Falta de lei e de informação beneficiam o cibercrime

Spacca" data-GUID="leonardo_bueno_melo.jpeg">A falta de legislação específica e de conhecimento técnico por parte de autoridades dificulta e compromete a eficiência do combate aos crimes cometidos por meio da internet. É o que afirma o perito criminal da Polícia Federal **Leonardo Bueno de Melo**, especialista em perícia em informática.

Segundo ele, o crime de pedofilia é uma mostra de que o atraso da legislação do país impõe barreiras que comprometem as ações policiais. Pela lei atual, é preciso provar que houve publicação ou divulgação do material de pornografia envolvendo criança para configurar crime.

Ou seja, não basta a Polícia achar o material do computador, tem de provar que ele foi transmitido e divulgado. Isso pode mudar, contudo, pode mudar com a aprovação do projeto de lei do senador Eduardo Azeredo (PSDB-MG). Pelo texto, ter as imagens armazenadas já é crime. O Senado aprovou o projeto de Azeredo, que tipifica 13 novos crimes, no começo deste mês. Há 10 anos em gestação no Legislativo, a proposta precisa ainda passar pelo crivo da Câmara dos Deputados.

O principal avanço do projeto, segundo Bueno de Melo, é adequar a nossa legislação para permitir a assinatura da Convenção de Budapeste que prevê cooperação entre diversos países no combate aos crimes cibernéticos. A proposta tipifica crimes como o acesso não autorizado a computadores e a difusão de códigos maliciosos, além de obrigar provedores a guardar informações, por três anos, para futuras investigações.

Recém indicado como instrutor do Grupo de Trabalho Latino-americano de Delitos Tecnológicos da Interpol, Bueno de Melo trabalha há cinco anos no combate ao crime cibernético em Brasília. Chefe substituto do Serviço de Perícias em Informática do Instituto Nacional de Criminalística, em entrevista à revista **Consultor Jurídico**, Bueno de Melo falou sobre crimes cibernéticos e o trabalho da Polícia no seu combate.

Leia a entrevista

ConJur — O país está preparado para lidar com os cibercrimes?

Leonardo Bueno de Melo — Temos duas grandes dificuldades. Uma delas ainda é o relativo desconhecimento técnico da Polícia, do Ministério Público, do Judiciário e até mesmo dos advogados de defesa de acusados. A outra dificuldade está na legislação, que impede uma ação rápida da Polícia. No caso dos crimes de informática, a ação rápida é crucial. As evidências digitais são voláteis. O site hoje está no ar, amanhã não está mais. O registro de uma mensagem de e-mail enviado pode ou não ser armazenado no computador, mas por limitações de custo, esse registro não fica muito tempo guardado.

ConJur — Até que ponto o desconhecimento técnico atrapalha?

Bueno de Melo — O desconhecimento técnico aliado à legislação deficiente que temos hoje faz com que aconteçam coisas como no caso da Operação Cavalo de Tróia [*que prendeu 26 pessoas acusadas de praticar fraudes bancárias pela internet*]: a pessoa é presa quatro, cinco vezes e, por alguma dificuldade de enquadramento legal, ou pelo não entendimento completo da situação por parte das autoridades, a pessoa é solta novamente. Isso incentiva esse tipo de crime, porque os lucros são muito grandes e o risco acaba sendo compensador.

ConJur — Dê um exemplo de deficiência na legislação para combate aos cibercrimes?

Bueno de Melo — Hoje em dia o crime de pedofilia se caracteriza pela publicação ou divulgação de material de pornografia envolvendo criança. O simples fato de a pessoa ter esse material não é crime. Então, no caso de crime cibernético, isso dificulta. Porque é preciso achar prova de que aquela mensagem foi transmitida. O fato de simplesmente achar a mensagem no computador da pessoa não configura crime. Para provar a transmissão da mensagem é preciso atuar junto ao provedor de serviço de internet que essa pessoa utiliza para fazer algum tipo de interceptação telemática.

ConJur — E como tem sido o trabalho junto aos provedores?

