Crimes de informática

Crimes em Espécie - Comuns e de Informática

Marco Aurélio Rodrigues da Costa*

Por muito importante, é não ter sido, ainda, pacificada a proteção do bem jurídico, face às imensuráveis divergências entre os grandes doutrinadores.

Acima citamos o furto de "chips" da Britsh Telecom, e ao primeiro impacto pode-se tratar de crime comum, pois a conduta não teria as duas premissas fundamentais dos "crimes de informática", quais sejam, o objetivo dos dados ou sistema, perpetrados através de computador.

Dada a importância do "chips" é que o professor da Universidade de Amsterdã, Hermann Cohen JEHORAM (1991, p. 277), fez publicar o artigo "Proteção do Chip", no qual inicia perguntando: "Chips podem ser comparados com qualquer outro objeto de proteção da propriedade intelectual?"

É de ser respondido que em literatura desatualizada, e esta evolui na mesma velocidade do avanço tecnológico dos computadores, sistemas e periféricos, encontram-se, com freqüência, tropeços na comparação de "chips" com "software". Como exemplo, se vê numa longa carta de 16.05.85 escrita pelo governo holandês à Comissão Americana de Patentes e Marcas Industriais. O então signatário queria provar que "chips" já eram protegidos pela lei dos direitos autorais, proteção que se dizia evidente a conta de decisões citadas, assegurando proteção ao "software", a ele, por conseguinte extensivo ao "chip".

A Associação entre "chip" e "software" de computador hoje em dia pode ser tecnicamente explicável, mas legalmente incorreta. "software" de computador é realmente "software" e, como tal, pode, no mínimo, ser comparado à obra literária, objeto clássico protegido pelo direito autoral. Não se considera neste contexto aquele misto de confusão e contradição, que hoje se diz ter havido nos EE. UU., quando a razão foi substituída pela euforia sobre a proteção do "software" como direito autoral.

"Chips", porém, são "hardware", microcomputadores, portanto máquinas. Em realidade, não se reivindica proteção dessas máquinas como tais, mas como desenho, que é chamado nos EE. UU. MASK WORK; topografia de produto semicondutores no Mercado Comum

europeu; e LAYOUT de circuito semicondutor integrado no Japão. O esboço de tratado preparado pela Organização Mundial de Proteção Industrial sobre o assunto é o mais claro quando fala de desenho de circuito integrado.

Desenhos podem ser protegidos pelo direito autoral? A resposta não pode ser universalmente dada como nos casos de obra literária e "software". Não há, realmente, em todo o direito de propriedade intelectual nenhum assunto que suscite tanta divergência nos sistemas nacionais, como a proteção dos desenhos, no campo do direito autoral, pois não se enquadrando nesse, obrigatoriamente, deveria ser apreciado no campo do Direito Criminal da Informática, porque é um bem que se tem e deve ser protegido.

Portanto, indelével, as peculiaridades que cercam o computador, seus componentes e a própria informática, necessitando, urgentemente, os doutrinadores encontrarem parâmetros, meios capazes de escriturarem o Direito Criminal da Informática, de modo a garantirem proteção desses bens, que, também, são jurídicos, à medida que geram direito, de uma ou de outra forma.

Muitos têm escrito a cada conduta ilegal, com o intuito de classificarem que esta ou aquela conduta é passível de ser um crime de informática, ou não, porém, o segmento mais claro, que estabelece linha cristalina entre os delitos comuns e os delitos de informática, é aquela que define os crimes de informática nas condutas em que o agente ativo visa aos dados ou sistemas do computador e, utiliza-se como meio para alcançá-lo, o computador.

Contudo, os crimes de informática encontram do Código Penal Brasileiro várias possibilidades de repressão pena, variando a sua tipificação conforme o bem jurídico que o agente pretenda atingir.

CRIMES COMUNS Considerações Gerais
Na nossa lei penal o patrimônio da pessoa física ou jurídica é tutelado pelo Código Penal, como também os crimes contra a divulgação de segredo. Todavia, observa-se que tais previsões legais podem e devem ser aplicadas às condutas que envolvem delitos de informática, principalmente naquelas em que o sistema de informática é ferramenta ou é alvo de delito comum, por isso, que buscamos na lei penal a possibilidade de tipificação de algumas condutas que envolvem o sistema de informática. Buscamos, a seguir, demonstrar a sua aplicabilidade aos delitos de informática, sem, conduto, aprofundar descrição e interpretação, pois, do contrário, estaríamos desvirtuando o objetivo deste trabalho.
Do Código Penal
FURTO

Objeto jurídico

O artigo 155 protege, inicialmente, a posse de "hardware" e "software", para depois a propriedade. É de ser entendido que o furto de "software" é a subtração de sistema que esteja instalado no computador. O furto simples de equipamento e sistemas são crimes comuns contra o patrimônio e a propriedade.

Sujeito ativo

É todo aquele que se apossa por meio de subtração para si ou para outrem de "hardware" ou "software", estejam eles na posse do proprietário ou na de terceiros. É aquele que tem na sua ação "animus furandi".

Sujeito passivo

É toda a pessoa física ou jurídica que tenha a posse ou a propriedade de computador ou sistema de informática.

Ação física

É a ação de subtrair, surripiar do domínio do proprietário ou de quem tenha a posse de computador ou sistema de informática.

Objeto material

É o computador ou o sistema alheio, que se acha na posse de outrem, seja proprietário ou não. É admissível, assim, no uso desautorizado do computador o furto de energia elétrica, e este é previsto no Código Penal (art. 155, § 3o.), porém, neste caso, esbarra no valor irrisório ou do prejuízo ínfimo da vítima.

Devem ser excluídos os furtos de "softwares" com objetivo de pirataria, este delito é tratado através dos crimes contra a propriedade imaterial, e alguns entendem ser nos crimes contra a propriedade industrial.

O bem objeto de furto, além de ser alheio, deve ser móvel. O computador é, por sua natureza, um bem móvel, o "software" que nele estiver contido por via de conseqüência é também, neste caso, um bem móvel. Os dados armazenados são, também, coisa móvel, porém é de se perquirir se o agente visava o tão somente o equipamento, se visava exclusivamente o "software" ou aos dados. É crime de informática puro.

Elemento subjetivo

Não existe furto sem dolo. O agente sempre tem a intrínseca vontade livre e consciente de praticar o delito, de subtrair o equipamento, não há que se discutir a sua forma culposa.

Consumação e tentativa

A consumação do furto de computador ocorre quando o bem sai da esfera da posse da vítima, para entrar na do agente ativo, de forma mansa e pacífica. A tentativa é admissível.

Furto noturno

Atende ao que determina a lei penal, como agravante do delito de furto, plenamente caracterizável.

Qualificadoras

Admitem-se as qualificadoras de destruição ou rompimento de obstáculos à subtração da coisa, no caso em que o agente necessite, para perpetrar o furto de informações, abrir a caixa do computador e mudar o chaveamento, para anular a senha de acesso ao disco rígido, por exemplo.

Quanto ao abuso de confiança é perfeitamente perceptível, quando o agente é empregado da vítima. A fraude pode ocorrer na hipótese de que , para furtar informações a agente usa de meios que caracterizem a conduta fraudulenta, como, no caso de dizer-se técnico da empresa que fornece manutenção do equipamento.

A escalada e o uso de chave falsa, somente se o agente, para entrar no local onde se encontra o computador necessita usar de meios anormais.

O furto por destreza não se aplica aos crimes de informática em razão das suas características, tanto do objeto o furto, como do meio.

DANO

O artigo 163, nos casos em que o agente visa à destruição, inutilização ou deterioração da coisa alheia (o computador, os periféricos, as informações e os sistemas) são aplicáveis à informática, bem como as qualificadoras de violência à pessoa ou grave ameaça; com emprego de substância inflamável ou explosiva; contra patrimônio da União, Estado, Município, empresa de economia mista ou que seja concessionária de serviços públicos; por motivos egoísticos ou com prejuízo considerável à vítima. Nesse caso tem que perquirir o "animus delinquendi".

Objeto jurídico

Concerne a tutela à inviolabilidade do patrimônio, aqui o computador, em razão de que o dano causado reduz ou suprime a utilização e o preço do computador.

Á informática concerne danos físicos ao computador na sua forma interna e externa. Se os danos visam à destruição do equipamento é aplicável, exclusivamente, o artigo 163 do Código Penal, porém, se os danos vão além da parte física do equipamento, atingindo "software" e dados, é de ser apurada a vontade do agente. Se visa ao "software" e/ou aos dados contidos no computador é crime puro de informática; contudo, não inviabiliza o concurso material.

