CRIMES DE INFORMÁTICA

Adriano Lopes Tavares[1]
Rafael Rocha dos Reis[2]

Resumo: Os avanços da tecnologia e o surgimento da Internet propiciaram o aparecimento de novos tipos penais, como também novas formas de praticar crimes já conhecidos. A informática passou a ser utilizada como instrumento para a execução de antigos e novos tipos penais. O objetivo do presente artigo é caracterizar os crimes de informática com enfoque na legislação penal, bem como fundamentação histórica da informática. Os crimes de informática são conceituados como sendo aquele praticado contra o sistema de informática ou através deste, incluindo-se o perpetrado através da Internet, pois pressuposto para acessar a rede é a utilização de um computador. A discussão neste trabalho são as facilidades que o ambiente virtual propicia para o cometimento de crimes, e a relação de anonimato de seus usuários. Isto é sem dúvida uma mola propulsora ao cometimento de crimes virtuais. O Brasil foi objeto de uma pesquisa acerca do tema e foi considerado um dos países com maior número de fraudes e crimes eletrônicos. E diante de tal fato, pergunta-se: o que são crimes de informática? Qual a postura do Direito em relação a esse problema? São questionamentos que serão trabalhados ao longo deste trabalho cientifico.
Palavras-chave: Informática, Crime Virtual, Internet, Computador.

COMPUTER CRIMES

Abstract: The advances in technology and the emergence of the Internet led to the emergence of new crimes, as well as new ways to commit already known crimes. The computer started to be used as a tool for the execution of old and new crimes. The aim of this paper is to characterize the computer crimes with a focus on criminal law as well as historical foundation of computer science. Computer crimes are highly regarded as one practiced against the computer system or through this, including the perpetrated over the Internet, as a prerequisite for accessing the network is to use a computer. The discussions in this paper are the facilities that the virtual environment provides for the commission of crime, and the anonymity of its members. This is undoubtedly a driving force behind the commission of cybercrime. Brazil was the subject of a search and was considered one of the countries with the highest number of frauds and electronic crimes. And before this fact, one wonders: what computer crimes are? What is the Law stance on this issue? These are questions that will be worked over this scientific work.
Keywords: informatics, Cybercrime, internet, Computer.

[1] Acadêmico do Curso de Direito da UniEvangélica.
[2] Professor do Curso de Direito da UniEvangélica.

Introdução

Informática é a ciência que tem como objetivo estudar o tratamento da informação através do computador. Este conceito ou esta definição é ampla devido a que o termo informática é um campo de estudo igualmente amplo. A informática provém da palavra de origem francesa *informatique,* união das palavras *information*, "informação", e *automatique*, "automática". Se trata de um ramo de engenharia que tem relação ao tratamento da informação automatizada mediante o uso de máquinas. Este campo de estudo, investigação e trabalho compreende o uso da computação para solucionar vários problemas mediante programas, desenhos, fundamentos teóricos, científicos e diversas técnicas (WALTER, 2006, *online*).

Chama-se, genericamente, de informática o conjunto das Ciências da Informação, estando incluídas neste grupo: a teoria da informação, o processo de cálculo, a análise numérica e os métodos teóricos da representação dos conhecimentos e de modelação dos problemas. Habitualmente, usa-se o termo Informática para referir-se ao processo de tratamento automático da informação por meio de máquinas eletrônicas chamadas computadores (CASTRO, 2005, *online*).

Crimes de informática necessitam da ferramenta computador para ser realizado e Carla Castro (2005, *online*) dá a definição de computador como: Computador é conceituado como sendo um processador de dados que pode efetuar cálculos importantes, incluindo numerosas operações aritméticas e lógicas, sem a intervenção do operador humano durante a execução. É a máquina ou sistema que armazena e transforma informações, sob o controle de instruções predeterminadas. Normalmente consiste em equipamento de entrada e saída, equipamento de armazenamento ou memória, unidade aritmética e lógica e unidade de controle. Em um último sentido, pode ser considerado como uma máquina que manipula informações sob diversas formas, podendo receber, comunicar, arquivar e recuperar dados digitais ou analógicos, bem como efetuar operações sobre a lei.

Crime de informática é aquele praticado com auxilio do sistema de informática ou contra, podendo ser compreendido aqueles crimes praticados contra o computador e também seus acessórios e os perpetrados através do computador.

Sendo assim podendo incluir neste contexto os crimes praticados através da Internet, pois a ferramenta para acessar a rede é o computador.

Segundo Augusto Rossini (2004, p.32):

> [...] o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

Em outras palavras podemos dizer que o delito informático pode ser praticado por várias pessoas e das mais variadas formas, podendo ser de propósito ou não, porém sempre terá o mesmo fim, que é ofender um terceiro, seja de forma direta ou indireta.

Para Bruno (2007, *online*) a Internet consiste em uma imensa rede, ou seja, é a rede mundial de computadores. A Rede das Redes que viabiliza a utilização de milhões de computadores conectados e interligados entre si, com objetivos dos mais diversos, como por exemplo, o envio de correios eletrônicos (e-mail), comércio eletrônico (*e-commerce*), governo eletrônico (*e-government*), ensino a distância (*e-learning*), etc.

