

Aires José Rover
| Doutor em direito | Universidade Federal de Santa Catarina |
| publicado em <http://infojur.ufsc.br/aires> |

CRIMES DE INFORMÁTICA

"Sou otimista por natureza. Contudo, toda tecnologia ou dádiva da ciência possui seu lado obscuro, e a vida digital não constitui exceção". (NEGROPONTE)

Com o avanço do uso do computador na sociedade atual há também o aumento dos chamados crimes de informática. Atualmente, o homem médio, vê-se às voltas com o computador de várias formas, desde os serviços mais simples aos mais complexos. Este mundo é realidade e os crimes que passam a ser cometidos com o uso desses meios também.

MARCO AURÉLIO RODRIGUES DA COSTA, pioneiro na discussão do tema dos crimes de informática no Brasil, analisou com muita propriedade este tema, fazendo uma verdadeira síntese do mesmo. A seguir, vários tópicos decorrem de seu pensamento.

O DELINQUENTE

Começamos com a suposição de que os crimes de informática são perpetrados por especialistas. Isto é um engano, pois com a multiplicação de equipamentos, tecnologia, acessibilidade e, principalmente, os sistemas disponíveis, qualquer pessoa pode ser autor de crime de informática, bastando conhecimentos rudimentares de computação, para ser capaz de cometê-los.

Hoje, boa parte desses crimes é crimes afeitos à oportunidade, perpetrados por agentes que têm a sua ocupação profissional ao manuseio de computadores e sistemas e em razão dessa ocupação cometem delitos, invariavelmente, contra seus empregadores. Além disso, o perfil do delinqüente de informática, é formado por pessoas inteligentes, gentis e educadas, com idade entre 24 e 33 anos. Devida a essa inteligência, geralmente privilegiada, são aventureiros, audaciosos e mantém com o computador e os sistemas um desafio constante de superação e de conhecimento. Para muitos é sua principal razão para trabalharem. Têm, nesse desafio, disputa, tanto com a máquina e seus elementos, como com os amigos que faz nesse meio, basta ver que os crimes de informática são perpetrados em co-autoria.

Suas condutas delituosas passam por estágios. No início trata-se apenas de vencer a máquina. Após percebem que podem ganhar dinheiro extra. E , por fim, em razão desse dinheiro extra, passam a fazê-lo para sustentarem os seus altos gastos.

TENTANDO CONCEITUAR

O tema proposto tem recebido denominações diversas. natureza dos delitos de informática, a complexidade e, principalmente, a ausência de unanimidade dos doutrinadores, fazem a dificuldade de definir os crimes de informática.

Isto posto, depreende-se que o crime de informática é todo aquele procedimento que atenta contra os dados, que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão.

Assim, o crime de informática pressupõe dois 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.

Conclui-se que aquele que atea fogo em sala que estiverem computadores com dados, com o objetivo de destruí-los, não comete crime de informática, do mesmo modo, aquele que, utilizando-se de computador, emana ordem a outros equipamentos e cause, por exemplo, a morte de alguém. Estará cometendo homicídio e, não crime de informática.

Crime de informática ou computer crime é qualquer conduta ilegal ou não autorizada que envolva processamento automático de dados e/ou transmissão de dados. Dessa forma, são crimes que se apresentam ou como novas maneiras de executar as figuras delituosas tradicionais, ora apresentam aspectos pouco conhecidos que não se adaptam às incriminações convencionais.

SISTEMAS OU INFORMAÇÕES

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.

Os sistemas de computadores e de comunicação seriam, fundamentalmente, os componentes imateriais ou intangíveis, ou seja, o "software" e o "hardware" seus componentes materiais.

Quando se cogita da proteção de bens imateriais, logo temos o exemplo da propriedade intelectual, como o Direito do Autor, que será objeto da próxima aula. No Brasil, como em outros países, existem leis específicas, o que demonstra o quanto é complexo esse novo direito que nasce, que é o Direito da Informática.

Por outro lado, discute-se também a proteção a bens jurídicos 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.

PROVA

É fato que há uma dificuldade especial em se aplicar o direito nessas situações, especialmente em se consolidar provas capazes de, até, iniciar um inquérito policial, quiçá oferecer denúncia.

Para a busca da solução do problema devem ser apurados o meio, a localização do agente, o meio empregado, o objetivo, o resultado e os efeitos do resultado. E ainda há a questão da competência.

Consoante os direitos processuais brasileiros, civil e penal, dispomos de, grosso modo, cinco meios para que sejam provadas as alegações em juízo, como segue.

Há confissão (judicial ou extrajudicial, espontânea ou provocada, escrita ou verbal), quando o confitente admite como verdadeiro um fato contrário ao seu interesse e favorável ao adversário (artigo 348 do Código de Processo Civil). Isso no juízo civil, porque no juízo criminal, caso a infração não deixe vestígios, será indispensável o exame de corpo de delito, não podendo supri-lo a confissão do acusado (artigo 158 do Código de Processo Penal).

