e Inspeção para investigar a KCC por negligência e abandono de funções, e levou a SK Telecom e a KT à entidade reguladora e à Comissão de Comércio Justo, apontando que estas empresas utilizaram mal seu poder de mercado à custa dos interesses dos consumidores. O nnForum também foi bem sucedido em tornar o princípio da neutralidade da rede uma das questões mais controversas durante a campanha das eleições presidenciais de dezembro de 2012.

USO DE DPI E AS REDES P2P

Este caso também envolve a Korea Telecom. Desde junho de 2012 a KT vinha planejando bloquear o tráfego de P2P em sua rede - e fez um contrato com a Sandvine[12] para testar seus serviços. Diz-se que a KT pagou três bilhões de wons sulcoreanos
(KRW)[13] para a Sandvine pelo teste do serviço de rastreamento de conexões Internet e que iria passar a usar definitivamente o equipamento da Sandvine no final de 2012, pagando em torno de KRW 80 bilhões.

Não se sabe como a KT pode bloquear o tráfego P2P. Ao consultar o centro de informações da KT foi-me assegurado que eles não olham o conteúdo dos pacotes de informações dos assinantes. Em vez disso, eles simplesmente tornam invisíveis aos prestadores de serviços P2P as informações sobre assinantes que instalaram programas clientes para a entrega da grade P2P. A entrega da rede P2P é implementada por programas específicos distribuídos por provedores de serviços Internet ou por prestadores de serviços de armazenamento de arquivos online. O que eu ouvi de um funcionário da KT (que está no comando da gestão de tráfego P2P da empresa) é que a tecnologia específica para implementar a gestão do tráfego P2P na rede da Korea Telecom é segredo comercial e que eles só olham para os endereços contidos no cabeçalho IP e não para o número da porta.

Ao contrário de outras práticas comuns de restrições ao tráfego P2P[14], o caso KT tem pouco a ver com a gestão de congestionamento de tráfego ou com proteção de direitos autorais. A KT considera que todos os indivíduos que instalaram o programa cliente de P2P não são assinantes individuais: são assinantes corporativos que devem pagar taxas maiores para a utilização de rede da KT, uma vez que a utilizam para fins comerciais.

Até o momento em que este artigo foi escrito, a KT não parecia ter implementado seu plano. Uma possível razão para isso pode ser o trabalho que o KCC está realizando, de um esboço de padrão para a gestão e utilização racional de redes de comunicação, que visa definir os detalhes da “orientação para a neutralidade de rede e para o gerenciamento do tráfego da Internet.” Para a Korea Telecom, seria melhor para sua reputação esperar até que a norma seja promulgada, porque o projeto da agência reguladora parece legitimar o seu bloqueio de VoIP móvel e de tráfego P2P. Na verdade, o projeto de lei enumera a restrição de VoIP móvel como uma das formas admissíveis de gerenciamento de tráfego. Membros de organizações da sociedade civil criticaram este projeto pela falta de transparência no seu processo de elaboração, uma vez que deixou-se de ouvir os diversos interessados, incluindo os usuários finais, tornando o gerenciamento de tráfego uma chave-mestra nas mãos dos provedores de acesso à Internet.

---

1. Ver em http://en.wikipedia.org/wiki/Morris_worm

2. Ver em http://www.wired.com/science/discoveries/news/2006/04/70619

3. Ver em http://www.abusar.org.br/skype_brt.html

4. Ver em http://www.potaroo.net/ispcol/2012-07/allyourpackets.html. Ver também http://bit.ly/LQtYR4

5. É interessante observar que a CPPA define “o ato de inibir a transmissão ou recepção na comunicação eletrônica alheia” como escuta. A nossa história legislativa falha em lançar luz sobre o significado desta frase e não há jurisprudência sobre este tipo de situação.

6. Ver em http://www.mediaus.co.kr/news/articleView.html?idxno=24942

7. Este caso envolve um indivíduo que é professor numa escola secundária e trabalha para o Sindicato Coreano de Pro fessores e Trabalhadores da Educação. A suspeita sobre ele era a de notória “apreciação” pela Coreia do Norte.

8. “QOOK” é uma marca do serviço de conexão à Internet da KT.

9. Para detalhes sobre o Webwise, visite http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf

10. No terceiro trimeste de 2011, o market share da smart TV da LG era de 14.4% enquanto que o da smart TV da Samsung era de 22.5 %.

11. Os roteadores eram modelo GSR12316 e o endereço IP bloqueado f oi o 210.118.88.200.

12. N.E. Empresa asiática que oferece produtos e serviços para provedores de Internet, entre eles plataf ormas tecnológicas para gerenciamento de tráfego. Ver em http://www.sandvine.com

13. N.E.: o que equivale a aproximadamente três milhões de dólares.

14. De acordo com BEREC (A view of traffic management and other practices resulting in restrictions to the open Internet in Europe, 29 May 2012), as restrições reportadas com mais frequência são o bloqueio e/ou o “estrangulamento” do tráfego P2P tanto em redes fixas quanto em redes móveis em função do gerenciamento de congestionamentos do tráfego nas redes.

Categoria:

- poliTICs 14