Crimes virtuais

Autor: Emanuel Alberto Sperandio Garcia Gimenes

Juiz Federal Substituto

publicado em 30.08.2013

Resumo

O presente artigo aborda o desenvolvimento da Internet e, com ele, o surgimento de um novo gênero de criminalidade, caracterizado pela perpetração de condutas criminosas por via de computadores e no ciberespaço, atingindo os mais variados bens jurídicos tutelados pela legislação penal, além de outras condutas danosas ainda não tipificadas pelo ordenamento jurídico, trazendo ainda elementos a respeito do seu combate nos dias de hoje.

Palavras-chave: Crimes. Internet. Virtuais. Ciberespaço. Poder. Judiciário. Prestação. *Hacker*.

Sumário: Introdução. 1 O computador e a Internet. 1.1 A evolução do computador. 1.2 A evolução histórica da Internet. 1.3 A Internet no Brasil. 2 Segurança nos computadores e na Internet. 2.1 A necessidade de segurança. 2.2 Formas de violação à segurança. 2.3 Intrusos dos sistemas. 3 Crimes por meio dos computadores. 3.1 Conceitos e nomenclaturas. 3.2 *Hackers, Crackers*: a terminologia quanto ao sujeito ativo. 3.3 Classificações. 3.4 Crimes virtuais mais comuns. 3.5 Resposta estatal. Conclusão. Referências bibliográficas.

Introdução

As novas tecnologias da informação, especialmente a Internet, impulsionaram o processo de globalização econômica e cultural. Os avanços tecnológicos ligados à computação fizeram surgir a era dos *bits* e *bytes*, tornando o computador indispensável e aplicando suas técnicas nos mais diferentes lugares, passando a fazer parte do dia a dia das pessoas, das empresas e dos governos.

Ao separar as pessoas por uma interface e proporcionar o anonimato, a Internet e a realidade virtual alimentam no ser humano a sensação de liberdade. Essas mudanças, impulsionadas pelos avanços tecnológicos e pelas mídias, fizeram surgir novos paradigmas para a sociedade pós-moderna e para os sistemas que a organizam e regulam, como o Direito.

A sociedade, com o advento da informática, descobriu o poder da informação. A mudança de uma cultura escrita para uma cultura multimídia, e, portanto, não linear, impulsionada pelos avanços tecnológicos, trouxe novos parâmetros para a comunicação, assim como para a sociedade como um todo. Além disso, o avanço e a cotidianização da tecnologia informática nos impõem sérias reflexões sobre questões éticas, deontológicas, jurídico-políticas, de soberania e da censura estatal, culturais e político-sociais.

A Internet corresponde a um salto no desenvolvimento da humanidade, a uma mudança de paradigmas no pensar e no agir da sociedade, a uma revolução na história. Com o computador, é possível produzir muitas realidades, sendo que cada um cria a sua. No computador, cada indivíduo pode assumir muitas faces, pode mascarar-se, desempenhar vários papéis, mudar de raça, sexo, idade, voz, humor e atitudes, assumir muitas identidades, identidades novas e/ou falsas.

O computador e os jogos computadorizados tornam-se, em parte, substitutos dos parceiros reais. Tudo isso, na verdade, significa a dissolução do sujeito, da pessoa, do eu, da essência humana, da identidade, do gênero, e cria anonimato e distância. Isso ocorre em um mundo virtual, popularmente conhecido como "ciberespaço".

Ciberespaço, segundo o site Wikipédia – a maior enciclopédia virtual livre –, é

"o ambiente criado de forma virtual, por meio do uso dos meios de comunicação modernos, destacando-se entre eles a Internet. Esse fenômeno se deve ao fato de, nos meios de comunicação modernos, haver a possiblidade de pessoas e equipamentos trocarem informações das mais variadas formas sem preocupações.

Também conhecido como Cyberespaço, um termo muito comum na ficção científica (...) 'cyberespaço' (uma junção de cibernético com espaço) foi projetada por um escritor canadense de ficção científica, William Gibson, em 1984, no seu livro 'Neuromancer'."**(1)**

Gibson define o ciberespaço como um espaço não físico ou territorial, que se compõe de um conjunto de redes de computadores, por meio das quais todas as informações circulam.**(2)**

O Direito Penal encontra muitas dificuldades de adaptação dentro desse contexto. O Direito em si não consegue acompanhar o frenético avanço exponencial proporcionado pelas novas tecnologias, em especial pela Internet. É justamente nesse ambiente livre e totalmente sem fronteiras que se desenvolveu uma nova modalidade de crimes, comumente chamada de criminalidade virtual, perpetrada por agentes que se aproveitam da possibilidade de anonimato e da ausência de regras na rede mundial de computadores.

O aparecimento dos primeiros casos de crimes informáticos data da década de 1960, e estes nada mais eram que delitos em que o infrator manipulava, sabotava, espionava ou exercia uso abusivo de computadores e sistemas. A partir de 1980, houve um aumento das ações criminosas, que passaram a refletir em, por exemplo, manipulações de caixas bancários, abusos de telecomunicação, pirataria de programas e pornografia infantil, tornando-se hoje, infelizmente, algo presente no nosso cotidiano. *Vide,* por exemplo, os *e-mails* fraudulentos que recebemos diariamente, na tentativa de captura de nossos dados para utilização indevida *(phishing scam),* com o desvio de valores por *Internet banking*, entre outras condutas.

O presente trabalho destina-se a abordar a criminalidade perpetrada por meio de computadores, sobretudo pela Internet, tratando dos aspectos mais comuns das condutas criminosas cometidas via rede mundial de computadores, procurando relacionar os agentes e os bens jurídicos envolvidos.

1 O computador e a Internet

1.1 A evolução do computador

De uso cotidiano, um computador é um equipamento eletrônico, já quase considerado um eletrodoméstico. No sentido mais amplo, um computador é qualquer equipamento ou dispositivo capaz de armazenar e manipular, lógica e matematicamente, quantidades numéricas representadas fisicamente. Em geral, entende-se por computador um sistema físico que realiza algum tipo de computação.**(3)**

Foi na II Guerra Mundial que realmente nasceram os computadores atuais. A Marinha americana, em conjunto com a Universidade de Harvard, desenvolveu o computador Mark I, projetado pelo professor Howard Aiken, com base no calculador analítico de Babbage.

Mesmo que a tecnologia utilizada nos computadores digitais tenha mudado dramaticamente desde os primeiros computadores da década de 1940, quase todos os computadores atuais ainda utilizam a arquitetura de von Neumann,**(4)** proposta no final daquela década.

Atualmente, estamos na quinta geração de computadores, que tem como principal novidade a disseminação da Internet.**(5)**

1.2 A evolução histórica da Internet

A Internet é uma rede de redes em escala mundial de milhões de computadores que permite o acesso a informações e todo tipo de transferência de dados.**(6)**

A Internet nasceu praticamente sem querer. Foi desenvolvida nos tempos remotos da Guerra Fria, para manter a comunicação das bases militares dos Estados Unidos, ainda que o Pentágono fosse riscado do mapa por um ataque nuclear.

O que hoje forma a Internet como a conhecemos teve inicio em 1969, quando a empresa ARPA (*Advanced Research and Projects Agency*), com o objetivo de conectar departamentos de pesquisa, criou uma rede batizada com o nome de ARPANET. O objetivo de sua criação foi utilizá-la na guerra, pois com essa rede os dados valiosos do governo americano estariam espalhados em vários lugares, ao invés de centralizados em apenas um servidor. Isso evitaria a perda desses dados no caso de, por exemplo, um ataque inimigo que detonasse uma bomba no *campus*.

Antes da ARPANET já existia outra rede que ligava os departamentos de pesquisa e as bases militares, mas, como os EUA estavam em plena Guerra Fria e toda a comunicação dessa rede passava por um computador central que se encontrava no Pentágono, sua comunicação era extremamente vulnerável. Dessarte, se a antiga URSS resolvesse cortar a comunicação da defesa americana, bastava lançar uma bomba no Pentágono e toda comunicação entraria em colapso, tornando os Estados Unidos extremamente vulneráveis a mais ataques.

A ARPANET foi desenvolvida exatamente para evitar isso. Com um *backbone* que passava por baixo da terra (o que o tornava mais difícil de ser interrompido), ela ligava os militares e pesquisadores sem ter um centro definido ou mesmo uma rota única para as informações, tornando-se quase invulnerável.

Quando a ameaça da Guerra Fria passou, a ARPANET tornou-se tão inútil que os militares já não a consideravam tão importante para mantê-la sob a sua guarda. Foi, assim, permitido o acesso aos cientistas, que, mais tarde, cederam a rede para as universidades, as quais, sucessivamente, passaram-na para as universidades de outros países, permitindo que pesquisadores domésticos pudessem ter livre acesso a ela.

