CRIMES VIRTUAIS

Tiago Tadashi TAKUSHI[1]
Marcus Vinícius Feltrim AQUOTTI[2]

RESUMO: Com o avanço tecnológico ampliaram-se as fronteira da comunicação, e o mais importante, se não, o mais utilizado meio para comunicação é a Internet. E como de costume em todo meio há atos ilícitos, com a Internet não seria diferente, referindo-se então aos Crimes Virtuais ou de Internet.

Palavras-chave: Crimes virtuais. Crimes de Internet. Rede de computadores. Banco de dados. Computadores.

1 INTRODUÇÃO

Desde os tempos primórdios, o homem é um ser social, ou seja, necessita se comunicar. É a dicotomia de ouvir e ser ouvido.

Dessa forma, com a dinâmica da tecnologia, os avanços são utilizados para aumentar a praticidade e proporcionar conforto a pessoa que a utiliza.

Com o surgimento da Internet não poderia ser diferente. Internet é uma rede pública de computadores, cuja finalidade primordial é possibilitar a comunicação universal, sem fronteiras e sem censura.

Atualmente, se tornou uma ferramenta de extrema necessidade para o mundo globalizado. Com ela se adquire várias informações, sendo por ela que é transmitida toda e qualquer mensagem, documentos, imagens, sons, ou seja, qualquer tipo de dados que sejam utilizados por um computador. É um meio de comércio, e também um meio para criar relacionamentos.

---

[1] Discente do 4º ano do curso de Direito das Faculdades Integradas “Antonio Eufrásio de Toledo” de Presidente Prudente. e-mail: tttakushi@yahoo.com.br, Bolsista do Programa de Iniciação Científica V Encontro Toledo de Iniciação Científica.
[2] Docente do curso de Direito Penal das Faculdades Integradas “Antonio Eufrásio de Toledo” de Presidente Prudente. Mestre em Direito Público pela Universidade de Franca e-mail@ mvsaquotti@ig.com.br. Orientador do trabalho.

Mas sendo um objeto que proporciona conforto e utilidade, pode também ser utilizado como veículo de estimulo e induzimento para a prática, em tese, de crimes.

Figura-se como autores dos delitos os crackers, termo usado para designar quem pratica a quebra de um sistema de segurança, de forma ilegal ou sem ética; praticando vários outros delitos como estelionatos, falsificações de documento, acesso indevido a banco de dados.

Com o rápido avanço tecnológico, e também da prática de atos ilícitos utilizando como veículo o computador e a Internet, a doutrina e a jurisprudência, tentam acompanhar essa dinâmica, mas os legisladores são menos eficazes em elaborar leis sobre tais crimes.

2 CONCEITO DE CRIME VIRTUAIS OU DE INFORMÁTICA

As acepções de crimes de informática, também conhecidos como crimes virtuais, são amplas e variam de acordo com o ponto de vista de cada um.

Pode-se citar o professor Ulrich Sieber apud Sérgio Marcos Roque (2007, p. 24-25), que define o crime de informática como sendo: "[...] Any ilegal, unethical or unauthorized behavior involving automatic data-processing and/or transmission of data".

Tal conceito do professor Ulrich Sieber[3] foi adotada pela Organização para a Cooperação Econômica e de desenvolvimento, a OECD: "[...] a OECD propôs uma definição ampla, conceituando esse tipo de crime como sendo 'qualquer conduta ilegal não ética, ou não autorizada que envolva processamento de dados

[3] "Dr. Dr. hc Ulrich Sieber, diretor no Instituto Max Planck de Direito Penal Estrangeiro e Internacional, em Freiburg / Alemanha, é um professor honorário e professor na faculdade de Direito da Universidade de Freiburg e Universidade de Munique, um consultivo professor do departamento de Direito da Universidade de Renmin Pequim / China, e um professor convidado no Departamento de Direito da Universidade de Wuhan / China." Traduzido com Google Tradutor. Informações retiradas de <http://www.mpicc.de/ww/en/pub/home/sieber.htm> - acesso em 09.06.09.

e/ou transmissão de dados" (ROSA, 2002, p.53). Traduzindo, dessa forma, o conceito do professor Ulrich Sieber.

