Crime na internet ocorre por negligência de usuário

13/06/2007

Vive-se, atualmente, uma realidade global, matizada pela realidade local. Tanto isso é verdade que a própria internet é, a despeito de seu potencial de universalização, mais do que nunca, regional, consoante se pode comprovar a partir das estatísticas levantadas pelos trabalhos efetuados por firmas de IP *geotracking*. Estas são especializadas em pesquisar onde estão os consumidores do comércio eletrônico e de conteúdo eletrônico. Tal argumento pode ser extraído da obra *Who controls the Internet?*, de Tim Wu e Jack Goldsmith, professores de Direito na Columbia Law School e Harvard Law School, respectivamente.

Em uma sociedade global do risco, os crescentes avanços tecnológicos, como é o caso daqueles oriundos da ciência cibernética (ciência da automação e do controle), que engloba a informática e a telemática, fazem com que, a cada dia, para a realização do que antes era uma simples transação bancária, o cidadão comum enfrente novos gravames que foram admitidos por essa mesma sociedade pós-industrial, pautada, em verdade, pelos denominados riscos permitidos.

Descrevendo, analisando e criticando essa nova configuração estrutural, Ulrich Beck, famoso sociólogo tedesco, cunhou o termo *Risikogesellschaft* e Enrique Roviro del Canto, doutrinador espanhol, vislumbrando o âmbito da criminalidade cibernética, acrescentou ao termo "sociedade global do risco" os verbetes "informático e da informação". Ter-se-ia, então, atualmente, uma "sociedade global do risco informático e da informação".

Esses novos riscos imprevisíveis engendram, por conta da perplexidade social surgida, uma inflação de leis penais e uma notável expansão do Direito Penal, que, de forma, muitas vezes, simbólica, é utilizado como verdadeira panacéia para toda sorte de problemas, em vez de se manter como baluarte de um Estado Social e Democrático de Direito, como *ultima ratio*, no combate a fatos típicos, antijurídicos e culpáveis que causem lesões a determinados bens jurídicos penalmente relevantes.

O cidadão perplexo, vez por outra, acaba figurando como vítima dessas novas realidades tecnológicas, sendo certo que apenas as admitiu. Nada decidiu sobre a entrada desses *gadgets* em sua vida.

Em tempo, a "vitimodogmática" pode ser entendida como uma série de postulados de "vitimologia", por meio da qual se estuda o comportamento da vítima em face do ilícito penal, mais precisamente, os graus de sua contribuição para que esse fato delituoso acontecesse.

Voltando à figura do cidadão comum, nos dias de hoje, ele deixa de ir ao banco, evitando perda de tempo e dissabores como filas e possibilidades concretas de assaltos à mão armada, situações fáticas notadamente comuns em grandes cidades. Isso por conta, também, da decisão anterior de terceiro, no caso o sistema bancário, pelo *downsizing* e pela irreversível automação (essa decisão humana foi tomada sem qualquer participação do usuário, que apenas se sujeitou

a tanto).

O preço dessa comodidade, contudo, é o risco potencial de utilizar, em sua residência, ou em seu local de trabalho, quiçá, para os mais incautos, em um ambiente de rede sem fio (*wireless*), um sistema computacional comprometido, algo que pode levar à obtenção, por terceiros, de dados sensíveis desse usuário e dos próprios valores de sua conta bancária.

Como é cediço, mais de um bilhão de *e-mails* são enviados diariamente, mundo afora, e grande parte dessas missivas eletrônicas são correspondências indesejadas, os denominados *spams*. Muitos destes, são enviados por grupos especializados ou por indivíduos conhecidos por *spammers*. Já se fala em *spam gangs*, grupos especializados que mudam de denominação quase que diariamente.

Também se noticia, por conta disso e com algum estardalhaço, a futura criminalização da atividade de *spam*. E dá-lhe Direito Penal!

No bojo de muitas dessas correspondências indesejadas há programas de computador, tais como *viruses* e *worms*, conhecidos, também, como *malwares*. Após serem descarregados nos computadores dos usuários, sempre por meio de algo que atraia a atenção desse cidadão (e exemplos não faltam, seja pornografia, promoção de compra, mensagem ou cartão virtual de pretenso conhecido), passam a executar instruções naquele ambiente computacional da vítima. Tudo isso em prol dos interesses de lucro dos *cybercriminals*, valendo-se esses verdadeiros quadrilheiros do famoso golpe “clique aqui”. Até o nome do Departamento de Polícia Federal (DPF) já foi utilizado.