Ademais, sua validade não é absoluta, haja vista que o valor da confissão se aferirá pelos critérios adotados para os outros elementos de prova, e para a sua apreciação o juiz deverá confrontá-la com as demais provas do processo, verificando se entre ela e estas existe compatibilidade ou concordância (artigo 197 do Código de Processo Penal); qual seja, no juízo criminal ela somente se prestará para a condenação do réu se existirem outras provas.

A prova documental, pública ou particular, é admitida como prova no direito brasileiro, mas, por exemplo, o e-mail poderia ser considerado como um documento? A resposta é não. Primeiro porque é da essência de um documento que o mesmo seja assinado (ressalvadas as hipóteses legais relativas a telegramas, radiogramas, livros comerciais e outras); secundo porque onde lhe falta a intrínseca materialidade de quaisquer documentos, sobra sua implícita e etérea essência. Isso nos leva a concluir que a sua capacidade de prova estará sempre comprometida, podendo ser acrescida da necessidade de outros meios de prova em relação a seu conteúdo, tais quais a prova pericial, a testemunhal. Isto vale para qualquer outro documento eletrônico, imagem, texto, som, etc.

A prova pericial consiste em exame, vistoria ou avaliação. Todavia o juiz não está adstrito ao laudo pericial, podendo formar a sua convicção com outros elementos ou fatos provados nos autos. A perícia é o mais eloqüente e adequado meio de se fazer a prova judicial no campo da informática, desde que observadas as formalidades de procedimentos cautelares próprios.

A inspeção judicial ocorre quando o juiz, de ofício ou a requerimento da parte, inspeciona pessoas ou coisas, a fim de se esclarecer sobre fato que interesse à decisão da causa (artigo 440 do CPC). É uma prova difícil pois sistemas de informática não são nem pessoa nem coisa. Mas é possível inspecionar o hardware, por exemplo.

Sempre que um fato não for provado documentalmente, por confissão ou por perícia, é admissível a prova testemunhal.

CLASSIFICAÇÃO DOS CRIMES DE INFORMÁTICA

Segundo MARCO AURÉLIO RODRIGUES DA COSTA, 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.

Veja esta classificação:

1. fraudes no nível da matéria corporal ou do "hardware", ou seja, contra a integridade física do computador;
2. fraude ao nível do input, ou seja, na entrada de dados;
3. fraudes ao nível do tratamento dos dados, ou seja, modificação apenas dos programas, sem atingir os dados;
4. fraudes ao nível do output, ou seja, intervenção no resultado obtido a partir de dados corretos, corretamente tratados.

Não obstante as diferentes classificações existentes, entendemos que os crimes de informática dever ser classificados, segundo MARCO AURÉLIO RODRIGUES DA COSTA, 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.

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.

É o caso em que o agente objetiva realizar operações de transferência ilícita de valores de outrem, utilizando-se do computador para alcançar o resultado da vantagem ilegal, e, o computador é ferramenta essencial.

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.

CRIME DE INFORMÁTICA COMUM

São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta para a perpetração de crime comum, tipificável na lei penal. Dessa forma, o sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta. Como exemplo temos os casos de estelionato, e as suas mais amplas formas de fraude.

Neste caso, é comum a idéia de que se incorpore 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.

CRIMES COMUNS

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.

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

Os casos em que o agente visa à destruição, inutilização ou deterioração da coisa alheia (o computador, os periféricos, as informações e os sistemas) - dano - 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. Visa, tão somente ao "hardware", não atingindo o "software" e as informações contidas no equipamento.

A apropriação Indébita ocorre quando o agente tem a posse ou detenção do equipamento e dele se serve para perpetrar vários delitos de informática. Há o aumento de pena se o delituoso age em razão de ofício, emprego ou profissão. 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 delinquentes que tenham conhecimento técnico. Veja o exemplo das fraudes contra as instituições financeiras.

Crimes contra a liberdade individual - Nessa, a informática é meio para violar direitos à intimidade, ao segredo ou à liberdade das comunicações. A divulgação de segredo, por exemplo, são ações que resultem em violação de segredo, coletados e captados por meio da informática, de forma desautorizada, e, principalmente, se produzirem danos à vítima.

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.

Crimes contra a ordem econômica - O sistema legal ainda contempla proteção aos crimes contra a ordem econômica e contra as relações de consumo. Trata desde a ação de utilizar ou divulgar programa de processamento de dados que permita ao contribuinte possuir informação contábil, realizando fraude fiscal, até ações que atinjam o direito dos consumidores.