Sujeito ativo

É todo aquele agente que visa causar dano ao equipamento de forma a causar prejuízo ao proprietário ou a quem tenha a posse dele. É importante ser buscada a vontade do agente, no caso, tem que ter tão somente o "animus dolandi"".

Sujeito passivo

É todo aquele que tem o uso e o gozo do equipamento.

Ação física

Forma comissiva, caracteriza-se quando o agente busca o dano através de ação idônea a atingir seu objetivo ilícito.

Na forma omissiva o agente permite que ocorra o dano ao equipamento, permitindo que ações outras visem a destruir, inutilizar ou deteriorar o equipamento.

Elemento subjetivo

Admite dolo e culpa. No dolo o agente tem a vontade consciente de alcançar o resultado dano. Na forma culposa, pratica ação arriscada que inutiliza, deteriora ou destrói o equipamento, por exemplo, danos causados ao disco rígido, por imprudência, por imperícia ou negligência.

Objeto material

Visa, tão somente ao "hardware", não vislumbrando os danos de "softwares" e das informações contidas no equipamento.

Consumação e tentativa

Admite, plenamente, a forma tentada na sua ampla concepção doutrinária, legal e jurisprudencial, bem como se consuma ao alcançar a destruição, deterioração ou inutilização do equipamento.

APROPRIAÇÃO INDÉBITA

O artigo 168 é uma das figuras típicas que é afeita aos crimes de informática. O agente, quase sempre, tem a posse ou detenção do equipamento, e dele se serve para perpetrar vários delitos de informática. Portanto agrega-se com propriedade a causa de aumento de pena se o delituoso age em razão de ofício, emprego ou profissão.

Objeto jurídico

É, também, delito que objetiva o patrimônio, aqui "hardware". Atingindo com mais freqüência empregadores, sejam eles pessoa física ou jurídica.

Sujeito ativo

É todo agente que se apropria coisa de que tem em sua guarda. É comum nas relações de emprego e de confiança.

Sujeito passivo

Em princípio, qualquer pessoa que suporta o prejuízo pela apropriação indevida, podendo ser pessoa física ou jurídica.

Ação física

Ocorre após o agente ativo receber para guarda o "hardware", de que após se apropria com o "animus domini".

Objeto material

São todos os tipos de equipamentos que fazem parte do "hardware", tais como, vídeo, unidade centra de processamento (CPU), mouse, impressoras, scanners, etc., porém inaplicável a informações sob a forma de dados ou o "software".

Elemento subjetivo

Como qualquer crime, dessa natureza, requer a apropriação indébita, o dolo genérico, que constitui a vontade livre e consciente do agente em apropriar-se do equipamento, com a intenção de tê-lo para si.

É, no entanto, não é admissível a culpa na apropriação indébita, pois, no caso do agente apropriar-se do computador pensando ser seu, estará agindo ao impulso do erro de fato.

Consumação e tentativa

É difícil a caracterização da consumação. É necessário um profundo exame do elemento subjetivo combinado com os atos exteriorizados pelo agente, e, mesmo assim, nem sempre é possível captar-se a consumação.

A tentativa é matéria jamais pacificada, vez que alguns doutrinadores entendem impossível a tentativa; outros, pelo elemento subjetivo e os atos exteriores podem caracterizar a tentativa.

"In casu", é de ser seguido a regra geral desposada pela lei penal, que determina o "iter" e a vontade do agente seja perceptível.

ESTELIONATO

O artigo 171 é, também, um dos instrumentos que permite alcançar a agente de crimes de informática, porque o "caput" prevê, substancialmente muitas condutas desenvolvidas contra o computador e os seus sistemas. Os "crimes de informática", por enquanto, no artigo 171 o meio mais eficaz aplicar o Direito Penal, visto que, a abrangência das condutas tipificadas são perfeitamente enquadradas, na sua generalidades, a todos os tipos de condutas delitivas contra o computador, periféricos, sistemas e informações.

Sujeito ativo

É o agente que se locupleta com a vantagem ilícita, que se utiliza dos meios informáticos a induzir ou manter a vítima ou alguém em erro, é pois á regra.

Sujeito passivo

É a pessoa jurídica ou física que suporta o prejuízo pela ação delituosa.

Ação física

O que caracteriza o estelionato na informática é o meio fraudulento, o artifício, o ardil que é usado pelo agente ativo para atingir o patrimônio de outrem.

O computador, como meio fraudulento é, em nossos dias, uma ferramenta poderosa e eficiente nas mãos de delinqüentes que tenham conhecimento técnico, haja vista que, por exemplo, os maiores prejudicados por este tipo de delito tendo como ferramenta os meios informáticos, são as instituições financeiras.

A fraude eletrônica é, para muitos, o sinônimo de crime de informática, por isso, incontáveis são as formas físicas aptas a alcançar a consumação do delito de estelionato, pela via eletrônica.

Dolo

Requer o dolo genérico, ou seja, a vontade livre e consciente de praticar o fato punível e antijurídico.

Consumação e tentativa

Consuma-se pelo alcance da vantagem ilícita, em prejuízo alheio. É, também, admissível na forma tentada, na sua amplitude conceitual, porém, é de ser buscado o meio utilizado pelo agente, vez que impunível o meio inidôneo.

Por outra, é de ser ressaltado o estelionato, que tem como ferramenta os meios informáticos, é de difícil coleta de provas, pois, os conceitos de admissibilidade dos meios informáticos como meio probante, são, ainda, insipientes em consolidá-los como meio hábil de prova. São necessárias muitas pesquisas e coleta de elementos circunstanciais para iniciar-se, até, o próprio inquérito policial.

DIVULGAÇÃO DE SEGREDO

A regra do artigo 153 (Código Penal) permite, de forma extensiva, se pode aplicar às ações que resultem em violação de segredo, coletados e captados por meio da informática, de forma desautorizada, e, principalmente, se produzirem danos à vítima.

Mesmo entendimento deve ser aplicado ao que se refere ao artigo 154 (Código Penal), o qual, ao nosso entender, nada mais seria do que uma causa de aumento de pena, referente ao artigo 153.

Tal entendimento exsurge, por exemplo, nos sedimentos da transmissões de mensagens via computador. Principalmente hoje, com o advento da grande infovia que é a INTERNET, vez que, o usuário tem endereço eletrônico, no qual recebe suas correspondências informatizadas.

Objeto material

É o documento ou a correspondência, seja ela na forma que for, pois a norma visa a proteger a liberdade individual, e assim, qualquer violação de meio físico de armazenamento de segredo tem que ser considerado como documento ou correspondência.

Sujeito ativo

É todo aquele agente que viola correspondência ou documento eletrônico, passando a divulgar segredo neles contidos.

Sujeito passivo

Aqui cabe ampliar o entendimento desposado pelo Código Penal. Como o delito se concretiza pela violação e divulgação de segredo, esta ação não só atinge o destinatário, como também, o remetente, pois o segredo pertence a ambos, e a sua divulgação prejudica aos dois. Por isso, pode ser pessoa física ou jurídica.

Ação física

É o ato de violar e revelar o conteúdo de documento ou correspondência eletrônica, desde que contenha segredo. Aplica-se quando o agente viola o computador visando os segredos armazenados nos acumuladores do equipamento, assim, pois, trata-se de um crime puro de informática.

Elemento subjetivo

É o dolo, a vontade consciente e livre de violar e divulgar o segredo contido em meios eletrônicos.

Elemento material subjetivo

No caso da informática, muitos segredos podem e são mantidos em arquivos de dados. Se violados e divulgados, ter-se-ia a aplicação dos artigos 153 e 154 do Código Penal, c/c a norma de informática penal própria, pois, entendemos, neste caso, um crime de informática puro, todos na forma do artigo 69 do Código Penal.

A Lei dos direitos autorais
Contra a propriedade intelectual

Os direitos autorais são regulados em nosso país pela Lei n. 5.988, de 14 de dezembro de 1973 e pela Lei n. 6.895, de 17 de dezembro de 1980. A primeira definindo direitos morais e patrimoniais do autor e a segunda adequando a violação de direito de autor à Convenção Internacional celebrada em Genebra em 29 de outubro de 1971 e promulgada no Brasil pelo Decreto 76.906, de 24 de dezembro de 1975.

Assim o artigo 184 do Código Penal, tem a redação dada pela Lei 6.895/80, portanto, aplicável aos crimes de informática que envolverem direitos autorais, principalmente nos crimes de pirataria, cópias de sistemas não autorizada.