Com isso, tais programas maliciosos passam a executar as mais diversas instruções, normalmente em modo *background* (segundo plano), o que impede, até mesmo para o mais arguto e paranóico usuário, a detecção de tais coletas de dados sensíveis e encaminhamento aos criminosos cibernéticos dessas informações, por intermédio de *e-mails*, desta feita para uma conta de correio eletrônico, adredemente criada pelos criminosos cibernéticos. Então, eles poderão fazer uso ilícito de tais dados e senhas, para fins de obtenção de vantagem patrimonial indevida, normalmente, por meio de “laranjas”.

Tudo sem qualquer violência ou grave ameaça à pessoa!

Naturalmente, que o crime organizado já percebeu, há tempos, que o filão e o bordão agora é “invada o sistema computacional do elo mais fraco, o usuário, em vez de tentar invadir o sistema bancário (seja pela porta giratória, seja pelo ambiente computacional)”, cujos sistemas de segurança da informação são praticamente insuperáveis. Isso se deve ao astronômico valor investido nessa seara, sendo certo que não há invasão computacional relatada desde os primórdios do sistema *on-line* de transações eletrônicas bancárias, nos idos do primeiro lustro da década de 90 do século passado, talvez por uma clara opção desse modelo de negócios, não se sabe ao certo.

Ademais, é cada vez mais comum a cooptação, por parte de quadrilhas especializadas, antigamente, em assalto a bancos, de técnicos e de pessoas com profundo conhecimento de ambientes de redes de computadores, de segurança da informação, de programação de computadores e, também, de criação de sistemas operacionais. Essas pessoas são recrutadas para fins de cometimento de grandes golpes no ambiente virtual e as cifras anuais são estimadas na casa das centenas de milhões de reais.

Tal cooptação de pessoal com conhecimentos técnicos pode ocorrer por meio de ameaças, bem assim por compartilhamento de ganhos financeiros, consoante pode ser constatado a partir da atuação profícua da Unidade de Repressão a Crimes Cibernéticos, do Departamento de Polícia Federal, que, em apenas dois anos de atuação, já prendeu mais de seiscentos "*crackers*" e "laranjas".

Da análise do perfil desses criminosos com profundo conhecimento técnico, percebe-se que alguns entraram para essa modalidade de crime por ganância, outros foram, de fato, cooptados sob ameaças a eles infligidas ou a seus familiares.

Sendo certo que, a despeito de inúmeras prisões, tais delitos apenas crescem, exponencialmente, coloca-se o problema da atuação preventiva, tanto do Estado, quanto da sociedade civil organizada e, é claro, do vislumbrado elo mais fraco, o próprio usuário de ambientes computacionais.

Surge, aqui, a questão central deste artigo, a saber, a possibilidade de autocolocação em risco da pretensa vítima imediata de *phishing scam*.

Ora, qualquer cidadão, mesmo que detentor de poucas luzes, sabe que viver em nossa sociedade pós-industrial é viver sob riscos, pois esses gravames permitidos apenas crescem mais e mais, frutos que são de avanços tecnológicos inexoráveis. Nos tempos atuais a tecnologia incide, qual verdadeira espiral, sobre a base de conhecimentos tecnológicos, disso gerando invenções e inovações, em um ritmo inacreditável.

O sistema de voz sobre IP (voIP) está presente em nossas vidas há poucos anos, mas é apto para demonstrar algo que era, até então, inimaginável. O repensar do modelo de negócios da telefonia internacional convencional.

No que concerne aos novos riscos permitidos, a *mass media* está aí, diariamente, para alertar a cidade acerca dos inúmeros riscos, sejam naturais, sejam criações de decisões humanas.

João Guimarães Rosa já alardeava que "viver é muito perigoso", em sua obra prima, isso nos idos da década de 50 do século passado. Na sociedade pós-industrial pode-se bradar que "viver é muito mais perigoso", pois os riscos são globais e muitas vezes a vítima imediata sequer contribuiu para que tais riscos existissem, ela apenas aceitou a existência de tais riscos, os denominados riscos permitidos (cada vez mais amplos e comuns hoje em dia).

Em certas situações, contudo, é fácil constatar que a potencial vítima exerce papel na consecução do delito, a despeito de seu grau de instrução formal, que é normalmente alto, no âmbito dos crimes cibernéticos de cariz patrimonial.

Alessandra Orcesi Pedro Greco assevera que “por meio do estudo da evolução do conceito de vítima, percebemos que hoje ela não pode mais ser entendida como um ser inerte face ao crime; observamos que não só ela interage com o autor do crime, como, em alguns casos, pode até criar o risco para si própria, colocando-se em uma situação que a levará ao resultado danoso”.