Nos anos 1970, as universidades e outras instituições que faziam trabalhos relativos à defesa tiveram permissão para se conectar à ARPANET. Em 1975, existiam aproximadamente 100 *sites*. Os pesquisadores que mantinham a ARPANET estudaram como o crescimento alterou o modo como as pessoas usavam a rede. Os pesquisadores haviam presumido anteriormente que o maior problema seria manter a velocidade da ARPANET alta o suficiente, contudo, na realidade a maior dificuldade se tornou a manutenção da comunicação entre os computadores.

No final dos anos 1970, a ARPANET tinha crescido tanto que o seu protocolo de comutação de pacotes original, chamado de *Network Control Protocol* (NCP), tornou-se inadequado. Em um sistema de comutação de pacotes, os dados a serem comunicados são divididos em pequenas partes. Essas partes são identificadas de forma a mostrar de onde vieram e para onde devem ir, da mesma forma como ocorre com os cartões-postais no sistema postal. Assim também como os cartões-postais, os pacotes possuem um tamanho máximo e não são necessariamente confiáveis. Os pacotes são enviados de um computador para outro até atingir seu destino. Se algum deles for perdido, ele poderá ser reenviado pelo emissor original. Para eliminar retransmissões desnecessárias, o destinatário confirma o recebimento dos pacotes.

Depois de algumas pesquisas, a ARPANET mudou do NCP para um novo protocolo, chamado TCP/IP (*Transfer Control Protocol/Internet Protocol*), desenvolvido em UNIX. A maior vantagem do TCP/IP era que ele permitia um

crescimento praticamente ilimitado da rede, além de ser fácil de implementar, pois contava com uma variedade de plataformas diferentes de *hardware* de computador.

Foi na década de 80 que surgiu a Internet que conhecemos hoje, pois ao longo dessa década diversas instituições dos EUA e de outros países foram se interligando, criando uma grande rede, mas ainda sem o cunho comercial.

Em 1982 foi estabelecido o padrão IP/TCP, até hoje usado na rede, tornando-se obrigatório em 1983. Somente nesse momento pôde-se conceituar a Internet como um conjunto de redes interligadas.

Em 1990, a ARPANET foi desativada pelo Departamento de Defesa, sendo substituída pelos *backbones* da NSFNET, e foi criado um sistema de hipertexto com o auxílio do CERN. Nesse ano, o Brasil também foi conectado à NSFNET.

Foi somente no ano de 1990 que a Internet começou a alcançar a população em geral. Neste ano, o engenheiro inglês Tim Bernes-Lee desenvolveu a *World Wide Web*, possibilitando a utilização de uma interface gráfica e a criação de sites mais dinâmicos e visualmente interessantes. A partir desse momento, a Internet cresceu em ritmo acelerado.

O Mosaic foi a base do que temos do conceito da Internet, pois era possível literalmente navegar de uma página para outra, de um *site* para outro, sem precisar usar comandos complexos, como os existentes no WAIS e no Gopher. O conteúdo também podia ser criado usando um simples editor de texto e uma linguagem simples que foi chamada de HTML (*HiperText Markut Language*).

Em 1994, surgiram serviços de entrega pela rede (Pizza Hut), o primeiro banco *online* e os primeiros *shoppings* virtuais, e, em 1995, a Internet foi privatizada, com o estabelecimento de provedores independentes.

A década de 1990 tornou-se a era de expansão da Internet. Para facilitar a navegação, surgiram vários navegadores (*browsers*) como, por exemplo, o Internet Explorer, da Microsoft, e o Netscape Navigator. O surgimento acelerado de provedores de acesso e de portais de serviços *online* contribuíram para esse crescimento. A Internet passou a ser utilizada por vários segmentos sociais. Os estudantes passaram a buscar informações para pesquisas escolares, enquanto os jovens a utilizavam para pura diversão em *sites* de *games*. As salas de *chat* tornaram-se pontos de encontro para um bate-papo virtual a qualquer momento. As empresas descobriram na Internet um excelente caminho para melhorar seus lucros e as vendas *online* dispararam, transformando a Internet em verdadeiros *shopping centers* virtuais. Por sua vez, desempregados iniciaram a busca de empregos por meio de *sites* de agências de empregos ou enviando currículos por *e-mail*.

No início, a Internet tinha poucos serviços, sendo o *e-mail* o serviço mais utilizado. Posteriormente, foram criados o FTP (transferência de arquivos) e o Telnet (acesso de sessões em *hosts*). Nos dias atuais, é impossível pensar no mundo sem a Internet. Ela tomou parte dos lares de pessoas do mundo todo. Estar conectado à rede mundial passou a ser uma necessidade de extrema importância. A Internet também está presente nas escolas, nas faculdades, nas empresas e em diversos locais, possibilitando acesso às informações e notícias do mundo em apenas um *click*. Atualmente, é possível acessar a Internet por microcomputadores (incluindo *notebooks* e *palm-tops*), celulares, *video games* e até geladeiras. A conexão pode ser feita por linhas telefônicas fixas e móveis, por cabo, por satélite, por rádio e por infravermelho.

1.3 A Internet no Brasil

A história da Internet no Brasil começou bem mais tarde, só em 1991, com a RNP (Rede Nacional de Pesquisa), uma operação acadêmica subordinada ao MCT (Ministério de Ciência e Tecnologia).

Em 1991, a RNP (Rede Nacional de Pesquisas) trouxe a Internet para o Brasil, sendo o seu objetivo o de atender à conexão das redes de universidades e centros de pesquisas, mas logo as esferas federal e estadual começaram também a se interligar.

Em 1994, no dia 20 de dezembro, a Embratel lançou o serviço experimental a fim de conhecer melhor a Internet.

Em 1995, finalmente, os Ministérios de Comunicações e de Ciência e Tecnologia abriram a Internet para operação comercial, e os provedores puderam contratar conexões com a RNP e, depois, com a Embratel. Enfim, houve a abertura ao setor privado da Internet para exploração comercial da população brasileira.

A RNP ficou responsável pela infraestrutura básica de interconexão e informação em nível nacional, tendo controle do *backbone*.**(7)**

Atualmente, o Brasil possui diversos *backbones* inteligando todos os Estados do país, bem como centenas de conexões com outros países.

2 Segurança nos computadores e na Internet

2.1 A necessidade de segurança

Na Internet, espaço e tempo perdem sensivelmente seu significado, especialmente o espaço, que é suprimido. Na questão espaço/tempo, podemos dizer que um acontecimento ocorre depois de outro acontecimento, podemos medir os pontos entre acontecimentos por meio de eventos na forma de intervalos de espaço-tempo; na Internet, porém, esse intervalo praticamente não existe, tudo é instantâneo.

Para André L. M. Lemos, no ciberespaço há a transcendência da matéria:

“Depois da modernidade, que controlou, manipulou e organizou o espaço físico, vemo-nos diante de um processo de desmaterialização pós-moderna do mundo. O ciberespaço faz parte do processo de desmaterialização do espaço e de instantaneidade temporal contemporâneos, após dois séculos de industrialização moderna que insistiu na dominação física de energia e de matérias e na compartimentalização do tempo. Se na modernidade o tempo era uma forma de esculpir o espaço, com a cibercultura contemporânea nós assistimos a um processo em que o tempo real vai aos poucos exterminando o espaço.”**(8)**

Com o ciberespaço, a geografia como a conhecemos (física) desaparece, surgindo uma nova geografia – algo que não é material, mas ainda assim é real. O ciberespaço é um não lugar, ou um lugar imaginário, a que só temos acesso pelo computador. Mesmo assim, ele está ligado à realidade pelo uso que temos feito dele nos dias atuais, transformando-o em um espaço intermediário entre duas realidades.

Praticamente todas as pessoas físicas e jurídicas, de uma forma ou de outra, interagem no ciberespaço, pois a Internet se tornou indispensável em nossas vidas, possibilitando inúmeras facilidades que se estendem de simples contatos sociais até operações bancárias. Porém, justamente por se expandir por praticamente todas as residências, empresas e órgãos públicos, seu livre acesso redunda em problemas ligados à segurança desse sistema, sobretudo quando se trata de operações que envolvam informações que não sejam públicas, tais como dados sigilosos, informações pessoais e bancárias.

O problema da segurança informática pode ser decomposto em vários aspectos distintos, sendo mais relevantes os seguintes: autenticação, confidencialidade e integridade.