Contra a propriedade industrial

Infrações típicas da área dos negócios, ou crimes do colarinho branco, não acarretam muitos processos penais, preferindo os interessados recorrer a acordo comerciais e indenizações na área civil. De um modo geral a propriedade industrial compreende o direito exclusivo do autor de uma descoberta ou de uma invenção de apropriar-se dela, o direito de uso exclusivo de marca de indústria ou comércio, desenho ou modelo, nome ou designação especial que distinga seus produtos de similares. Todos são passíveis de terem como meio o computador e seus sistemas.

O Código da Propriedade Industrial é a Lei n. 5.772, de 21 de dezembro de 1971, que conservou, em matéria criminal, os dispositivos da lei que veio substituir, o Decreto-lei n. 7.903, de 27 de agosto de 1945, que já previa essas infrações.

A Lei do "software"
A Lei n. 7.646, de 18 de dezembro de 1987, denominada Lei de Informática, no seu artigo 2º declara que o regime de proteção à propriedade intelectual de programas de computador é o direito do autor - Lei n. 5.988, de 12 de dezembro de 1973, mas com as modificações que estabelece para atender às peculiaridades inerentes aos programas de computador.

Um problema agregado a este assunto são as leis que protegem a propriedade intelectual é que vão se tornando obsoletas em razão das novas formas de "pirataria".

A indústria do "software" é um dos negócios mais rendosos da atualidade, com um mercado global de mais de 77 milhões de dólares no ano de 1994, segundo dados do Departamento de Comércio dos EUA. Na maioria dos países, o número de computadores e sistemas tem crescido de forma vertical, e se prevê um crescimento contínuo em todo o mundo, e a pirataria de sistemas e programas tem ameaçado seriamente o futuro econômico desta industria. A cópia ilegal de programas obstaculiza a inovação e destrói os incentivos econômicos necessários para a criação de novos programas e aplicações.

Em razão disso é que se deve aplicar com rigor as normas existentes a coibir tias práticas delituosas, bem como, incentivar a edição de legislação que possa acompanhar a evolução dos programas e das técnicas de vilipendio dos direitos intelectuais.

CRIMES DE INFORMÁTICA EM ESPÉCIE

Contra um sistema de informática

Os atentados contra o sistema de informática podem, de acordo com o objeto material da ação apresentar duas modalidades, as ações dirigidas contra o próprio computador, enquanto elemento físico, suas peças, acessórios, ou contra dados e informações nele contidos.

Contra o computador

Aí estão compreendidos os furtos comuns do próprio computador, do material de que é feito ou seus componentes, a sua apropriação indébita, portanto, até aqui, plenamente tipificados e resolvidos no âmbito da legislação comum. Não merecendo, todavia, a comporem os crimes de informática, pois o computador representa apenas um objeto, como outro qualquer, sobre o qual recaí a ação criminosa, de modo que se trata de crime contra o patrimônio. Portanto, delito comum.

Quando a ação criminosa visa a ser a danificação, sabotagem informática, inclusive os atos praticados contra os suportes materiais da informação, como disquetes, fitas magnéticas, etc., são, essencialmente, delitos que devem ser classificados como crimes de informática, pelas suas características e objetivo do autor dessa conduta ilegal .

Torna-se, de outra banda, muito mais difícil quando envolve situação em que é necessária a interpretação, no campo prático, dos chamados furtos de uso do computador, ou furto de tempo do computador. Tal utilização abusiva do computador consiste no uso desautorizado pelo proprietário, geralmente cometido por empregado, durante ou fora de suas horas de trabalho, com o fim específico de auferir proveito próprio.

A ocorrência costuma ser enfrentada com indulgência pelos lesados, todavia, seja reprimida em algumas legislações pois não deixa de representar um desfalque patrimonial ou desapossamento da coisa por certo lapso de tempo, além de importar no desgaste do material e da máquina, quando não a sua perda.

No Brasil, sabidamente não é prevista na norma material penal, porém existem criações jurisprudências, que, via de regra, têm descaracterizado a conduta do furto de uso, pois os julgados são rigorosos no sentido de que para ser caracterizado o furto de uso exigem enérgicas condutas, quais sejam, o uso momentâneo da coisa subtraída e sua devolução intacta no lugar de onde foi retirada; ausência de ânimo de apropriar-se da coisa. E, assim é manifesta a Jurisprudência:

"Para a caracterização do furto de uso a coisa subtraída depois de usada normalmente, deve ser imediatamente devolvida . Não basta a simples intenção de devolvê-la nem a alegação de que circunstâncias independentes da vontade do agente impediram-no de restituí-la. A

prevalência da ilicitude da ação é sempre dirigida em relação ao fato genérico, isto é, o furto comum"(TACRIM-SP AC - Rel. Renato Mascarenhas - JUTACRIM 80/402).

Demonstra-se, portanto, que atendidos requisitos elencados, sempre o julgador atenderá ao acusado, que é absolvido quando a coisa foi subtraída sem ânimo definitivo de apropriar-se e depois devolvida, num curto espaço de tempo, nas mesmas condições e estado que estava anteriormente. Nos casos dos veículos assim furtados, os Tribunais exigem, porém, que a gasolina gasta seja recolocada pelo usuário antes da devolução, sob pena de ficar caracterizado o furto do combustível, esse sim merecedor de sanção.

Nessa esteira, seguramente, os nossos Tribunais chamados a manifestar-se sobre o furto de uso num caso concreto, é muito provável apliquem os critérios para isentar de punição o seu autor, principalmente se a ação se restringir à subtração de tempo e disponibilidade da máquina simplesmente.

Contudo, tal entendimento é aceitável para casos em que o prejuízo é irrelevante, porém, não será solução satisfatória para atender a situações em que o prejuízo seja de monta, ou se tal conduta é freqüente, ou, ainda, fique caracterizado um abuso de confiança , também não incriminado na nossa legislação.

Exsurge, desta conduta de "furtum usus", a possibilidade de furto de energia , como já decidiu a Corte de Cassação belga, em 23.09.81, já que a lei penal brasileira, em matéria de furto, equipara à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.

Embora tais soluções, furto da energia elétrica ou de arquivos ou relatórios formatados, também, parece-nos inadequado, pois, não se trata de penalizar a ínfima consumação feita pelo autor, ou o desgaste irrisório do computador, mas sim o enriquecimento ilícito em detrimento do proprietário do computador.

Seria necessário, haja vista que não existe no nosso Código Penal a figura de furto de uso, que se cuidasse dessa situação na legislação especial, na área especifica de informática. No presente resta tão somente ao proprietário do computador buscar a via judicial civil para ter ressarcido o seu dano e/ou prejuízo.

A prática delituosa conhecida no meio informático como "superzapping", que é a quebra do programa do computador. É a paralisação do computador, impedindo que ele realize operações normais e, com isso, permite o acesso ao banco de dados e memória e, portanto, a todo o sistema informático.

Contra dados e/ou sistemas de computador
Atos contra as informações que o computador mantém e fornece podem consistir na cópia desautorizada das informações nele contidas, na alteração de parte ou o todo das informações armazenadas pelo computador, ou a destruição completa dos dados pela exclusão do conteúdo dos suportes.

a) a cópia desautorizada, também chamada de pirataria informática, não se enquadra na apropriação indébita nem no delito de furto, pois não se trata de coisa corpórea, mas de informação copiada. Nem há subtração pois seu proprietário não é desapossado dela. Não havendo também estelionato, pela ausência de meio fraudulento, a questão deve ser remetida para a área de proteção da propriedade imaterial, ou, mais precisamente aos direito do autor, embora, ao nosso entendimento se trate de delito de informática, como já externado em sua amplitude e definição.

b) outra forma de atentados contra os dados e/ou informações, a alteração dos programas do computador que pode ser efetuada pela troca de cartões, discos ou fitas por outros de conteúdo falsificado ou modificados permitido o acesso a banco de dados, registros e codificações, também classificado espionagem de informática.

Tal fato também é tratado no âmbito do direito autoral e a exclusividade da utilização dos programas, porém, pode e invariavelmente envolve procedimentos de falsificação, portanto, passível de ser incriminada na legislação penal comum.

Uma das mais conhecidas técnicas consiste na sabotagem de um programa, a qual consiste em se colocar no computador outras instruções no lugar das originais, ou outro programa que irá coexistir com o original, alterando-o sem destruí-lo.