Nada mais verdadeiro, mormente em uma nova tônica de Direito Penal supra-individual, em que os bens jurídicos a serem protegidos não estão relacionados com sujeitos passivos facilmente individualizáveis, mas, sim, por número indeterminado de pretensas e potenciais vítimas.

Muitas vezes é exatamente o que ocorre nas situações que levam à consumação do delito de furto qualificado mediante fraude (alguns entendem tratar-se de estelionato), nos casos de *phishing scam*.

Dos estimados 250 milhões de usuários de computadores conectados à internet, mundo afora, por meio de serviços de banda larga, e que efetuam suas movimentações bancárias através de serviços *on-line*, quantos desses têm instrução formal baixa ou desprezível? Uma provável minoria, certamente.

Por que, então, os crimes de *phishing scam* seguem crescendo? Por que, afinal, o “clique aqui” é, ainda, um perigo real tão grande, a despeito da maciça informação disponibilizada a esses usuários?

Parte desse problema diz respeito, talvez, à autocolocação em risco da vítima imediata dessa modalidade criminosa.

O incauto “navegador” que resolve utilizar seu ambiente computacional para realizar transações bancárias *on-line*, por meio da rede mundial de computadores, sem que cuide de manter atualizados seus sistemas operacionais, seus aplicativos de detecção de intrusões e de detecção de vírus de computador, que abre arquivos anexos e clica em *hiperlinks* em mensagens de *e-mails* recebidas, que não cuida de deixar sua condição de verdadeiro analfabeto funcional da “sociedade digital” (pois o nível de conhecimento de micro-informática e de segurança da informação de inúmeros usuários é inacreditável, em termos negativos), certamente, toda vez que estiver se valendo do ambiente computacional, na Internet, estará, também, colocando a si próprio em risco (e, quiçá, muito além do permitido), contribuindo, dessa forma, para a consecução do delito, afastando-se assim a tradicional postura da vítima de crimes patrimoniais, como meros “sujeitos passivos” do ilícito penal.

Mesmo que a curiosidade crônica assole qualquer usuário de ambiente computacional e o “clique aqui” entremostre-se irresistível, em computadores pessoais com sistemas de segurança atualizados é difícil que o intento do criminoso resulte proveitoso. Frisa-se que se considera uma irresponsabilidade a utilização de computadores pessoais, conectados à rede mundial, sem os devidos *patches* de atualização e de segurança do sistema operacional, bem assim a presença de um sistema de detecção de intrusões e de aplicativos detectores de vírus de computadores, todos, é claro, devidamente atualizados.

Um *software* de criptografia de dados também é algo desejável, pois quanto mais obstáculos um criminoso tiver que suplantar, mais propenso a desistir da empreitada ele estará.

Senhas de acesso simplórias, mantidas por anos a fio inalteradas, são, há muito, temas de anedotas no meio especializado (segurança da informação). Contudo, mais do que problemas pontuais acerca da segurança de sistemas computacionais, o que mais impressiona é uma postura, aparentemente, esperada das instituições bancárias que fornecem o serviço *on-line*: o paternalismo, esquivando-se os usuários dos serviços de quaisquer responsabilidades, até mesmo de alcançarem uma educação formal mais robusta a respeito desses serviços, apontando uma postura consentânea com a clássica posição de sujeito passivo.

Qual é o papel do usuário/proprietário desse ambiente computacional em face de evento que é dado como quase inevitavelmente certo?

O cidadão que vislumbra rio bravio, com fortes corredeiras e correnteza, arriscar-se-á a ali nadar e mergulhar, a despeito de placas de aviso e de orientação de moradores das redondezas? Provavelmente não, salvo se tiver comportamento quase suicida.

A sociedade global dos riscos permitidos cobra um preço de seus participantes. No mais das vezes, parte desse preço é a conscientização acerca desses riscos que foram permitidos não especificamente pelo indivíduo, mas, sim, pela sociedade como um todo.

Eis aqui uma das razões deste opúsculo: a multiplicação de conhecimento. Ora, o cidadão comum quase sempre não sabe, mas deveria saber: um computador pessoal conectado à internet, por meio de serviço de banda larga, poderá ser “ownado” (invadido, dominado e mantido à disposição do criminoso cibernético, sem rastros, para que ele possa utilizá-lo sempre que o desejar) em questão de minutos.

Nesses casos, a transformação em *zoombie machine* daquele computador que acessa a internet sem o nível de proteção adequado é questão de pouco tempo.