Bueno de Melo — Esbarramos em outra dificuldade, também legal, de conseguir a quebra de sigilo. Os provedores hoje, por falta de legislação, não têm obrigação de manter essas informações armazenadas para serem disponibilizadas para a Polícia. Muitos provedores exigem mandados judiciais. Quando começa a investigação, nós não temos o endereço da máquina, temos apenas o endereço IP (Internet Protocol), que permite identificar a localização do computador. Muitas vezes, por conta da burocracia, entre o momento em que a gente fez o levantamento dos IPs e o momento em que a gente foi na casa das pessoas, passaram-se alguns meses. E aí a pessoa pode ter vendido o computador ou formatado o Windows. Nós dependemos do provedor para fazer a conversão do endereço lógico da máquina para o endereço físico. Hoje, tentamos intercalar a investigação puramente digital com a investigação tradicional que envolve, por exemplo, escuta telefônica e campana, onde os policiais acompanham a pessoa. Muitas vezes se recorre à investigação tradicional mais do que se deveria por deficiência no levantamento de informação junto aos meios digitais.

ConJur — Qual a expectativa com a nova legislação?

Bueno de Melo — O projeto do senador Eduardo Azeredo (PSDB-MG) tem a grande meta de adequar a nossa legislação para permitir a assinatura da Convenção de Budapeste [*que regulamenta a troca de informações sobre crimes cibernéticos entre os países-membros*]. Eu acho que é extremamente válido justamente porque vai favorecer o fortalecimento da cooperação internacional. É fundamental trabalhar junto com outros países.

ConJur — Em comparação com outros países, como está o Brasil no que diz respeito ao combate aos crimes cibernéticos?

Bueno de Melo — Em relação aos equipamentos, o Brasil está alinhado aos mais avançados países do mundo. Hoje temos computadores, softwares e equipamentos especializados para toda a parte de perícia. Em relação à capacitação técnica, também temos uma posição de destaque, inclusive anualmente organizamos uma conferência internacional bastante grande, a ICCyber (Conferência Internacional de Perícias em Crimes Cibernéticos). Essa conferência é a maior da América Latina e a do ano passado teve mais de 700 participantes de mais de 22 países.

ConJur — Então, o que falta ao Brasil?

Bueno de Melo — O país tem um nível de capacidade técnica bastante grande, porém, ainda não é o ideal. Precisamos melhorar muito e temos limitações por conta das questões legais. Acreditamos que, com a aprovação da nova lei, vamos estabelecer contatos internacionais importantes. Vai haver um salto muito grande na efetividade das nossas ações.

ConJur — Mas já não há uma rede de troca de informações com alguns países?

Bueno de Melo — O Serviço de Perícias em Informática (Sepinf) faz parte de uma rede 24 por sete de contatos (contato 24 horas, sete dias por semana), criada pelo G8 [*grupo dos sete países mais desenvolvidos do mundo e a Rússia*], cuja função é basicamente a preservação de evidências. A rede de contatos do G8 obviamente não tem o poder de fazer com que seja realizada uma busca e apreensão em outro país. E outros países também não podem requerer isso aqui. Essas ações dependem de acordos internacionais, de cartas rogatórias e outros instrumentos. Mas, pelo menos, essa rede de contatos nos aponta uma pessoa conhecida em outro país para a qual a gente pode ligar, conversar e esclarecer alguma dúvida técnica sobre as possibilidades de levantar alguma informação lá. Ajuda porque podemos pedir para essa pessoa entrar em contato com determinado provedor e solicitar que ele preserve informações até que os trâmites burocráticos legais sejam cumpridos para liberar as informações.

ConJur — O que já se obteve de concreto por meio dessa rede?

Bueno de Melo — Esbarramos de novo na questão da legislação e da cooperação. Precisamos recorrer ainda a cartas rogatórias e aí o trâmite se arrasta por alguns anos. Infelizmente, não tenho notícia de alguma coisa que tenha sido efetivamente solicitada por essa rede e respondida a tempo de ter algum

efeito prático e útil.

ConJur — E a parceria entre as instituições no Brasil, como entre a Polícia e o Ministério Público, tem funcionado bem?

Bueno de Melo — O sucesso das ações nessa área depende muito do promotor, do procurador ou do juiz que está encarregado do caso. Se eles têm conhecimento um pouco mais aprofundado, geralmente consegue-se com muito mais facilidade as quebras de sigilo e os mandados de busca e apreensão que precisamos. Quando eles não conhecem muito bem a realidade da informática, ficam mais receosos por medo de cometer algum abuso em relação ao direito de privacidade. Mas as promotorias dos estados estão em movimento grande para criar unidades internas específicas para tratar de cibercrimes, o que é uma coisa boa. Eu sempre recebo promotores interessados em saber mais sobre equipamentos, especificação de laboratório e quais seriam os requisitos que eles precisariam para atuar nessa área.

