Crimes de Computador

Paulo Marco Ferreira Lima

Como o senhor nos define os Crimes de Computador?

Crimes de computador são qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, tenha facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o autor ou que, pelo contrário, produza um benefício ilícito a seu autor embora não prejudique de forma direta ou indireta à vítima. Podemos dizer que existem dois tipos de condutas ilícitas havidas pelo meio eletrônico: Por primeiro as que poderiam ser recepcionadas pela legislação penal existente, porém, com causas de aumento de pena em face de sua potencialização pela internet e facilitação da manutenção do anonimato; de outra banda restariam condutas ignoradas como a invasão de computadores, a inoculação e difusão de vírus, falsa identidade entre outras.

Quais são suas principais características?

O Brasil não é a toa o campeão em "hackeamento" em termos mundiais. Em regra a legislação faz vistas grossas para a nova tecnologia facilitando, justamente, a impunidade e o crescimento desses crimes. O anonimato prevalece. E mesmo os crimes comuns somente se agigantam. Sugere-se, para o combate dessa nova criminalidade, a adaptação de leis e conceitos, visando a proteção dos bens jurídicos a serem tutelados pelo Direito Penal Informático. Muitos dos chamados crimes de computador são, na verdade, os crimes comuns cometidos com o auxílio de um computador; porém, estamos também diante de novas condutas não tipificadas que ofendem uma série de bens jurídicos penalmente tutelados, sem que sejam esses objeto de uma figura típica específica. As ações criminosas praticadas com essa nova tecnologia de informação, dirigidas contra a liberdade individual, contra o direito à intimidade ou ao sigilo das comunicações entre outras, ainda se encontram sem a devida repressão jurídico-penal.

As lacunas permanecem também em face da ausência de condutas consideradas antijurídicas e típicas atinentes às fraudes cometidas com a manipulação de dados e programas computadorizados, ou seja, as fraudes cometidas com a utilização abusiva de computadores através de adulterações em documentos eletrônicos, provocando danos financeiros. Tais ações se encontram em perigosa zona nebulosa de repressão penal.

A "Era da Informática" veio expor diversos bens de forma mais ampla e abrupta, sendo certo afirmar que os dados constantes em um documento eletrônico restam mais desprotegidos hoje do que quando restavam somente em um fino pedaço de papel.

Como poderíamos classificá-los?

A meu ver próprios (em sua maioria não tipificados pela legislação brasileira) e impróprios (crimes comuns em que a internet é usada como meio de potencializar o dano ao bem jurídico penalmente tutelado ou ajuda na ocultação do autor, dificultando ou impedindo a aplicação da lei). Didaticamente a classificação seria:- condutas delituosas perpetradas contra um sistema de informática, sejam quais forem as motivações do agente; crimes cometidos contra outros bens jurídicos, por meio de um sistema de informática.

Quais são atualmente as principais espécies delitivas?

Crimes ligados a transações financeiras e delitos contra a honra pelas redes.

Como o senhor verifica atualmente nossa legislação para combater esta modalidade de crime?

Me parece que lutamos com tacapes contra AR15. A ineficácia é traduzida pela proliferação. Quantos não receberam hoje em seus emails dezenas de tentativas de estelionato virtual.

Como é a situação no Direito Comparado?