A autenticação é o processo por meio do qual é validada a entidade de um utilizador. A confidencialidade reúne as vertentes de segurança que limitam o acesso à informação apenas às entidades autorizadas (previamente autenticadas), sejam elas utilizadores humanos, máquinas ou processos. Por sua vez, a integridade permite garantir que a informação a ser armazenada ou processada é autêntica, isto é, que não é corrompida. Esses aspectos e medidas objetivam impedir ou ao menos diminuir uma série de crimes e atos ilícitos que podem ser perpetrados pelos meios informáticos.

2.2 Formas de violação à segurança

Visando diminuir a segurança dos computadores e, por consequência, da própria Internet, observa-se a utilização de diversos mecanismos que se dispõem, sobretudo, ao compartilhamento de dados sem o consentimento do seu legítimo detentor. Nesse aspecto, merecem destaque:

a) ***Spamming* –** conduta de mensagens publicitárias por correio eletrônico para uma pequena parcela de usuários;
b) ***Cookies*** – são arquivos de texto que são gravados no computador de forma a identificá-lo. Assim, o site obtém algumas informações, tais como quem está acessando o *site*, com que periodicidade o usuário retorna à página da *web* e outras informações almejadas pelo portal;
c) ***Spywares*** – são programas espiões que enviam informações do computador do usuário para desconhecidos na rede. A propagação de *spywares* já foi muito comum em redes de compartilhamento de arquivos, como o Kazaa e o Emule;
d) ***Hoaxes*** – são *e-mails*, na maioria das vezes com remetente de empresas importantes ou de órgãos governamentais, contendo mensagens falsas, induzindo o leitor a tomar atitudes prejudiciais a ele próprio;
e) ***Sniffers*** – são programas espiões semelhantes ao *spywares* que são introduzidos no disco rígido e têm capacidade de interceptar e registrar o tráfego de pacotes na rede;
f**)*Trojan horse* ou cavalos de Troia** – quando instalado no computador, o *trojan* libera uma porta de acesso ao computador para uma possível invasão. O *hacker* pode obter informações de arquivos, descobrir senhas, introduzir novos programas, formatar o disco rígido, ver a tela e até ouvir a voz, caso o computador tenha um microfone instalado. Como boa parte dos micros é dotada de microfones ou câmeras de áudio e vídeo, o *trojan* permite fazer escuta clandestina, o que é bastante utilizado entre os criminosos que visam à captura de segredos industriais.

O computador pode sofrer diversos tipos de consequências, podendo vir a ser danificado parcialmente ou até mesmo totalmente.

Os crimes informáticos contra a máquina são aqueles que irão causar algum tipo de dano à máquina da vítima. Esse dano ocorre por meio de algum programa malicioso que é enviado via Internet, ou por meio dos infectores de *Boot* (dispositivo de inicialização do computador). São diversas as formas de ataque que um computador pode sofrer, como os ataques por vírus, *worms* e *trojans*.

Uma das possíveis maneiras de se cometer um crime informático é utilizar-se de um computador para obter dados sobre o usuário da máquina. O computador é apenas o meio com o qual a pessoa pretende obter os dados, e uma das muitas maneiras de se obter tais informações é utilizando programas *spywares*.

Um programa *spyware* pode vir acompanhado de *hijackers*, ou seja, alterações nas páginas da *web* que o usuário acessa. É o crime mais comum nos dias atuais, pois é por meio de alterações nas páginas, que seriam teoricamente seguras, que os *hackers* conseguem enganar os usuários mais desavisados e distraídos, que acabam fornecendo as informações desejadas. As invasões, além de poderem atacar o computador de um usuário, podem utilizá-lo como ponte de acesso para outras invasões maiores, protegendo, assim, os *hackers*, caso eles venham a ser descobertos. Uma grande curiosidade acerca dos crimes que vêm nos *e-mails* é a falsa ideia de que existem vírus de *e-mail*. Na verdade, a simples leitura da mensagem não acarreta nenhum mal. O que existe, sim, são *e-mails* contaminados por vírus e programas que, ao serem abertos, expõem os usuários que acabam abrindo os anexos da mensagem, os quais podem conter *spywares*, além de vírus e *worms*.

O exemplo mais clássico de uma tentativa de crime é o recebimento de um *e-mail*, seja na caixa pessoal ou da empresa, contendo um *link* que, ao ser clicado, pede autorização para instalar determinado programa.

2.3 Intrusos dos sistemas

Os intrusos dos sistemas atuam de duas formas distintas:

a) **intrusos passivos** – procuram apenas ler informações não autorizadas;
b) **intrusos ativos** – atuam de forma maliciosa, procurando efetuar alterações

não autorizadas nos dados.

Apesar de o termo *hacker* ter sido usado desde os anos 50 para descrever programadores "*free-lancer*" e de tecnologia de ponta, essa conotação tem caído em desuso, dando lugar a uma outra que tem sido popularizada pela mídia: *hacker* é aquele que obtém acesso não autorizado a um sistema de computadores.

Consta no Dicionário Aurélio a definição do que seja *hacker,* dispondo que é o

"indivíduo hábil em enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos destes, ger. a partir de uma conexão remota em uma rede de computadores; violador de um sistema de computação."

Genericamente, *hacker* é uma denominação para alguém que possui uma grande habilidade em computação. *Cracker*, *black-hat* ou *script kiddie*, neste ambiente, denomina aqueles *hackers* que têm como *hobby* atacar computadores. Portanto, a palavra *hacker* é gênero, e *cracker*, espécie.

Segundo um estudo realizado pelo site alemão Alldas.de, atualmente o Brasil abriga o maior grupo de *hackers* do mundo. Entre os feitos desse grupo, registram-se invasões contra o Pentágono, a Microsoft e a IBM americana.**(9)** Entre os grupos de *hackers*, os mais conhecidos, devido a sua voracidade em ataques a *sites*, são: Silver Lords, Brazil Hackers Sabotage, Prime Suspectz, Tty0 e Demônios. Esses cinco grupos brasileiros foram ranqueados pelo *site* alemão Alldas.de como os mais ativos mundialmente em termos de ataques virtuais a grandes empresas e a altos órgãos governamentais dos mais diversos países.

E o número de ataques continua crescendo: recentemente, no dia 30.01.2011, *hackers* brasileiros do grupo Anonymous divulgaram o início de uma ação para tirar do ar sites de instituições bancárias públicas e privadas no Brasil.**(10)**

No dia 23.01.2011, o *site* pessoal do vice-presidente da República, Michel Temer (PMDB), foi invadido por um grupo de *hackers* contrário ao projeto de lei americano Sopa (*Stop Online Piracy Act*).**(11)**

Em 29.11.2011, foi divulgado que o Palácio do Planalto iria contratar uma empresa para garantir maior segurança no acesso à Internet pelos usuários da rede da Presidência da República, entre eles a presidente Dilma Rousseff.

Logo no início do ano de 2011, um dia após a cerimônia de posse da presidente Dilma, o endereço eletrônico da Presidência ficou fora do ar devido a uma invasão de *hackers*. No primeiro semestre deste ano, mais de 200 *sites* públicos – dos quais 20 eram do governo federal – foram atacados em uma única semana, de acordo com estimativas do Serpro (empresa que administra parte dos *sites* do governo federal, entre eles o da Presidência).

A própria presidente já teve seu correio eletrônico invadido quando ainda era candidata ao Palácio do Planalto. Reportagem da Folha de São Paulo publicada em junho de 2011 mostrou que, durante a campanha eleitoral, um *hacker* invadiu o *e-mail* pessoal de Dilma e tentou vender um pacote de mensagens recebidas pela petista.**(12)**

Além disso, a mídia mundial repercutiu a invasão efetuada por *hackers* israelenses nos *sites* do governo do Irã.**(13)** Autodenominada “IDF Team”, a equipe invadiu portais dos ministérios da educação e da saúde do Estado persa, além do portal de uma emissora de TV, cuja programação é apresentada em inglês. Em todos eles, o conteúdo foi substituído por uma bandeira de Israel. Em outra ocasião, em 25.10.2011, foram liberadas na rede informações referentes a 2006 de mais de 9 milhões de moradores de Israel, revelando dados pessoais dessas pessoas para todo o mundo.**(14)**

Como visto, a questão da segurança no ciberespaço não é de interesse apenas das pessoas físicas ou das empresas, sendo altamente relevante para órgãos públicos, para agentes políticos e para o próprio Estado.