Esses fatos deveriam ter pelo legislador um cuidado maior, atentando a uma tipificação mais completa, pois a legislação que trata do direito do autor não seria suficiente para atender, porque comporta outros bens ou interesses que deveriam ter a proteção jurídica.

c) ainda poderia ocorrer a destruição total do programa do computador, seja pela exclusão (apagamento) do conteúdo dos suportes, seja pelo desvio de comando, com graves danos ao usuário.

Inserem-se nesta categoria os diversos métodos de atentados que são conhecidos por contaminação ou introdução de vírus no computador, que invadem os equipamentos destruindo ou alterando programas ou, ainda, impedindo o acesso a eles.

É um fenômeno recente e temido, o vírus eletrônico, que nada mais é do que a introdução de um programa no computador, que se reproduz sem autorização do usuário e interfere nos procedimentos normais da máquina, após ser ativado pelo próprio funcionamento do computador.

No Brasil são inumeráveis os computadores de empresas que tiveram elevados prejuízos pela inoculação desses programas que são chamados de vírus do computador, inclusive, empresas de grande porte como Petrobrás, Embratel, Banco Real, American Express, White Martins, BNDES, Universidade de São Paulo, PUC-RJ, e, o mais recente os computadores do Hipódromo da Gávea, no Rio de Janeiro, por ocasião do último Grande Prêmio Brasil, que foram inoculados pelo vírus Hiroshima 50 anos, que causou prejuízos elevados.

Os vírus chegaram ao Brasil pelas cópias piratas, outros são criações brasileiras, porém, são competentes para alcançarem seus objetivos, quase sempre devastadores. Uns são até benignos, como o "ping-pong", não causam danos aos computadores ou seus arquivos, contaminam apenas os disquetes do usuário. Outros, porém são devastadores, como o "sexta-feira 13", torna o computador mais lento, além de apagar os arquivos, e o tradicionalmente mais terrível, o "madona" que ao final de um strip-tease da cantora, avisa que o disco está se apagando.

De acordo com a Universidade Federal de São Paulo, os computadores podem ser contaminados por três modos diferentes:

quando um disquete com vírus é introduzido no computador;

quando programas e dados são passados por linhas telefônicas, através de modem de transmissão e

através de teclado, quando uma pessoa abre um programa e introduz, intencionalmente, um vírus.

Também a técnica denominada "lata do lixo" que consiste na procura em latas de lixo, especialmente dos grandes edifícios de escritórios, onde estão as matrizes dos grandes conglomerados, de restos de lançamentos de computadores, ordens, códigos, linguagem e outras informações.

Deve ser incluído o denominado "vandalismo", que consiste na destruição quer da máquina quer dos sistemas de processamento. Esses ataques são normalmente armados e são usados, na destruição dos equipamentos, bombas. Fatos desse gênero ocorreram na Austrália, África do Sul e Alemanha.

Ainda que se possa atribuir a empregados descontentes com a empresa, o mais comum é de terceiros ligados a ex-empregados. Outro tipo de vandalismo, mais civilizado, porém, ao sistema, altamente letal, é a destruição dos meios de armazenamento, seja pela destruição física ou por desmagnetização. Este, considerado o meio mais "asséptico".

Assim, por clara, a facilidade e o perigo que representam essas ações quando intencionalmente efetuadas por alguém para causar danos ao empregador ou concorrentes.

O enquadramento típico como dano intencional muitas vezes não reflete a amplitude do problema e da situação, pois essa conduta delituosa só se verifica na hipótese da ocorrência de prejuízos patrimoniais.

Um dos meios que os usuários encontraram para protegerem-se dessas investidas criminosas foram os programas de diagnósticos desenvolvidos para identificar e detectar a presença de certos vírus, além de informar procedimentos a serem seguidos pelo usuário em face de uma contaminação. De outra, medidas preventivas podem ser tomadas e têm sido

amplamente divulgadas, de modo a neutralizar os resultados danosos dessas ações, e, em casos extremos devém ser punidas com sanções previstas na lei civil e na lei penal.

Por intermédio de um sistema
Contra o patrimônio

Destaca-se o furto, o dano e o estelionato como as formas mais usuais de infrações contra o patrimônio, vez que, praticamente todas as infrações podem ser cometidas pela utilização de sistema de informática.

O estelionato, que é caracterizado pelo emprego de meios fraudulentos para obtenção de vantagem ilícita, alcança os exemplos mais conhecidos e mais freqüentes dessas condutas criminosas.

Destaca-se o caso de desvio, em geral praticada por funcionário, de frações de quantias ou contas arredondadas nos cálculos financeiros de clientes ou de empresas, acumulando-se lentamente em conta pessoal determinado pelo delinqüente.

De outra forma, através do uso de cartão personalizado, fornecido por instituições bancárias, para funcionar nas contas eletrônicas, por meio de código pessoal, de que o agente delituoso se apoderou por meio de furto, falsificação, ou mesmo tendo encontrado o cartão.

Neste caso, quando o próprio usuário do cartão utiliza para sacar valores além do limite, complica-se e carreia uma gama imensurável de entendimentos doutrinários em torno da questão. Entre nós, ampla a conceituação legal do estelionato permite compreender nessa figura qualquer vantagem ilícita em prejuízo alheio, por qualquer meio fraudulento, e facilita a sua aplicação.

Contra a liberdade individual

Nessa, a informática é meio para violar direitos à intimidade, ao segredo ou à liberdade das comunicações.

A fraude informática presta-se, com perfeição, à revelação de segredos. Dependendo do caso, a ação poderá ser tipificada por violação de correspondência, violação de segredo ou violação de segredo profissional, todas perfeitamente tipificadas no Código Penal , como crimes contra a liberdade individual.

É garantido a todos o direito de à intimidade e à vida privada, bem como à imagem da pessoa pela Constituição Federal de 1988, no seu artigo 5º, inciso X, o qual garante o direito à indenização pelo dano material ou moral decorrente de sua violação. Porém, a lei penal vigente não prevê adequada proteção a esses interesses, que são alvos constantes pela utilização de novas técnicas eletrônicas ou sistemas de informática.

Contra a propriedade imaterial

Presta-se com eficiência a informática para a prática de violações dos direitos da propriedade literária e artística e, também, dos privilégios de invenção. Esses ataques são regulados pela legislação sobre direito autoral, na qual são definidas as modalidades, indicando sanções, que, por enquanto, face a inexistência de legislação específica, podem ser aplicados a determinadas condutas que se utilizam do computador e dos seus sistemas.

Na mesma medida e com o mesmo entendimento, as condutas que violam os privilégios de invenção, regulam-se pelo Código de Propriedade Industrial, e, na ausência de legislação específica aos delitos cometidos por meio de sistema de computador.

Via INTERNET

É importante que se tenha claro que a cada nova criação ou avanço tecnológico na área de informática também avançam os crimes de informática ou pela informática. Principalmente, quando exemplificamos, neste trabalho, que o computador e os sistemas que nele operam poderiam ser instrumentos de delitos comuns, não exageramos, pois no exemplo dado que, se através de um computador, pudesse ser dado uma ordem para matar alguém, por meio de várias combinações, seria um delito comum de informática. Para tanto, reproduzimos duas matérias publicadas em O Globo (1995, p.51), que dão a exata dimensão do uso do computador nos crimes comuns e do que o avanço tecnológico trouxe o uso delituoso da informática:

"JOVENS SÃO ATRAÍDOS POR INTERNAUTAS EXPERIENTES

Washington - A maioria dos menores nas casos já apurados de CIBERSEX foi atraída por adultos que se passavam por jovens, no computador. Um deles Alan Barlow, funcionário do Correio em Seatle, foi condenado a seis anos de prisão por ter tido relações sexuais com uma menina de dez, e também por ter tido contados obscenos por via eletrônica com meninos de vários estados. Uma lei federal, já em vigor, diz que é crime atrair menores a relações sexuais. Além disso, transportar material pornográfico de um estado para outro também é crime. Por isso, vários juristas têm opinado que não seria necessária mais uma lei para coibir abusos. O caso de Barlow, um inveterado usuário das BBS pornográficas encontradas na INTERNET ilustra isso. Ele acabou caindo numa armadilha banal: foi preso em Mamaronack, no estado de Nova York, onde tinha marcado, por computador, um encontro com um adolescente de 14 anos, com quem vinha se correspondendo obscenamente via "e-mail". Nestas intensas conversas por escrito, ele dizia ter 13 anos. Na verdade tem 51."