O doutrinador Gilberto Marques Bruno (2002, *online*) define Internet como:

> [...] a internet nada mais é que uma forma moderna de comunicação entre as pessoas, cuja construção estrutural reside única e exclusivamente, na universalidade de conteúdos, que em linhas gerais demandam mecanismos tecnológicos de segurança.

Sendo assim a Internet é um avanço tecnológico capaz de unir as mais distantes pessoas, através de diversas formas diferentes, seja em canais de bate papos, seja em canais de estudos, pesquisas, com o grande avanço tecnológico que está acontecendo, o valor dos produtos está ficando cada vez mais acessível, de forma que a internet está conseguindo unir as mais diferentes classes.

Resina (2006, p.27) pede para não deixar de observar que a internet grafada com a inicial minúscula é referência a uma rede interna de computadores de determinada empresa, e que ao tratar da Rede Mundial de Computadores ou a Grande Rede deve-se utilizar a palavra em estudo com inicial maiúscula, ou seja, Internet, por se tratar de um nome próprio. Tratamento idêntico deve ser dado a grafia da palavra rede quando em referência à Internet, ou seja, Rede ou Grande Rede (RESINA, 2006, p. 28, *op. cit.*).

Escorço Histórico

Segundo Gabriel Gugik (2009, *online*) a informática teve como marco inicial para a sua evolução histórica o ábaco, que é de origem oriental, e que o ocidente conhece desde o século IIIA.C, sendo utilizado por alguns Países do Ocidente, ao longo dos anos sendo utilizado até mesmo nos dias de hoje, sendo considerado o primeiro computador do mundo.

Entre os séculos XVII e XIX, os matemáticos e filósofos John Napier (1614), Blaise Pascal (1624), G.W, Thomas de Colmar (1818), von Leibnitz (1671) e Charles Babbage juntamente realizaram trabalhos e pesquisas conjuntas na produção do que viria a ser o computador, como hoje o concebemos (RAMALHO, 2003, p.32).

Somente em 1946 foi criado o primeiro computador eletrônico, com fins militares, conforme explica Carla Rodrigues Araujo de Castro (2003, p.3):

> O primeiro computador eletrônico data de 1946 foi criado pelas necessidades militares. Denominou-se ENIAC e foi utilizado para montar tabelas de cálculo das trajetórias dos projéteis. Em 1951 apareceram os primeiros computadores em série e, com a rápida e avassaladora evolução tecnológica, temos hoje os computadores pessoais e os notebooks.

Para o processamento de estatísticas demográficas do censo americano foi criada uma máquina pelo americano Herman em 1898 reduzindo o trabalho de dez para dois anos. Criando então a Tabulating Machine Company, que depois tornou-se a International Business, mais conhecida como IBM (CAMPOS, 2005). O matemático inglês de nome Alan Turing (1912), foi o responsável pela construção do primeiro computador digital eletrônico a válvula, projeto esse que passou a ser chamado de colossos. O húngaro John von Newman que é matemático é considerado o arquiteto do computador moderno. Em 1951, Eckert e Mauchly construíram a Remington-Rand. Em seguida, surgiu o primeiro computador a ser produzido comercialmente: o UNIVAC. Daí houve um desenvolvimento generalizado, iniciando nos EUA, com a inauguração do IBM 701, e, por sequência em países da Europa. Atualmente, o Japão e a Coreia colocam-se na frente do desenvolvimento tecnológico em todo mundo (CAPRON, 2004, p.26).

Conforme Almeida (2007, *online*) os computadores de 4ª geração surgiram nos anos 60, sendo que a INTEL foi a responsável por projetar o microprocessador que serviu como exemplo para os microcomputadores atuais. O ALTAIR foi o primeiro microcomputador colocado no mercado. No ano de 1974 um estudante da Universidade de Harvard, conhecido como Bill Gates, juntamente com seu amigo Paul Allen fabricaram o sistema operacional do ALTAIR, e mais tarde fundaram juntos a Microsoft.

No começo da década de 1970, tiveram várias discussões a respeito de colocar a informática no meio do Direito, entre as bases para a negação dessa introdução estava aquela que dizia que os juízes e legisladores se tornariam "automáticos", porém chegaram ao consenso de que o computador jamais foi feito para substituir o homem (ALMEIDA, 2007, *online*).

Assim sendo provando que o computador que trabalharia em função do direito e não o direito em função do computador, em sentido *lato sensu*, conceberia o Direito utilizando-se da informática como ferramenta para poder desenvolver de melhor forma o serviço. O certo é que a informática nada representa do que mais uma ferramenta do Direito, e não o contrário (ALMEIDA, 2007, *online*).

Segundo Bruno (2007, *online*) no meio tecnológico não há nenhum aparelho que tenha se desenvolvido tanto e com tal velocidade como o computador, o qual está inserido em todos os tipos de serviços, sendo de forma direta ou indireta, havendo serviços que simplesmente param sem o computador, quantas empresas simplesmente não trabalham sem o auxilio da internet, sem aquela consulta que precisa ser feita na Internet.