Fabrizio Rosa (2002, p. 53-54) também conceitua o crime de informática como sendo:

> 1. [...] É a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. o 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. assim, o 'Crime de Informática' pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se *software* e *hardware*, para perpetrá-los; 4. a expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

Já Sergio Marcos Roque (2007, p. 25), conceitua crime de informática como sendo "toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material."

Em fim, mesmo tendo diferentes posições para tipificar o crime, o meio sempre será o mesmo, sendo o instrumento o computador e o meio pelo qual o ato é praticado é a Internet.

3 O CRIME E SUAS QUALIFICAÇÕES

São várias as classificações utilizadas nos crimes de Internet. Um delas é a divisão do crime em próprio e impróprio. “Os primeiros são aqueles que somente podem ser efetivados por intermédio de computadores ou sistemas de informática, sendo impraticável a realização da conduta por outros meios. [...] impróprios admitem a prática por diversos meios, inclusive os meios informáticos” (CASTRO, 2003, s.p.)

Outra classificação seria a tripartida, também citada por Aldemário Araújo Castro (2003, s.p), dividida em:

> a) os crimes de informática puros, onde o agente objetiva atingir o computador, o sistema de informática ou os dados e as informações neles utilizadas; b) os crimes de informática mistos, onde o agente não visa o sistema de informática e seus componentes, mas a informática é instrumento indispensável para consumação da ação criminosa e c) os crimes de informática comuns, onde o agente não visa o sistema de informática e seus componentes, mas usa a informática como instrumento (não essencial, poderia ser outro o meio) de realização da ação.

Ainda, classificá-lo em de acordo com a estação. Se a estação for próxima, por exemplo uma rede interna, ou se for uma estação remota, como a Internet.

Mas todas essas as classificações não são eficazes, e geralmente são aplicadas para fins didáticos, isso ocorre pelo fato da dinâmica dos computadores e da Internet. A evolução proporcionada por elas é muito grande, assim como as novas formas delitivas que vão surgindo. Dessa maneira, tornam obsoletas essas classificações.

4 TIPOS DE CRIMES

São muitos os tipos de crimes possíveis de se praticar diante de um computador que possua Internet, mas o que geralmente ocorre é a sua difícil tipificação, pois o ordenamento jurídico brasileiro não possui leis suficientes para regulamentar os crimes virtuais. A seguir são abordados de uma forma geral os crimes mais praticados.

4.1 Crime de Dano

A conduta do crime de dano é apagar, modificar, destruir ou inutilizar, parcial ou completamente, dados ou programas de computador de maneira indevida ou não autorizada, sendo essa conduta crime de informática puro. Essa conduta estava regulada pelo PL n° 84-A/99, o qual, até a presente data, continua em trâmite e não há previsões para ser constituída como lei.

4.2 Crime de Veiculação de Pornografia Através da Internet

Essa tipificação desse crime consistia em 2 tipos de conduta que seriam a de oferecer serviço e/ou oferecer informação, de caráter pornográfico, via rede de computadores, a Internet. Também seria regulada pelo PL n° 84-A/99.

Mas atualmente houve uma alteração apresentada no Estatuto da Criança e do Adolescente, pela Lei n° 11.829 de 25 de novembro de 2008, que em

seu art. 247 até o art. 247-E, regulamentam sobre imagens de crianças ou adolescentes relacionadas a pornografia por meio da Internet.

Os art. 247-A até E, acrescentados pela Lei n° 11.829/08, tipificam as condutas “Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar divulgar, adquirir, possuir ou armazenar”, por quaisquer meios, vídeos ou imagem pornográficas que envolvam crianças ou adolescentes.

A norma se torna abrangente por citar “[...] por qualquer meio, inclusive por meio de sistema de informática ou telemático...” (ECA, art. 241-A “*caput*”), assim não abre lacunas para especulações quanto à tipificação dos crimes.