A Europa pela Convenção de Budapeste (assinada inclusive pelo Brasil) se compromete em uma criação de legislação com tipos abertos e unificados. Há uma tendência forte do Direito Europeu buscar a "Common Law". Os Estados Unidos começaram a legislar sobre os crimes de informática no fim da Década de 1970. O ordenamento jurídico-penal americano tem no combate à criminalidade econômica uma prioridade, isto explicando a enormidade de recursos intelectuais e financeiros dispendidos na luta contra os comportamentos desviantes nesta área. Tal priorização levou a um cuidado de tutelar o direito informático, uma vez que essa seria a estrada na qual transitaria boa parte das relações econômicas das épocas futuras. Criou-se, em virtude disso, uma respeitável estrutura legislativa que protege contra o ataque a sistemas eletrônicos, o uso ilegítimo de passwords, invasões eletrônicas na privacidade, entre outras transgressões. A primeira e a principal legislação federal, que cuidou de responsabilizar criminalmente as condutas efetivadas no meio informático, foi a CFAA ("Computer Fraud and Abuse Act". de 1986) que tipificou condutas como a de intrusão informática para obtenção de segredos nacionais com intenção de prejudicar o país, ou para obter vantagens financeiras. É esta, até hoje, a principal peça legislativa aplicável à maioria dos delitos informáticos, embora muitas outras leis regionais possam ser usadas para perseguir diferentes tipos de crimes de computador.

As duas leis Federais dos EUA mais utilizadas para a repreensão aos crimes de computador são: 18 USC, CAPÍTULO 47, SEÇÃO 1029, e a SEÇÃO 1030, de 1994 que modificou e atualizou a "Computer Fraud and Abuse Act".

Foram introduzidas modificações no sentido de complementar a Lei de Privacidade das Comunicações Eletrônicas de 1986, no sentido de suprir a anterior omissão à proteção legal à interceptação de comunicações eletrônicas. Foi também alterada a CFAA, com o intuito de coibir o ato de transmitir vírus ou qualquer outra espécie de programa destrutivo maligno, punindo a transmissão de programa, informação, códigos ou comandos que causem danos ao computador, a sistemas informáticos, às redes, à informação, aos dados ou a outros programas.

Interessante é apontar que o legislador americano procurou não definir os vírus

informáticos, mas sim descrevê-los, com o intuito de capacitar a legislação para coibir qualquer forma de ataque aos sistemas informáticos que possa advir com a diversificação tecnológica.

Outro aspecto interessante quanto à repreensão penal à disseminação de vírus de computador naquele país é que a legislação dos EUA diferencia o tratamento penal daqueles que de maneira temerária (culposa) lançam ataques de vírus, daqueles que assim agem com intenção (dolo) de causar danos efetivos. Define, do presente modo, dois níveis para o tratamento legislativo: primeiro para aquele que cria o vírus e, dolosamente, o dissemina (estabelecendo para aqueles que intencionalmente causam um dano pela transmissão de um vírus uma pena de até 10 anos de prisão mais multa); e para aqueles que o transmitem de forma negligente (a sanção para esses casos fica em torno de tão somente pena de multa até um ano na prisão).

Em geral, são coibidas pela estrutura legislativa quaisquer condutas que de alguma forma: atentem contra o sigilo de informação eletrônica de defesa nacional, de assuntos exteriores, de energia atômica ou qualquer outra informação restrita e de caráter estratégico; envolvam a um ordenador pertencente a departamentos ou agências do governo dos Estados Unidos; envolvam banco ou qualquer outra classe de instituição financeira; envolvam comunicações interestaduais ou internacionais; afetem pessoas ou ordenadores em outros países ou estados.

Existem propostas legislativas nacionais nesta seara?

Há vários anos sem nenhuma resposta do Congresso Nacional.

Qual o panorama desta modalidade de criminalidade com o advento das redes sociais?

O Facebook casou com a paixão brasileira de fazer amizades. Há mais de 600.000.000 milhões de usuários, em grande parte brasileiros. Isto sem contar Orkut, Myspace entre outras. É possível imaginar a proporção que ganha, por exemplo, uma ofensa racial neste contexto?

Na forma atual da sociedade, parte da educação é passada às crianças e adolescentes através da internet. As escolas e as famílias, e o próprio Estado por omissão, abrem as portas da internet para as crianças e jovens. Criou-se uma sociedade em que o uso das redes sociais é fator de integração social também no mundo real, pois são ali registradas por seus usuários blogs que contam detalhes de suas ações cotidianas, tais como fotografias, diários e uma enorme gama de informação, expondo sentimentos, experiências, conquistas, alegrias e tristezas e, assim, facilitando a ação de pedófilos, seqüestradores, etc.