"SEXO "ON-LINE" NOS EUA SEDUZ ADOLESCENTES E DESAFIA A CENSURA
(Jose Meirelles Passos- Correspondente)

Washington - Depois de dois dias de desespero, sem qualquer pista ou informação correta da Polícia sobre o paradeiro de sua filha Tara, de 13 anos, Lisa Noble decidiu ligar o computador da menina e verificar o seu "e-mail" - Correio Eletrônico. "Venha para cá. Nós poderemos correr pelo quarto, nus, o dia todo, a noite toda", dizia a última mensagem enviada à menina de St. Mathews, subúrbio de Lousville, em Kentucky. O convite era assinado por George e vinha de longe, de São Francisco, Califórnia. Logo depois, revirando

sua gaveta, ela encontrou cópias impressas de diálogos que Tara vinha mantendo com George durante várias semanas. O material era típico CYBERSEX, isto é, sexo cibernético, como vêm sendo denominadas as conversas sexuais via computador, a cada dia mais abundantes e intensas, e que agora estão sob ameaça de censura pelo Governo do EUA. Dias atrás, cinco casos semelhantes ao de Tara Noble serviram de argumento no Senado para aprovar a chamada Lei de Decência das Comunicações por ampla maioria de votos (84 a 16), provocando uma polêmica nacional. Muita gente crê que ela infringe o direito de livre expressão, sacramentado na Primeira Emenda da Constituição americana. Todos os cinco casos registrados desde janeiro passado envolveram crianças e adolescentes - descritos como CYBERPORN, a pornografia cibernética que circula através da INTERNET, o sistema interliga hoje 50 mil redes com cerca de 35 milhões de usuários (também conhecidos por internautas), em pelo menos 150 países. "A INTERNET tem sido chamada de enorme e ilimitada biblioteca internacional. E a emenda Exon limita a todos nós à seção infantil dessa biblioteca", reagiu Mike Godwin, advogado da Eletronic Frontier Foudation, instituição que promove informática. Um dos problemas da lei será a execução. Em muitos casos é impossível descobrir o autor de uma mensagem eletrônica. Quando a mãe de Tara Noble revelou o seu achado à Polícia de Lousville, o delegado local entrou em contato com o FBI - a Polícia Federal americana - e também com o Serviço Secreto. Agentes de suas respectivas Unidades de Crimes por Computador foram mobilizados. Mas a menina só foi encontrada porque ela mesma acabou ligando para a mãe, 13 dias depois de seu desaparecimento. "Mamãe quero voltar para casa", disse ela, de um telefone público, revelando seu endereço em São Francisco. No dia seguinte enquanto a mãe a levava de volta, o FBI prendia George por ter tido relações sexuais com uma menor.

Descortina-se, pelos artigos reproduzidos, que a rigor não são crimes de informática, ao nosso entender, porém, a informática foi instrumento de preparação de um delito comum, qual seja, entre nós, crimes contra a liberdade sexual.

Afloram, de tais fatos, em nosso ordenamento jurídico, crimes de estupro qualificado (arts. 213 e 224, do CP) e posse sexual mediante fraude (art. 215, do CP), demonstrando que a informática pode ser instrumento hábil para serem alcançados delitos comuns, e, nem por isso ser classificado como crime de informática.

Ainda, observa-se da matéria reproduzida que a norma aprovada pelo Senado Americano - a Lei de Decência da Comunicações - insere a conduta delitiva na correspondência via INTERNET. Desde já, e sem a profundidade de se conhecer o texto exato da norma, se transplantada para o Direito Penal pátrio, exsurgem dificuldades, tais como qual o foro competente ? O Código Penal adota a teoria finalista da ação, onde foi consumado o delito? Pode admitir a forma tentada ou a possibilidade de dolo ou culpa? Pode ocorrer o concurso de normas e de delitos?

Assim, ao nosso entender, esse tipo de crimes especiais, que envolvem crimes comuns e crimes de informática, devem ser avaliados pelo legislador brasileiro, pois as redes, a INTERNET é uma realidade em nossas casas, hoje, e, prestam-se a muitos outros tipos de delitos que estão inseridos ou não no Código Penal e na Legislação Penal Extravagante. Todavia, toda e qualquer legislação sobre crimes de informática, se forem meios a outros, não podem seguir a regra subsunção aos delitos comuns, pois assim, não evoluímos no

Direito Penal de Informática, porque os operadores do direito têm que experimentar um regramento nesse sentido, para construírem esse Direito que não é futuro, é presente.

O Direito penal de informática vigente

O Direito Penal de Informática caracteriza-se pela sua absoluta pobreza. A Parte Especial do Código Penal data de 1940 e as normas incriminadoras são de um tempo em que sequer existia o computador, de modo que as normas vigentes somente podem ser aplicadas aos crimes de informática de forma incidental a tais hipóteses.

O legislador brasileiro somente preocupou-se com o mau uso do computador, vez que a legislação existente dirige-se especificamente à pirataria de "software", jamais ao crime de informática, por excelência.

Também, os doutrinadores brasileiros acompanham a tendência internacional que protege o "software" ao entendimento do que seja direito autoral. O legislador aceita essa posição. Para tanto, a Lei 7.646, de 18 de dezembro de 1987, definiu em seus artigos 35 e 37 dois crimes que expressam esse entendimento:

Art. 35 - Violar direitos de autor de programas de computador:

Pena: Detenção, 6 (seis) meses a 2 (dois) anos e multa.

Art. 37 - Importar, expor, manter em depósito, para fins de comercialização, programas de computador de origem externa não cadastrados:

Pena: Detenção, de 1 (um) ano a 4 (quatro) anos e multa.

O artigo 35 retrata, com clareza meridiana, o objetivo do legislador em proteger o direito autoral, sem, contudo, mesmo assim, ser caracterizado como um crime de informática, e, sim, crime contra o direito autoral.

O artigo 37 cria a figura típica de contrabando de informática. O objeto jurídico é, tão somente, o erário público, prejudicado pela evasão da renda e da proteção dos "softwares" nacionais. Também, a norma carrega a amplitude da incidência genérica, tal como, no artigo 334 do Código Penal, o delito de contrabando e descaminho.

Pela simples leitura, vê-se que as regras legais citadas são manifestamente imperfeitas e insuficientes para os fins que se destinam, tanto assim, que com a mudança em matéria de política de informática, o delito de contrabando de "software" não cadastrado, já não mais tem razão de existir, vez que, hoje, não mais é necessário que seja cadastrado junto ao Ministério da Indústria e Comércio.

Ainda, ao apreço da norma nacional, que tem por finalidade, apenas, proteger a propriedade intelectual, em relação ao programa de computador, como manifestação de propriedade imaterial, fazendo-o da mesma forma que o Código Penal o faz, para a violação do direito

autoral em geral. Todavia, a pena prevista é, em muito mais gravosa que a determinada pela Lei Substancial Penal (detenção de três meses a um ano e multa).

O sistema legal ainda contempla proteção aos crimes contra a ordem econômica e contra as relações de consumo. No âmbito da ordem tributária, a Lei n. 8.137. de 27 de dezembro de 1990, define uma nova forma de mau uso do computador, qual seja, ação de utilizar ou divulgar programa de processamento de dados que permita ao contribuinte possuir informação contábil diversa que é , por lei, fornecida à Fazenda Pública, sendo apenado com detenção de seis meses a dois anos e multa. É, pois, um programa de computador destinado a permitir a fraude fiscal.

Ante essa paupérrima legislação, o aplicador do direito é obrigado a servir-se dos delitos tradicionais para o combate aos crimes de informática. Têm-se que muitas das condutas que caracterizam o crimes de informática, poderiam ser enquadradas na figura típica do estelionato. Todavia a velocidade do desenvolvimento tecnológico no setor de informática, não garante que se possa, eternamente, manter a aplicação do nosso Código Penal, ou seja, o enquadramento dos crimes comuns às condutas típicas do delitos de informática. Some-se a essa dificuldade presente, as diversas doutrinas e correntes que pululam a matéria criminal de informática, e mais, as próprias divergências em torno da aplicação do Direito Alternativo e a corrente que defende programa de descriminalização, que vertem profundas dificuldades ao aplicador do direito.

O projeto da nova Parte Especial do Código Penal
A proposta da nova Parte Especial do Código Penal, que deverá ser apresentada pelo Ministério da Justiça ao Congresso Nacional, no que diz respeito à tutela penal dos interesses e dos bens advindos ou redefinidos em sua importância, pela Sociedade de Informação Pós-Industrial, caracteriza-se por estabelecer um caminho próprio.