Ao analisarmos o principio *omnis potestas a lege*, vê-se claramente que a informática está totalmente ligada de forma a ser uma ferramenta utilizada pelo Direito, e, tendo em vista a grande evolução dela, o meio jurídico tenta acompanhar essa grande evolução, de uma forma que o Direito estará em constante mudança, devido ao fato dos avanços tecnológicos que estão em constante Segundo Resina (2006, p.28) a Grande Rede surgiu no fim da década de sessenta e interligava inicialmente as unidades da Advanced Research Projects Agency (ARPA) que era um dos órgãos do governo norte-americano sendo que a definição inicial para a criação da Internet foi a questão de segurança, e em seguida lhe foi atribuída a finalidade para a educação e pesquisa. Tal questão relacionava-se com o ambiente da guerra fria que tentava prevenir um suposto ataque nuclear soviético que

afetasse a rede de informações americana. Hoje em dia a Internet não tem dono, podendo ser usada por quem desejar.

A Internet no conceito de Carla Rodrigues de Araujo de Castro (2003), Internet é uma grande rede de comunicação mundial, onde estão interligados milhões de computadores, sejam eles universitários, militares, comerciais, científicos ou pessoais, todos interconectados. É uma rede de redes, que pode ser conectada por linhas telefônicas, satélites, ligações por micro-ondas ou por fibra ótica.

A Grande Rede passou a ter importância em 1973, sendo assim o seu marco inicial, com a criação do Protocolo de Controle e Transmissão/Protocolo Internet (TCP/IP) por VintCerf. O protocolo mencionado acima é um sistema que possibilita a diversos computadores se comunicarem entre si, a doutrinadora Jane Resina denomina o TCP/IP como o “esperanto da Internet”, como sendo esperanto a linguagem universal (RESINA, 2006, p. 29).

Foi um destaque imenso a criação do Protocolo de Controle e Transmissão, pois esse acontecimento permitiu a configuração atual, fazendo com que houvesse a conexão entre diferentes computadores com configurações e sistemas operacionais distintos, sendo assim possibilitou a ligação de diversos usuários em locais e países distantes formando, portanto um mundo sem fronteiras, dessa forma não é necessário o computador x ter a mesma configuração do computador y para que os mesmos estejam conectados, quando se fala de um mundo sem fronteiras não versa somente a respeito da distância entre países, mas também do rompimento das barreiras econômicas, pois na Internet todos são tratados de forma igualitária.

Os primeiros crimes de informática começaram a ocorrer na década de 1970, na maioria das vezes era praticado por especialistas em informática, o qual o objetivo era driblar os sistemas de seguranças das empresas, com um foco principal nas instituições financeiras.

Atualmente o perfil das pessoas que praticam crimes de informática já não são as mesmas da década de 1970, os usuários mudaram, hoje em dia qualquer pessoa que tenha um conhecimento não tão aprofundado, mas que tenha acesso á internet pode praticar algum crime de informática, o usuário doméstico hoje já tem um conhecimento bem maior sobre o uso de computadores e tecnologia voltada para internet.

Conceito e classificações dos crimes informáticos

Diferentes denominações são oferecidas aos crimes que ocorrem na Rede Mundial de Computadores, ora os doutrinadores chamam de crimes cibernéticos, ora de crimes virtuais, ou crimes de informática, entre outras denominações. É certo que ainda não há denominação assente tais crimes, mas com o advento da legislação pertinente é muito provável que uma nomenclatura se firme (BLUM, 2007, *online*).

Seguindo o pensamento de Carla Castro (2006, *online*) a Internet e outros meios eletrônicos possibilitam a prática de diversos delitos, alguns complexos outros nem tanto, mas que exigem uma rápida e eficaz resposta do Estado. Tal solução deve ser antes de tudo especializada e pontual.

Ressalte-se que o avanço tecnológico tem proporcionado o incremento de crimes comuns, ex: furto, o que resulta na afirmação de que tais delitos crescem na proporção do avanço tecnológico que vivenciamos (ABRUSIO, 2007, *online*).

Considera-se crime de informática aquele praticado contra o sistema de informática ou através deste, abrangendo, portanto, o computador, seus acessórios e a internet (CASTRO, 2007, *online*).

Para Carla Castro (2007, *online*) o crime informático possui características próprias e também complexas, haja vista a necessidade de um conhecimento especializado na coleta e utilização das evidências eletrônicas. Frise-se também que é da natureza do próprio meio a volatilidade e fragilidade que, curiosamente, se entrelaçam com a facilidade da recuperação de rastros e outros indícios típicos.

A doutrinadora Carla Rodrigues Araújo de Castro distingue duas modalidades de crimes cibernéticos:

> A primeira consiste em uma nova forma de praticar crimes antigos, nos quais o computador e a Internet são utilizados como simplesmente instrumentos para a prática do delito. A outra modalidade agrupa condutas inéditas, ou seja, aquelas que nasceram com a era digital. A referida doutrinadora sugere que no primeiro grupo deve-se aplicar a lei vigente, haja vista que a Internet é utilizada como uma forma para cometer delitos antigos, ou já preexistentes ao surgimento da Internet, ex: ameaça via e-mail. Já quanto aos novos delitos o problema de punição se instala, tendo em vista que a legislação penal vigente no Código Penal data de 1940 (RODRIGUES, 2007, *online*).