Mas a norma é específica, pois se encontra no ECA, sendo assim, só poderá ser aplicada quando envolver criança ou adolescente, não abrangendo os demais casos em que há vítimas maiores de idade.

4.3 Estelionato e Fraude

A figura do estelionato, conhecida pelo art. 171 do Código Penal, consiste em obtenção de vantagem ilícita, para si ou para outrem, induzindo ou mantendo a vítima em erro, mediante artifício, ardil, ou fraudulento. Consuma-se quando há a vantagem ilícita, em prejuízo alheio, frisando-se a ultima parte, em que necessita haver o prejuízo alheio. Citando Remy Gama Silva (2000, p.8), a figura de fraude se encaixaria na esfera da informática como fraude informática quando “esta seria a lesão ao patrimônio por meio enganoso, consumando-se, também, com o alcance da vantagem ilícita, em prejuízo alheio.”

Em sua obra, Remy Gama Silva (2000, p.8), descreve alguns exemplos:

> É utilizada em muitos casos de crimes econômicos, como manipulação de saldos de contas, balancetes em bancos, etc, alterando, omitindo ou incluindo dados, com o intuito de obter vantagem econômica. A fraude informática é o crime de computador mais comum, mais fácil de ser

> executado, porém, um dos mais difíceis de ser esclarecido. Não requer conhecimento sofisticado em computação e pode ser cometido por qualquer pessoa que obtenha acesso a um computador. Tradicionalmente a fraude envolve o uso de cartões de bancos roubados ou furtados. Usando software específico, pode-se codificar amplamente as informações eletrônicas contidas nas tarjas magnéticas dos cartões de bancos e nos de crédito.

Ressaltando para finalizar, novamente, que para que haja estelionato em todos os casos acima descritos, necessita do elemento "prejuízo alheio" para configurar a figura de estelionato.

4.4 Crime Contra Privacidade

A privacidade, pelo Dicionário Aurélio, refere-se à vida privada, ou seja, vida íntima, significando intimidade. É um direito, denominado Constitucional, assegurado pela Constituição Federal, em seu art. 5°, inciso X, dizendo que "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação".

Com a grande difusão de computadores, a privacidade se tornou um problema para a sociedade, sendo motivo de preocupação de várias pessoas. Isso ocorreu, pois com a evolução da tecnologia, os meios de acesso de dados pessoais foram ampliados.

Remy Gama Silva (2000. p. 9), cita que:

> A maioria dos estatutos de privacidade internacionais inclui providências que limitam o direito de acesso em dados pessoais de outra pessoa. A proteção legal destas pessoas está ligada a providencias para o crime de calúnia e proteção de segredo profissional, principalmente no campo médico. [...] Para a União Européia a proteção da privacidade contra ofensas causada por tecnologia moderna é de grande importância, porém, esta proteção deveria ser resolvida em regulamentos de direito civil. O recurso da lei criminal, só deveria ser utilizado em ultimo caso. As providências criminais necessitam descrever precisamente os atos proibidos, devendo evitar cláusulas vagas e imprecisas. Em princípio, infrações de privacidade relacionadas aos crimes da informática, só deveriam ser apenadas se o agente as efetuasse com intenção dolosa.

Podemos concluir então que há possibilidade de serem punidos esses criminosos virtuais, mas que há também a necessidade da criação de leis, e tomando a precaução para não criá-las com cláusulas vagas e imprecisas.

A doutrina define crime como sendo fato típico, antijurídico e culpável, e o Código Penal em seu art. 1° disciplina que "Não he crime sem lei anterior que o defina. Não há pena sem prévia cominação legal", dessa forma, sem tais leis, não se pode exigir ato punitivo dos autores desses atos, pois não será considerados como crimes.

