UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE DIREITO

ANTÔNIO HELI MALZONI SARAIVA

ASPECTOS GERAIS DOS CRIMES DIGITAIS E REGULAMENTAÇÃO NO ORDENAMENTO JURÍDICO BRASILEIRO

Campina Grande - PB
2010

ANTÔNIO HELI MALZONI SARAIVA

ASPECTOS GERAIS DOS CRIMES DIGITAIS E REGULAMENTAÇÃO NO ORDENAMENTO JURÍDICO BRASILEIRO

Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Centro de Ciências Jurídicas da Universidade Estadual da Paraíba – UEPB, como requisito parcial para obtenção do Grau de Bacharel em Direito. Sob a orientação da Profª. Drª. Rosimeire Ventura Leite

Campina Grande - PB
2010

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL – UEPB

S243a Saraiva , Antônio Heli Malzoni.

Aspectos gerais dos crimes digitais regulamentação no ordenamento jurídico brasileiro [manuscrito] / Antônio Heli Malzoni Saraiva. – 2010.

55 f.

Digitado.
Trabalho Acadêmico Orientado (Graduação em Direito) – Universidade Estadual da Paraíba, Centro de Ciências Jurídicas, 2010.
"Orientação: Profa. Dr. Rosimeire Ventura Leite, Departamento de Direito Público".

1. Direito Penal 2. Crimes Digitais I. Título.

21. ed. CDD 345.02

Antônio Heli Malzoni Saraiva

ASPECTOS GERAIS DOS CRIMES DIGITAIS E REGULAMENTAÇÂO NO ORDENAMENTO JURÍDICO BRASILEIRO

Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Centro de Ciências Jurídicas da Universidade Estadual da Paraíba – UEPB, como requisito parcial para obtenção do Grau de Bacharel em Direito. Sob a orientação da Profª. Drª. Rosimeire Ventura Leite

Aprovado em: 26 / 11 / 2010

BANCA EXAMINADORA

Rosimeire Ventura Leite

Profª. Drª. Rosimeire Ventura Leite – CCJ/UEPB
Orientadora — Nota

Prof. Esp. Claudio Simão de Lucena Neto – CCJ/UEPB
Examinador — Nota

Prof. Msc. Amilton de França – CCJ/UEPB
Examinador — Nota

*À **família**, pelos sacrifícios, esforços, e constante apoio e carinho.*

*Aos **amigos**, pela paciência, tolerância e senso de humor.*

*À **Deus**, pela existência e proteção.*

***Dedico**.*

AGRADECIMENTOS

Agradeço a **Deus**, pois se não fosse ele não estaríamos aqui;

Aos meus familiares, por infinitos motivos. Em especial aos meus pais **Jânio** e **Hermínia**, meus irmãos **Raphael** e **Ismael**, meu sobrinho **Gabriel,** minha tia **Marister,** e meu primo **Moisés**;

Aos meus avós (in memorian) pela significativa e inesquecível passagem em minha vida;

Aos meus grandes amigos, **Ademar**, **Állysson**, **Arsênio**, **Bruno**, **Cadu**, **Carlos**, **Elizete**, **Filipe**, **Gadé**, **Gugu**, **Guilherme**, **Igor**, **Jeanine**, **João Adolfo**, **Mário**, **Mikkael**, **Nayanne**, **Shelldon**, **Wendson**, e em especial a **Rembrandt** (in memorian), por participarem dos melhores momentos que vivi até hoje;

A minha orientadora, **Rosimeire**, pela disponibilidade e boa vontade e me ajudar neste trabalho.

Aos meus professores, sempre tão atenciosos, que com paciência e dedicação me conduziram com sabedoria por esse mundo do Direito.

A todas as pessoas que diretamente ou indiretamente me apoiaram e incentivaram na conclusão desta grande fase de minha vida.

A todos, meu sincero **MUITO OBRIGADO!**

"A ambição do homem é tão grande que para satisfazer a uma vontade presente, ele não pensa no mal que em breve daí pode resultar."

Henry Ford

LISTA DE SIGLAS

ARPANET - Advanced Research Projects Agency Network

CD - Compact Disk

CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CF - Constituição Federal

CP - Código Penal

CPP - Código de Processo Penal

ENIAC - Eletronic Numeri Integrator and Calculator

ICP - Infra-Estrutura de Chaves Públicas

LSI - Largue Scale Integration

MP - Medida Provisória

TCP/IP - Transmission Control Protocol/Internet Protocol

WWW - World Wide Web

RESUMO

Os benefícios e conveniências proporcionados pelos grandes avanços tecnológicos ao decorrer dos últimos anos causaram uma crescente digitalização das condutas e práticas humanas no mundo inteiro. Essa nova realidade social modificou subitamente áreas como economia, comunicação, educação, e claro, o campo jurídico. Consequentemente, tais avanços propiciaram também o surgimento de novas formas de crimes – os Crimes Digitais - e com eles o surgimento dos criminosos digitais, que se adaptaram à tecnologia e evoluíram, tornando-se aptos a praticarem ilícitos em meio virtual, realizando condutas desonestas e condenáveis, movidos por inúmeros tipos de interesse, agindo por intermédio de computadores e redes de Internet, e incentivados ainda mais em razão da crescente dependência da sociedade às tecnologias digitais. Ante essa nova realidade criminosa discute-se a evolução da criminalidade digital e as suas consequências principalmente na esfera penal e processual penal, mas também em outras áreas do Ordenamento Jurídico. Dessa forma faz-se necessário analisar os aspectos jurídicos dos crimes digitais, seus conceitos e definições, objetivos, classificações, o perfil dos principais agentes, a aplicabilidade ou não das normas já existentes a essas novas condutas, e analisar as propostas de leis que visão regular o assunto, assim como, quando necessário, apontar em determinados casos a necessidade de novas formas penais específicas para suprir a existência de eventuais lacunas jurídicas.

Palavras-Chaves: Crimes Digitais. Tecnologia. Direito Penal.

ABSTRACT

The benefits and convenience offered by major technological advances over the past years have caused a growing digitization of human behaviors and practices worldwide. This new reality suddenly changed social areas such as economics, communication, education, and of course the legal field. Therefore, these advances also brought about the emergence of new forms of crime - the Computer Crime - and with them the emergence of cybercriminals, who have adapted to technology and evolved, becoming able to practice illegal in the virtual environment, performing and deceptive conduct condemnable, propelled by numerous types of interest, acting through computers and Internet networks, and encouraged even more because of the increasing dependence of society to digital technologies. Given these new realities criminal discusses the evolution of digital crime and its consequences especially in criminal and procedural law, but also in other areas of the legal system. Thus it is necessary to examine the legal aspects of digital crime, its concepts and definitions, goals, classifications, the profile of the main agents, the applicability or not of the existing laws for these new conducts, and to consider proposals for laws that wants regulate the matter and, when necessary, in some cases point out the need for new ways to meet the specific criminal existence of any legal holes.

Keywords: Digital Crimes. Technology. Criminal Law.

SUMÁRIO

INTRODUÇÃO

O avanço tecnológico é um fenômeno de escala global, a cada dia novas notícias ao redor do mundo relativas a alguma nova tecnologia é divulgada, avanços que vão desde a um simples novo software doméstico para facilitar algum trabalho específico, até o desenvolvimento de novas técnicas medicinais revolucionárias que prometem curas milagrosas, proporcionando assim o salvamento de várias vidas.

Dentre os principais feitos da humanidade no âmbito da tecnologia, está a informática, e dentro deste mesmo campo, a Rede Internacional de Dados, mais conhecida como Internet*,* que trouxe mais velocidade de informação, conforto, facilidade, segurança, dentre inúmeros outros benefícios. O crescimento tecnológico da esfera digital proporcionou tantos avanços para a sociedade moderna que é quase impossível imaginar o mundo caso ela não existisse. Como os grandes aeroportos funcionariam sem computadores regulando o controle do tráfego aéreo? Ou se poderia projetar e fazer funcionarem complexos de geração de energia em massa como as grandes hidroelétricas? Como se decifraria o código genético humano, num programa do porte do Projeto Genoma, que gerou avanços inimagináveis na área da medicina? Além de conquistas complexas como estas, atividades corriqueiras como ir ao banco, fazer compras, ler alguma notícia, ou se comunicar visualmente com outras pessoas, agora podem ser executadas sem a presença física, seja através de um computador pessoal ou de dispositivos como celulares e vários outros similares.

No entanto, com o constante avanço tecnológico nacional e mundial surgiram novas modalidades criminais, ou a prática dos crimes já existentes, só que por meios não tipificados. Os Crimes Digitais, como são chamados, são praticados por pessoas que se adaptaram à tecnologia, tornando-se aptos a praticarem ilícitos no meio digital por intermédio de computadores e/ou da Internet, afim de, por exemplo, burlar sistemas de segurança de bancos e transferir dinheiro para contas fantasmas, invadir sistemas para obtenção de dados pessoais sem autorização, ofender, ameaçar ou iludir pessoas para a obtenção de alguma vantagem ilícita, e mais uma infinidade de práticas claramente criminosas.

Sabendo que o direito é responsável pela regulamentação e solução das problemáticas da sociedade, essa discussão sobre os crimes digitais tem se tornado

cada vez mais relevante e necessária, no sentido de estabilizar a vida em sociedade, sem que a utilização criminosa dos meios digitais prejudique os inúmeros benefícios que a tecnologia proporciona. Dessa forma, alguns dos principais problemas neste campo são relativos à necessidade ou não de uma legislação especifica para a proteção de bens jurídicos digitais, e de outros igualmente relevantes, que possam ser ofendidos por meio da informática, uma vez que o juiz, em respeito ao princípio da legalidade e da anterioridade da lei penal, não pode punir alguém por uma conduta que não seja previamente considerada crime. É uma garantia fundamental e constitucional do cidadão. Da mesma forma, não pode, ao sentenciar, aplicar analogicamente ao caso concreto atípico norma que tipifica conduta aparentemente semelhante, pois no Direito Penal, a analogia só pode ser aplicada para beneficiar o réu.

Por essa razão, para que não fique impune aquele que pratica condutas claramente criminosas nos meios digitais, faz-se necessária a criação de uma lei com figuras penais próprias, mas exclusivamente para as quais não caiba a aplicação da legislação penal vigente, pois tem que se ter em mente que a lei penal também não retroage a não ser para favorecer o réu, ou seja, a criação de novos tipos penais, incriminando condutas já previstas como crimes em nossa legislação vigente, mas com tipificação específica, poderá deixar impunes todos aqueles que as praticaram antes da entrada em vigor da nova lei. Por essa razão é necessário atentar para as condutas típicas de Internet realmente nocivas que já não sejam consideradas crimes pela legislação penal vigente.

Mas afinal, o que são crimes digitais? Como separá-los dos crimes comuns? Como saber se a conduta de alguém pode ser considerada um crime digital? A doutrina mundial começa a se preocupar com este tema, e embora ainda não se tenha chegado a um consenso em relação a vários aspectos, inclusive quanto à definição do que eles realmente sejam, uma reflexão deve ser feita entre o que é extralegal, e o que não é ético. A solução para um determinado problema deve ser de acordo com a atividade que é desempenhada, só quando a conduta é determinante para ser verdadeiramente criminosa é que deve ser buscada a proibição criminal.