A segunda espécie de delitos cibernéticos atinge bens jurídicos novos, quais sejam, dados, informações, sites, *home pages*, e-mails e etc. Têm portanto, uma especialidade que juntamente com a ausência de leis que tipifiquem tais condutas dificultam e impossibilitam a punição Estatal. Há doutrina que classifica os crimes de informática como crimes virtuais, sendo o gênero, e as espécies em crimes virtuais puros e crimes virtuais impuros (ATHENIENSE, 2006, *online*).

Na ótica de Atheniense (2006, *online*) os crimes virtuais impuros seriam aqueles ainda que cometidos no ambiente da Grande Rede seria possível a aplicação da legislação penal vigente, art. 139, do Código Penal: " Difamar alguém, imputando-lhe fato ofensivo á reputação- Detenção, três meses a 1 (um) ano e multa".

Como se vê o tipo penal em comento não impõe óbice alguma a sua aplicação no ambiente virtual, haja vista que o crime de difamação pode ser praticado em um site de relacionamento, como pode ser praticado por palavras proferidas. No caso de crime virtual impuro basta aplicar a legislação vigente, sem nenhum empecilho.

Insta observar que a maioria das leis penais foi elaborada para tratar de bens jurídicos corpóreos, de modo que a primeira impossibilidade que nasce da aplicação da legislação vigente aos crimes cibernéticos é esta, haja vista que a grande maioria dos bens jurídicos atingidos pelos delitos cometidos na Grande Rede são de natureza incorpórea. Os delitos cibernéticos que possuem tais bens jurídicos são os denominados crimes virtuais puros, como por exemplo aqueles que violam bancos de dados, alteram bancos de dados, invasões a sites, disseminação de vírus, entre outros (ATHENIENSE, 2007, *online*).

Na visão de Alexandre (2007, *online*) há quem proponha punição para os crimes virtuais puros com base na legislação vigente, entretanto não há que se cogitar tal posicionamento, haja vista a discrepância de bens jurídicos como visto acima. Daí nasce a necessidade da rápida aprovação de uma legislação pertinente aos crimes virtuais puros.

Visão interessante de crimes na Grande Rede é a exposta por Gilberto Marques Bruno. Este doutrinador considera a Internet como um paraíso de informações que por sua vez se consubstanciam em riquezas e que em razão disto atrai tantos criminosos. Sobre a análise do crime eletrônico, o doutrinador o compara ao delito comum. No delito eletrônico o meliante deixa de lado a utilização de meios

coercitivos para com suas vitimas, substituindo- os por equipamentos sofisticados e com tecnologia de ponta. De modo que saem do cenário criminoso virtual as armas para dar lugar aos computadores, acessórios, recursos e softwares (BRUNO, 2007, *online*).

Para Gilberto Marques Bruno, crimes eletrônicos "são aqueles atos praticados, que estejam relacionados as informações que se encontram arquivadas em bancos de dados ou em trânsito através de computadores". E concluindo seu pensamento o doutrinador ainda ressalta que é necessária a obtenção de dados de forma ilícita, utilizando-os com o animus de ameaçar e/ou fraudar a vítima, sempre se utilizando do meio eletrônico. Assim, verifica-se que em tal delito é necessária a intenção de causar temor, prejuízo á vítima, mediante a utilização de uma forma ilegal de acesso ao meio eletrônico de informação, para se obter os dados e informação da vítima (BRUNO, 2007, *online*).

O Prof. Ulrich Sieber em seu estudo, dispõe que os crimes de informática em "formas atuais de crime de computador", sendo estas contravenções de privacidade, as afrontas econômicas, a espionagem, a pirataria de software e outras formas de pirataria de produtos, a sabotagem, a fraude, os conteúdos ilegais, as ofensas, o homicídio, o crime organizado e a guerra eletrônica.

O Dr. Vladimir Aras classifica três categorias como principais:

> a) "uma primeira, onde estão substancialmente unidos pela circunstância que o computador constitui a necessária ferramenta de realização pela qual o agente alcança o resultado legal".
> b) "a segunda categoria de crimes do computador, poderia incluir todos aqueles comportamentos ilegítimos que contestam os computadores, ou mais precisamente, seus programas".
> c) "a última categoria deveria juntar todas as possíveis violações da reserva sobre a máquina, aqui entram em consideração as habilidades de colheita e elaboração de todo tipo de dados" (2008, *online*).

Crimes cibernéticos mais frequentes

Das condutas danosas praticados no ciberespaço podemos citar as mais corriqueiras como sendo: Crimes contra a honra: São os crimes de calúnia (art. 138), difamação (art. 139) e injúria (art. 140). Os criminosos se aproveitam do anonimato e assim os mesmos podem praticar seus crimes em blogs, chats, enviando spams, através da publicação em *homepages*, entre outros meios de postagens na internet.

Esses crimes devem contar com agravante no inciso III, do artigo 141, do Código Penal, pela facilidade de divulgação proporcionada pela Internet. Crimes contra a liberdade individual: São os crimes de ameaça (art. 147), inviolabilidade de correspondência (arts. 151 e 152), divulgação de segredos (arts. 153 e 154), disseminação de segredos compreendidos ou não em sistemas de informação ou banco de dados da Administração Pública (artigo 153, inciso I) (BRUNO, 2007, *online*).