4.5 Espionagem e Sabotagem Informática

A espionagem informática configura-se pela alteração de programas ou trocas de peças, modificando a programação originária facilitando dessa forma o acesso aos dados, registros de uma máquina. Há o acesso de computadores, intencional e não justificado de pessoas não autorizadas pelo proprietário ou operador de um computador, configurando assim um comportamento criminal. Geralmente estes tipos de acessos são realizados de pontos remotos, através de redes de telecomunicações, sendo de extrema dificuldade a localização após a invasão.

O autor se aproveita de falhas ou a inexistência de segurança do sistema, utilizando programas específicos para invadir e subtrair dados. Quando são subtraídas partes corpóreas como discos, CD's, são tomadas as providencias penais tradicionais, como furto e apropriação. Mas quando são copiados informações e dados através dos sistemas de telecomunicações, surge a questão sobre a extensão da aplicação da legislação penal.

É importante observar o texto a seguir de Remy Gama Silva (2000. p. 6-7), quais as providências que são tomadas em diversos paises quanto a qualificação de tal crime virtual:

> Países como a Áustria, Bélgica, Alemanha, Grécia e Itália, são relutantes em aplicar as providências tradicionais em roubo (denominação utilizada nestes países) e apropriação de informações de dados, porque suas leis geralmente requerem que o bem seja corpóreo e retirado com a intenção de privar permanentemente a vítima. Na França, aplicação da legislação penal tradicional, seria possível dentro de alguns casos específicos. Nos Estados Unidos, alguns tribunais consideram as informações contidas no computador como propriedade, no senso de apropriação tradicional e em muitos Estados americanos as legislações definem os dados de computador ou a informação sigilosa, como propriedade, ou valor, a fim de habilitar a aplicação da apropriação. O termo propriedade insinua exclusividade, posse, enquanto que a informação tende a ser concebida como um bem público. Destaque-se as informações pessoais e as confidenciais. No direito pátrio, o furto não requer comentários neste trabalho, já a denominação furto de informações merece algumas observações. Comparando-se analogicamente, a informação e a energia elétrica, temos que a informação pode ser bem móvel, passível de furto. Sendo bem móvel pode-se, usufruir, gozar, modificar, etc, ou seja, é propriedade. Havendo a alteração em programas de computador, por meio da espionagem, para a transferência ou subtração de informações e dados do computador para uma pessoa não autorizada, conclui-se pela existência do furto de informação. Seguindo esta linha de raciocínio a apropriação pode existir, quando os dados ou informações não forem subtraídos, mas sim, copiadas por meio de artifícios eletrônicos mantendo-as intactas, sem que seu proprietário perceba que estas foram clonadas. Raramente este tipo de delito aparece em estatísticas oficiais, constituindo um perigo se comparado com a espionagem tradicional, pois em sistemas de computador são armazenadas enormes quantidades de dados em um espaço muito pequeno e estes dados podem ser copiados rapidamente e facilmente com a ajuda de tecnologia moderna, inclusive pela rede de telecomunicação.

A sabotagem informática é a destruição ou danificação de material ou componente pertencente a um computador. O objetivo da sabotagem é causar danos físicos e lógicos, visando inutilizar dados e outras informações valiosas contidas em determinada máquina.

Esse ato envolve tanto o agente que tem acesso e/ou que não tem acesso, pois este irá introduzir programas conhecidos como vírus[4] para que sejam destruídos os dados desejados. A modificação ou a retirada de dados do sistema ou de suas funções, impedindo o seu funcionamento regular, são consideradas atividades criminais, pois poderá envolver vantagem econômica sobre um concorrente, ou com o propósito de extorquir pessoas. Nesses casos, opera-se tradicionalmente, configurando extorsão, cabendo provar a violência ou grave ameaça para obter a vantagem devida. Mas nos casos de infecção de computador

[4] Vírus de computador são programas formulados especialmente para gerar, de alguma forma, danos aos computadores. Eles são, inclusive, capazes de se auto-copiar para outros programas ou modificarem suas estruturas a fim de não serem detectados pelos antivírus. Informações retiradas de <http://gtrh.tche.br/ovni/virus/modulo1.htm> - acesso em: 09.06.09.

por vírus, é de extrema dificuldade, pois pode haver culpa da vitima também, que possa ter usado programas infectados, ou acessado páginas pela Internet infectadas. Nesses casos é sempre importante ter o backup [5] dos principais arquivos do computador.