3 Crimes por meio dos computadores

3.1 Conceitos e nomenclaturas

Ao lado dos benefícios que surgiram com a disseminação dos computadores e do acesso à Internet, surgiram crimes e criminosos especializados na linguagem informática, proliferando-se por todo o mundo. Tais crimes são chamados de crimes virtuais, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, delitos cibernéticos, crimes transnacionais, dentre outras nomenclaturas. À medida que o número de conexões entre computadores cresce, cresce também o da criminalidade neste meio, com criminosos incentivados pelo anonimato oferecido pela rede e pelas dificuldades de investigação no ambiente virtual.

Para definir o que seja o crime virtual, trazemos conceitos de alguns estudiosos no assunto.

Para Ramalho Terceiro,**(15)**

"os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo; por isso, ficaram usualmente definidos como sendo crimes virtuais. Ou seja, os delitos praticados por meio da Internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas."

Segundo Augusto Rossini,**(16)**

"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 e a confidencialidade."

A denominação "delitos informáticos", segundo Rossini, abarca crimes e contravenções penais, alcançando não somente aquelas condutas praticadas no âmbito da Internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível "conexão" à Rede Mundial de Computadores, ou a qualquer outro ambiente telemático. Ou seja, uma fraude em que o computador é usado como instrumento do crime, fora da Internet, também seria alcançada pelo que se denominou "delitos informáticos". Mais: para o autor, "delito informático" é gênero, do qual "delito telemático" é espécie, dada a peculiaridade de ocorrer no e a partir do inter-relacionamento entre os computadores em rede telemática usados na prática delitiva.

Guilherme Guimarães Feliciano**(17)** apresenta conceito bem amplo de "criminalidade informática":

"Conheço por criminalidade informática o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (*hardware*, *software*, redes, etc.)."

Deborah Fisch Nigri**(18)** descreve o "crime informático" como um ato lesivo cometido por meio de um computador ou de um periférico com a intenção de se obter uma vantagem indevida. Segundo essa autora, os conceitos anglo-saxônicos limitam-se a denominar o direito de informática de *computer law* ou *legal aspects of computers* e, no caso mais específico de crimes informáticos, *computer crime*, isso porque o uso da palavra "informática" lhes é praticamente desconhecido.

Importante colacionar o conceito para "crime de informática" cunhado pela Organização para a Cooperação Econômica e Desenvolvimento da ONU: "crime de informática é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento de dados e/ou transmissão de dados".

Em outras palavras, o crime virtual é qualquer ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão em que um computador conectado à rede mundial de

computadores (Internet) seja o instrumento ou o objeto do delito.

Alguns autores classificam estes crimes em puros e impuros (ou mistos), sendo que os puros seriam as condutas que ainda não foram tipificadas, necessitando de lei que crie tipos penais específicos para a persecução das condutas, e os impuros ou mistos seriam os tipos penais já existentes e que podem ocorrer no ciberespaço.

Assim, percebe-se que não há um consenso sobre o que é considerado como crime virtual, tão menos há uma denominação aceita pela maioria.

Atualmente, não há legislação específica definindo o que é crime na rede. Assim, eventuais condenações são feitas com base no Código Penal, que foi reformado em 1984 – antes, portanto, da existência da Internet.

3.2 *Hackers*, *crackers*: a terminologia quanto ao sujeito ativo

Para se aplicar a devida sanção penal, deve-se ter fixo um sujeito infrator, um dos elementos intrínsecos da ação.

Diante desse fato é que os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo e, por isso, ficaram usualmente definidos como sendo crimes virtuais. Outrossim, os delitos praticados por meio da Internet são denominados de crimes virtuais devido à ausência física de seus autores e de seus partícipes.

Um dos grandes problemas relativos aos denominados cibercrimes é o fato de ser difícil identificar o criminoso, tendo em vista que é difícil garantir a identidade do imputado.

Por *hacker* se entende uma pessoa com grande conhecimento na área de informática. Mas, segundo Plantullo,**(19)**

"é uma pessoa física que detém, como objeto, a investigação da integridade e da segurança de um sistema qualquer de computador. Utilizasse de técnicas avançadas para invadir sistemas e detectar suas respectivas falhas. Todavia, não os destrói ou prejudica."

Por sua vez, o termo *cracker* se refere às pessoas que possuem um grande conhecimento de programação e de segurança em sistemas de computação. Tais pessoas utilizam esse conhecimento para tirar vantagens pessoais, como destruição de sistemas por mero vandalismo ou aplicação de condutas para diversos fins ilícitos, como o estelionato eletrônico.

3.3 Classificações

Crime informático é aquele que tutela o bem jurídico inviolabilidade dos dados informáticos.

Vianna**(20)** classifica os crimes informáticos em:

a) **crimes informáticos impróprios –** aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados);
b) **crimes informáticos próprios –** aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados);
c) **delitos informáticos mistos –** são crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa;
d) **crimes informáticos mediatos ou indiretos –** é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação.

Segundo Guimarães e Furlaneto Neto, os crimes informáticos podem ser classificados em virtuais puros, mistos e comuns.

a) **Crime virtual puro** – compreende qualquer conduta ilícita, a qual atenta o *hardware* e/ou o *software* de um computador, ou seja, tanto a parte física

quanto a parte virtual do microcomputador;
b) **Crime virtual misto** – o que utiliza a Internet para realizar a conduta ilícita, e cujo objetivo é diferente do citado anteriormente. Por exemplo, as transações ilegais de valores de contas correntes;
c) **Crime virtual comum** – é utilizar a Internet apenas como forma de instrumento para realizar um delito que se enquadra no Código Penal, como, por exemplo, distribuição de conteúdo pornográfico infantil por diversos meios, tais como *messengers*, *e-mail*, *torrent* ou qualquer outra forma de compartilhamento de dados.

Crime informático, e-crime, cibercrime, crime eletrônico ou crime digital são termos utilizados para se referir a toda atividade em que um computador ou uma rede de computadores é utilizada como ferramenta, base de ataque ou meio de crime.

Adicionalmente, embora os termos crimes eletrônicos ou cibercrimes sejam mais apropriadamente utilizados para descrever atividades criminais que façam uso de computadores ou de uma rede de computadores, eles também são utilizados para descrever crimes tradicionais, tais como fraude, roubo, chantagem, falsificação e apropriação indébita, nos quais computadores ou redes de computadores são usados para facilitar as atividades ilícitas.

Segundo Guimarães e Furlaneto Neto,**(21)** crime informático significa "qualquer conduta ilegal, não ética ou não autorizada que envolva o processamento automático de dados e/ou a transmissão de dados". Essa categoria de crime apresenta algumas características, dentre elas a transnacionalidade – pois não está restrita apenas a uma região do globo –, a universalidade – trata-se de um fenômeno de massa, e não de elite – e a ubiquidade – ou seja, está presente nos setores privados e públicos.

O crime por computador pode acarretar danos tanto pessoais como empresariais.

Além da classificação anterior, também podemos categorizar tais crimes em dois tipos básicos: crimes cometidos utilizando o computador como ferramenta para cometer a infração e crimes cometidos contra o computador em si, nos quais o objeto é danificado ou prejudicado de alguma forma. De um modo geral, crimes informáticos podem ser definidos como toda atividade criminal que envolva o uso da infraestrutura tecnológica da informática, incluindo acesso ilegal (não autorizado), interceptação ilegal (por meio do uso de técnicas de transmissão não públicas de dados de computador, para, de ou fora do sistema de computadores), obstrução de dados (danos a dados de computador, deteriorização dos dados, alteração ou supressão dos dados de computador), interferência nos sistemas (interferência nos sistemas de computadores quanto a entrada, transmissão, apagamentos, deteriorização, alteração ou supressão de dados de computador), uso indevido de equipamentos, falsificação de IPs e fraude eletrônica.

O criminoso informático é denominado – vulgarmente – *hacker*, e este pode ser classificado em dois tipos: interno e externo.

3.4 Crimes virtuais mais comuns

Crimes virtuais são os delitos praticados por meio da Internet que podem ser enquadrados no Código Penal brasileiro, e os infratores estão sujeitos às penas previstas na lei.

O Brasil é um país que não tem uma legislação definida e que abranja, de forma objetiva e geral, os diversos tipos de crimes cibernéticos que ocorrem no dia a dia e que aparecem nos jornais, na televisão, no rádio e nas revistas.

