



## **Por democracia e liberdade na rede mundial de computadores**

A aprovação do Projeto de Lei Iniciado na Câmara (PLC) 89/2003, sobre crimes eletrônicos, representa uma ameaça a direitos fundamentais e traz regras que criminalizam o acesso legítimo a conteúdos digitais. O substitutivo de autoria do Senador Eduardo Azeredo (PSDB-MG) foi votado em 9 de julho pelo Senado Federal e agora segue para a Câmara dos Deputados.

Longe de ser a melhor solução para evitar crimes eletrônicos, o PLC 89 pode trazer graves conseqüências para o direito à privacidade, à inclusão digital, à comunicação, para o desenvolvimento e a inovação da internet.

Em nome do combate ao crime cibernético, em especial à pedofilia e à fraude eletrônica, o projeto restringe liberdades de cidadãos e cidadãs, ao abranger e tipificar uma enorme gama de práticas legítimas e até mesmo de políticas desejáveis para o desenvolvimento.

Como, a despeito da intenção dos legisladores, a lei será aplicada em toda a extensão territorial do país com base na sua redação final, a restrição de direitos dos cidadãos em termos genéricos pode representar grave ameaça à democracia. Mesmo após emendas que alteraram artigos que criminalizavam a troca de dados na internet, e a conseqüente redução de danos, o projeto continua configurando um obstáculo ao desenvolvimento da internet no Brasil. Não só por sua essência e caráter penais, mas também pelos artigos que legitimam a violação da privacidade, a criminalização de usuários, bem como por aqueles que protegem o setor financeiro em detrimento dos provedores de internet e usuários de serviços de bancos na rede.

Entre os principais problemas que a nova versão do projeto não conseguiu resolver estão as redações do art. 2º, que altera o artigo 285 do código penal, do 6º, que altera o famoso art. 171 da mesma legislação, e do art. 22.

Ao impedir o acesso não autorizado pelo “legítimo titular” a redes de computadores ou dispositivos eletrônicos protegidos, o art. 2º é tão genérico que destravar um CD ou DVD para ouvir em outro dispositivo ou desbloquear um celular, para utilizá-lo por outras operadora, poderão ser considerados crimes.

O art. 6º enquadra em crime de estelionato eletrônico quem “difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado”. Como a definição de “código malicioso” é muito vaga e ampla (“conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida”), um código necessário para destravar um CD, DVD ou celular poderá se enquadrar nela, criando brechas para criminalização de práticas legítimas. A indústria interessada em bloquear mídias e dispositivos poderá fazê-lo e, mesmo após o período de proteção, o usuário que quebrar as travas impostas a ele poderá ser considerado um criminoso. Pior que isso:

é sem precedentes a criminalização de “ato preparatório” - ou seja, não o crime em si, mas uma ação anterior necessária para cometê-lo, já que a mera difusão de código malicioso será considerada crime e não apenas a quebra do sistema.

Já o art. 22 obriga os responsáveis pelo provimento de acesso à rede mundial de computadores, comercial ou do setor público, a não só manterem os dados de endereçamento eletrônico e hora de cada conexão efetuada, como a “informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indício de prática de crime [que tenha ocorrido no âmbito da rede por que é responsável]”. Essa é uma clara violação ao art. 5º, inciso X, da Constituição Federal, segundo o qual são “invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

O artigo dá margem para absurdos como a identificação prévia de todos os usuários da rede como potenciais suspeitos de crimes. Para fazer um paralelo com o mundo não virtual, imagine se um segurança privado tivesse que solicitar a identificação de cada cidadão a cada vez que este circulasse por um determinado bairro. E empresas teriam o registro de quem passou por ali, a que horas e, no caso de ocorrência de crime na região, todos os transeuntes daquele horário seriam potenciais suspeitos! Sem contar a possibilidade de um desastroso vazamento ou comercialização de bancos de dados com hábitos de internautas. No mundo físico, não há precedentes de tamanha restrição à privacidade e à liberdade. Por que então isso poderá ser feito na internet?

Para agravar o problema, o artigo 22 obriga os provedores de acesso a manter o controle de dados e de navegação de todos os usuários que fizeram uso da rede. Assim, cada lan-house, telecentro, administração municipal das cidades digitais ou qualquer um que forneça rede sem fio (wi-fi) terá que solicitar informações cadastrais de usuários e controlar todos aqueles que utilizam a rede a cada momento, durante três anos. O projeto de lei obriga o provedor, empresa que oferece serviço de acesso à internet em cada região, a fornecer os endereços das máquinas que redistribuem a conexão.

Na prática, o projeto inviabiliza uma série de avanços no que diz respeito à inclusão digital em milhares de municípios brasileiros, na contramão das iniciativas que buscam a universalização da banda larga para a população. Assim, o que seria uma política desejável, de expansão de acesso à rede, passa a ser desencorajada pelo projeto que representa a o primeiro grande marco regulatório da internet no Brasil.

Vale ressaltar que, na mesma madrugada em que foi votado o PL 89/2003, foi aprovado também o projeto de lei 250/2008, proposto pela Comissão Parlamentar de Inquérito (CPI) da Pedofilia. Ele contou com o apoio de entidades que atuam no combate a este crime na rede, como a Safernet, diferentemente do 89/2003, já que a compreensão é de que este último, a despeito de ter sido defendido sob o baluarte do combate à pedofilia, extrapolava seus objetivos mais latentes e restringia a liberdade dos usuários.

Para além do projeto 250/2008, já há mecanismos de legislação específica que permitem a investigação de crimes que este projeto de lei busca tipificar. Parece razoável aplicá-los ao universo eletrônico, garantindo especial atenção à fraude e à



pedofilia. Mas não: o projeto qualifica como crimes práticas bastante genéricas, dando margem às mais diversas interpretações, e não define, ou o faz de maneira muito difusa e pouco clara, o que são “titular da rede”, “restrição de acesso”, “código malicioso”, “dado eletrônico alheio”.

Assim, partindo diretamente para a esfera criminal, sem que tenhamos criado sequer um marco regulatório civil para a Internet, o Brasil segue na contramão da maior parte dos países desenvolvidos, que primeiro regulamentaram o uso da internet na esfera civil, para depois estabelecer regras no direito penal.

Em se tratando do primeiro grande marco regulatório da internet no país, esta poderia ter sido a grande oportunidade de se avançar na regulamentação dos direitos civis dos cidadãos e usuários da rede. Mas, ao contrário, o projeto, em vez de garantir a privacidade, legitima a sua violação. Em vez estimular a inclusão digital, a desencoraja.

As inúmeras tentativas de alterar e corrigir falhas do projeto realizadas até o momento mostraram-se frustradas e ineficazes. Isso porque seus pressupostos penais, sua estrutura 'frankenstein' e suas definições abrangentes inviabilizam a sua transformação em um fundamental e bom marco regulatório para a internet no Brasil. Agora, cabe aos nossos representantes na Câmara dos Deputados a responsabilidade de não aprovar projeto de lei tão oneroso à democracia e à liberdade na rede mundial de computadores, à inclusão digital e ao desenvolvimento do país.

Brasil, 22 de julho de 2008  
Intervozes – Coletivo Brasil de Comunicação Social