Depois de um grande estudo realizado na doutrina existente chegou-se a conclusão que os crimes que mais ocorrem no ambiente virtual são: pornografia infantil; pirataria de software; delitos relacionados com cartão de crédito e outras fraudes (BLUM, 2002, *online*).

Em 2001, a doutora Lúcia Helena Blum fez um estudo emblemático sobre pornografia infantil e a classificou em três categorias. A primeira relaciona-se ao começo da Grande Rede, em que os usuários interessados em fotos eróticas de pouca intensidade trocavam entre si pela Rede, tornando-as públicas. A segunda categoria liga-se essencialmente ao desenvolvimento tecnológico empreendido pela informática, ou seja surgiram empresas que somente disponibilizavam o acesso ao site ou link mediante algum pagamento, eram as publicações *online*. Tais empresas também foram responsáveis pela criação das transações financeiras pela Internet. A última modalidade de pornografia é a mais preocupante, haja vista que liga-se diretamente com a pedofilia e outros materiais obscenos, que incluem desde rituais macabros a fotos de mutilações.

Tais condutas são mantidas sob certo sigilo devido ao anonimato e as técnicas de criptografia. O exemplo mais recente é o de empresas que se especializam em comercializar aqueles materiais mediante o pagamento de uma taxa (BLUM, 2001, p. 31).

Em um estudo apurado sobre o tema de pedofilia tem-se que a prática desta conduta abjeta em algumas civilizações antigas não era somente aceita, mas também estimulada. Atualmente, é sabido que não há espaço para se tolerar tal prática, entretanto o advento da Internet veio a fomentar a pornografia infantil que se liga diretamente a pedofilia (BLUM, 2001, *online*).

Antes da criação e disseminação da Grande Rede um pedófilo não tinha muitas facilidades de se comunicar com outro, ou mesmo iniciar um processo de aproximação da vítima. A Internet com a vantagem do anonimato veio a facilitar a

propagação da pornografia infantil e, por conseguinte da pedofilia. Fazem-se necessárias as palavras do doutrinador Ricardo Alcântara Pereira (2006, p.139):

> Diante desse novo conteúdo social os pedófilos formaram uma comunidade on-line, com identidade psicológica, passaram a nutrir um sentimento de pseudolegitimação e partiram em busca daquilo que passaram a chamar de " carne fresca ", vitimando, para tanto, milhares de crianças pelo mundo afora, principalmente nos países subdesenvolvidos, com a finalidade de produzir matéria para dezenas de milhares de sites.

O doutrinador Alberto Silva Franco e Rui Stocco em análise dos crimes contidos no Estatuto da Criança e do Adolescente em obra clássica sobre legislação penal extravagante da edição de 2001, já antevia a solução legislativa para a não punição de crimes que ocorriam na rede e ainda não tinham punição por não encaixarem nos tipos penais existentes a época. Tais considerações parece que foram levadas a sério pelo legislador de 2003, pois quando da reforma dos crimes do ECA inclui várias teses defendidas por aqueles autores em seu trabalho de vanguarda. Compara-se a redação o antigo 241, "fotografar ou publicar cena de sexo explicito ou pornografia envolvendo criança ou adolescente: Pena de reclusão de um a quatro anos".

E diante de tal tipo penal algumas ações penais foram trancadas por entenderem os juízes que a denuncia pelo crime do art. 241, de condutas que se espalhavam na Internet feria frontalmente o principio Constitucional da Legalidade ou da Reserva Legal. Para uma completa compreensão de tema intrincado faz necessária a transcrição de alguns trechos do voto do Desembargador Eduardo Mayr no Habeas Corpus impetrado:

> Divulgar não é publicar: quem publica, divulga, certamente; mas nem todo aquele que divulga, publica. A divulgação pode ser por qualquer forma, até oral, mas a publicação não prescinde da existência de objeto material corpóreo. Assim é que a transmissão, pela Internet, e por solicitação ministerial, de imagens pornográficas envolvendo crianças, para adolescentes e adolescentes, enquanto não definida adequadamente como crime, é conduta atípica, não se podendo afirmar infratora do disposto no art.241 do ECA...

A pornografia infantil na Internet hoje tem um tipo penal especifico no Estatuto da Criança e do Adolescente, qual seja, o art. 241, inclui claramente o uso da Internet:

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:
> Pena - reclusão de 2 (dois) a 6 (seis) anos, e multa.
> § 1º Incorre na mesma pena quem:
> I - agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;
> II - assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo;
> III - assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo.
> § 2º A pena é de reclusão de 3 (três) a 8 (oito) anos:
> I - se o agente comete o crime prevalecendo-se do exercício de cargo ou função;
> II - se o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial.

Louvável, portanto, o estudo e as criticas de Rui Stocco e Alberto Silva Franco, verdadeiros expoentes do Direito Penal moderno brasileiro, que modificaram sensivelmente não só o referido artigo, mas permitiu a inclusão de tantos outros tipos que hoje servem melhor a proteção integral da criança e do adolescente no Brasil. O delito de pirataria de software consiste em apropriação indébita e na conduta de vendas de programas de computador sem a devida licença do autor. A lei nº 9609/1998 dispôs sobre propriedade intelectual de programa de computador e sua comercialização no Brasil (TAVARES, 2007, *online*).