Na ausência de uma legislação específica, aquele que praticou algum crime informático deverá ser julgado dentro do próprio Código Penal, mantendo-se as devidas diferenças. Se, por exemplo, um determinado indivíduo danificou ou foi pego em flagrante danificando dados, dados estes que estavam salvos em CDs de sua empresa, o indivíduo deverá responder por ter infringido o artigo 163 do Código Penal, que é "destruir, inutilizar ou deteriorar coisa alheia: pena – detenção, de um a seis meses, ou multa". Os crimes informáticos, mesmo sem

uma lei específica, podem ser julgados pela lei brasileira. Seguem abaixo os principais crimes perpetrados no Brasil.

a) **Pirataria**: Copiar dados em CDs, DVDs ou qualquer base de dados sem prévia autorização do autor é entendido como pirataria de acordo com a Lei 9.610/98. De acordo com o art. 87 desta lei, "o titular do direito patrimonial sobre uma base de dados terá o direito exclusivo, a respeito da forma de expressão da estrutura da referida base". As penas podem variar de 2 meses a 4 anos, com aplicação ou não de multa, a depender se houve reprodução parcial ou total, venda ou disponibilização ao público via cabo ou fibra óptica;
b) **Dano ao patrimônio**: Previsto no art. 163 do Código Penal. O dano pode ser simples ou qualificado, sendo considerado qualificado quando "o dano for contra o patrimônio da União, do Estado, do Município, de empresa concessionária de serviços públicos ou de sociedade de economia mista". Observa-se que, para ser qualificado, o objeto do dano deverá ser da União, do Estado, do Município, de empresa concessionária de serviços públicos ou de sociedade de economia mista, podendo ser aplicado, por exemplo, àqueles crimes de sabotagem dentro de repartições públicas. A mesma lógica é utilizada quando se trata de vírus, por ser considerado como tentativa (perante comprovação) de dano. A punição para dano simples é de detenção, de um a seis meses, ou multa. Já para dano qualificado, a pena prevista é detenção de seis meses a três anos e multa;
c) **Sabotagem informática**: A sabotagem, em termos econômicos e comerciais, será a invasão de determinado estabelecimento, visando prejudicar e/ou roubar dados. Segundo Milton Jordão, "consiste a sabotagem informática no acesso a sistemas informáticos visando a destruir, total ou parcialmente, o material lógico ali contido, podendo ser feita por meio de programas destrutivos ou vírus". A lei apenas prevê punição de 1 a 3 anos de prisão e multa, porém não inclui a sabotagem informática em seu texto;
d) **Pornografia infantil**: O art. 241 do Estatuto da Criança e do Adolescente proíbe "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". A punição para quem infrinja este artigo do estatuto é de detenção de 2 a 6 anos e multa;
e) **Apropriação indébita**: O Código Penal faz menção apenas à apropriação indébita de bens materiais, tais como CPU, mouse e monitor, ficando excluída a apropriação de informações. Contudo, se a apropriação se der por meio de cópia de *software* ou de informações que legalmente pertencem a uma instituição, podem-se aplicar punições por pirataria. A pena para apropriação indébita está prevista no artigo 168, sendo de reclusão de 3 a 6 anos e multa para quem praticar ato fraudulento em benefício próprio;
f) **Estelionato**: Neste tipo de crime, o Código Penal pode ser aplicado de acordo com o seu artigo 171, desde que o crime tenha sido consumado. Segundo Da Costa, o estelionato "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, uma vez que impunível o meio inidôneo". A pena é de reclusão de 1 a 5 anos e multa;
g) **Divulgação de segredo**: O Código Penal nada cita caso o segredo seja revelado via computador, sendo tratado da mesma forma que se divulgado por documento, por se tratar de uma forma de correspondência;
h) **Crimes contra a liberdade individual**: São os crimes de ameaça (artigo 147), de inviolabilidade de correspondência (artigos 151 e 152), de divulgação de segredos (artigos 153 e 154) e de divulgação de segredos contidos ou não em sistemas de informação ou bancos de dados da Administração Pública (artigo 153, § 1º-A);
i) **Difamação, injúria e calúnia**: São os crimes de calúnia (artigo 138), de difamação (artigo 139) e de injúria (artigo 140). Os criminosos são incentivados pelo anonimato, e os crimes podem ocorrer em *chats*, *blogs*, pelo envio de *spams* e por meio de publicações em *homepages*, dentre outros meios de postagem eletrônica. Podem ocorrer nas redes sociais, por exemplo, se alguém divulgar informações falsas que prejudiquem a reputação de outra pessoa, ofendam a dignidade do outro ou maldosamente acusem alguém de criminoso, desonesto ou perigoso;
j) **Falsa identidade**: Ocorre quando alguém mente seu nome, idade, estado civil, sexo e outras características com o objetivo de obter alguma vantagem ou prejudicar outra pessoa.

O crime do artigo 151, crime de violação de correspondência, é um tipo plenamente aplicável à conduta de interceptação e violação de *e-mails*. Já os tipos previstos na Lei 6.538/78 são inaplicáveis, pois essa dispõe sobre os serviços postais explorados pela União, por meio de empresa pública vinculada ao Ministério das Comunicações. Neste tipo, o bem jurídico tutelado é a integridade dos Serviços Postal e de Telegrama nacionais, devendo a correspondência se dar por meio da via postal ou por telegrama, hipóteses às quais o *e-mail* não se amolda.**(22)**

O bem jurídico protegido nos tipos de furto e roubo é o patrimônio. Por isso, é desnecessária a criação de outro tipo penal somente para discriminar o meio de execução do delito, que costuma ser realizado por manipulação de dados (fraude por manipulação de um computador contra um sistema de processamento de dados) para modificação de depósitos bancários e obtenção de vantagem econômica, ou, ainda, pela obtenção de dados como senhas para manipular contas bancárias e obter vantagem financeira.

Quanto ao crime de estelionato, para sua configuração se faz necessário induzir ou manter alguém em erro mediante ardil – ao menos uma determinada pessoa, e não um sistema eletrônico –, é necessário haver uma relação psicológica entre o autor e a vítima, que deve se sentir iludida.

É nesse terreno que os criminosos se utilizam de suas maiores artimanhas, servindo-se de cavalos de Troia, clonando *sites* e utilizando a engenharia social.

Além dos crimes citados, também podem ocorrer na Internet crimes de lavagem de dinheiro e de invasão de privacidade, pixações em *sites* oficiais do governo, vandalismo, sabotagem, crimes contra a paz pública, pirataria em geral, espionagem, lesões a direitos humanos (terrorismo, crimes de ódio, racismo, etc.), destruição de informações, jogos ilegais, falsificação do selo ou sinal público, falsidade ideológica, modificação ou alteração não autorizada de sistema de informação, violação de sigilo funcional, fraude em concorrência pública, dentre inúmeros outros.

Ultimamente, uma modalidade de crime que vem se tornando muito comum na Internet é o envio de *e-mail* simulando ser de algum órgão estatal conhecido, como é o caso da Receita Federal, do TSE (Tribunal Superior Eleitoral), da Polícia Federal e da Serasa. A metodologia empregada é enganar o proprietário do *e-mail* com uma mensagem dizendo que existe alguma pendência com o órgão e que este deve clicar em algum *link* para solucionar tal situação ou até mesmo para saber mais detalhes sobre o fato. Ao clicar em tal *link*, o usuário é redirecionado para uma página cujo intuito é instalar um programa conhecido como sanguessuga no computador da vítima. A partir desse momento, o criminoso começa a receber dados sigilosos.

Outra modalidade bem comum emprega a mesma metodologia de envio de *e-mail* à vítima, mas, ao invés de o remetente da mensagem ser um órgão oficial do governo, os criminosos utilizam nomes de instituições financeiras. Essa modalidade de envio de *e-mail* é bem mais específica, pois a vítima deve possuir laço com a instituição financeira utilizada. Ao clicar no *link* contido no *e-mail*, o usuário é direcionado a uma falsa página do banco, onde deve digitar seus dados bancários para uma suposta atualização bancária. Após a digitação, o remetente da mensagem recebe todos esses dados e, com isso, pode efetuar diversas transações bancárias, lesando a vítima.

Há crimes cujo intuito é demonstrar a fragilidade de sistemas, como é o caso das recentes invasões às páginas de órgãos oficiais.

Existe uma infinidade de crimes virtuais; muitos ainda nem possuem um *modus operandi* conhecido, e outros ainda nem foram descobertos.