Diante das evidentes proporções da criminalidade existente por meio dos meios digitais, o poder estatal não pode deixar de preservar os direitos dos cidadãos

e de prevenir e reprimir os crimes, para que dessa forma todos possam ter acesso seguro à comunicação e às informações que os meios digitais proporcionam, sem que a sua privacidade, intimidade, integridade e propriedade sofram violações e lesões. Portanto, expor algumas das principais formas de práticas de crimes digitais, identificar sua origem histórica, conceitos e classificações, as definições de alguns dos principais criminosos do meio, e como a legislação brasileira age, e pretende agir, analisando os principais projetos de leis em tramitação, é o que será focado neste trabalho.

1 ASPECTOS GERAIS DOS CRIMES DIGITAIS

1.1 HISTÓRICO

Não se pode falar em crimes digitais sem antes entender a evolução histórica dos meios pelos quais são praticados, e o principal deles, que deu base para todos os outros dispositivos digitais é o computador. O primeiro aparelho que efetivamente se pode definir como computador foi criado por interesses militares e data de 1946. Recebeu o nome de ENIAC, e foi utilizado na confecção de tabelas de cálculos para a trajetória de bombas e projéteis. Mas para se chegar a tanto, várias etapas foram superadas, com esforços de vários matemáticos e filósofos, como bem destaca Liliane Paesani:

> A história deixou registradas algumas das mais interessantes realizações do homem no campo da informática. Depois do advento do "ábaco", pouco ou quase nada de significativo foi desenvolvido na área de processamento de dados. É necessário dar um salto de quase 20 séculos para chegar, em 1614, aos matemáticos e filósofos John Napier (1614), Blaise Pascal (1624), G.W.von Leibnitz (1671), Thomas de Colmar (1818) e Charles Babbage (1822), que desenvolveram estudos e trabalhos que serviram de base para as mais recentes pesquisas em computação. Herman Hollerith (engenheiro americano:1860-1929), baseado nas idéias de Jacquard, construiu em 1898 a primeira máquina para processamento de estatísticas demográficas do censo americano, reduzindo o trabalho de dez para dois anos. Criou a empresa Tablating Machine Company, atual International Business Machines (IBM). (PAESANI, 2002, p. 19)

Em 1951 apareceram os primeiros computadores em série, chamados de "primeira geração", que tinham como características o enorme tamanho e peso. De 1958 a 1965 passaram a ser conhecidos como "segunda geração", tornaram-se bem mais leves e consideravelmente mais potentes. Então em 1969 nos Estados Unidos nasceu a internet, primeiramente chamada de ARPANET, e foi criada com a intenção de se montar um sistema em que todos os pontos estivessem interligados e que os dados transmitidos pudessem trafegar em qualquer sentido. Assim como o computador, a Internet também foi criada para uso militar, no auge da guerra fria, para atender as demandas do Departamento de Defesa americano, que necessitavam de comunicação entre pontos estratégicos que não pudessem ser destruídos por bombardeios.

Em 1965 surgiu a “terceira geração” de computadores, com dimensões ainda menores e mais leves, sistemas operacionais mais avançados, múltiplas linguagens de programação e velocidade de processamento altíssima.

Então finalmente em 1975 surgiu a “quarta geração”, que dura até hoje, claro que ainda com constantes evoluções em velocidade de processamento, capacidade de armazenamento de dados e inúmeras outras, mas sempre com características que ocasionaram a subida de geração, como os circuitos interligados em longa escala – LSI – e microprocessadores. É durante esta geração, em 1982, que o nome Internet é primeiramente utilizado e depois de um ano se estabelece o controle de transmissão protocolar do protocolo de internet - TCP/IP – que tornou-se obrigatório é a linguagem utilizada até hoje por todos os computadores conectados à rede. Apenas oito anos depois, em 1991, é que foi criado um sistema que facilitaria muito a navegação pela rede e que sem ele seria impossível navegar na Internet, que é o sistema de hipertexto World Wide Web (Rede de alcance mundial), ou - WWW.

De acordo com o Dicionário Enciclopédico de Informática, de Ana Helena Fragomente, computador pode ser definido como:

> 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 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 lei. (FRAGOMENTE, 1986, p.125)

Acompanhando as evoluções do computador e da internet, Fabrizio Rosa (2005) observa que os primeiros registros de crimes digitais datam desde os anos 60, como a manipulação de computador, sabotagem de computador, espionagem e uso ilegal de sistemas de computador, dentre outros casos.

A partir da década de 70 os crimes digitais começaram a evoluir, o que propiciou um grande aumento na freqüência em que eram cometidos, passaram a ser praticados, na maioria dos casos, por especialistas em informática cujo principal objetivo num primeiro momento era simplesmente invadir os sistemas de segurança de grandes empresas apenas com o intuito de provarem-se capazes e ficarem famosos. Logo que descobriram as vantagens econômicas que seus conhecimentos

poderiam lhes proporcionar, as instituições financeiras passaram a ser alvos dos principais ataques.

A partir dos anos 80 surgiram os primeiros casos de vírus e pirataria, então iniciou-se por parte de grandes empresas um trabalho especializado para se combater essas novas ameaças. O problema é que quanto mais a tecnologia avançava no campo da segurança, esse mesmo avanço poderia também ser aproveitado no campo da criminalidade, uma vez que os criminosos com grande poder de conhecimento e adaptação utilizavam as novidades a seu favor.

Hoje em dia, com a massiva disseminação dos computadores, e especialmente com o surgimento das redes, logicamente houve uma grande mudança no perfil dos usuários, assim como no dos criminosos. Dentro de nossa atual realidade qualquer pessoa física ou jurídica pode praticar ou ser vitimas dos crimes digitais. Essa nova tendência da substituição dos documentos de papel pelos documentos digitais, a utilização de serviços e operações financeiras on-line, o dinheiro eletrônico, compras on-line a liberdade e anonimato proporcionado pela internet, dentre ouros fatores, está causando um enorme impacto na natureza de crimes tradicionais como, o roubo, a fraude e a falsificação, pois agora são cometidos mais frequentemente por pessoas utilizando meios digitais, graças às inúmeras facilidades e oportunidades que as novas tecnologias e os novos ambientes digitais proporcionam. Atualmente, a pornografia, a pedofilia, as drogas, a fraude, os direitos autorais, a espionagem e transferências de tecnologias são as principais preocupações das autoridades policiais investigativas.

Temos que considerar que nos últimos 10 anos ocorreu uma crescente preocupação por parte da comunidade mundial a respeito do abuso e a apropriação de informações digitais e a utilização de computadores para se cometer crimes, a repressão a estas condutas já ocorre em vários países, sobretudo nos mais avançados tecnologicamente. Em algumas legislações, modificou-se o Código Penal, em outras, editaram-se leis extravagantes. No Brasil, alguns dispositivos que tratam especificamente de crimes digitais já existem no Código Penal e em algumas legislações extravagantes, e há previsão de que novas leis que regulam tal matéria e tramitam atualmente no senado e no congresso sejam aprovadas. Como será abordado mais adiante.

1.2 CONCEITO

Por se tratar de um assunto que envolve conhecimento paralelo entre duas disciplinas completamente distintas, ou seja, Direito e Informática, não existe ainda uma definição consensual de crimes digitais, seja na doutrina nacional ou estrangeira. Para contribuir ainda mais com tal discussão, a nomenclatura utilizada para referir-se aos crimes digitais é bastante ampla.

Como destaca Vladmir Aras (2001), vários podem ser os nomes relativos aos crimes digitais, como por exemplo, delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, crimes telemáticos, crimes informacionais, crimes virtuais, ciberdelitos, cibercrimes, dentre outros. Não existe consenso técnico ou doutrinário quanto ao nome jurídico genérico dos delitos que ofendem interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos (*hardwares*[1]), redes de computadores e programas de computador (*softwares*[2]).

Para Ivette Senise, todas essas condutas revelam:

> [...] uma vulnerabilidade que os criadores desses processos não haviam previsto e que careciam de uma proteção imediata, não somente através de novas estratégias de segurança no seu emprego, mas também de novas formas de controle e incriminação das condutas lesivas. (FERREIRA, 2000, p.210)

Para Ramalho Terceiro:

> [...] 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. (RAMALHO TERCEIRO, 2002, p. 1)

Segundo Augusto Rossini:

> [...] 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

---

[1] Segundo o Dicionário Michaelis, Hardware é o conjunto de unidades físicas, componentes, circuitos integrados, discos e mecanismos que compõem um computador ou seus periféricos.

[2] Software é qualquer programa ou grupo de programas que instrui o hardware sobre a maneira como ele deve executar uma tarefa, inclusive sistemas operacionais, processadores de texto e programas de aplicação.

> 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. (ROSSINI, 2004, p. 110)

João Marcello de Araújo Júnior conclui que o Crime digital consiste em:

> Uma conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder à obtenção de uma vantagem ilícita, porém praticada, sempre com a utilização de dispositivos habitualmente empregados nas atividades de informática. (ARAÚJO JUNIOR, apud MONTEIRO NETO, 2003, p. 45)

De qualquer forma, para Klaus Tiedeman (apud FERREIRA, 2000, p. 207) “o crime virtual designa todas as formas de conduta ilegais realizadas mediante a utilização de um computador, conectado ou não a uma rede”, tais condutas podem ir desde a pirataria de programas de computador, até fraudes nos sistemas bancários on-line, assim como abusos nos sistemas de telecomunicação.

A melhor definição considerada pela maioria dos doutrinadores é a de Ivette Senise Ferreira (2000, p. 209) "constitui crime de informática toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão".

Abordando de forma mais técnica, o crime digital pode ser definido como algum ato ilícito perpetrado contra um sistema digital ou de informação, ou por intermédio dele. Segundo K. C Laudon e J. P. Laudon (2001, p. 16), define-se por sistema digital ou sistema de informação uma série de componentes inter-relacionados que armazenam, coletam, processam, distribuem, ou recuperam as informações de um sistema com o objetivo de facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório em empresas e outras organizações, ou ainda para facilitar o trabalho e/ou estudo de pessoas físicas. Estes componentes são divididos em técnicos (*hardware*, *software*, banco de dados, telecomunicações), organizacionais (procedimentos para operar o sistema) e humanos (profissionais de sistemas e/ou usuários).

Apesar dos vários entendimentos acima observados, se conclui que a definição de Crime Digital deve estar intrinsecamente relacionada ao bem jurídico que se almeja proteger, pois diferente dos delitos tradicionais ou comuns, que podem ser praticados contra os sistemas de computação, por exemplo, o dano ou o furto, o crime digital é aquele praticado contra bens jurídicos digitais e o conjunto de dados e informações contidos nos sistemas de informação utilizando-se de meios digitais para tanto. Ou seja, se um empregado de uma grande empresa insatisfeito

com seu salário, derrama água e assim danifica o seu computador de trabalho, ele comete o crime comum de dano, e não um crime digital, pois apesar de danificar os dados contidos na memória do computador, a vontade subjetiva do agente não era causar dano ao bem jurídico digital, além de que ele não utilizou nenhum método informatizado para atingir seu objetivo. Se no mesmo exemplo o empregado para vingar-se da empresa transfere um vírus poderoso para o computador da empresa através da internet ou mesmo de um CD, que danifica os dados do computador permanentemente, aí sim, sua ação pode ser definida como crime digital.