Os crimes de informática estão contidos em um Capítulo do Código Penal definidos como "Dos Crimes Contra à Ordem Sócio-econômica", da Parte Especial do Código Penal. O supracitado Capítulo conta com apenas oito artigos. Três destes artigos tratarão, especificamente, dos crimes de informática, enquanto outros três dispositivos tratarão da adequação de normas já existentes aos bens intangíveis redefinidos na sua importância, enquanto outros dois têm a finalidade de reprimir atos de atentado considerados especialmente graves à privacidade dos indivíduos, e perpetrados através do computador.

LICKS e ARAÚJO JÚNIOR (1994, p. 98), assim analisam essas novas normas, afirmando que "podemos dizer que, enquanto três artigos tratarão de computer crime, outros cinco estarão relacionados com o computer misuse."

Vê-se, pois, que os doutrinadores, a priori de um entendimento crítico, tanto no aspecto quantitativo, bem como o qualitativo, porque o Direito Da Informática, "in casu", o Direito Criminal da Informática, face a tantas doutrinas e as próprias complexidades apresentados pela Ciência da Informática, seguramente, não poderia o Brasil, tratar essa área do direito, não mais emergente, todavia, cada vez mais presente na vida do povo brasileiro, com tão pouca profundidade.

Propostas

Nessa nau de incerteza quanto ao Direito Criminal de Informática, e, também pode-se dizer, da própria incerteza do Direito Criminal Brasileiro, verifica se que outros projetos tramitam no legislativo brasileiro. Atualmente, estão em tramitação no Congresso Nacional os seguintes Projetos:

- Projeto de Lei do Senado n. 75 de 1989, que dispõe sobre a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. E, foi absorvido por outro, de n. 137 de 1989, que assim é redigido:

Art. 1º - - Constituem crimes contra a liberdade individual:

I - violar, mediante processo técnico ou qualquer outro meio, o resguardo sobre foto, imagem, escrito ou palavra da vida privada de alguém;

Pena - detenção de três meses a um ano.

II - fornecer ou utilizar, indevidamente, dado da vida privada de alguém, constante de fichário automatizado;

Pena - detenção de três meses a um ano.

Art. 2º - As penas cominadas no artigo anterior serão aumentadas até o dobro, se o agente houver atuado com fim de lucro ou abuso de função.

Art. 3º - A Ação Penal, nos crimes previstos nesta lei depende de representação.

O projeto não é, especificamente, uma norma voltada aos crimes de informática. É, na verdade, uma miscelânea entre o direito de imagem, a privacidade, e mau uso do computador. Além disso, pela sua vinculação aos delitos contra a vida privada e imagem, dependem de representação, enquanto que os crimes de informática não devem ser inscritos pela dependência de representação, e, sim, nos delitos de ordem pública.

- Tramita na Câmara do Deputados o Projeto n. 4.597, de 1990, que foi substituído pelo de n. 597, de 1991, que dispõe sobre o crime de interferência nos sistemas de informática, com a seguinte redação:

Art. 1º - Pratica crime quem, objetivando prejuízo de alguém, a um sistema, a computador, a equipamento que acompanha o sistema ou a computador:

a)destrua ou altere, dolosamente, ou utilize de modo indevido, programa de computador a que tem acesso;

b)abuse, por qualquer outra forma, de seu direito de acesso a computador, a sistema de computação, de transmissão de dados, ou de processamento de dados de qualquer espécie;

Pena - detenção de um a quatro anos e multa de igual ao valor do proveito visado ou do risco de prejuízo da vítima;

c)introduza, dolosamente, em computador, computador ou instrução-comando que destrua ou altere programa armazenado no computador, ou por qualquer forma que altere o seu desempenho;

Pena - detenção de um a quatro anos e multa igual ao valor do proveito visado ou do risco de prejuízo da vítima;

d)utilize senha de outrem para obter acesso indevido a um sistema ou a um computador;

Pena - detenção de um a três anos e multa igual ao valor do proveito visado ou do risco de prejuízo da vítima;

e)obtenha intencionalmente, sem estar devidamente autorizado, acesso a um sistema ou a um computador;

Pena - detenção de um a três anos e multa ao igual valor do proveito visado ou do risco de prejuízo da vítima;

Art. 2º - A interferência não intencional, por negligência, impudência ou imperícia, constitui crime culposo.

Pena - multa igual ao prejuízo causado. Mínimo de CR$ 170.000,00 (cento e setenta mil cruzeiros). Na reincidência, detenção de um a três meses e multa igual.

O projeto supra tem características mais próximas do que almejam os doutrinadores brasileiros, embora, ainda esteja distante, não da perfeição jurídica, do mínimo que atenda ao presente tecnológico, de modo a proteger o sistema, o computador, seus periféricos, e também o uso adequado.

Apesar de não preencher às necessidades da área de informática, é o mais completo, e tem nos especialistas, tanto da informática como do direito, ferrenhos defensores da sua aprovação. Todavia, entendemos que a normatização dos crimes de informática devem ser mais amplos, abrangendo um maior leque de condutas, bem como, ao detalhamento, pois vê-se que o projeto utiliza-se de verbos nucleares de grande abrangência, permitindo a criminalização de condutas que não são, ao nosso entender, passíveis de mensurá-las, tais como abuso, pois o conceito de abuso é amplamente subjetivo, o que permitiria inadequação da norma penal no mundo dos fatos.

O Sr. Presidente da República remeteu mensagem ao Congresso Nacional, de modo a dar seqüência à política de liberação dos meios de informática. Essa mensagem foi transformada em Projeto de Lei n. 997/91, que regula a proteção da propriedade intelectual de programas de computador e sua comercialização no País, e , dele exsurge:

eliminação das restrições a empresa nacional para distribuição e comercialização de programas de computador de origem externa;

a eliminação do exame de similaridade entre o produto estrangeiro e o nacional;

eliminação do cadastramento de programas de computador;

possibilidade de importação de cópias de programas de computador sem contrato de distribuição, objetivando maior competitividade do setor;

reforços aos direitos e garantias aos usuários de programas de computador.

O Projeto de Lei de autoria do então Senador Maurício Corrêa, que leva o n. 152, de 1991, a muitos tem a característica de ser o que introduz as maiores e mais importantes inovações, pois visa a garantir os dados de propriedade do usuário, de modo que o bem a ser protegido é a inviolabilidade dos dados e da comunicação. Entende, ainda, o projeto, que não se criaram novos crimes, o que foi alterado é a forma de cometimento dos delitos.

Assim, pois é o texto do projeto:

Art. 1º - Consideram-se crimes contra a inviolabilidade dos dados a sua comunicação a prática das condutas descritas nos arts. 2º e 3º desta lei.

Art. 2º - Violar o sigilo de dados, acessando informação contida em sistema ou suporte físico de terceiro, sem autorização deste;

Pena - Detenção de um a seis meses e multa.

§ 1º - Se o acesso se faz com uso indevido de senha ou de processo de identificação magnética de terceiro.

Pena - detenção de três meses a um ano e multa.

§ 2º - Se o acesso resultar vantagem econômica indevida, em detrimento ao titular do sistema, pune-se o fato como estelionato qualificado nos termos do artigo 4º desta lei.

Art. 3º - Inserir em suporte físico de dados, ou em comunicação de dados, programa destinado a funcionar clandestinamente no sistema de terceiro, causando nele efeito indesejado por seu titular.

Pena - detenção de um a seis meses e multa.

§ 1º - Se resulta perda definitiva de informação contida no sistema

Pena -detenção de seis meses a dois anos e multa.

§ 2º - Se, além da perda de informação, resulta prejuízo econômico para o titular do sistema.

Pena - Detenção de um a três anos e multa.

Art. 4º - A realização de conduta descrita nesta lei como meio para a prática de qualquer crime qualifica-o, agravando a pena de um sexto até a metade.

Art. 5º - A Informação ou dado constante de sistema eletrônico que, por qualquer razão, tenha relevância nas relações entre pessoas, considera-se "documento", punindo-se sua adulteração material e ideológica nos termos do Código Penal, como qualificadora do art. 4º desta lei.

Parágrafo Único - Para fins deste artigo considera-se "documento público" a informação constante de sistema:

a)pertencente ou a serviço de órgão público da administração direta ou indireta, instituição financeira, Bolsa de Valores ou estabelecimento de ensino oficial ou reconhecido;

b)em condições de autorizar pagamento, quitação, movimentação de conta corrente ou qualquer transferência de valores;

c)destinado ao acesso público, pago ou gratuito, a informações comerciais, econômicas ou financeiras."