Logicamente, no que atine à atuação do usuário de computadores, há de se distinguir a situação de uma pessoa que sofre as conseqüências do crime daquela que contribui, efetivamente, para que o crime aconteça, por meio de atitudes de autocolocação em risco.

A situação fática de usuário de computador pessoal que se vale dos serviços bancários *on-line* (*home banking* e similares), que conta com serviço de banda larga para conexão à rede mundial de computadores, que ignora, ou aparenta ignorar, as orientações constantes, tanto da *mass media*, quanto dos fornecedores desses serviços *on-line*, da real necessidade de utilização instrumental adequado para usufruir desses serviços é algo que configura, aparentemente, a denominada autocolocação em risco da pretensa vítima imediata de crimes, mormente os de *phishing scam*.

Isso, é claro, não atenua a conduta do criminoso cibernético, não afasta, em grau algum, a elevada lesão da conduta dos sujeitos ativos de tais delitos, muitos deles componentes de verdadeiras quadrilhas ou de organizações criminosas, *stricto sensu*. Não, isso nunca!

O que se quer demonstrar aqui é a real necessidade de investimento maciço em educação formal do usuário de ambientes computacionais, como política pública eficaz de redução de números de crimes desse jaez, algo muito mais pertinente que o, tantas vezes discutido, "simbolismo" na esfera penal.

Tanto as instituições bancárias, quanto o Estado e seus órgãos competentes, devem investir nesse espectro de verdadeira inclusão digital, pois, entre outros fatores, a prevenção é, certamente, menos onerosa e menos traumática que a repressão, esta nem sempre "eficaz".

Para reforçar o que acima vai dito um exemplo dado por Claus Roxin, em sua obra *Estudos de Direito Penal*, é bastante elucidativo. Ora, é sabido que há mais automóveis hoje em dia na República Federal da Alemanha do que carroças ou diligências no século XIX naquele mesmo país, mas com o desenvolvimento dos chamados *Wegfahrsperren* (bloqueadores de sistemas de automóveis) reduziu-se, drasticamente, o número de furtos de veículos automotores na Alemanha.

Isso é algo apto a impedir a afirmação simplória de que, naquele país, furtam-se mais veículos automotores, hoje em dia, do que carroças, antigamente, apenas pela discrepância de números absolutos desses dois meios de transporte.

Não é, portanto, sempre verdadeiro que há necessidade de recrudescimento de penas, de novas criminalizações e penalizações para fatos que são, estatisticamente, numerosos na sociedade atual. A ação preventiva é, sempre, muito mais eficaz.

O Direito Penal deve ser utilizado com *ultima ratio*, e tão-só quando todos os outros meios de controle social já se mostraram ineficazes.

Assim, no âmbito dos crimes de *phishing scam*, afastar-se-ia, parcialmente, a utilização do Direito Penal como panacéia para tão drástico problema moderno, cujas cifras de prejuízos são dantescas, a partir de investimento maciço em educação formal de usuários de computadores pessoais. Seria a morte anunciada do famigerado "clique aqui".

Com medidas preventivas eficazes como aquelas sugeridas aqui, afasta-se a figura de "sujeito passivo" do delito, tão tradicional no Direito Penal.

Apregoa-se, portanto, a educação formal do usuário de computadores pessoais, conectados à internet, como meio de diminuir a utilização do caro e, muitas vezes, ineficaz Direito Penal.

Ressalte-se que, segundo ensinamento de Jesús-María Silva Sanchez, vez por outra, essa utilização é instrumentalizada pelos governantes, por meio da *mass media*, de forma simbólica, para fins de regular a vida na sociedade global do risco permitido, "administrativizando-se" o Direito Penal.

Quanto maior a educação formal dos usuários de computadores pessoais, menores as chances dos criminosos cibernéticos de se locupletarem das situações de risco permitido criadas pela atual "sociedade global do risco informático e da informação".

Notas de rodapé

1 – GRECO, Alessandra Orcesi Pedro. *A autocolocação da vítima em risco*. São Paulo, Revista dos Tribunais, 2004, p. 103.

2 – Mormente por meio de banda larga, onde os IP *numbers* são, em sua maioria, fixos, diferentemente do acesso discado, verdadeiro endereçamento dinâmico de IP *numbers*.

3 – GRECO, Alessandra Orcesi Pedro. *A autocolocação da vítima em risco*. São Paulo, Revista dos Tribunais, 2004, p. 105.

Fonte: https://conjur.jumps.com.br/2007-jun-13/crime_internet_ocorre_negligencia_usuario/