A Grande Rede influiu na comercialização e cópia dos programas de computador, houve um aumento da facilidade de acesso e reprodução. O Brasil destaca-se como campeão de pirataria de softwares, perdendo somente para os países asiáticos, a taxa de reprodução sem autorização é superior a oitenta por cento dos programas comercializados (BRUNO, 2007, *online*).

Há de se ressaltar que o problema da pirataria envolve antes de tudo questões culturais, sociais e econômicas. A coibição da prática de tal delito não se resume somente a legislação penal, efetivas apreensões e prisões, mas atinge um problema social. Deve-se agir conjuntamente para se coibir tal mal. Assim como em outros aspectos penais sabe-se que uma só ação de nada adiantará, mas nesta será tais fatos se evidenciam de sobremaneira, ao passo que o ambulante vende o programa de computador pirateado por não ter emprego, sendo uma renda familiar

sem recorrer ao crime, e a população mais carente efetua as compras destes produtos, em razão de os originais serem jamais acessíveis ao seu pode aquisitivo. Vê-se, portanto, que a atuação deve ser conjunta e não míope como se é de costume fazer (BARRET, 2006, *online*).

O uso de cartões de créditos na Grande Rede é motivo infindável de inúmeras fraudes e crimes. Não há legislação específica que regulamente o uso, gerando, portanto, um grande vazio causador de grandes danos aos usuários. A informação que se tem é que qualquer pessoa responsável por um provedor de acesso tem condições de utilizar as informações dos cartões, podendo utilizá-las ilicitamente. O problema reside no fato de que não só o responsável pelo provedor tem acesso, mas qualquer pessoa munida de ferramentas adequadas pode interceptar as informações digitadas no site. Ressalta-se que as empresas de cartão de crédito tem trabalhado bastante para o desenvolvimento de uma melhor tecnologia para segurança nas transações, afinal o comércio eletrônico só tende a crescer cada dia que se passa (RAMOS, 2007, *online*).

O estelionato eletrônico tem ganhado espaço dentre os crimes cibernéticos mais em razão da curiosidade e ingenuidade da vítima que muitas vezes acredita que foi contemplada com promoções estapafúrdias. Mas alguns doutrinadores como Gilberto Bruno costumam conceituar tal tipo como uma fraude que envolve um falso comerciante e um consumidor com boas intenções, visando adquirir uma mercadoria oferecida á venda, sejam mercadorias físicas, digitais ou mesmo serviços ou mercadorias publicadas. Lembrando que este delito também não tem tipificação legal especifica (BRUNO, 2007, *online*).

O crime de *hacking* envolve um acesso a um certo sistema por particular que tenha permissão insuficiente, ou um determinado usuário externo ao sistema, acessando-o sem nenhuma permissão. Tal definição é fornecida por Neil Barret no texto de Gilberto Bruno. Este doutrinador assevera que denominação acima definida inexistente na seara jurídica brasileira, entretanto o nome hacker é conhecido de grande parte da população (BARRET, 2007, *online*).

O doutrinador Hélio Santiago Ramos Jr (2007, *online*) nos oferece uma concepção de hacker um tanto esclarecedora, qual seja:

> Há diversos mecanismos e formas de invadir a privacidade do individuo na Internet e se obter informações particulares que não se encontravam a disposição, aqueles que detêm a prática de interceptar dados e obter ilegalmente informações, independente da

> finalidade ou não de causar um dano ou um prejuízo, chama-se tal individuo de hacker.

Gilberto Bruno (2007, p.13) esclarece duas condutas do hacker, quais ela poderá ser relativa a pessoa, consistente na obtenção sem devida autorização de dados pessoais, caracterizando assim, a prática do delito de violação da intimidade do individuo. Poderá outro assim, representar invasão para obtenção de bens digitais, como um programa de computador, informação legalmente protegida, a qual o hacker não possuiria licença alguma para modificar, apropria ou destruir.

Ensina a doutrinadora Carla de Castro (2003, p.219/220), que existe ainda outro conceito para autor delitivo no processo de crimes de informática (conforme Amaro Moraes e Silva Neto citado por ela em sua obra), qual seja, os crackers, que são pessoas especializadas em quebrar senhas. Ao contrário dos hackers, os crackers têm intenção criminosa (o cometimento de fraudes, espionagem, etc.). Amaro Morais e Silva Neto diferenciam os hackers dos crackers: hacker é aquela pessoa que é instigada exclusivamente pelo fato de romper as defesas de um sistema operacional – ai encerra sua batalha mental. Já o cracker é aquele que inicia seu trabalho quando existe o rompimento das defesas do sistema operacional sob ataque, visando obter lucros para si ou para outrem, sempre prejudicando terceiros.

Essas pessoas no meio em que vivem são tidas como heróis em razão de suas condutas delituosas cibernéticas. Esses “heróis” digitais não vivem sem seus objetos, como: computadores, celulares, painéis de LED, roteadores. É notável que o avanço da tecnologia trouxe inúmeros benefícios para a humanidade, porém como em qualquer inovação temos os lados positivos e negativos, sendo a facilidade da realização de crimes no anonimato um dos pontos negativos dessa nova evolução.