1.3 CLASSIFICAÇÕES

Da mesma forma que não existe consenso doutrinário quanto ao conceito de crimes virtuais, também não há quanto a suas classificações, todavia, uma classificação muito destacada na doutrina internacional é a exposta por HERVÉ CROZE e YVES BISMUTH (apud FERREIRA, 2000, p.215), que diferenciam duas categorias de crimes virtuais:

I - Os crimes cometidos contra um sistema de informação, qualquer que seja a motivação do agente;

II - Os crimes cometidos contra algum outro bem jurídico, por meio de um sistema de informação.

No primeiro caso, temos o crime de informática propriamente dito, sendo o computador o meio de execução e o alvo, podendo ser objetos de tais condutas o computador, seus periféricos, os dados ou o suporte lógico da máquina e as informações contidas em sua memória de armazenamento. No segundo caso, o computador é apenas o meio de execução, para que se consiga o resultado-crime, sendo as práticas ilícitas de natureza patrimonial as mais comuns nesta espécie, principalmente as que atentam contra o direito de autor, o patrimônio financeiro e a liberdade individual.

Levando em consideração a finalidade do delito e nesse caso afastando os crimes comuns, Jean Pradel e Cristian Feuillard (apud FERREIRA, 2000, p.213) classificam:

I - Manipulações para obtenção de dinheiro;

II - Manipulações para obtenção de informações.

Tal classificação merece destaque, pois afasta os crimes já previstos pelo ordenamento jurídico, classificando apenas os verdadeiros crimes virtuais; entretanto, não abrange todos os possíveis delitos que podem ser cometidos contra os sistemas de informação, uma vez que muitos destes são cometidos somente com a finalidade de causar algum dano ao equipamento, sem a intenção de obter alguma vantagem econômica ou informacional.

Considerando a forma de atuação do agente, o professor Klaus Sieber (apud MONTEIRO NETO, 2003, p. 47) propõe a seguinte classificação:

I - Fraude por manipulação de um computador contra um sistema de processamento de dados;

II - Espionagem informática;

III - Sabotagem informática;

IV - Furto do tempo;

V - Acesso não autorizado;

VI - Ofensas tradicionais.

O primeiro caso se trata da alteração de dados dentro de um sistema de informação com a finalidade de obter vantagem ilícita. Pode ocorrer, por exemplo, por meio da alteração de resultados ou por meio da introdução de dados falsos; Já na espionagem informática, o delito acontece com a utilização de um sistema de informação, com o objetivo principal de obter alguma informação ou dados, que estão sob sigilo; A sabotagem informática tem como objeto o próprio sistema e pode ser considerado um dos mais lesivos delitos praticados por meio de um sistema de informação, efetua-se pela destruição dos dados ou informações, através de programas criados pelos agentes, como por exemplo, vírus ou subprogramas que uma vez acionados prejudicam os programas principais destruindo-os ou distorcendo o seu funcionamento, fazendo assim com que o sistema fique inapto a processar. Pode ocorrer também quando estes mecanismos distorcem os dados já armazenados, o que acarreta inúmeros prejuízos aos programas principais; O furto de tempo é a prática ilícita considerada mais comum e mais disseminada dos crimes digitais, ocorre quando pessoas não autorizadas utilizam um sistema digital (ou sistema de informação), para fins particulares. Geralmente acontece com certa

freqüência em empresas, quando um funcionário sem possuir autorização para acessar a rede virtual viola os sistemas de segurança e utiliza o computador e seus recursos para fins alheios aos interesses da empresa; O acesso não autorizado destaca-se como o crime digital que mais evoluiu com o nascimento da Internet, trata-se de acesso por uma pessoa sem autorização a um sistema digital restrito no qual o invasor agindo ilegalmente pode ter acesso a informações sigilosas; E por ultimo, as ofensas tradicionais consistem em valer-se do sistema digital para prática de crimes tradicionais como, por exemplo, a falsificação de documentos. Podem ser praticadas por meio de um sistema de informação ou que tenha a sua parte física como objeto.

Observando os avanços doutrinários internacionais, mas abordando de forma diversa, os autores nacionais passaram a acatar quase com unanimidade os elementos básicos da classificação exposta por Luis Flávio Gomes (apud ELIAS, 2001, p. 105), que divide os crimes digitais em duas categorias semelhantes, que são os crimes praticados contra o computador em sentido amplo e crimes por meio de computador.

Da mesma forma, Damásio de Jesus (apud ARAS, 2001) classifica os crimes digitais em: crimes digitais puros ou próprios e crimes digitais impuros ou impróprios. Os próprios são aqueles praticados por meio de um sistema digital, onde o resultado da conduta se opera no próprio meio digital, sendo o sistema virtual o bem jurídico protegido. Os crimes impuros ou impróprios são aqueles em que o sistema digital funciona meramente como instrumento para a prática de condutas danosas a bem jurídicos que já são protegidos por outras normas penais incriminadoras, não relacionadas a bens digitais. Esta classificação é a mais aceita no Direito Digital brasileiro.

Entende-se assim que, os crimes virtuais podem ser cometidos na modalidade de atividades tradicionais, ou seja, crimes que também podem ser cometidos sem o uso de um meio virtual, como furto, fraude, falsificação, dano, etc. Ou na modalidade específica, ou seja, crimes que só podem ser efetuados com o uso de um meio virtual, por exemplo, o acesso não autorizado, a transmissão de vírus, furto ou roubo de informações digitais privadas, material ofensivo divulgado no mundo virtual, invasão de sites comerciais e pessoais, pirataria tecnológica e audiovisual entre inúmeros outros.

Entretanto, Monteiro Neto (2003, p. 48) observa a necessidade da reformulação dos sistemas de classificação excluindo dos seus conteúdos os crimes já previstos por normas penais protetoras de outros interesses jurídicos que não os digitais, como por exemplo:

I - Quantos aos efeitos dos crimes digitais: Crimes digitais de efeitos tangíveis; Crimes digitais de efeitos intangíveis. Classificam-se como crimes digitais de efeitos tangíveis as condutas que apesar de serem praticadas em meio digital produzem também efeitos diretos no mundo real. Já as ações que caracterizam crimes digitais intangíveis afetam tão somente os elementos imateriais formadores do sistema digital, com os dados armazenados, em processamento ou em transmissão.

II - Quanto aos efeitos: Crimes digitais de mero acesso; Crimes digitais de dano ou lesão. Os crimes digitais de mero acesso se consumam com o simples acesso ao sistema digital, sem que seja necessário que do referido ato resulte algum dano a dados ou ao próprio sistema. Já os crimes digitais de dano ou lesão são aqueles que de maneira direta danificam o sistema sem necessidade da obtenção de alguma vantagem econômica ilícita para o infrator.

Para Monteiro Neto (2003, p. 49) classificações nesse sentido facilitam o estudo e divisão efetiva da matéria, sem desmerecer o valor doutrinário e didático dos sistemas classificatórios dos outros autores. Deve-se observar que estes sistemas serviram para evidenciar a distinção entre crimes comuns e crimes digitais, uma vez que o uso dos sistemas digitais para praticar condutas já incriminadas por tipos penais não pode ser considerado um crime digital.

Se o sistema virtual não passou de um mero meio de execução, isto no máximo poderia resultar na alteração da pena do crime. Nesses casos, é dever do legislador a criação de qualificadoras e majorantes ou minorantes alternativas para as condutas praticadas por meio digital que afetam bens jurídicos já protegidos, evitando assim a previsão de tipos penais extremamente específicos simplesmente pelo surgimento de uma nova forma de execução.

1.4 SUJEITO ATIVO DO CRIME DIGITAL E PERFIS CRIMINOLÓGICOS

Com uma nova modalidade de crime nasce também uma nova modalidade de criminoso. Os agentes que praticam condutas ilegais na esfera do mundo digital possuem características e motivações muitas vezes distintas, dessa forma é necessária uma análise detalhada dos principais perfis criminológicos dos sujeitos ativos.

Monteiro Neto (2003, p. 42) explica que muitos deles são normalmente pessoas que trabalham no ramo informático, em geral são trabalhadores internos vinculados a empresas, e são motivados para a prática de crimes por questões financeiras, perspectiva de promoção, vingança, para chamar a atenção, entre outros. Escondem-se atrás do anonimato da Internet, que dificulta e muito a investigação da conduta ilegal. Na maioria das vezes quando descobertos alegam desconhecimento do crime que praticaram e se escondem atrás da justificativa de praticarem o ato apenas por “brincadeira”.

Ainda para Monteiro Neto (2003, p. 42) os objetivos do criminoso podem ser divididos em três estágios de motivação: Instinto aventureiro, ou seja, o agente é movido tão somente pelo desafio de superação da máquina; Ganhar dinheiro extra, quando superada a máquina e satisfeito o ego, o criminoso descobre um jeito fácil e “seguro” de ganhar dinheiro extra; Prática de infrações para sustentar seu alto custo de vida, ou seja, a ambição do segundo estágio é potencializada pelos retornos obtidos.

Túlio Lima Vianna (2003) classifica os perfis dos criminosos digitais mais comuns em:

I - Curiosos: movidos por curiosidade, não causam danos aos dados armazenados ou em tráfego pelas redes, apenas violam a privacidade das vítimas e o sigilo dos dados em trânsito pelos sistemas computacionais;

II - Pichadores digitais: procuram auto-afirmação dentro da rede, agindo com o único objetivo de serem reconhecidos e famosos no universo virtual;

III - Revanchistas: formados por ex-funcionários ou empregados descontentes que se utilizam dos conhecimentos adquiridos na empresa para sabotá-la;

IV - Vândalos: agem simplesmente pelo prazer de causar danos às vítimas;

V - Espiões: agem com a finalidade de adquirir informações confidenciais armazenadas nos sistemas computacionais das vítimas. As informações podem ter caráter comercial ou não;

VI - Ciberterroristas: possuem motivações políticas ou religiosas e utilizam-se do meio digital para realizarem atividades criminosas que possibilitem a divulgação de suas crenças.

VII - Ladrões e estelionatários: tem objetivos de lesar o patrimônio das vítimas.

No âmbito dos criminosos especialistas em computadores e meios digitais, a figura mais ligada à prática de crimes por intermédio de sistemas informáticos é a do *hacker*, terminologia que deriva da palavra em inglês *Hack,* que significa cortar, golpear, daí o termo ter sido adotado para designar aqueles que quebram a segurança para aprender sobre algo que a maioria das pessoas não tem acesso. No entanto, esse termo é gerador de inúmeras controvérsias, pois na comunidade virtual, a terminologia "*hacker*" dificilmente é associada a fins criminosos, sendo atribuída tão somente a um indivíduo extremamente hábil no campo digital que invadem sistemas com um objetivo nobre, por exemplo, verificar a segurança de determinada rede e informar o problema às empresas responsáveis, ou simplesmente para aprimorar suas técnicas.