3.5 Resposta estatal

O primeiro decreto condenatório por crime eletrônico no Brasil foi proferido pela juíza da 3ª Vara da Justiça Federal de Campo Grande (MS), Janete Lima Miguel. Isso apenas vem confirmar que nossa legislação vigente pode ser aplicada aos crimes cibernéticos.**(23)**

Embora não estejam satisfatoriamente codificadas em leis, dado o caráter tecnológico do tema, extremamente flexível, as condutas de crimes digitais, em especial os que utilizam a Internet, já estão sendo adequadas à legislação positiva existente, na qual encontram guarida, ainda que incidental, variando a sua tipificação conforme o bem jurídico agredido.**(24)**

Embora a Internet ainda seja considerada por muitos como um território livre, sem lei e sem punição, a realidade não corrobora essa tese. Diariamente, o Judiciário vem coibindo a sensação de impunidade que reina no ambiente virtual e combatendo a criminalidade cibernética com a aplicação do Código Penal, do Código Civil e de legislações específicas, como a Lei n° 9.296 – que trata das interceptações de comunicação em sistemas de telefonia, informática e telemática – e a Lei n° 9.609 – que dispõe sobre a proteção da propriedade intelectual de programas de computador.

Grande parte dos magistrados, advogados e consultores jurídicos considera que cerca de 95% dos delitos cometidos eletronicamente já estão tipificados no Código Penal brasileiro por caracterizarem crimes comuns praticados por meio da Internet. Os outros 5%, para os quais faltaria enquadramento jurídico, abrangem transgressões que só existem no mundo virtual, como a distribuição de cavalos de Troia, vírus eletrônicos e *worms* (vermes, em português).

Para a maioria, a Internet não é um campo novo de atuação, mas apenas um novo caminho para a realização de delitos já praticados no mundo real, bastando apenas que as leis sejam adaptadas para os crimes eletrônicos. E é isso o que o Poder Judiciário vem fazendo no Brasil, adaptando e empregando vários dispositivos do Código Penal e legislação esparsa no combate ao crime digital.

Como demonstrado no capítulo 3, a lista de artigos utilizados para a punição de crimes virtuais é extensa: insultar a honra de alguém (calúnia – artigo 138); comentar, em *chats*, *e-mails* e outros, de forma negativa, sobre raças, religiões e etnias (preconceito ou discriminação – artigo 20 da Lei n° 7.716/89); espalhar boatos eletrônicos sobre pessoas (difamação – artigo 139); enviar ou trocar fotos de crianças nuas (pedofilia – artigo 247 da Lei n° 8.069/90, o Estatuto da Criança e do Adolescente – ECA); ameaçar alguém (ameaça – artigo 147); insultar pessoas considerando suas características ou utilizar apelidos grosseiros (injúria – artigo 140); utilizar dados da conta bancária de outrem para desvio ou saque de dinheiro (furto – artigo 155); usar logomarca de empresa sem autorização do titular, no todo ou em parte, ou imitá-la de modo que possa induzir à confusão (crime contra a propriedade industrial – artigo 195 da Lei n° 9.279/96); monitoramento não avisado previamente (interceptação de comunicações de informática – artigo 10 da Lei n° 9.296/96); usar cópia de *software* sem licença (crimes contra *software* "Pirataria" – artigo 12 da Lei n° 9.609/98), dentre outros tipos penais.

O STJ, como guardião e uniformizador da legislação infraconstitucional, vem consolidando a aplicação desses dispositivos em diversos julgados. Por exemplo, já firmou o entendimento de que os crimes de pedofilia e de divulgação de pornografia infantil por meios eletrônicos estão descritos no artigo 241 da Lei n° 8.069/90 (apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive pela rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente) e previstos em convenção internacional da qual o Brasil é signatário.

Mais do que isso: a Corte concluiu que, por si só, o envio de fotos pornográficas pela Internet (*e-mail*) já constitui crime. Com base no artigo 241 do Estatuto da Criança e do Adolescente (ECA), os ministros da Quinta Turma do STJ cassaram um *habeas corpus* concedido pelo Tribunal de Justiça do Estado do Rio de Janeiro (TJ-RJ) que determinava o trancamento de uma ação penal sob o argumento de que o ECA definiria como crime apenas a "publicação" – e não a mera "divulgação" – de imagens de sexo explícito ou pornográficas de crianças ou adolescentes.

Os casos de furto e estelionato virtual também já foram devidamente enquadrados pelo STJ. A Terceira Seção consolidou o entendimento de que a apropriação de valores de conta corrente mediante transferência bancária

fraudulenta via Internet sem o consentimento do correntista configura furto qualificado por fraude. Entendeu que a fraude é utilizada para burlar o sistema de proteção e vigilância do banco sobre os valores mantidos sob sua guarda, e também decidiu que a competência para julgar esse tipo de crime é do juízo do local da consumação do delito de furto, que se dá no local onde o bem é subtraído da vítima.

Em outra decisão, cujo relator foi o ministro Felix Fischer, a Quinta Turma do STJ definiu claramente que, mesmo no ambiente virtual, o furto mediante fraude não se confunde com o estelionato, já que no furto a fraude é utilizada para burlar a vigilância da vítima e, no estelionato, o objetivo é obter consentimento da vítima e iludi-la para que entregue voluntariamente o bem.

Portanto, as condutas chamadas de crimes virtuais (embora inexista legislação específica) encontram-se tipificadas em textos legislativos existentes (Código Penal e legislação esparsa) e, ao contrário do que alguns autores afirmam, a aplicação da lei já existente a essas condutas não é caso de analogia, pois não são crimes novos, não são novos bens jurídicos necessitando de tutela penal. A novidade da criminalidade virtual fica por conta do *modus operandi*, ensejando estudo de como o criminoso tem feito uso das novas tecnologias, fazendo com que os estudiosos e os aplicadores do Direito tenham que renovar seus conceitos.

Relevante mencionar que as denúncias de crimes praticados pela Internet têm aumentado. Dados do Ministério Público Federal (MPF) apontam que, entre 2007 e 2008, o número de procedimentos abertos na Procuradoria para investigar crimes cibernéticos subiu 318%. Em 2007, foram abertas 620 investigações, menos de um terço dos 1.975 procedimentos abertos somente em 2008.

A respeito da atuação jurisdicional contra o combate aos crimes virtuais, o *site* do Jornal Folha de São Paulo noticiou em 24.11.2008 o seguinte:

"Os crimes praticados por meio da Internet, que em 2002 motivaram apenas 400 sentenças, crescem vertiginosamente no país. Seis anos depois, o número chega a 17 mil sentenças tratando dos chamados crimes virtuais, informa o *blog* do Josias de Souza.
A notícia vem do STJ (Superior Tribunal de Justiça) e serve para desmistificar a ideia de que a Internet seria uma espécie de território sem lei.
A Justiça vem enquadrando os novíssimos crimes cibernéticos no velhíssimo Código Penal brasileiro, editado em 1940, ainda sob o governo Getúlio Vargas.
Segundo o STJ, cerca de 95% dos delitos cometidos pela Internet já estão previstos no Código Penal e apenas são cometidos em um ambiente novo: a Internet."**(25)**

Conclusão

"A parte está no todo, assim como o todo está na parte." Assim começa Juremir Machado da Silva o seu artigo "Pensar a vida, viver o pensamento".**(26)** Frase que descreve perfeitamente a conjuntura global em que vivemos, na qual não existe mais isolamento.

A Internet ensejou uma revolução na vida das pessoas, das empresas e dos Estados. Nada nem ninguém se encontra completamente isolado do ciberespaço, o qual trouxe inúmeros benefícios a nossa sociedade, muitos dos quais já foram referidos nos capítulos anteriores. Conforme já dizia Nicholas Negroponte,**(27)** a revolução tecnológica permitiu que a sociedade passasse "dos átomos aos *bits*". E a virtualização da realidade não deixa de se expandir, tanto que já existem salas de aula virtuais, igrejas virtuais e até religiões**(28)** baseadas na virtualidade da Internet. É a verdadeira simulação de um mundo.

Contudo, o efeito colateral dessa integração das pessoas físicas e jurídicas com a Internet foi o surgimento de uma nova criminalidade, que se utiliza do espaço virtual para perpetrar seus desígnios. O aparecimento dessa nova modalidade de crimes ensejou uma séria alteração na atuação policial para o seu combate, pois, a partir de então, os crimes que ocorriam apenas no "mundo concreto" passaram a ser cometidos no mundo virtual, ou seja, via Internet.

A resposta a este novo tipo de criminalidade encontra dificuldades em face dos

princípios de territorialidade e de soberania, fazendo com que os Estados procurem auxílio internacional, criando uma rede de integração e cooperação globais. Talvez seja necessário criar normas internacionais para o combate desta nova criminalidade.

Cabe aos estudiosos do Direito o trabalho para a evolução da dogmática penal segundo uma nova realidade mundial para que o ciberespaço não se transforme em um universo paralelo onde as regras do Direito não tenham alcance.