Legislação penal acerca dos crimes cibernéticos

Entrou em vigor no dia 30/02/2012 a Lei Federal nº 12.737/2012 que trata sobre os crimes de Internet, que foi apelidada de Lei Carolina Dieckmann, que tipifica os crimes informáticos, com a inclusão no Código Penal dos artigos 154-A e 154 - B, dos parágrafos primeiro e segundo no artigo 266 e parágrafo único no artigo 298. Essa legislação traz uma equiparação da clonagem de cartões á falsificações de documentos pessoais. Isso representa um avanço, porque antes havia uma

grande dificuldade em criminalizar quem clona cartões e obtém dados, uma vez que só era possível incriminá-lo no momento em que realiza a fraude.

O artigo 154-A versa sobre o crime de invasão de dispositivo informático, no qual o bem protegido é a inviolabilidade dos segredos, ou seja, os dados e informações armazenados no computador, podendo ser de pessoas físicas como de pessoas jurídicas de direito privado (empresas) e de direito público (estado, órgãos e entidades) (2012, CPP).

Toda a população tem o conhecimento de que a tecnologia da informação e de armazenamento de dados, principalmente através da Internet, trouxeram inúmeros benefícios, porém também tornou-se um meio para a prática do crime contra a inviolabilidade dos segredos, principalmente pelo fato de ter sido possível dificultar e por tanto tempo até impedir a identificação do agente criminoso, que reiterava o seu comportamento estimulado pela impunidade (SANTOS, 2002, *online*).

De acordo com Márcio André Lopes Cavalcante (2012, *online*) com o uso cada vez mais frequente e pelo número maior de pessoas que se utilizam das ferramentas da informática, as pessoas tem se deparado com as ações criminosas em todos os lugares, seja em ambientes pessoais como em ambientes de trabalho, gerando um sentimento de insegurança e preocupação. Como já sabemos grande parte da população já foi vítima de ações de hackers que resultaram nos mais variados danos e prejuízos. Somente agora o legislador tipificou como crime as ações do criminoso informático.

Vejamos as novas alterações contidas no texto da lei:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

> § 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal." (2012, CPP)

Sendo assim qualquer pessoa que praticar qualquer conduta descrita no tipo penal acima terá cometido o crime, sendo que o tipo penal é expresso e claro quando restará configurado o delito, inclusive na forma qualificada.

O artigo 154-A especifica que nos casos do crime de invasão de dispositivo informático a ação penal somente poderá ter prosseguimentos e houver representação, com exceção se o delito tiver sido cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviço público (ANDREATO, 2012, *online*).

Humberto Theodoro Júnior ensina que a convicção do magistrado estará condicionada:

> a) aos fatos nos quais se funda a relação jurídica controvertida;
> b) às provas desses fatos, colhidas no processo;
> c) às regras legais e máximas de experiências;
> d) e o julgamento deverá sempre ser motivado (2005, p. 385).

Segundo Eudes Quintino (2012, *online*) quando ocorre o delito é preciso saber primeiro qual a pessoa que foi vítima, para podermos saber se a ação penal será pública condicionada a representação ou incondicionada. Quando for o caso de ser incondicionada a autoridade policial poderá instaurar o inquérito policial e mais tarde a ação penal poderá ser proposta assim que tiver notícia da prática do delito, para analisar a autoria e a materialidade, este ato poderá ser praticado considerando o prazo prescricional pela pena máxima que poderá ser aplicada (artigo 107 e seguintes do Código Penal Brasileiro). Vale ressaltar que para que aconteça a apuração do crime não é necessário que tenha ocorrido expressa e anterior manifestação de vontade da vítima.

Ao analisarmos o caso da ação penal ser condicionada (primeira parte do dispositivo - regra), que é a qual é aplicada na grande maioria dos casos, em que a vítima não tiver no rol da exceção, será obrigatório a representação para que seja possível a propositura da ação penal por um representante do Ministério Público. Nesta hipótese se a vitima não representar não haverá propositura de ação (QUINTINO, 2012, *online*).

A vítima (ou seu representante legal, caso ela seja incapaz) devem representar no prazo máximo de seis meses após a descoberta do autor do crime (art. 38, CPP, e art. 103, do CP), lembrando que é possível a retratação até o oferecimento da ação penal. Depois de decorrido o prazo decadencial de seis meses, acontecerá a extinção da punibilidade e nada mais poderá ser feito contra o autor do crime. Esta regra é utilizada para a maioria dos usuários das ferramentas da informática.

Sendo assim caso a vítima do crime tenha provas que possibilitem a apuração da autoria e materialidade e queira ver o autor do crime punido, deverá manifestar a sua vontade à autoridade policial competente ou a um representante do Ministério Público no prazo legal, sendo feito de preferência por escrito e com o auxilio de um advogado. Não esqueça que a representação e de vontade da vitima, pois é ela que dá ao Estado plenos poderes para dar prosseguimento na ação (SARDINHA, 2013, *online*).

A lei ainda trouxe dois novos delitos informáticos, quais sejam:

> Art. 266. Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
> § 1o Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)
> “Falsificação de documento particular
> Art. 298.Falsificação de cartão Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.”