Nogueira define *hacker* como:

> Aquele que tem conhecimentos profundos de sistemas e linguagens de programação, principalmente Unix e C. Conhece as falhas de segurança dos sistemas e está sempre à procura de novas falhas. Invade sistemas pelo prazer de provar a si mesmo que é capaz, sem alterar nada. (NOGUEIRA, 2008, p.62)

No âmbito da comunidade informática, o termo correto para definir aqueles que cometem crimes e condutas reprováveis nos meios digitais é o de *Crakers*, estes sim, são considerados os vilões do meio digital, ou seja, são *hackers* não éticos, ou "maus", que recorrem à criminalidade digital, invadindo sistemas com interesses patrimoniais ou danosos.

De acordo com Rosa Fabrizio:

> Ao mesmo tempo que se vê surgir toda uma explosão de serviços e oportunidades através da rede, surge também a figura do individuo que se utiliza do computador para atos ilegais. Nesse passo, nasce a figura do

> "criminoso digital", a exemplo dos *crackers,* sujeitos que invadem sistemas, roubam arquivos, destroem discos rígidos [...] (ROSA, 2006, p.22)

Vários estudos tentaram classificar os diversos tipos de *hackers* e *crackers*, mas um que merece destaque é o de Túlio Lima Vianna (2003), que os classificam em:

I - *Crackers* de servidores: crackers que invadem computadores ligados em rede;

II - *Crackers* de programas: crackers que quebram proteções de softwares cedidos a título de demonstração para usá-los por tempo indeterminado;

III - *Phreakers*: *crackers* especialistas em telefonia móvel ou fixa, atua principalmente na obtenção de ligações telefônicas gratuitas;

IV - Desenvolvedores de vírus, *worms* e *trojans*: programadores que criam softwares que causam algum dano ao sistema do usuário afetado;

V - Piratas: indivíduos que clonam programas fraudando direitos autorais;

VI - Distribuidores de Warez: Webmasters que disponibilizam em suas páginas, software sem autorização dos detentores dos direitos autorais.

De qualquer forma, independentemente dos objetivos ou das motivações pessoais, o fato é que *hackers e crackers* invadem sistemas informáticos e consequentemente violam a privacidade e o sigilo dos dados contidos nesses sistemas, o que por si só já configura crime na maioria dos países de primeiro mundo. No entanto, é importantíssimo ressaltar que devido à suposta complexidade da informática, suas expressões e linguagens peculiares, assim como a especificidade de conhecimentos exigidos, muitos acreditam que o criminoso digital, ou seja, o agente causador das práticas ilícitas virtuais, tem necessariamente que ser um ilustre perito na operação de computadores e sistemas digitais, inserindo-se nas categorias de *hackers* ou *crackers*. Trata-se de um grande engano, pois se sabe que hoje em dia com a difusão de conhecimentos e as facilidades resultantes do desenvolvimento e evolução dos meios digitais, qualquer indivíduo que possua a mínima noção de como operar um computador pode ser considerado um criminoso digital em potencial. Logicamente na maioria dos casos o sujeito ativo tem grande conhecimento na esfera digital, mas não se pode generalizar.

2 IMPLICAÇÕES PROCESSUAIS PENAIS

2.1 PRINCÍPIO DA RESERVA LEGAL

Após a delimitação mais clara sobre as proporções do crime digital, e os perfis dos principais sujeitos ativos, também se faz necessária a análise dos delitos digitais existentes no ordenamento jurídico brasileiro e dos principais projetos de lei que visam regular a matéria, mas antes, para se ter uma melhor noção a respeito da vontade e entendimento dos legisladores, é necessária uma análise das implicações processuais penais pertinentes ao assunto.

É com essa evolução legislativa que surge um novo ramo do Direito Penal, o Direito Penal Digital, que possui elementos peculiares e se adequa a nova realidade e a nova onda criminológica que surge. Partindo do conceito clássico de crime, que estabelece como elementos indispensáveis deste, a ocorrência de fato típico, antijurídico e culpável, deve-se observar algumas considerações à cerca do princípio da reserva legal.

No ordenamento jurídico nacional o Princípio da Reserva Legal é também uma garantia constitucional, pois possui valor social garantidor da liberdade individual. Quando a Constituição Federal de 1988 expressamente preceitua que "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal." [3], entende-se a necessidade da existência da conduta por lei anterior ao fato para que determinado ato seja considerado como crime, sendo assim considerado lícito qualquer ação que não seja prescrita como crime em norma penal incriminadora, pois como resultado direto do princípio da reserva legal temos o princípio da tipicidade de um fato. Ou seja, um fato, uma conduta humana, seja uma ação ou omissão, só poderá ser considerada como infração a ordem jurídica penal, ou seja, será típico, caso exista norma penal incriminadora prévia que descreva de forma taxativa e pormenorizada todos os elementos da conduta humana tida como ilícita.

---

[3] Constituição Federal artigo 5º inciso XXXIX.

Tal questão é considerada importante em vista da evidente ausência de regulamentação dos crimes informáticos, ou seja, poucas são as normas de natureza penal que estabelecem as condutas criminosas de caráter digital, e as que existem são extremamente específicas a determinados sujeitos ativos ou passivos, não possuindo assim caráter abrangente, não punindo assim condutas similares. É a não regulamentação da matéria que facilita o aumento da criminalização digital. Necessitasse então da elaboração de normas penais que venham a reger o assunto coibindo e punindo a prática de ilícitos desta natureza.

2.2 PERSECUÇÃO PENAL E AUTORIA

O Estado só tem o direito de punir alguém através do processo, e é na ação penal que deve ser deduzida em juízo a pretensão punitiva. Para que se possa ser proposta a ação penal é necessário que o Estado disponha de certo número de elementos probatórios que demonstrem a ocorrência da infração penal e de sua autoria. A forma mais comum para a apuração desses elementos é o inquérito policial, cujo objeto é a apuração dos elementos probatórios que configurem a infração penal, para então servir de base à ação penal. O inquérito policial é necessário, mas não é, pois, imprescindível à propositura da ação penal.

À junção da atividade investigatória com a ação penal se dá o nome de persecução penal. Esta significa segundo Mirabete (2006, p. 166) "ação de perseguir o crime", e é composta por formas preestabelecidas porque segundo Damásio (2002, p. 166) no sistema processual penal brasileiro impera o princípio nulla poena sine judicio: "o Estado tem obrigação de não punir o agente senão nos moldes determinados pela sanctio juri, ao passo que o criminoso tem o direito de não ser punido além daqueles limites".

No que se refere aos crimes digitais, como já observado, sua execução possui as facilidades oferecidas pela Internet, quando deste espaço se aproveitam usuários com intenções criminosas. Portanto, o acesso anônimo aos sistemas de informação e comunicação favorece o uso indevido da tecnologia por usuários com a intenção de cometer crimes. Por essa razão, nota-se que nos crimes digitais há

grande dificuldade de se realizar a persecução criminal, uma vez que a internet dispõe de inúmeros recursos que favorecem a impunidade, tais como o anonimato dos usuários e a falta de um órgão central de controle da rede que contribua nas investigações. Depois que um crime digital ocorre, as mesmas características que facilitaram a conduta danosa dificultam a identificação do agente ativo da infração, já que como o indivíduo não precisa ir ao local do crime para cometê-lo, sua identificação é bastante dificultosa.

Para Denning & Baugh Jr (apud ARAS, 2001) os criminosos digitais utilizam várias técnicas para assegurar-lhes o anonimato, algumas delas são:

I - O uso de test accounts, que são contas fornecidas gratuita e temporariamente por alguns provedores e que podem facilmente ser obtidas a partir de dados e informações pessoais falsas;

II - A utilização de anonymous remailers, ou seja, contas que retransmitem e-mails enviados por meio de provedores de Internet que garantem o anonimato;

III - A clonagem de celulares para acesso à Internet, de forma a evitar a identificação do local da chamada e de seu autor, por meio do rastreamento do sinal;

IV - A utilização de celulares pré-pagos, uma vez que tais aparelhos podem ser adquiridos com dados pessoais falsos e são de difícil rastreamento.

De acordo com Ana Mara dos Santos (2007, p. 85) , quando alguém comete um crime digital, são-lhe necessários dois elementos identificadores: O endereço da máquina que envia as informações e o da que recebe tais dados, ou seja, os IP's[4], que são representados por números que nada revelam sobre o usuário nem sobre os dados que estão sendo transmitidos, apenas do computador utilizado. Portanto, o meio de identificação através do endereço de IP nem sempre é eficaz, pois apesar de até poderem identificar o computador usado na prática ilícita, o autor ainda será desconhecido, como por exemplo, quando o computador utilizado seja público, como de bibliotecas, escolas, ou lan houses. Outra grande dificuldade é a obtenção de informações necessárias para a apuração de crimes junto aos provedores de acesso à internet, pois é comum que os provedores não mantenham os dados armazenados por tempo suficiente, tendo em vis que em média o inquérito policial demora seis meses para sua apuração. Podendo ocorrer a impunidade penal

[4] IP significa Internet Protocol, ou seja, Protocolo da Internet.

aos imputados por falta de prova devido a perca de informações, fator que deve ser regulamentado com prioridade, tanto de responsabilização aos provedores, como a possibilidade de realização de procedimentos.

Outro fator que dificulta bastante a identificação da autoria é a implicação de mais de um país em determinado ato criminoso. Com isso a identificação dos autores torna-se ainda mais dificultosa, tendo que recorrer a tratados ou cartas rogatórias, processos ainda mais lentos que se esbarram em legislações específicas de cada país. Para isso organismos internacionais tentam um acordo que permita a padronização e troca de informações de forma que priorize a agilidade nos processos de identificação.

Quanto à atribuição da autoria de documentos e mensagens, os problemas processuais também existem, a não ser quando o usuário do computador faça uso de uma assinatura digital, já que sem a qual dificilmente se poderá determinar quem praticou determinada conduta. Mesmo assim, a assinatura digital apenas afere credibilidade ao documento ou mensagem, e dessa forma só será possível a presunção de que o agente cometeu a conduta investigada, e no Direito Penal, não se admitem presunções, ainda mais quando se trata da possibilidade de uma condenação.

De acordo com Vladmir Aras (2001), um método mais seguro de atribuição de autoria em crimes digitais é quando o autor se vale de elementos corporais para obter acesso a redes ou computadores, no caso de mecanismos que somente validam acesso mediante a verificação de dados biométricos do indivíduo. Sem isso a entrada no sistema é vedada. Os mecanismos mais comuns são: a análise da íris e retina do usuário, a leitura eletrônica de impressão digital, ou ainda a análise da voz do usuário.

Comentando sobre o criminoso digital, Alexandre Jean Daoun e Renato Blum (apud LUCCA, 2000, p. 118) observam que: "O cidadão do mundo virtual é, antes de tudo, um cidadão do mundo real e da mesma forma deve ser encarado como agente criminoso". Sendo assim, independentemente da classificação que se adote, é de suma importância a formulação de elementos e práticas, além de treinamento efetivo das autoridades competentes para combater e identificar os autores desses crimes.