Vê-se, pois, que o projeto é abrangente, inovador, porém, ainda, observa-se que a generalidade é a tônica dos verbos nucleares do tipo. É, ratificamos, necessário que as condutas sejam pormenorizadas, de modo a dar a característica do tipo que se quer punir. Apesar dos avanços, em termos de projeto, já que a legislação brasileira é pobre sobre o tema, é importante que os crimes de informática sejam normatizados ao abrigo do conhecimento técnico de condutas ilícitas, evitando-se, assim, as lacunas ocasionadas pela generalidade do seus núcleos.

Esta é a quarta parte de um trabalho do autor, escrito em outubro de 1995,
na conclusão de seu curso na Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS)
CRIMES DE INFORMÁTICA (III)

Direito Penal de Informática

Marco Aurélio Rodrigues da Costa
advogado em Uruguaiana (RS)
Face ao espaço considerável que ocupa na vida cotidiana, a informática apresenta-se no Brasil como na maioria dos países, como um fator dos mais relevantes nas relações econômicas e sociais e, conseqüentemente, nas relações jurídicas de qualquer natureza, sejam elas cíveis, administrativas, comerciais, etc.

Henry BOLSOY aponta (apud FERREIRA, 1992, p.143) três ordens de relações da informática com o Direito Penal:

"a) a informatização da documentação penal", que compreende o famoso fichário policial e os arquivos judiciários e dos serviços de segurança, contra os quais muitas vezes se faz necessário reforçar as medidas de proteção e as garantias individuais pela excessiva ou leviana intromissão dos órgãos estatais na vida privada dos cidadãos.

Nesse sentido a Constituição Federal Brasileira, de 05 de outubro de 1988, temos:

"conceder-se-á habeas data:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes nos registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo."

Essa garantia constitucional visa a prevenir que atos dos órgãos públicos, baseados em informações sigilosas, permaneçam ignorados pelo interessado, que ficaria assim impedido de qualquer defesa ou objeção.

"b) a informação dos procedimentos administrativos e processuais", melhorando e aperfeiçoando a distribuição da justiça, aliviando os trabalhos judiciários e facilitando o cumprimento das sentenças e execuções penais.

Os órgãos da Justiça Penal Brasileira, principalmente de grandes centros urbanos, vêm-se se modernizando e se aparelhando com o processamento automático de dados, o qual , mais do que uma conveniência, tornou-se uma necessidade imperiosa ante ao grande volume de processos que superlotam os nosso tribunais e, na área penal, pela facilidade que esse procedimento representa para a correta informação sobre antecedentes dos acusados, por exemplo.

"c)a informática a serviço da delinqüência", permitindo-se falar em infrações favorecidas pela informática.

Esses crimes de informática ora apresentam apenas novas maneiras de executar as figuras delituosas tradicionais, ora apresentam aspectos pouco conhecidos, que não se adaptam às incriminações convencionais e seus autores aos tipos criminosos comuns.

Uma das exteriorizações mais freqüentes é a fraude praticada com diferentes formas de manipulação de dados e programas ou utilização abusiva do computador. Mas, também, o furto, a apropriação indébita, o vandalismo, causando consideráveis prejuízos patrimoniais, são formas comuns de abuso da informática, além de que, são realizados na área do Direito Penal Econômico (crimes do colarinho branco), ou contra a liberdade individual (violações

da intimidade ou sigilo das comunicações, ou, na área do direito do autor ou da proteção de marcas de indústria e comércio (sabotagem ou espionagem industrial).

De outra banda, inúmeros problemas e grandes prejuízos podem ser causados pelas ações praticadas contra o funcionamento da própria máquina, como é o caso dos disseminação proposital do chamado VÍRUS do computador, destruindo programas fichários do usuário e, o caso mais recente, que teve repercussão em todos os meios de comunicação do mundo, foi a ação do vírus HIROSHIMA 50 ANOS, que atacou os computadores do Hipódromo da Gávea, quando da realização do Grande Prêmio Brasil, causando prejuízos de grande monta, e tal ação criminosa foi atribuída ao grupo ecológico internacional "GREENPEACE".

E quais dessas condutas têm relação com o Direito Penal?

Duas grandes fendas emergem de pronto: por um angulo a tipificação dessas condutas que se inserem em razão do meios empregados e seus agentes o "white collar crim" (crime do colarinho branco).

De outro a complexidade dos sistemas de computadores e eles próprios, que dificultam a que se descubra o golpe, como impedem que as raras provas cheguem à Justiça.

Aqueles que tratam do Direito Penal, qualquer que for a fase (policial ou judicial) têm profundas dificuldades em consolidar provas capazes de, até, iniciar um inquérito policial, quiçá oferecer denúncia.

Para se ter a idéia dessa complexidade e da própria dificuldade em aplicar o direito vigente, Valdir SZNICH (1992, p.15) alenta a hipótese de que:

"o agente dá uma ordem ao computador - dentro da programação - repete realizando-se, espaçadamente, a mesma operação. Tem-se inicialmente o que se chama delito à distância, mas que para a doutrina penalista de pouca valia tem para o agente. No caso citado o agente realiza uma conduta delituosa e, dada a programação, de tempos em tempos essa mesma conduta se repete. Que espécie de infração temos aí? Crime instantâneo de efeitos permanentes, crime permanente ou continuado?"

Como se vê, para tal solução tem ser apurado o meio, a localização do agente, o meio empregado, o objetivo, o resultado e os efeitos do resultado, sem falar que emerge, necessariamente, a questão da competência. Para tanto, digamos que o agente estivesse em uma cidade e o resultado foi alcançado em outra e o lesado, ainda, em cidade distinta de ambas.

Tal delito, seguramente, trará problemas de ordem jurídica material e processual, portanto, temos como improrrogável ser escrito o Direito Criminal Brasileiro de Informática.

OS SISTEMAS DE CLASSIFICAÇÃO DOS CRIMES DE INFORMÁTICA

Diversas classificações são propostas para ordenar o estudo da matéria, sendo mais comuns os que se baseiam na distinção entre os crimes tradicionais, pela utilização da informática, e , noutra categoria, as outras ações de abuso de informática, específicos dessa área.

Essa é, exemplificando, a classificação de Ivete Senise FERREIRA (1992, 9. 147), que se baseia no trabalho de Martine BRIAT, que distingue:

manipulação de dados e/ou programas a fim de cometer uma infração já prevista pelas incriminações tradicionais;

falsificação de dados ou programas;

deteriorização de dados e programas, e entrave à sua utilização;

divulgação, utilização ou reprodução ilícitas de dados e programas;

uso não autorizado de sistema de informática;

acesso não autorizado a sistema de informática.

Ivete Senise FERREIRA, preferiu em sua classificação, não fazer menção aos computadores nem os seus elementos técnicos, os quais podem sofrer modificações muito rápidas pelo avanço da tecnologia neste setor.

Outras pessoas pensam de modo diferente, como Marc JAEGER (1985, p.23) que, além de preferir o termo fraude informática, tomado no sentido lato, para designar todos os ilícitos penais ou ações repreensíveis ligadas à informática, distingue nelas duas categorias apenas:

fraudes propriamente ditas;

atentado à vida privada.

Todavia, existia a possibilidade de, na prática, várias dessas ações se misturarem, e com esse entendimento propõe Hermann Cohem JEHORAM (1991, p. 278) para as fraudes uma classificação que se baseia no próprio equipamento utilizado:

fraudes no nível da matéria corporal ou do "hardware", ou seja, contra a integridade física do computador;

fraude ao nível do input, ou seja, na entrada de dados;

fraudes ao nível do tratamento dos dados, ou seja, modificação apenas dos programas, sem atingir os dados;

fraudes ao nível do output, ou seja, intervenção no resultado obtido a partir de dados corretos, corretamente tratados.

Muitos doutrinadores, porém, baseiam-se na finalidade visada pelo autor do delito para classificá-lo, que envolvem os crimes de informática aqueles que se enquadram no Código Penal ou aqueles que não são cometidos por meio de computador, mas, sim, por ocasião da utilização dele, e depois distinguem duas características:

a) manipulações para obtenção de dinheiro, em sentido do proveito econômico;

b) manipulações para obtenção de informações de forma individual, ou seja, não teria direito.

Essas inúmeras outras classificações constituem uma tentativa para analisar a complexidade das situações que na prática podem surgir com a utilização abusiva da informação, bem como medidas legais para evitá-las.

Também, por peculiares, transcrevemos a classificação de Hervé GROZE e Yves BISMUTH, (1986, p. 207);

os atos dirigidos contra um sistema de informática, por qualquer motivo;

os atos que atentam contra outros valores sociais de um sistema de informática.