Os conceitos apresentados neste trabalho expõem a polêmica e a controvérsia, em face da complexidade do tema, sobre o que se entende por crimes virtuais, uma vez que a própria denominação desta nova criminalidade não é uníssona. Ao passo que, para alguns, os crimes virtuais são condutas típicas, antijurídicas e culpáveis que somente têm sua forma de execução diferenciada, pois são implementados por meio da Internet, para outros, são condutas ilícitas que necessitam de tipificação, não encontrando amparo na legislação vigente.

Ao concluirmos este trabalho, constatamos que uma das muitas dificuldades da resposta estatal para estes crimes é que o meio em que eles ocorrem é mais rápido, praticamente instantâneo, além do que quase não deixam pistas, mas causam dano a bens juridicamente protegidos. Dessarte, faz-se necessária uma ampla, rápida e efetiva resposta estatal, quer por meio de repreensão policial, quer na forma de atuação jurisdicional.

Apesar das mudanças que ocorreram na sociedade, decorrentes dos novos paradigmas que vêm guiando as políticas planetárias, os bens jurídicos que esse novo modelo de criminalidade (criminalidade eletrônica ou virtual) tem atingido continuam os mesmos, não sendo necessária a criação de novos tipos penais para dar efetiva resposta aos seus agentes. Não obstante, o Estado deve oferecer mais segurança ao ambiente da Internet.

Em suma, os chamados crimes virtuais nada mais são que condutas que afetam bens jurídicos já protegidos pela lei penal; portanto, são condutas típicas.

Referências bibliográficas

BLOG do Josias: crimes cibernéticos geram 17 mil sentenças judiciais. **Folha de São Paulo**, 24 nov. 2008. Disponível em: < **http://www1.folha.uol.com.br/folha/informatica/ult124u471204.shtml**>. Acesso em: 24 fev. 2012.

BLUM, Renato M. S. Opice; ABRUSIO, Juliana Canha. Os hackers e os tribunais. **IBDI –** Instituto Brasileiro de Direito da Informática, 9 mar. 2004. Disponível em: <**http://www.ibdi.org.br/index.php?secao=&id_noticia=287&acao=lendo**>. Acesso em: 12 mar. 2012.

BURROWES, FREDERICK B. A proteção constitucional das comunicações de dados: Internet, celulares e outras tecnologias. **Rev. Jur.**, Brasília, v. 9, n. 87, p. 09-24, out./nov., 2007.

COLLI, Maciel. **Cibercrimes:** limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2010.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

CRESPO, Marcelo Xavier de Freitas; SYDOW, Spencer Toth. Novas tendências da criminalidade telemática. **Revista de Direito Administrativo**, Rio de Janeiro, n. 246, set./dez. 2007.

CRESPO, Marcelo Xavier de F. **Noções introdutórias aos delitos informáticos**. 2010 (Artigo publicado no seminário de crimes Cibernéticos do portal "justributario.com.br").

O QUE são spyware, hijackers. **Dicionário UOL**. Disponível em: <**http://tecnologia.uol.com.br/dicionarios/dicionario-a.jhtm**>.

DUNN, John E. Hackers israelenses invadem sites do governo do Irã. **IDG Now**, 27 jan. 2012. Disponível em: <**http://idgnow.uol.com.br/seguranca/2012/01/27/hackers-israelenses-invadem-sites-do-governo-do-ira/**>. Acesso em: 31 jan. 2012.

FELICIANO, Guilherme Guimarães. Informática e criminalidade. Parte I: lineamentos e definições. **Boletim do Instituto Manoel Pedro Pimentel**, São Paulo, v. 13, n. 2, p. 35-45, set. 2000.

FELINTO, Erick. **A religião das máquinas:** ensaios sobre o imaginário da cibercultura. Porto Alegre: Sulina, 2005.

SITE de Michel Temer é invadido por hackers. **Folha de São Paulo**, 23 jan. 2012. Disponível em: <**http://www1.folha.uol.com.br/poder/1038304-site-de-michel-temer-e-invadido-por-hackers.shtml**>. Acesso em: 31 jan. 2012.

FOREQUE, Flávia. Planalto reforça segurança para acesso de informações da web. **Folha de São Paulo**, 29 nov. 2011. Disponível em: <**http://www1.folha.uol.com.br/poder/1013639-planalto-reforca-seguranca-para-acesso-de-informacoes-da-web.shtml**>. Acesso em: 31 jan. 2012.

FRANCO, Alberto Silva. Globalização e criminalidade dos poderosos. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 8, n. 31, p. 102-136, jul./set. 2000.

VAZAM na web dados pessoais de quase toda a população de Israel. **IDG Now**, 25 out. 2011. Disponível em: <**http://idgnow.uol.com.br/seguranca/2011/10/25/vazam-na-web-dados-pessoais-de-quase-toda-a-populacao-de-israel/**>. Acesso em: 31 jan. 2012.

GAUER, Ruth M. Chittó. Conhecimento e aceleração: mito, verdade e tempo. In: GAUER, Ruth M. Chittó (org.). **A qualidade do tempo:** para além das aparências históricas. Rio de Janeiro: Lumen Júris, 2004.

GOMES, Luiz Flávio; BIANCHINI, Alice. Globalização e direito penal. In: **ESCRITOS em homenagem a Alberto da Silva Franco**. São Paulo: Revista dos Tribunais, 2003.

KOLB, Anton. Ontologia e antropologia virtuais. In: KOLB, Anton; ESTERBAUER, Reinhold; RUCKENBAUER, Hans-Walter (org.). **Ciberética:** responsabilidade em um mundo interligado pela rede digital. São Paulo: Loyola, 2001.

LEMOS, André L. M. Estruturas antropológicas do ciberespaço. **Textos de Cultura e Comunicação**, Salvador, n. 35, p. 12-27, jul. 1996. Disponível em: <**http://www.facom.ufba.br/pesq/cyber/lemos/estrcy1.html**>. Acesso em: 10 mar. 2012.

LIMA NETO, José Henrique Barbosa Moreira. **Violação de direitos autorais na Internet**. 7 jul. 1996. Disponível em: <**http://www.juridica.com.br/fra_textos_atuali.asp?CodArtigo=36**>. Acesso em: 10 maio 2005.

LYOTARD, Jean-François. **A condição pós-moderna**. 7. ed. Rio de Janeiro: José Olympio, 2002.

MIRABETE, Julio Fabbrini. **Manual de direito penal**. 8. ed., rev. e ampl. São Paulo: Atlas, 1994. v. 1. Parte geral: arts. 1º a 120 do CP.

MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via Internet. **Jus Navigandi**, Teresina, a. 4, n. 37, dez. 1999. Disponível em: <**http://www1.jus.com.br/ doutrina/texto.asp?id=1828**>. Acesso em: 12 mar. 2012.

MORIN, Edgar. As duas globalizações: comunicação e complexidade. In: _____. **As duas globalizações:** complexidade e comunicação, uma pedagogia do presente. Porto Alegre: Sulina, 2001.

NEGROPONTE, Nicholas. **A vida digital**. São Paulo: Companhia das Letras, 1995.

NETO, Mário Furlaneto; GUIMARÃES, José Augusto Chaves. **Crimes na internet:** elementos para uma reflexão sobre a ética informacional. Disponível em: <**http://www.cjf.jus.br/revista/numero20/artigo9.pdf**>.

NEVES, Márcio. Hackers planejam ataques a sites de bancos; Itaú já saiu do ar. **Folha de São Paulo**, 30 jan. 2012. Disponível em:

<http://www1.folha.uol.com.br/mercado/1041332-hackers-planejam-ataques-a-sites-de-bancos-itau-ja-saiu-do-ar.shtml>. Acesso em: 31 jan. 2012.

NIGRI, Deborah Fisch. Crimes e segurança na Internet. **In Verbis**, Rio de Janeiro: Instituto dos Magistrados do Brasil, ano 4, n. 20, p. 34-41, 2000.

OLIVEIRA, Felipe Cardoso Moreira de. **Criminalidade informática**. 2002. Dissertação (Mestrado em Ciências Criminais), Faculdade de Direito, PUCRS, Porto Alegre, 2002.

PAIVA, José Roberto. **Sexo e pornografia infantil na Internet**. 06 mar. 1999. Disponível em: <**http://www.prosex.org.br/pornografia.html**>.

PODVAL, Roberto; BICUDO, Tatiana Viggiani. Para onde caminhamos? In: **ESCRITOS em homenagem a Alberto Silva Franco**. São Paulo: Revista dos Tribunais, 2003.

PRADO, Luis Regis. **Curso de direito penal brasileiro**. 2. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2001. v. 1. Parte geral : arts. 1º a 120.

REALE JÚNIOR, Miguel. **Instituições de direito penal**. Rio de Janeiro: Forense, 2002. v. 1. Parte geral.