2.3 JURISDIÇÃO E COMPETÊNCIA

Uma vez que um conflito de interesses opostos não é resolvido pelo entendimento mutuo das próprias partes, nasce a obrigação de que o Estado o resolva através do devido processo legal, já que, em regra, no ordenamento jurídico brasileiro é vedado a autotutela, que é a utilização da força por uma das partes afim de resolver um conflito. Assim, ao Estado pertence a função de compor os litígios, reintegrando e assegurando a ordem e a paz da sociedade.

Para se cumprir a tarefa de dar de forma justa a cada uma das partes o que é seu, o Estado age através da jurisdição. A jurisdição não pode ser exercida ilimitadamente por qualquer juiz, e um juiz não pode julgar todas as causas. Dessa forma, a jurisdição é distribuída por lei entre os vários órgãos do Poder Judiciário, através da repartição de competências. A distribuição de parcelas da jurisdição em competências é prevista na própria Constituição Federal, na cláusula assecuratória do art. 5º, LIII[5], cujo objetivo é facilitar e proteger a administração da justiça.

Para Fernando Capez, Jurisdição pode ser definida como:

> [...] a função estatal exercida com exclusividade pelo Poder Judiciário, consistente na aplicação de normas de ordem jurídica a um caso concreto, com a conseqüente solução do litígio. É o poder de julgar um caso concreto, de acordo com o ordenamento jurídico por meio de um processo. (CAPEZ, 2009, p.199)

Ainda segundo Capez (2009, p. 200) a jurisdição pode ser comum ou especial, a jurisdição especial se subdivide:

I - Justiça Eleitoral;

II - Justiça Militar;

III - Justiça Trabalhista

A justiça comum subdivide-se em:

I - Justiça Federal (artigo 109, IV, da CF), à qual compete processar e julgar os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas

---

[5] Art. 5, Constituição Federal, LIII. Ninguém será processado nem sentenciado senão pela autoridade competente.

públicas, excluídas as contravenções penais de qualquer natureza, que sempre serão de competência da justiça estadual, de acordo com a Súmula 38 do STJ.

II - Justiça Comum Estadual, à qual compete julgar tudo que não for de competência das jurisdições especiais e federal.

Já a competência Capez define em poucas palavras como:

> A delimitação do poder jurisdicional (fixa os limites dentro dos quais o juiz pode prestar jurisdição). Aponta quais os casos em que podem ser julgados pelo órgão do Poder Judiciário. É, portanto, uma verdadeira medida da extensão do poder de julgar. (CAPEZ, 2009, p.201)

De acordo com Julio Mirabete (2006, p. 170), a delimitação da competência realiza-se em virtude de dois elementos: da causa criminal e dos atos processuais. No primeiro, a competência é delimitada observando a natureza do litígio, que por sua vez é determinada de acordo com a causa a ser julgada; essa é a competência material. Pelo segundo elemento, a competência é definida de acordo com as fases do processo ou o objeto do juízo, ou ainda, com o grau de jurisdição; essa é a competência funcional.

Na competência material, a concretização do poder jurisdicional abstrato sofre delimitação em três aspectos: em razão do território; em razão da natureza da infração e em razão da qualidade da pessoa do réu. Nesses termos, o art. 69, do Código de Processo Penal estabelece:

> Art. 69. Determinará a competência jurisdicional:
> I - o lugar da infração:
> II - o domicílio ou residência do réu;
> III - a natureza da infração;
> IV - a distribuição;
> V - a conexão ou continência;
> VI - a prevenção;
> VII - a prerrogativa de função.

A grande pertinência para se debater a questão da competência no âmbito dos crimes digitais vem dos casos em que estes sejam cometidos através da utilização da internet, visto que os efeitos de uma conduta praticada em um determinado local podem ser surtidos instantaneamente em outro completamente diferente. No tocante a fixação da competência nos delitos cometidos dentro das fronteiras do próprio país, nosso ordenamento jurídico é claramente eficiente com suas regras para a fixação de competência. A problemática se aponta nas questões em que outros países estejam envolvidos.

Celso Henrique Vallim (apud FREITAS DA SILVA & MONTEIRO NETO, 2009) observa que a maior dificuldade ao se observar o conceito de jurisdição e

territorialidade na internet existe graças à internacionalidade da rede, uma vez que nesta não existem limites estatais, de forma que um artigo publicado em determinado país, poderá estar disponível no mundo inteiro. Assim, a implicação processual penal em relação à jurisdição e à competência na internet se deve ao fato de que esta criou um espaço indefinido e sem limites territoriais, onde a comunicação e a troca de informações ocorrem ilimitadamente.

Pelo fato da internet possuir um alto grau de complexidade, a fixação da jurisdição competente para a propositura da ação penal pode se tornar um problema, e dessa forma podem surgir controvérsias sobre a matéria uma vez que o caso concreto seja apreciado.

Como bem salienta Freitas da Silva e Monteiro neto (2009) a grande discussão fundamenta-se no fato de que na maioria das vezes os crimes digitais constituem crimes à distância ou são crimes plurilocais; ou seja, é possível que a ação e/ou a consumação de um crime digital ocorram em lugares diferentes.

Nessa questão Capez (2009, p. 203) entende que nos crimes à distância, ou seja, crimes praticados e consumados em países diferentes, se aplica o art. 6º, CP[6], que se refere ao local do crime para o efeito da extraterritorialidade, em conformidade ao art. 70 do CPP, que dispõe:

> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
> § 1º Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.
> § 2º Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.
> § 3º Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção.

Desta forma, quando um crime tem início em território estrangeiro e se consuma no Brasil, é considerado praticado no Brasil. Do mesmo modo, tem eficácia a lei penal nacional quando os atos executórios do crime são praticados no território brasileiro e o resultado se produz em país estrangeiro. Nesse caso, o foro

---

[6] Art. 6, do Código Penal dispões que “Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”.

competente será o do lugar em que foi praticado o último ato de execução no Brasil ou, caso o último ato de execução seja praticado fora do território nacional, o local estrangeiro onde se produziu o resultado, ou seja, quaisquer dos países envolvidos são competentes para julgar o caso.

O problema é que cada país rege-se de acordo com as suas leis e são soberanos. Da mesma forma que o ordenamento jurídico nacional dispõe que um juiz brasileiro pode invocar para si a competência para processar e julgar um delito consumado em nosso solo, mas praticado em outro país, as leis deste determinado país podem ter a mesma previsão. Ou ainda pode ocorrer a hipótese de uma certa conduta ser considerada crime no Brasil, mas não ser em determinado país.

A respeito dessa questão, Érica Lourenço de Lima Ferreira observa a necessidade de uma cooperação internacional para a resolução destes conflitos:

> De maneira concreta sobre os problemas apresentados pela nova criminalidade, cita-se a declaração realizada em dezembro de 1997 pelos membros do G-8; a conclusão foi nas palavras de Santiago Muñoz Machado, que, para combater uma praga transfonteiriça como esta, é imperativo ter-se em conta as vias de uma cooperação internacional, já que indiscutível que uma parte da delinqüência informática emigrou até a internet, inclusive, a proposta Norte-Americana é a da criação de uma política do ciberespaço comum, contudo não aceita porque colocaria em questão a soberania e as ações dos Estados. Existem poucas jurisdições de caráter supraestatal (OCM organização Mundial do Comércio), TPI [Tribunal Penal Internacional], são algumas delas, ainda mais que possuem competência para intervir nas controvérsias geradas no ciberespaço; no âmbito regional europeu, há o Tribunal de Justiça Comunitário ou Tribunal Europeu de Direitos Humanos. (FERREIRA, 2007, p.159)

Nessa linha, a Convenção sobre a Criminalidade Informática do Conselho da Europa, ou Convenção de Budapeste[7], decretou em seu artigo 22, §5º:

> Quando mais de uma parte reivindicar jurisdição com relação a uma alegada infração estabelecida de acordo com esta Convenção, a partes envolvidas deverão, quando for apropriado, consultar-se, a fim de determinar a jurisdição mais apropriada para processar.

Entende-se então que a cooperação internacional é de grande importância para a delimitação de competências e julgamento de crimes digitais de caráter internacional, uma vez que tal matéria, apesar de mais freqüentes em determinados países, é um problema mundial, que cada vez mais se adapta as necessidades e práticas da sociedade.

---

[7] A Convenção de Budapeste começou a vigorar no ano de 2001 com o objetivo de proteger a sociedade contra a criminalidade na internet por meio da adoção de legislação adequada e do avanço da cooperação internacional.

2.4 COLETA DE PROVAS

A prova é um dos elementos principais de qualquer ação penal. No entendimento de Julio Fabbrini Mirabete:

> Para que o juiz declare a existência da responsabilidade criminal e imponha sanção penal a uma determinada pessoa, é necessário que adquira a certeza de que foi cometido um ilícito penal e que seja ela a autora. Para isso deve convencer-se de que são verdadeiros determinados fatos, chegando à verdade quando a idéia que forma em sua mente se ajusta perfeitamente com a realidade dos fatos. Da apuração dessa verdade trata a instrução, fase do processo em que as partes procuram demonstrar o que objetivam, sobretudo para demonstrar ao juiz a veracidade ou falsidade da imputação feita ao réu e das circunstâncias que possam influir no julgamento da responsabilidade e na individualização das penas. Essa demonstração que deve gerar no juiz a convicção de que necessita para o seu pronunciamento é o que constitui a prova. Nesse sentido, ela se constitui em atividade probatória, isto é, no conjunto de atos praticados pelas partes, por terceiros (testemunhas, peritos etc.) e até pelo juiz para averiguar a verdade e formar a convicção deste último. Atendendo-se ao resultado obtido, ou ao menos tentado, provar é produzir um estado de certeza, na consciência e mente do juiz, para sua convicção, a respeito da existência ou inexistência de um fato, ou da verdade ou falsidade de uma afirmação sobre uma situação de fato, que se considera de interesse para uma decisão judicial ou a solução de um processo. (MIRABETE, 2006, p.274-275)

Ou seja, objeto da prova é aquilo sobre o que o juiz deve adquirir o conhecimento para resolver o litígio; é o fato criminoso e sua autoria, e não somente isso, mas todas as circunstâncias objetivas e subjetivas, todos os acontecimentos relevantes que possam influir na responsabilidade penal e na fixação da pena ou de medida de segurança. Já os meios de prova são as ações empregadas para investigar, conhecer ou comprovar a verdade real dos fatos, da autoria e das circunstâncias do crime. Por este motivo não há limitação dos meios de prova. Como o processo penal visa o interesse publico ou social de repressão ao crime, a investigação deve ser a mais ampla possível e assim nada impede que se utilizem provas com a utilização de meios técnicos ou científicos, como gravações em fitas magnéticas, fotos, filmes, videofonograma, desde que obtidas licitamente.

No processo penal brasileiro, para que haja embasamento para a efetiva denúncia e sentenciamento de uma pessoa, é necessário que se observem os indícios de autoria e materialidade, logo, a falta de comprovação da identidade do autor e o conseqüente nexo de causalidade entre a conduta e o resultado descaracterizam a culpabilidade do agente e a ilicitude do tipo. Nesse contexto, o

maior problema da investigação criminal relacionado aos crimes digitais é a pouca ou quase nenhuma presença de evidências da conduta delituosa praticada pelo autor ou autores indiciados.