Na primeira categoria, que constitui o verdadeiro núcleo da delinqüência informática, segundo GROZE e BISMUTH, situam-se os variados componentes que atentam contra o material, seja contra os suportes lógicos ou dados do computador.

Na segunda categoria, pode-se dizer que cabem todas as espécies de infrações previstas nas leis penais, lembrando que ao nosso entender não é delito de informática, pois os meios da informática são meros instrumentos de delitos comuns, como o exemplo já citado, daquele que por meio de um computador emana instruções para matar alguém. Não estará cometendo um crime de informática, e, sim, um homicídio, artigo 121, "caput", do Código Penal.

Não obstante as classificações elencadas, entendemos que os crimes de informática dever ser classificados quanto ao seu objetivo material, a saber:

Crime de Informática Puro

São aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. Entendemos serem os elementos que compõem a informática o "software", o "hardware" (computador e periféricos), os dados e sistemas contidos no computador, os meios de armazenamento externo, tais como fitas, disquetes, etc.

Portanto são aquelas condutas que visam exclusivamente a violar o sistema de informática do agente passivo.

As ações físicas se materializam, por exemplo, por atos de vandalismos contra a integridade física do sistema, pelo acesso desautorizado ao computador, pelo acesso indevido aos dados e sistemas contidos no computador.

Portanto, é crime de informática puro toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.

Crime de Informática Misto

São todas aquelas ações em que o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação.

Quando o agente objetiva, por exemplo, realizar operações de transferência ilícita de valores de outrem, em um determinada instituição financeira utilizando-se do computador para alcançar o resultado da vantagem ilegal, e, o computador é ferramenta essencial, defrontamo-nos com um crime de informática misto.

É crime de informática misto porque incidiriam normas da lei penal comum e normas da lei penal de informática. Da lei penal comum, por exemplo, poder-se-ia aplicar o artigo 171 do Código Penal combinado com uma norma de mau uso de equipamento e meio de informática. Por isso não seria um delito comum apenas, incidiria a norma penal de informática, teríamos claramente o concurso de normas (art. 70, CP).

Crime de Informática Comum

São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta a perpetração de crime comum, tipificável na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta.

Como exemplo, os casos de estelionato (art. 171, CP), e as suas mais amplas formas de fraude. Quando o computador é ferramenta escolhida pelo agente ativo, que poderia escolher outros meios diversos da informática. Porém, é de se pensar na possibilidade de qualificadora para o delito de estelionato o uso do sistema de informática.

Despiciendo aclarar a aplicabilidade aos crimes comuns das normas penais vigentes, porém, poder-se-ia, atendendo a essa classificação, incorporar ao Código Penal agravantes pelo uso de sistema de informática, vez que é meio que necessita de capacitação profissional e a ação delituosa por esta via reduz a capacidade da vítima em evitar o delito.

Posto isto, entendemos ser a presente classificação apta a elaboração de legislação que possa alcançar os delitos de informática, sem contudo, correr-se o risco de sobreposição de normas, e, assim, também, entendemos que é meio hábil à formação de um eficaz Direito Penal de Informática.

CRIMES DE INFORMÁTICA E SEUS OBJETIVOS

Antes mesmo da classificação dos crimes de informática, é de ser avaliados e analisados os bens cuja proteção devem ser objeto do ordenamento jurídico vigente, ou através de novos tipos específicos.

Existe ainda hoje uma bipolarização em torno de que bem jurídico é fundamentalmente protegido pelo Direito Penal de Informática, se os sistemas ou se as informações.

O Organização para a Cooperação Econômica e Desenvolvimento, FERREIRA, 1992, p. 141., apesar de definir de forma ampla os delitos de informática, é favorável à proteção da informação, embasada na importância das informações na sociedade pós-industrial.

O National Center For Computer Crime Data, dos EE. UU., (apud LICKS e ARAÚJO, 1994, p. 89) defende a posição de que o Direito Criminal de Informática é concebido para proteger os sistemas de computadores e das comunicações, além da informação.

Deve, assim, ser entendido, que a preocupação do Direito Criminal de Informática com os sistemas de computadores e de comunicação deve-se, fundamentalmente, à proteção dos seus componentes imateriais ou intangíveis, ou seja, o "software" e dados, e os dados que ainda não contam com a mesma proteção do outro componente, o "hardware".

Embora a distinção entre "hardware" e "software" seja pacífica do ponto de vista técnico fático, não podemos dizer o mesmo quanto às implicações jurídicas. O Direito ainda caminha lentamente para a implementação de um sistema jurídico que proteja os bens incorpóreos e imateriais tão bem como os bens materiais.

Quando se cogita da proteção de bens imateriais, logo temos o exemplo da propriedade intelectual, como o Direito do Autor, um dos mais antigos dispositivos de proteção da propriedade imaterial, que visa a dar proteção ao autor da obra.

Neste ponto, por oportuno, deve ser aberto um nicho de informação, no que tange ao direito sobre propriedade imaterial, mais precisamente o Direito do Autor.

A obra criada por computador é uma forma tornada possível pela técnica da informática e que se amplifica com os modernos sistemas de inteligência artificial.

Mas logo surge quem pretenda atribuir-se direitos exclusivos em relação a essa obra; e mais quem pretenda que a tutela seja outorgada pelo Direito do Autor. Assim, já a lei inglesa de 1988, na sua seção 178, prevê que para as obras geradas em circunstâncias não há autor humano; mas, paradoxalmente, considera autor a pessoa por quem foram empreendidas às disposições ("arrangements") necessárias para a criação da obra. Em última análise, acaba por beneficiar o produtor. Também no Japão, o dono da máquina é dono de tudo o que ela produz.

Em Portugal, porém, nenhuma proteção é admissível. Porque a obra criada por computador nem é objeto de proteção específica, nem cai em nenhum dos tipos existentes.

No Brasil, nessa área, especificamente, existe a Lei n. 5.988, de 14 de dezembro de 1973, que regula os direitos autorais, sem, contudo, qualquer dicotomia sobre minúcia da informática. É uma norma genérica. Em relação à informática, temos a "Lei do Software", Lei n. 7.646, de 28 de outubro de 1987, que foi regulamentada pelo Decreto n. 96.036, de 12 de maio de 1988, que dá proteção jurídica somente ao "software".

Tal fenda foi aberta para demonstrar o quanto é complexo esse novo direito que nasce, que é o Direito da Informática, e, para nós, o Direito Criminal da Informática.

Assim, durante muito tempo os bens jurídicos imateriais de uma forma geral foram confundidos com os objetos protegidos pelos institutos da propriedade intelectual. Não se deve pensar que só porque os bens como a invenção e a criação, protegidos pela propriedade intelectual foram durante muito tempo os únicos bens imateriais mensuráveis, aferíveis e protegidos pelo direito patrimonial, que eles são os únicos bens imateriais relevantes para o Direito, atualmente. É. pois, um instituto diferente da propriedade intelectual e o segredo de indústria ou de comércio, estes já respaldados por diversas legislações, onde o bem tutelado é essencialmente uma informação ou conhecimento, e não a criação intelectual.

Fora da esfera patrimonial do direito privado, têm-se, no campo dos direitos fundamentais da pessoa humana, a tutela de bens imateriais, aí, de uma aferibilidade e mensurabilidade mais subjetiva, mas nem por isto inexistentes ou irrelevantes. Tais direitos também já são assegurados e protegidos por inúmeros dispositivos legais, tanto na comunidade internacional como nas legislações.

O computador vem trazer novos desafios para os crimes já previstos nestas três modalidades de entendimento, através de formas quanto ao meio de cometimento de tais delitos. A detecção e a efetiva acusação de crimes já tipificados nos crimes em que se utiliza o computador torna-se maior o grau de reprovabilidade da conduta face ao maior dano causado por crimes contra tais bens empregando-se a informática, bem como o necessário elevado nível intelectual do delituoso.

O computador é usado para a prática de um delito, do mesmo modo que outros artefatos. Discute-se, então, a criminalização de tais meios de cometimento, visto que certos crimes se tornam quase impossíveis de tipificar, provar e processar quando praticados no ambiente informático.

Discute-se agora a proteção a bens jurídicos redefinidos em sua importância, como o dado, a informação e as redes de computadores. Tal redefinição é proveniente das transformações sofridas pela sociedade pós-industrial, com o impacto causado pela moderna tecnologia da informação.

Esta é a terceira parte de um trabalho do autor, escrito em outubro de 1995,
na conclusão de seu curso na Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS)

* advogado em Uruguaiana (RS)