ConJur — Onde entra o trabalho do perito em informática neste contexto?

Bueno de Melo — Antes de ser perito em informática, ele é perito criminal. Então, quando necessário, está capacitado para fazer outros tipos de perícia. Além de perito, ele é policial e muitas vezes se vê obrigado a desempenhar funções também típicas de policial, principalmente quando estouram operações. O sujeito não vai para as operações para fazer perícia, vai fazer apreensão. Vai como técnico que sabe o que deve ser apreendido e o que não deve. A função dos peritos de informática exige uma série de conhecimentos, não só de internet e de rede, mas de criptografia. O perito tem que ter um conhecimento bastante profundo dos sistemas operacionais para poder recuperar arquivos apagados ou corrompidos. Hoje nós somos 137 peritos no país. É insuficiente ainda. Mas há cinco anos eram 30 os peritos.

ConJur — A Polícia já identificou um perfil de quem está envolvido com crimes na internet no Brasil?

Bueno de Melo — São pessoas de bom nível social. E recentemente temos identificado que têm conexões internacionais. Hoje há dois grandes crimes praticados pela internet: a pedofilia o *fishing scam*. No caso da pedofilia, não há intenção de lucro, de aproveitamento financeiro na maior parte dos casos. O *fishing scam* é uma forma de infectar a máquina para roubar informações dela. São esses os dois grandes problemas do Brasil. No exterior já há uma preocupação muito grande, que aqui ainda não estamos enfrentando, que seria o próximo passo em relação ao *fishing scam* — a chamada *botnets*.

ConJur — E o que é *botnets*?

Bueno de Melo — É o uso do *fishing scam* ou de alguma outra técnica que, no lugar de procurar obter informações de senha bancária ou cartão de crédito, tentar instalar um vírus ou código malicioso na máquina para que ela possa ser controlada remotamente. Criam-se verdadeiros exércitos de máquinas infectadas. O usuário não tem a menor idéia que o computador está infectado porque ele continua funcionando normalmente. Mas é aberta uma porta lógica, um canal com o criminoso, que tem milhões de máquinas infectadas e usa isso basicamente para extorsão. Ele liga para o dono de um site comercial

grande e pede dinheiro para não tirar o site dele do ar. Se a pessoa não paga, o criminoso dá um comando para os milhares de computadores e todos acessam o site ao mesmo tempo. A conseqüência da ação é que os servidores não suportam e o site sai do ar. Se for um site de vendas online, principalmente site de comércio eletrônico, o prejuízo é muito grande. No Brasil isso ainda não está em nível preocupante. O que há de mais comum no Brasil são e-mails “clique aqui”, para roubar senhas bancárias.

ConJur — Gostaria que explicasse como, por meio do IP, se consegue localizar os endereços físicos dos computadores?

Bueno de Melo — O responsável por essa tradução é o provedor de internet. Cada computador tem que ter um endereço IP para fazer uma conexão válida, mandar e receber dados. O endereço IP é formado por quatro números de três dígitos cada um. Existe um organismo que é responsável por fazer a distribuição desse endereço de IP aos provedores de internet, aos órgãos públicos e aos países. Então, o Brasil recebeu o intervalo de endereço de IPs que ele pode usar para os computadores daqui acessarem a internet. Existe também aqui o Comitê Gestor da Internet que, junto com algumas outras entidades, faz o controle. Como o número de IPs é limitado, o que as empresas fazem para economizar IP é usar IPs dinâmicos. Ou seja, o usuário só recebe um IP quando acessa a internet. Com o computador desligado, o IP é liberado, o provedor pega de volta, e o atribui para outro assinante. Então, só o provedor sabe qual assinante estava usando determinado IP em determinada hora. A NET, que é uma empresa grande, guarda o registro e abre mediante ordem judicial. Mas provedores pequenos, de cidades de interior, por exemplo, não guardam esses dados. E a Polícia nada pode fazer porque não há lei que o obrigue a armazenar os dados.

Date Created
20/07/2008