Geralmente, a conduta criminosa praticada pelos sujeitos ativos dos crimes digitais permanece sem provas porque a invasão de um sistema de informação ou computacional não deixa nenhum vestígio, e no anonimato da internet a autoria desse procedimento fica extremamente complicada de se apurar. Mesmo uma perícia minuciosa pode deixar de apontar evidências e, em conseqüência disso, a prova do delito pode permanecer sem identificação por falta total de pistas.

A questão se torna ainda mais delicada quanto ao valor pericial dos dados obtidos em meio eletrônico. De acordo com Ariel Foina e Igor Reis (2004, p. 59), a prova pericial proveniente da análise de computadores, principalmente no que diz respeito à invasão de sistemas e ao processo de rastreamento, pode ser produzida basicamente:

"I - Por meio de perícia feita por especialista direto no sistema que foi vítima." Os autores afirmam que essa seria a condição ideal para a perícia técnica, uma vez que constitui no todo um procedimento técnico que deve ser feito no computador, para tentar registrar todos os dados existentes num determinado sistema, no exato momento em que ele fora invadido. Porém, o rigor dessas condições para a coleta de provas infelizmente não ocorre na prática;

"II - com base em registros de sistema produzidos e fornecidos pelos respectivos administradores." Os autores revelam que, pela dificuldade das condições ideais apontadas acima, geralmente o perito acaba trabalhando em cima de registros eletrônicos fornecidos pelos administradores de sistema, na tentativa de produzir um laudo pericial que aponte para o possível autor dos delitos.

A prova digital por si só não constitui uma prática inteiramente confiável e, por essa razão nem todas são aceitas pelo Direito como documento digital com validade jurídica. No Brasil, o Instituto Nacional de Tecnologia da Informação é o órgão encarregado de atribuir validade jurídica a documentos eletrônicos, conferindo a autenticidade e integridade. Quem dá essa garantia legal é a Medida Provisória 2.200-2, que Institui a Infra-Estrutura de Chaves Públicas Brasileira, ou ICP-Brasil, e transforma o Instituto Nacional de Tecnologia da Informação em autarquia. A Medida Provisória dispões em alguns dos seus artigos que:

> Art. 1º - Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.
> [...]
> Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.
> § 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários.
> § 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Como se percebe, essa medida provisória reconhece a assinatura digital baseada na criptografia assimétrica de chave pública e privada para garantir a identificação e a integridade dos documentos eletrônicos, desde que via de regra a chave pública esteja em uma autoridade certificadora, não excluindo a possibilidade da utilização de meios de provas digitais que não possuam certificados emitidos pelo ICP-Brasil, desde que as partes envolvidas entrem em acordo quanto a sua validade, ou seja reconhecido pela parte a quem for oposto.

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, criptografia:

> É a ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias; proteger a integridade de transferências eletrônicas de fundos. Uma mensagem codificada por um método de criptografia deve ser privada, ou seja, somente aquele que enviou e aquele que recebeu devem ter acesso ao conteúdo da mensagem. Além disso, uma mensagem deve poder ser assinada, ou seja, a pessoa que a recebeu deve poder verificar se o remetente é mesmo a pessoa que diz ser e ter a capacidade de identificar se uma mensagem pode ter sido modificada. Os métodos de criptografia atuais são seguros e eficientes e baseiam-se no uso de uma ou mais chaves. A chave é uma seqüência de caracteres que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número utilizado pelos métodos de criptografia para codificar e decodificar mensagens.[8]

Freitas da Silva e Monteiro neto (2009) observam que a utilização de documento eletrônico como meio probatório é assunto de grande controvérsia no ordenamento jurídico brasileiro. Todavia, a corrente majoritária entende por sua

[8] BRASIL. CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet** - parte I: conceitos de Segurança. Disponível em: <http://cartilha.cert.br/conceitos/sec8.html#sec8>. Acesso em: 20 out. 2010

admissibilidade. Neste ponto, discute-se se o documento eletrônico deve ser classificado como prova pericial ou documental. A teoria mais aceita é que ele seja tido como prova pericial, pois as provas que podem ser apresentadas para a indicação de autoria de ilícito executado por meio eletrônico são vestígios materiais do crime que necessitam de perícia técnica.

3 CRIMES DIGITAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

3.1 PREVISÃO LEGAL DE CRIMES DIGITAIS IMPRÓPRIOS

A necessidade de uma legislação penal para a proteção de bens jurídicos informáticos e de outros, igualmente relevantes, que possam ser ofendidos por meio de computadores é um dos problemas que vem sendo apresentado aos operadores do Direito. A variedade de crimes que podem ser praticados pelos meios virtuais é bastante vasta. Muitas condutas já tipificadas nas leis penais brasileiras são realizadas com a utilização dos meios digitais, cuja finalidade do meio empregado é atingir de forma mais efetiva e rápida o resultado pretendido pelo agente.

Essas condutas afetam bens jurídicos de diversas categorias, classificados de acordo com a prevalência do bem ao qual se dirige a tutela da lei. Como já comentado, não se trata propriamente de crimes digitais específicos, mas de crimes comuns em que o sistema informatizado ou dispositivo de comunicação é apenas o instrumento utilizado na sua execução.

Neste rol de condutas já tipificadas como crimes comuns, praticados por meios virtuais podemos citar as mais frequentes:

Crimes contra a honra: São os crimes de calúnia (artigo 138, CP), difamação (artigo 139, CP) e injúria (artigo 140, CP). Os criminosos são motivados pelo anonimato e os crimes podem ocorrer em salas de bate papo, blogs, pelo envio de spams, através de publicações em páginas de internet, dentre outros meios de postagem eletrônica. Estes crimes devem contar com a majorante do inciso III, artigo 141, do Código Penal[9], pela facilidade de divulgação proporcionada pela Internet.

Crimes contra a liberdade individual: São os crimes de ameaça (artigo 147, CP), inviolabilidade de correspondência (artigos 151 e 152, CP), e divulgação de segredos (artigos 153 e 154 CP).

O crime do artigo 151, crime de violação de correspondência, é um tipo plenamente aplicável a conduta de interceptação de e-mail e sua violação, se

[9] Art. 141, Código Penal, III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria.

equipararmos a correspondência eletrônica à correspondência tradicional, o que é possível uma vez que comunicação telegráfica ou radioelétrica dirigida a terceiro, assim como conversação telefônica entre pessoas também são tuteladas pelo artigo 151 do CP, em seu § 1º, e a Internet, neste aspecto, é apenas uma evolução dos meios de comunicação, pois o bem jurídico que visa proteger é o sigilo das informações, a liberdade de comunicar-se e se expressar através de correspondência. Marcio Coimbra (2000) destaca que o sigilo das informações contidas em uma correspondência digital também é garantia fundamental, estando previsto no artigo 5º, inciso XII, da Constituição Federal a proibição da sua violação.

Crimes contra o patrimônio: Compreende os crimes de furto (artigo 155, CP), extorsão (artigo 158, CP), dano (artigo 163, CP) e estelionato (artigo 171, CP). O bem jurídico protegido nos tipos de furto e roubo é o patrimônio, então é desnecessária a criação de outro tipo penal somente para discriminar o meio de execução do delito que costuma ser através de 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, a obtenção de dados como senhas para manipular contas bancárias e obter vantagem financeira. O que podem sim serem criadas como já observado antes são novas formas de majorantes e qualificadoras que se adequem aos tipos.

No crime de dano podemos considerar típicas as condutas de destruição de elementos de hardware e software do computador através de um vírus digital. Entretanto a danificação apenas de softwares gera discussão na doutrina, pois alguns autores não consideram o software “coisa”. Todavia, um Projeto de lei que ainda está sendo apreciado, equivale os dados digitais à “coisa”, como será visto mais precisamente adiante neste trabalho.

Quanto ao crime de estelionato, sua tipificação versa que o crime configura-se ao se induzir ou manter alguém em erro mediante ardil ou qualquer outro meio fraudulento. É necessária uma relação psicológica entre autor e vítima, que deve se sentir enganada. É nesta área que os criminosos utilizam de seus maiores artifícios, através de cavalos-de-tróia, sites clonados e utilizando a engenharia social, dentre inúmeros outros métodos.

Crimes contra os costumes: São os crimes de favorecimento à prostituição (artigo 228 CP), de escrito ou objeto obsceno (artigo 234 CP) e a pedofilia (artigo

241, da Lei 8.069/90). É muito comum encontrar sites de pornografia e de prostituição, aliás, é muito difícil fazer uma pesquisa em um site de busca, sobre qualquer tema, em que não apareça pelo menos um resultado indicando um link sobre pornografia.

Segundo Wilson Donizete Liberati (2008, p. 14), a lei 8069/90 que estabeleceu o Estatuto da Criança e do Adolescente (ECA) revolucionou o Direito Infanto-Juvenil. Esta lei dispõe em seu art. 241, alterado pela lei 11.829/08, o crime de informática, a saber:

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena - reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

.Nos incisos I, II, III do § 1º, incluídos pela Lei 10.764/03 (pedofilia) os agentes incorrem na mesma pena quando:

> 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.

Segundo o § 2º, a pena será de reclusão de 3 a 8 anos se:

> I - o agente comete o crime prevalecendo-se do exercício de cargo ou função;
> II – o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial.

Liberati (2008, p. 15) explica que o crime previsto no art. 241 do ECA preocupa-se com a garantia “do direito à dignidade, ao respeito, à imagem, à liberdade sexual e ao domínio do corpo de criança e adolescente”. O citado autor ainda inclui como objeto jurídico da norma incriminadora “o pudor e a moralidade públicos, considerados enquanto analisados o comportamento indivíduo do grupo social”.

Os provedores de acesso à Internet começaram a se preocupar com a responsabilidade penal, depois da promulgação das Leis Federais 10.764/03 e 11.829/08, que alteraram o art. 241 do Estatuto da Criança e do Adolescente, que trouxeram conseqüências bem mais severas para quem comete tais crimes. Apesar de uma grande parte dos crimes puramente digitais ainda não estarem prevista em

lei, o ordenamento jurídico brasileiro já conta com algumas condutas tipificadas, demonstradas a seguir.

3.2 PREVISÃO LEGAL DE CRIMES DIGITAIS PRÓPRIOS

Determinados delitos praticados pelos meios digitais e virtuais se referem especificamente aos sistemas de informações. Ao contrário dos chamados crimes eletrônicos impróprios ou impuros, que já são bem regulados pelas leis em vigor, poucos são os tipos de condutas atualmente tipificadas no ordenamento jurídico brasileiro que se referem exatamente a crimes digitais específicos.

Como bem observa Monteiro Neto (2003, p. 51), presentes no conjunto de normas brasileiras, esses crimes encontram-se de maneira esparsa em alguns tipos penais contidos em normas específicas de determinado ramo do Direito, são eles**:**

I - O art. 10 da lei Federal nº 9296/96, que considera crime:

> Art. 10. Realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
> Pena - reclusão de 2 a 4 anos e multa.