Segundo André Sardinha (2013, *online*) o primeiro crime é para proteger todo e qualquer serviço telemático ou de informação de utilidade pública das ações de criminosos da informática, que venham a interromper o serviço. Um exemplo é o que acontece quando algum site de relevância (ex: Ministérios do Governo Federal,

Mídia) não pode ser acessado através da internet pela ação de alguém, causando prejuízo aos seus usuários.

Sendo o segundo crime um efeito da modernidade e pelo fato de cada vez mais pessoas utilizarem o cartão de crédito para efetuarem pagamentos e compras. Um dos efeitos dessa modernidade são as falsificações de cartões de crédito para fins de vantagem ilícita. Porém geralmente este crime andará juntamente com outros, como furto, roubo e estelionato. A semelhança em ambos os delitos e que a ação penal se procede independentemente de representação, ou seja, é pública incondicionada (SARDINHA, 2013, *online*).

No ordenamento jurídico pátrio, não há qualquer empecilho para a utilização de provas eletrônicas, conforme versa o art. 225 do Código Civil:

> As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas, fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão.

Referências

ALMEIDA, Fábio Portela Lopes de. Crimes na Internet. Santa Catarina. **Buscalegis**. Disponível em: http://www.buscalegis.ufsc.br/arquivosQCrimes_na_internet. Acesso

em: 30 de abril 2013

ANDREATO, Danilo. 2012. Disponível em: http://www.daniloandreato.com.br/tag/lei-

12-7372012. Acesso em: 25 de maio 2013

ATHENIENSE, Alexandre. Crimes virtuais puros e impuros. **Buscalegis**. Santa Catarina. Disponível em: http://www.buscalegis.ufsc.br/arquivos/m9-crimesVPEI.htm. Acesso em: 01 de maio 2013

BECCARIA, Cesare. **Dos delitos e das penas.** 2.ed. 2.tiragem. Tradução de J. Cretella Jr. E Agnes Cretella. São Paulo: Revista dos Tribunais, 1999.

BIANCHINI, Alice; e GOMES, Luiz Flávio. **O direito penal na era da globalização.** São Paulo: Revista dos Tribunais, 2002.

BLUM, Renato M.S. Opice; ABRUSIO, Juliana Canha. Crimes eletrônicos. **Buscalegis**, Santa Catarina, 28 mar.2007. Disponível em: http://www.buscalegis.ufsc.br/arquivos/crimes_eletronicos.htm. Acesso em: 02 de maio 2013

BOFF, Cesar. 2009. Disponível em: http://www.sti.br.inter.net/hackio/frames. Acessado em : 29 de maio 2013

BRUNO, Gilberto Marques. Considerações quanto a prática de crimes eletrônicos no âmbito do "world wide web". **Buscalegis**. Santa Catarina. Disponível em: http://www.buscalegis.ccj.ufsc.br. Acesso em: 04 de maio 2013

BRUNO, Marcos Gomes da Silva. **Manual do Direito Eletrônico e Internet.** São Paulo: Lex Editora S.A. 2006

CASTRO, Carla Rodrigues Araújo. Impunidade na Internet. **Direitonet**. Disponível em: http://www.direitonet.com.br/doutrina/artigos/x/44/44/444/ Acesso em: 22 de maio 2013_____. **Crimes de Informática e seus Aspectos Processuais.** 2 ed. Rio de Janeiro, Ed. Lumen Juris, 2003.

CAMPOS, Eduardo Faria de Oliveira. **Direito e Internet: direitos autorais e a tecnologia.** 2005. p.613.

CAPRON, H.L, JOHNSON, J.A. **Introdução a Informática.** Ed. 8. São Paulo: Prentice Hall, 2004.

CHANDLER, A.D. **Século Eletrônico:** A história da evolução da indústria eletrônica e de informática. São Paulo: Campus, 2002.

FRANCO, A.S. **Leis penais especiais e sua interpretação jurisprudencial.** 6.ed. São Paulo: Revista dos Tribunais, 2000.

GUGIK, Gabriel. **A história dos computadores e da computação.** 2009. Disponível em: http://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm. Acesso em: 26 de maio 2013

GALVÃO DA ROCHA, Fernando A.N., **Criminalidade do computador.** RT 718/522-535. São Paulo: Revista dos Tribunais, 1995.

JÚNIOR, Humberto Theodoro. **Curso de Direito Processual Civil.** Forense. Rio de Janeiro. 2005. p.381

LOPES DA SILVA, Rita de Cássia. **Direito Penal e sistema informático.** São Paulo: Revista dos Tribunais, 2003.

MIRABETE, Júlio Fabbrini. **Manual de Direito Penal.** 16.ed, rev, atual. São Paulo: Atlas, 2000.

_____. **Código de Processo Penal Interpretado.** São Paulo. Atlas. 2004. p. 278.

NOGUEIRA, Sandro D`Amato. **Crimes de Informática**. Sandro D`Amato Nogueira-Leme/SP:BH Editora, 2008- p.580

RAMALHO, J.A. **Introdução á Informática:** teoria e prática. 4. ed. São Paulo. Futura, 2003.