CRIMES PUROS DE INFORMÁTICA

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. Veja casos mais específicos: Violação de sistema de processamento ou comunicação de dados causando dano a outrem ou obter qualquer vantagem. Pode o agente fazê-lo produzindo alteração temporária ou permanente e com o uso de senha ou outro processo de identificação de outrem. É o acesso não autorizado a sistema de informática.

Atentado contra a integridade de sistema de processamento ou comunicação de dados, desenvolvendo ou introduzindo comando, instrução ou programa, com o fim de causar dano a outrem, obter indevida vantagem ou satisfazer sentimento ou interesse pessoal. Não deixa de ser falsificação de dados ou programas. Também classificada espionagem de informática, a alteração dos programas do computador pode ser efetuada pela troca de cartões, discos ou fitas ou por conteúdo falsificado ou modificados permitido o acesso a banco de dados, registros e codificações. . 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.

Sabotagem informática ou destruir, inutilizar ou deteriorar o funcionamento ou a capacidade de funcionamento de sistema ou comunicação de dados alheios, seja pela exclusão (apagamento) do conteúdo dos suportes, seja pelo desvio de comando, com o fim de causar dano a outrem, obter vantagem ou satisfazer interesse ou sentimento pessoal.

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.

Furtos de uso do computador, ou furto de tempo do computador. Seria a utilização, sem autorização de quem de direito, de recurso de rede. 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.

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 específica 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.

Devassa de sigilo de dado ou tráfico de dados pessoais ou destinar dado ou informação de caráter pessoal, constante de sistema de processamento de dados ou em qualquer suporte físico, à pessoa não autorizada ou a fim diverso daquele ao qual a informação se destina, sem permissão do interessado.

Violação do dever de informar ou deixar de dar conhecimento ou retificar informação pessoal constante e acessável por sistema de processamento ou comunicação de dados ou suporte físico de entidade governamental ou de caráter público, quando exigido pelo interessado.

Divulgação, utilização ou reprodução ilícitas de dados e programas ou 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.

PROJETOS DE LEI

A proposta da nova Parte Especial do Código Penal caracteriza-se por estabelecer um caminho próprio para os crimes de informática, contidos no Capítulo "Dos Crimes Contra a 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.

Projeto de Lei do Senado n. 137 de 1989, que dispõe sobre a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. 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.

Projeto n. 597, de 1991, que dispõe sobre o crime de interferência nos sistemas de informática, objetivando prejuízo de alguém, a um sistema, a computador, a equipamento que acompanha o sistema ou a computador. Apesar de não preencher as necessidades da área de informática, é o mais completo, e tem nos especialistas, tanto da informática como do direito, ferrenhos defensores da sua aprovação.

Comete crime alguém que:

- a) destrua ou altere programa de computador a que tem acesso;
- b) abuse de seu direito de acesso;
- c) introduza, dolosamente, instrução-comando que destrua ou altere a programação;
- d) utilize senha de outrem para obter acesso;
- e) obtenha intencionalmente, sem estar devidamente autorizado, acesso;

O projeto de Lei n. 152, de 1991, 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. Por exemplo, se o acesso resultar vantagem econômica indevida, pune-se o fato como estelionato qualificado. Além disso, prevê um tratamento especial ao chamados "documentos públicos".

CONCLUINDO

Ao concluirmos esta temática vemos como determinante o desconhecimento da terminologia por parte dos operadores do direito que leva a equívocos na interpretação jurídica de condutas específicas e características da ciência informática.

É evidente a variedade e a velocidade com que se aprimoram os métodos delitivos, ao mesmo tempo em que cresce o uso de computadores. Isto não quer dizer que não seja exequível a aplicabilidade das normas penais existentes, que na sua maioria ainda resolvem boa parte dos problemas existentes. Não é difícil constatar que não ocorre o uso da lei penal vigente aos delitos de informática, pelo desconhecimento dos aplicadores do direito e assim, fica-se a exigir novas leis quando não seriam necessárias.

Note-se que isto vale também para os vários delitos perpetrados via internet. Veja-se o caso da pedofilia. Agora, é fácil perceber que há dificuldades relativas ao transnacionalismo da rede, o que dificulta a definição dos territórios competentes para julgamento e por outro lado, a busca de prova em meio tão desprovido de garantias e vigilância. Esta situação exigiria a edição de uma legislação unificada e internacional.

BIBLIOGRAFIA

- COSTA, Marco Aurélio Rodrigues da. Crimes de informática. Jus Navegandi. Advogado em Uruguaiana (RS).
- CORREIA, Gustavo Testa. Aspectos jurídicos da Internet. São Paulo: Saraiva.2000.
- OLIVO, Luis Carlos Cancellier de. Direito e internet. A regulamentação do ciberespaço. Florianópolis: Edufsc, 1998.