Este artigo regulamenta o art. 5º, inciso XII da CF/88. O dispositivo legal acima disposto estabelece como crime o ato de interceptar comunicações, mas não qualquer tipo de comunicação, até porque seria um fato absurdo, visto que o ser humano possui inúmeras formas de se comunicar, dessa forma, a mencionada lei enumera quais os tipos de interceptação são passíveis de punição por serem consideradas ilícitas. Dentre os tipos relacionados, está a interceptação de comunicação eletrônica. Logo, qualquer interceptação não autorizada de comunicação realizada entre sistemas computacionais e eletrônicos constitui ato ilícito tipificado pelo artigo 10 da Lei nº 9.296/96. Exemplo singular da interceptação da comunicação informática, ou seja, da troca de informações ou de dados feitas por meios informáticos, é a interceptação e violação de e-mails**.**

A respeito do tema, a ementa de um acórdão proferido pelo Tribunal de justiça de Santa Catarina:

> CRIME DE INTERCEPTAÇÃO DE COMUNICAÇÃO (LEI N. 9.296/96, ART. 10) - INVASÃO A PROVEDOR DE INTERNET E COMPUTADORES DE SEUS USUÁRIOS - DOMÍNIO TOTAL SOBRE AS MÁQUINAS -

> TIPICIDADE - RECURSO NÃO PROVIDO. Configura o crime do art. 10 da Lei n. 9.296/96, a conduta de quem "invade" provedor de internet, apropriando-se dos logins e senhas de seus usuários e, assim, "invadindo" seus computadores, aos quais tinha livre e desimpedido acesso, podendo, inclusive, apagar arquivos de sistema, como, de fato, o fez.

II - O art. 153, § 1º-A do Código Penal, com a redação dada pela Lei Federal nº 9983/2000, que tipifica o crime de divulgação de segredo:

> Art. 153.....
> § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informação ou banco de dados da Administração Pública.
> Pena detenção de 1 a 4 anos e multa.

O delito tipificado no § 1º - A do artigo 153 do Código Penal, a violação de segredo, só adquire a natureza de crime digital quando as informações sigilosas estiverem contidas em meios digitais como os bancos de dados de computadores, pois somente assim um bem computacional seria lesado pela pratica do ilícito, ou seja, se violaria o sigilo dos dados computacionais existentes no sistema.

III - O art. 313-A, do Código Penal, introduzido pela Lei nº 9983/2000, que tipificou o crime de inserção de dados falsos em sistemas de informação, com a seguinte redação:

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou banco de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.
> Pena - reclusão, de 2 a 12 anos e multa.

O artigo 313 – A, introduzido no Código Penal tipificou a conduta de manipulação de dados em sistema da Administração Pública. Em meio às particularidades do fato típico encontra-se mais uma vez a restrição da prática da conduta a determinados sistemas informatizados, ou seja, aqueles a serviço da Administração Pública, assim como a necessidade de que o mesmo seja praticado por funcionário público, limitando-se assim o campo de atuação do tipo penal, o que por força de sua extrema especificidade deixa uma série de condutas ilícitas desprovidas de sanção legal. A conduta criminosa em questão visa impedir de forma direta que um funcionário público manipule ou facilite a manipulação de dados contidos em sistema de informática ou banco de dados da Administração Pública. A manipulação pode consistir na inserção de dados falsos no sistema, na alteração ou exclusão de dados corretos, não importando se o interesse do autor da conduta era a obtenção de alguma vantagem econômica ilícita ou de causar dano**.**

IV - O art. 313-B, do Código Penal, introduzido pela Lei nº 9983/2000, que tipificou o crime de sistema de informação, com a seguinte redação:

> Art. 323-B: Modificar ou alterar, o funcionário, sistema de informação ou programa de informática sem autorização ou solicitação de autoridade competente.
> Pena - detenção de 3 meses a 2 anos e multa.

Trata o artigo 313 – B do Código Penal do crime que comete o funcionário público que altera ou modifica sistema de informática ou programa de computador sem a devida autorização. É necessário ressaltar que os delitos capitulados nos artigos 313-A e 313-B do Código penal nacional são considerados pela maioria da doutrina como crimes de mão própria, ou seja, só podem ser cometidos por funcionários públicos, limitando-se, desta forma, ainda mais o campo de aplicação da lei incriminadora.

V - O art. 325, § 1º, incisos I e II, introduzidos pela Lei nº 9983/2000, tipifica novas maneiras de violação de sigilo funcional:

> Art. 325.....:
> §1º.....
> I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informação ou banco de dados da Administração Pública.
> II – se utiliza indevidamente, do acesso restrito.
> Pena de detenção de 6 meses a 2 anos, ou multa.

O inciso I do artigo do § 1º do artigo 325 do Código Penal pune o funcionário que de alguma forma possibilita a terceiro não autorizado o acesso a banco de dados ou sistemas de informática da Administração pública, não importando qual o meio utilizado pelo agente para facilitar o acesso indevido. Trata-se de dispositivo legal extremamente importante que busca impedir a facilitação dos acessos indevidos. Entretanto este crime adquire um caráter peculiar em nosso ordenamento, pois em razão da ausência de dispositivos legais reguladores da matéria aplicáveis a todos os agentes, somente o funcionário público seria punido, não recaindo nenhuma punição sob quem acessou o banco de dados ou o sistema de informática.

Já o inciso II do parágrafo 1º do artigo 325 do Código Penal visa punir o funcionário que dotado de autorização para acessar informações ou para realizar atividades de cunho restrito no sistema informático, arbitrariamente extrapola os limites de sua autorização, acessando dados não permitidos ou praticando atividades indevidas.

VI - O art. 12 da Lei Federal nº 9609/98, que tipifica o crime de violação de direitos de autor de programa de computador:

> Art. 12. Violar direitos de autor de programa de computador:
> Pena - Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
> Pena - Reclusão de um a quatro anos e multa.
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
> § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
> I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
> II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.
> § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

VII - O art. 2º, inciso V, da Lei Federal nº 8137/90, que considera crime:

> Art. 2.....
> V - Utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública.
> Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa.

Além de constituir violação contra a ordem tributária, se trata de crime eletrônico porque o programa utilizado para processar os dados inseridos no sistema altera o correto tratamento dos mesmos fazendo com que o resultado do processo seja maculado. Em outras palavras, os dados corretos são processados por um programa alterado que, objetivando fraudar as informações processadas, modifica o resultado.

VIII - O art. 72 da Lei nº 9504/97, que cuida de três tipos penais eletrônicos de natureza eleitoral:

> Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:
> I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;
> II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;
> III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

No delito tipificado no inciso I, temos a ocorrência de duas situações ilícitas. A primeira é o acesso não autorizado a sistema informático, que por si só já se configura como fato punível como crime informático. Entretanto o tipo penal atrela ao acesso o intuito de alterar-se os dados relativos a contagem dos votos. Só quando verificadas essas duas condições a conduta se torna punível. O ato lesa interesses jurídicos distintos dos bens computacionais, mas opera-se por meio de lesão a estes, uma vez que a segurança do sistema foi violada e a integridade dos dados foi deturpada em face de sua manipulação.

No crime capitulado no inciso II, tem-se um conjunto de condutas lesivas a bens informáticos tais como apagar ou transmitir dados e informações. O tipo penal visa proteger a corrupção do tratamento correto de dados utilizados pelo serviço eleitoral, quer seja pelo desenvolvimento ou pela introdução de comando, instrução ou programa que por qualquer meio, manipulação, transmissão de dados, entre outros, altere o correto processamento e o resultado dos dados inseridos no sistema computacional a serviço do pleito eleitoral.

No inciso III se verifica, mesmo que possua aplicação restrita, a tipificação da conduta intitulada pela doutrina como dano informático, ou seja, efetuar dolosamente dano ao equipamento utilizado na votação com objetivo de evitar o acesso aos dados nele contidos ou a própria destruição do suporte físico de armazenamento dos dados.

Entretanto, em face da restrição cometida pelo legislador, estas situações ficaram desprotegidas uma vez que somente o caso específico foi regulamentado, ou seja, crimes perpetrados unicamente contra sistemas eletrônicos utilizados pela Justiça Eleitoral, o que infelizmente ainda deixa uma lacuna na lei, pois se tratam de condutas que de forma genérica que podem ser praticadas contra qualquer sistema de informação, o que demonstra a necessidade de repensar-se o modo de elaboração das normas legais aplicáveis à matéria.

Os exemplos enumerados demonstram que apesar do surgimento de legislação relacionada com a matéria dos crimes digitais, a regulamentação existente é esparsa e extremamente específica aplicando-se a determinados temas. Em conseqüência disto uma gama de condutas ilícitas encontram-se carentes de punição em face da ausência de normas legais atinentes ao assunto como um todo. Deve-se então elaborar diploma legal que trate a matéria de forma técnica,

criminalizando as condutas que atentem contra os sistemas informáticos e seus dados independentemente do seu proprietário, não importando se ente público ou privado, se a Administração Pública ou particular, ressaltando-se que uma vez escalonado os graus de importância dos mais variados sistemas informáticos se deve estipular algumas qualificadoras para condutas que atentem contra os mais importantes. Logo, em face de uma evidente lacuna normativa que ocasione a falta de sanção a uma gama de novos atos ilícitos, se deve com urgência elaborar dispositivos legais para regular o tema.

3.3 PROJETOS DE LEI EM TRAMITAÇÃO

Atualmente existem vários projetos de leis em tramitação que buscam regular e adaptar a legislação brasileira às novas tendências tecnológicas, e consequentemente, tratar e tipificar os delitos digitais, dentre os inúmeros projetos, três se destacam por disporem sobre sua definição, tipificação e penalidades, são eles: o PL da Câmara nº 89/03, do Deputado Luiz Piauhylino; o PL do Senado nº 137/00, do Senador Leomar Quintanilha; e, o PL no Senado nº 76/00 do Senador Renan Calheiros.

Devido à grande ligação e importância entre os três projetos, um substitutivo foi proposto, unindo as três sugestões. Trata-se de um PL substitutivo, cuja elaboração contou com a participação de diversos especialistas em Direito Penal e em tecnologia de informação e comunicação. Acompanhando o substitutivo um parecer do Senador Eduardo Azeredo, relatando a importância da matéria e analisando os três projetos de lei referidos.

O novo projeto aglutinou as três proposições para tipificar condutas realizadas mediante uso de sistemas eletrônicos, digital ou similares, de rede de computadores, ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares, além de dá outras providências. Para isso, o PL substitutivo, com vinte e três artigos, altera o Código Penal, o Código Penal Militar, o Estatuto da Criança e do Adolescente (Lei nº

8.069/90), a Lei de Interceptação Telefônica, Lei do racismo (Lei nº. 7.716/89) e, por fim, a lei de repressão uniforme (Lei n. º 10.446/02).

Em maio de 2005 o PLC 89/03 foi aprovado na Comissão de Educação, em votação terminativa e foi ao Plenário por cinco sessões, mas as Medidas Provisórias obstruíram a votação, dessa forma toda a tramitação voltou ao início, pois os PLS apensados obrigam aos três Projetos de Lei irem à Câmara e lá tramitarem por uma Comissão Especial. Em agosto de 2005, foi aprovado o apensamento do PLS 76 de 2000 e do PLS 137 de 2000 ao PLC 89 de 2003. Em 20 de junho de 2006 a primeira versão do substitutivo foi aprovada pela Comissão de Educação do Senado, que considerou as propostas pertinentes, votando pela aprovação do substitutivo, que então foi encaminhado para a Comissão de Constituição e Justiça, quando em julho de 2008 foi aprovado, sendo então encaminhado para o plenário onde foi aprovado, e posteriormente remetido à Câmara dos deputados. Onde ainda encontra-se em tramitação.

