Triangulação no acesso à internet - Aspectos positivos e negativos

Por Paulo Sá Elias,

A agência de notícias *Reuters* divulgou recentemente uma notícia assinada por *Tamora Vidaillet* que a suspensão da censura imposta pelo Governo Chinês a determinados *websites* estrangeiros tinha validade somente durante a realização da reunião da APEC (Cooperação Econômica Ásia-Pacífico). Assim, como de costume, logo após o término da reunião, o governo chinês voltou a proibir o acesso a diversas páginas na Internet.

A notícia me fez lembrar dos serviços prestados pela *Safeweb (www.safeweb.com)* [1]. A triangulação no acesso à Internet permite que um usuário tenha acesso a determinado endereço "proibido" ou que deseja privacidade por meio de um terceiro servidor que fará por ele a conexão, recebendo e enviando os pacotes de informações, em regra criptografados (escritos de forma cifrada, em códigos e de difícil decriptação), para seu computador. Desta forma, se eventualmente alguém interceptar a conexão do usuário com o seu provedor, seja discado ou ADSL (banda larga), estará diante do seguinte cenário: o usuário "x" o tempo todo conectado em um só endereço (o da *Safeweb*, por exemplo, caso este seja o serviço de triangulação escolhido) e trocando informações criptografadas. Resultado: para fins periciais nada poderá ser esclarecido. É o drama. Volto a ratificar que a questão probatória é o grande problema nestas questões de Internet e informática.
A maioria dos criminosos que atuam na Internet, além de utilizar técnicas variadas, como alteração do cabeçalho dos pacotes do IP (*IP Spoofing)*, utilizam o recurso apresentado acima. É importante ressaltar que o serviço prestado pela *Safeweb* tem grande importância para garantir a liberdade de comunicação na Internet. Um exemplo clássico é o caso da censura imposta pelo governo chinês. Sobre o tema, inclusive, testemunhamos a favor de *Safeweb* (http://fugu.safeweb.com/sjws/solutions/testimonials_safeweb.html). O serviço é indispensável e de relevada importância. *Importante lembrar que a empresa prestadora do serviço pode ser obrigada judicialmente a fornecer informações que facilitem a identificação do usuário, principalmente agora, após os atentados terroristas nos Estados Unidos que deram ensejo a diversas alterações na legislação norte-americana no tema.*

Por isso que sempre dissemos que a apreensão tempestiva dos computadores dos criminosos, quando identificados, especialmente de sua unidade de disco rígido pode ser de vital importância para manter a integridade de eventual conteúdo probatório residual. Vide: (http://tolvanen.com/eraser) - *software* que parece capaz de apagar "definitivamente" dados em discos rígidos. Não se deve aceitar a apresentação, tão-somente, da unidade de disco rígido, já que obviamente é possível a apresentação de outra unidade. Importante a apreensão inesperada e tempestiva do computador, a fim de evitar formatação, substituição de unidade de disco rígido, etc. Me lembro de um lojista na avenida Paulista, em São Paulo, capital, que possuía em seu computador um *winchester* (unidade de disco rígido) removível em uma bandeja. Por mais inacreditável que possa parecer, havia um orifício na torre do computador. Dizia ele que com a chegada da fiscalização, bastava "*puxar o 'winchester' e colocar outro no lugar*". Segundo ele, a operação acontecia em razão de determinadas

informações de interesse fiscal que eram armazenadas na unidade de disco removível. Vejam a criatividade criminosa.
Por fim, é possível ainda que os autores de crimes pela Internet utilizem "*cyber*cafés", locais públicos para acesso à Internet, tais como livrarias e *shopping centers* para dificultar o rastreamento. Ressalte-se, por oportuno, que determinados serviços desta natureza possuem sistema de circuito fechado para filmagem dos usuários (com gravação e arquivo das imagens por determinado período de tempo). Tal informação, associada a testemunhas e outros dados probatórios podem ser úteis nas investigações de delitos do gênero.

O contato com os provedores de Internet também é indispensável, já que é possível encontrar tecnicamente rastros de determinadas operações em "trilhas de auditoria - *log*" e outras informações importantes nos servidores.

Paulo Sá Elias é Professor Universitário de Direito, advogado especialista em Direito da Informática e Tecnologia da Informação.

[1] Importante citar a *Anonymizer* (www.anonymizer.com), que funciona desde 1996. Mas atualmente os serviços prestados pela *Safeweb* são bem melhores em nossa modesta opinião técnica, além de totalmente gratuitos

Fonte: http://www.direitonet.com.br/doutrina/artigos/x/48/55/485/