A mídia internacional menciona também caso de extorsão que teve sua origem em uma interação através das redes sociais : "O pesadelo começou com uma brincadeira: três adolescentes visitavam um site de videochat e cederam ao pedido de mostrarem rapidamente os seios em frente à webcam. Uma semana depois, uma das garotas, moradora do Estado de Indiana, com 17 anos, começou a receber e-mails com ameaças de um desconhecido. Ele dizia que havia capturado a imagem dela na webcam e a exporia no MySpace a menos que ela posasse para mais fotos e vídeos explícitos. E pelo menos duas vezes ela obedeceu, com medo do que o sujeito pudesse fazer. Finalmente, a polícia e as autoridades federais foram envolvidas no caso e, em junho deste ano, acusaram formalmente um rapaz de 19 anos, do Estado de Maryland, por casos de exploração sexual. Casos como este têm acontecido com frequência cada vez maior nos Estados Unidos, onde já se cunhou inclusive o termo "sextorsion", ou sextorsão, em tradução livre, em referência a estas extorsões sexuais praticadas via internet. Nos juizados estaduais e federais não há um registro completo ou um número confiável de casos em que há extorsão sexual pela internet, mas as autoridades dão como exemplo outros casos recentes que ficaram bem conhecidos. Em Wisconsin, Anthony Stancl, 18 anos, foi sentenciado em fevereiro a 15 anos de prisão assim que descobriram que ele fingia ser uma menina no Facebook para enganar os garotos que eram seus colegas de aula e fazer com que eles lhe enviassem, pelo celular, fotos em que apareciam nus. Stancl usava depois as fotos para chantagear os garotos e obrigá-los a fazer sexo com ele. Não acreditamos que essa nova espécie de extorsão seja exclusiva dos americanos. É bem possível que práticas como essas aconteçam no território nacional e permaneçam como parte da cifra negra, até por inexistir uma devida atenção jurídica ao tema ou até mesmo pela ineficácia de um "Law

enforcement" adequado para receber e processar os crimes praticados por via da internet, quanto mais quando envolvem denúncia de abuso sexual.

O senhor acredita que o pensamento jurídico brasileiro não soube encarar os crimes de computador?

Com certeza não. A figura do avestruz que coloca a cabeça na terra quando o perigo chega parece a metáfora mais condizente. As autoridades policiais, Ministério Público e Poder Judiciário, em regra, tratam a questão como de menor importância e demonstram pouca atenção, talvez até por desconhecimento da nova tecnologia quanto aos crimes cibernéticos, sempre tentando passar ao largo, como se toda a inovação nessa área pudesse ser simplesmente desprezada e recepcionada sem esforço pelo ordenamento jurídico e pela estrutura policial já existente. Tal não ocorre no sistema jurídico americano que, até pela tradição do "Common Law" e de tipos abertos, permite um acompanhamento mais pontual e dinâmico com a tecnologia informática, reprimindo de forma mais eficaz as condutas perpetradas pela e com o uso da rede.

Como o senhor avalia a jurisprudência que vem se formando sobre o tema?

Quase sempre agindo por analogia. Coisa, a meu ver, incompatível com o Direito Penal. No Brasil, em que pese à existência de legislação disciplinando crimes na área de informática desde a Lei n.º 7.646, de 1987 (revogada pela Lei n.º 9.609, de 19 de Fevereiro de 1998), muito ainda há que ser feito no sentido de criar um sistema jurídico protetor de dados eletrônicos e sistemas informáticos.

Não há, ainda, embora existam diversos projetos legislativos em tramitação, figuras típicas eficientes para reprimir todas as condutas criminosas cometidas por meio de computadores ou contra seus dados e sistemas.