REALE, Miguel. **Paradigmas da cultura contemporânea**. São Paulo: Saraiva, 1996.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SILVA, Evandro Lins e. A globalização e seus meandros. In: **ESCRITOS em homenagem a Alberto Silva Franco**. São Paulo: Revista dos Tribunais, 2003.

SILVA, Juremir Machado da. Pensar a vida, viver o pensamento. In: MORIN, Edgar. **As duas globalizações:** complexidade e comunicação, uma pedagogia do presente. Porto Alegre: Sulina, 2001.

SILVA, Tadeu Antonio Dix. Pensamento único e frente ideológica na globalização hegemônica. In: **ESCRITOS em homenagem a Alberto da Silva Franco**. São Paulo: Revista dos Tribunais, 2003.

SOROS, George. **Globalização**. Rio de Janeiro: Campus, 2003.

VIANNA, Túlio Lima. **Fundamentos de direito penal informático**. Rio de Janeiro: Forense, 2003.

WERTHEIM, 1999, p. 231. Apud: FELINTO, Erick. Tecnognose: tecnologias do virtual, identidade e imaginação espiritual. In: _____. **A religião das máquinas:** ensaios sobre o imaginário da cibercultura. Porto Alegre: Sulina, 2005.

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de direito penal brasileiro:** parte geral. 3. ed., rev. e atual. São Paulo: Revista dos Tribunais, 2001.

ZANELLATO, Marco Antonio. Condutas ilícitas na sociedade digital. **Caderno Jurídico da Escola Superior do Ministério Público de São Paulo:** Direito e Internet, São Paulo, a. 2, v. 1, n. 14, p. 167-230, jul.

Notas

1. CIBERESPAÇO. In: WIKIMEDIA FOUNDATION. **Wikipédia**: a enciclopédia livre. 7 abr. 2006. Disponível em: <**http://pt.wikipedia.org/w/index.php?title=Ciberespa%C3%A7o&oldid=1813906**>. Acesso em: 16 fev. 2012.

2. LEMOS, André L. M. Estruturas antropológicas do ciberespaço. **Textos de Cultura e Comunicação**, Salvador, n. 35, p. 12-27, jul. 1996. Disponível em: <**http://www.facom.ufba.br/pesq/cyber/lemos/estrcy1.html**>. Acesso em: 16 fev. 2012.

3. COMPUTADOR. In: WIKIMEDIA FOUNDATION. **Wikipédia**: a enciclopédia livre. Disponível em: <**http://pt.wikipedia.org/w/index.php?title=Computador**>. Acesso em: 08 mar. 2012.

4. A arquitetura de von Neumann descreve o computador com quatro seções principais: A unidade lógica e aritmética (ULA), a unidade de controle, a memória, e os dispositivos de entrada e saída (E/S ou I/O). Essas partes são interconectadas por fios e barramentos.

5. ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004. p. 24-25.

6. INTERNET. In: WIKIMEDIA FOUNDATION. **Wikipédia**: a enciclopédia livre. Disponível em: <**http://pt.wikipedia.org/w/index.php?title=Internet**>. Acesso em: 08 mar. 2012.

7. Coluna dorsal de uma rede, o *backbone* representa a via principal de informações transferidas por uma rede, neste caso, a Internet.

8. LEMOS, André L. M. Estruturas antropológicas do ciberespaço. **Textos de Cultura e Comunicação**, Salvador, n. 35, p. 12-27, jul. 1996. Disponível em: <**http://www.facom.ufba.br/pesq/cyber/lemos/estrcy1.html**>. Acesso em 16 fev. 2012.

9. RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **Crimes virtuais**. 2005. Disponível em: <**http://www.advogadocriminalista.com.br**>. Acesso em: 27 jun. 2005.

10. NEVES, Márcio. Hackers planejam ataques a sites de bancos; Itaú já saiu do ar. **Folha de São Paulo**, 30 jan. 2012. Disponível em: <**http://www1.folha.uol.com.br/mercado/1041332-hackers-planejam-ataques-a-sites-de-bancos-itau-ja-saiu-do-ar.shtml**>. Acesso em: 31 jan. 2012.

11. SITE de Michel Temer é invadido por hackers. **Folha de São Paulo**, 23 jan. 2012. Disponível em: <**http://www1.folha.uol.com.br/poder/1038304-site-de-michel-temer-e-invadido-por-hackers.shtml**>. Acesso em: 31 jan. 2012.

12. FOREQUE, Flávia. Planalto reforça segurança para acesso de informações da web. **Folha de São Paulo**, 29 nov. 2011. Disponível em: <**http://www1.folha.uol.com.br/poder/1013639-planalto-reforca-seguranca-para-acesso-de-informacoes-da-web.shtml**>. Acesso em: 31 jan. 2012.

13. DUNN, John E. Hackers israelenses invadem sites do governo do Irã. **IDG Now**, 27 jan. 2012. Disponível em: <**http://idgnow.uol.com.br/seguranca/2012/01/27/hackers-israelenses-invadem-sites-do-governo-do-ira/**>. Acesso em: 31 jan. 2012.

14. VAZAM na web dados pessoais de quase toda a população de Israel. **IDG Now**, 25 out. 2011. Disponível em: <**http://idgnow.uol.com.br/seguranca/2011/10/25/vazam-na-web-dados-pessoais-de-quase-toda-a-populacao-de-israel/**>. Acesso em: 31 jan. 2012.

15. RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. **Jus Navigandi**, Teresina, a. 6, n. 58, ago. 2002. Disponível em: <**http://jus2.uol.com.br/doutrina/texto.asp?id=3186**>. Acesso em: 20 abr. 2006.

16. ROSSINI, 2004, p. 110.

17. FELICIANO, Guilherme Guimarães. Informática e criminalidade. Parte I: lineamentos e definições. **Boletim do Instituto Manoel Pedro Pimentel**, São Paulo, v. 13, n. 2, p. 35-45, set. 2000. p. 42.

18. NIGRI, Deborah Fisch. Crimes e segurança na Internet. **In Verbis**, Rio de Janeiro: Instituto dos Magistrados do Brasil, Ano 4, n. 20, p. 34-41, 2000. p. 38.

19. PLANTULLO, V. L. **Estelionato Eletrônico**. Crutiba: Juruá, 2002.

20. VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de

Janeiro: Forense, 2003.

21. NETO, Mário Furlaneto; GUIMARÃES, José Augusto Chaves. **Crimes na Internet**: elementos para uma reflexão sobre a ética informacional. Disponível em: <**http://www.cjf.gov.br/revista/numero20/artigo9.pdf**>.

22. OLIVEIRA, Felipe Cardoso Moreira de. **Criminalidade informática**. 2002. Dissertação (Mestrado em Ciências Criminais), Faculdade de Direito, PUCRS, Porto Alegre, 2002. p. 73.

23. BLUM, Renato M. S. Opice; ABRUSIO, Juliana Canha. Os hackers e os tribunais. **IBDI –** Instituto Brasileiro de Direito da Informática, 9 mar. 2004. Disponível em: <**http://www.ibdi.org.br/index.php?secao=&id_noticia=287&acao=lendo**>. Acesso em: 12 mar. 2012.

24. MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via Internet. **Jus Navigandi**, Teresina, a. 4, n. 37, dez. 1999. Disponível em: <**http://www1.jus.com.br/doutrina/texto.asp?id=1828**>. Acesso em: 12 mar. 2012.

25. BLOG do Josias: crimes cibernéticos geram 17 mil sentenças judiciais. **Folha de São Paulo**, 24 nov. 2008. Disponível em: < **http://www1.folha.uol.com.br/folha/informatica/ult124u471204.shtml**>. Acesso em: 24 fev. 2012.

26. SILVA, Juremir Machado da. Pensar a vida, viver o pensamento. In: MORIN, Edgar. **As duas globalizações**: complexidade e comunicação, uma pedagogia do presente. Porto Alegre: Sulina, 2001. p. 13-20.

27. NEGROPONTE, Nicholas. **A vida digital**. São Paulo: Companhia das Letras, 1995.

28. WERTHEIM, 1999, p. 231. Apud: FELINTO, Erick. Tecnognose: tecnologias do virtual, identidade e imaginação espiritual. In: _____. **A religião das máquinas:** ensaios sobre o imaginário da cibercultura. Porto Alegre: Sulina, 2005.

Referência bibliográfica (de acordo com a NBR 6023: 2002/ABNT):
GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais. **Revista de Doutrina da 4ª Região**, Porto Alegre, n. 55, ago. 2013. Disponível em:
<http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html>
Acesso em: 09 set. 2013.