5 COMPETÊNCIA E JURISDIÇÃO

Outro problema seria o conflito de competência e jurisdição que ocorre nos crimes virtuais, isso ocorre pois a rede de troca de informações, denominada Internet, é global, possibilitando dessa forma que o criminoso possa estar do outro lado do mundo, mas que a vitima seja de nacionalidade brasileira.

O real problema ocorre quando o crime é internacional. O que envolveria competências extraordinárias extraterritoriais, pois o Brasil segue o princípio geral da territorialidade, onde as leis se limitam ao território brasileiro, não se aplicando ao exterior.

Sergio Marques Roque (2007. p. 60-61), em sua obra coloca que:

> [...] a questão que suscita maiores dúvidas é a dos crimes à distanciam como nos casos dos delitos praticados através da Internet quando a ação é executada em um país e seus efeitos ocorrem no Brasil.
> Como resolver, então, este problema? A solução estaria na celebração de tratados internacionais. mas para isso ser possível há necessidade da existência, primeiramente, da dupla incriminação, ou seja, que as condutas constituam crime em ambos os países.
> Outra questão que se coloca é a extradição, pois como o Brasil não concede a extradição e um seu cidadão para ser processado em um outro pais, haverá reciprocidade no caso da ação ter sido praticada em território estrangeiro por cidadão não brasileiro.

[5] Backup significa cópia de segurança. Fazer uma cópia de segurança dos dados armazenados em seu computador ou seu site é muito importante, não só para se recuperar de eventuais falhas, mas também para evitar uma possível infecção por vírus ou até uma invasão do sistema de dados. As cópias podem ser simples como o armazenamento de arquivos em CD Rom ou em disquetes, ou as mais complexas como o espelhamento de um disco rígido inteiro em um outro disco de computador. Informações retiradas de <http://www.rjhost.com.br/faq/90/hospedagem-de-site/o-que-backup.html> - acesso em: 09.06.09.

Com certeza essa seria a melhor solução, mas necessita de tratados celebrados entre os Estados, quando à isso somente dependerá das partes para que se realize uma solução mais adequada.

6 CONCLUSÃO

É a pura realidade dizermos que, mesmo que o ordenamento jurídico fosse rápido em criar novas leis, estas estariam obsoletas em pouco tempo. O fato é que a tecnologia é possui uma dinâmica no qual está sempre em modificação, dessa forma, sempre haverá novas práticas de atos que serão consideradas ilícitas. Mas mesmo assim, deveriam ser criadas normas especificas para esses tipos de crimes.

De fato o ordenamento jurídico já está começando a se adaptar a essa nova modalidade de crimes, citando, por exemplo, as modificações do ECA, mas ainda falta muito para ser tipificado, havendo grandes lacunas em práticas que já estão se tornando comuns em nossa sociedade.

7 BIBLIOGRAFIA

CASTRO, Aldemario Araújo. **Internet e os Tipos Penais que Reclamam Ação Criminosa em Público.** In: Webly. Disponível em <http://www.webly.com.br/forum/lofiversion/index.php/t11293.html>. Acesso em 09.06.09.

DELMANTO, Celso. **Código Penal Comentado.** 5 ed. Rio de Janeiro: Renovar, 2000.

PAULINO, José Alves. **Crimes de Informática.** Brasília: Projecto Editorial, 2001.

ROQUE, Sérgio Roque. **Criminalidade Informática – Crimes e Criminosos do Computador.** 1 ed. São Paulo: ADPESP Cultural, 2007

ROSA, Fabrízio. **Crimes de Informática.** Campinas: Bookseller, 2002.

SILVA, Remy Gama. **Crimes da Informática.** Editora: CopyMarket.com, 2000.