As novidades que devem chegar com a aprovação do PL é a tipificação de diversas condutas criminais no meio digital, na sugestão de alteração, o PL primeiramente em seu art. 2 acrescenta o Capítulo IV ao Título VIII do Código Penal da seguinte forma:

> CAPÍTULO IV
> DOS CRIMES CONTRA A SEGURANÇA
> DOS SISTEMAS INFORMATIZADOS
> Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado
> Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:
> Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.
> Obtenção, transferência ou fornecimento não autorizado de dado ou informação
> Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.
> Ação Penal
> Art. 285-C. Nos crimes definidos neste Capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias. (Art. 2° do PLC 89/2003)

Em seguida, no art. 3, acrescenta o seguinte art. Ao Título I do CP:

> Divulgação ou utilização indevida de informações e dados pessoais
> Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:
> Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.
> Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte. (Art. 3° do PLC 89/2003)

Em seu art. 4° o PL equivale o dado eletrônico à "coisa", incluindo-o assim na tipificação do crime de dano, modificando a redação do caput. do art. 163 do CP para:

> Dano
> Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:
> ..... (NR) (Art. 4° do PLC 89/2003)

No art. 5, o PL acrescenta ao Capítulo IV do Título II da parte especial do CP o seguinte art.:

> Inserção ou difusão de código malicioso
> Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Inserção ou difusão de código malicioso seguido de dano
> § 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte. (Art. 5° do PLC 89/2003)

O art. 6 do PL modifica o art. 171 do CP, adicionando os seguintes dispositivos:

> Art. 171. .....
> .....
> § 2º Nas mesmas penas incorre quem:
> .....
> Estelionato Eletrônico
> VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado.
> § 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime previsto no inciso VII do § 2º, a pena é aumentada de sexta parte. (NR) (Art. 6° do PLC 89/2003)

Da mesma forma, o art. 7 do PL modifica os arts. 255 e 256 do CP, que passam a vigorar com as seguintes redações:

> Atentado contra a segurança de serviço de utilidade pública
> Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:
> ..... (NR)
> Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado
> Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou
> de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:
> ..... (NR) (Art. 7° do PLC 89/2003)

Tratando da Falsificação Eletrônica. Os arts. 8° e 9° do PL modificam os caputs. Dos arts. 297 e 298 do CP, que passam então a vigorar da seguinte forma:

> Falsificação de dado eletrônico ou documento público
> Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento público verdadeiro:
> .....(NR)
> Falsificação de dado eletrônico ou documento particular
> Art. 298. Falsificar, no todo ou em parte, dado eletrônico ou documento particular ou alterar documento particular verdadeiro:
> .....(NR) (Art. 8° e 9° do PLC 89/2003)

A partir do art. 10 até o seu art. 15, o PL continua tipificando e regulamentando condutas criminosas no âmbito digital, só que as mudanças agora incidem sobre o Código Penal Militar, o que foge um pouco do objetivo do trabalho, por essa razão não necessitam serem expostos aqui. Continuando do art. 16° até o 18°, o PL elenca definições e medidas importantes para toda sua regulamentação. São elas:

> Art. 16. Para os efeitos penais considera-se, dentre outros:
>
> I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;
>
> II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;
>
> III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;
>
> IV – código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;
>
> V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;

> VI – dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.
>
> Art. 17. Para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado.
>
> Art. 18. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. (Art. 16°, 17° e 18° do PLC 89/2003)

Essa definição de conceitos é muito importante para se atender aos interesses dos que desconhecem quaisquer denominações, contribuindo assim para um melhor entendimento da matéria por parte daqueles que possuem o dever de assegurar o correto uso das tecnologias digitais. O art. 18 reforça ainda mais o interesse do legislador em combater esse tipo de criminalidade.

O art. 19° regula a lei que pune o racismo, o art. modifica o inciso II do §3° do art. 20, e traz uma ótima novidade para o sistema de repressão aos crimes dessa natureza, situação que já existe na prática, decorrente de alguns termos de ajustamentos de conduta formulados pelos Ministérios Públicos Estaduais e Federal com alguns provedores. A redação dispões que:

> "Art. 20 .....
>
> .....
>
> § 3º.....
>
> .....
>
> II – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.
>
> ....." (NR) (Art. 19° do PLC 89/2003)

Em seu art. 20 o PL modifica o caput do art. 241 do Estatuto da Criança e do Adolescente, passando então a vigorar com a seguinte redação:

> "Art. 241. Apresentar, produzir, vender, receptar, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:
>
> ....." (NR) (Art. 20° do PLC 89/2003)

O art. 21 altera o art. 1º da Lei de Repressão Uniforme, passando a vigorar com a seguinte redação:

> "Art. 1º .....
>
> .....

> V – os delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado.
>
> ....." (NR) (Art. 21° do PLC 89/2003)

Em seu art. 22 o PL visa atribuir uma maior responsabilidade aos responsáveis pelo provimento da Internet, seja no setor público ou privado. Ele dispõe que:

> Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:
>
> I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;
>
> II – preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;
>
> III – informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.
>
> § 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento.
>
> § 2º O responsável citado no caput deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.
>
> § 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001. (Art. 22° do PLC 89/2003)

E por ultimo, o art. 23 dispõe que:

> Art. 23. Esta Lei entra em vigor 120 (cento e vinte) dias após a data de sua publicação. (Art. 23° do PLC 89/2003)

São de grande notoriedade as mudanças que esse Projeto de Lei propõe, tanto que existem diversas manifestações, muitas por parte da comunidade internauta, contra a aprovação do projeto, graças ao rigor com que ele trata condutas comuns e cotidianas, como baixar uma música sem o devido pagamento dos direitos, ou desbloqueios de aparelhos celulares com a utilização de softwares não autorizados. Também existem críticas por parte de especialistas no ramo da

tecnologia digital, que argumentam que o projeto de lei dificulta a inclusão digital e viola a privacidade dos usuários que, terão seus dados de conexão à Internet rastreados e armazenados pelos provedores de acesso por três anos, além de que quem se conecta a internet com intenção de cometer crime vai cuidar, a exemplo do que ocorre com fraudes na área financeira, onde os serviços eletrônicos já são bastante controlados, de antes burlar os controles, velhos ou novos, com identificações falsas ou com provedores externos que lhe ofereçam o anonimato.

Observa-se que de fato o projeto de lei necessita de algumas mudanças, pois apesar de conter várias inovações no campo da criminalidade digital, regulando bem algumas matérias, é evidente a presença de dispositivos que criam tipos abertos e subjetivos de crimes (art. 2º), e que legalizam esquemas privados de espionagem, definidos ou impostos também de maneira vaga e subjetiva, caso do art. 22 do PL.

No mais, atualmente tem-se que destacar que, ao se falar de crime digital, a conduta danosa mesmo não prevista em lei penal definindo-a como crime, poderá ensejar reparação cível com multas variáveis de acordo com o resultado obtido, a ser estipulada pelo juiz, devido à grande subjetividade e abrangência de conceitos como danos morais e materiais.

CONSIDERAÇÕES FINAIS

Ao longo do trabalho ficaram evidentes os grandes avanços tecnológicos que de fato trouxeram inestimáveis benefícios à humanidade, destacando como o principal deles a informática, que se originou nos Estados Unidos com fins militares, mas devido a sua vasta aplicabilidade evoluiu rapidamente, e proporcionou o surgimento de outro marco da evolução tecnológica, a Internet, que por sua vez logo passou de instrumento militar à utilidade doméstica e comercial e espalhou-se pelo mundo inteiro. Mas infelizmente, junto a gama de benefícios oriundos dos avanços dos meios digitais, surgiram também grandes problemas, e dentre estes, os Crimes Digitais, que no passo da tecnologia e da globalização, surpreenderam e modificaram as relações econômicas, sociais e jurídicas da sociedade.

Em face de um novo tipo de criminalidade, os países passaram a buscar uma forma de combater os delitos e proteger os bens jurídicos da sociedade, e apesar de ainda não existirem consensos entre os doutrinadores nacionais e internacionais quanto aos conceitos e classificações específicas dos crimes digitais, é notória preocupação em analisar e delimitar os principais campos de atuação dos criminosos, suas características, e principalmente os aspectos legais relevantes, como autoria, jurisdição, competência, princípios, assim como as medidas que eventualmente deverão ser tomadas a fim de adaptar as legislações às novas diretrizes criminológicas.

Dessa forma, com base nas características e perfis dos principais criminosos digitais, verificamos que apesar de num primeiro momento serem exclusivamente pessoas entendidas no assunto, hoje em dia não mais são necessariamente peritos e especialistas no campo da tecnologia informacional e virtual, já que qualquer pessoa com o mínimo de conhecimento de informática está apta a cometer crimes digitais. Verificamos também que além de cometerem os novos tipos de crimes já mencionados, também praticam os já tipificados crimes comuns, só que utilizando os meios digitais para atingirem seus objetivos. Ou seja, em determinados casos, a lei brasileira já tipifica condutas em que o fato de utilizarem ou não um computador para determinada prática de crime não prejudica a tipificação legal. No entanto, nesses casos, é necessária a elaboração de eventuais

majorantes e qualificadoras mais severas que se adequem à ação do criminoso, a fim de desencorajar ainda mais as práticas de crimes comuns por meios virtuais, visto que neste campo, o criminoso goza de inúmeros fatores que contribuem para sua impunidade, como o caso do anonimato.

Ao analisarmos nossa atual legislação, observamos que algumas espécies de crimes puramente digitais também já contam com previsão legal, mas infelizmente ainda são poucas, e encontram-se em legislações esparsas e com tipificações muito específicas, por essa razão, inúmeras novas propostas de projetos de leis tramitam no Congresso e no Senado Federal, em especial o PLC 89/2003, que aglutinou três outras proposições a fim de tipificar condutas realizadas mediante uso de sistemas eletrônicos, digital ou similares, de rede de computadores, ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares, fato este que demonstra que o legislador brasileiro está consciente da importância da matéria.

Por fim, diante dessa perspectiva e com base no constante avanço da tecnologia e da Internet no Brasil e no mundo, o Estado deve adaptar seu ordenamento jurídico o mais rápido possível, a fim de assegurar a proteção da sociedade, prevenindo e punindo aqueles que denigrem os interesses alheios. Para tanto, os órgãos de persecução criminal devem organizar setores especializados no combate à criminalidade digital, que deverá contar com planejamento, preparo e treinamento específico. E uma vez que o processo evolucionário tecnológico continua acontecendo a cada dia que passa, é preciso que o Estado e seu ordenamento jurídico continuem dispostos a acompanhar as transformações digitais e as novas formas de criminalidade que eventualmente virão, do mesmo modo que os profissionais do direito, especialmente juízes, delegados e membros do ministério público, se habilitem aos novos desafios impostos pelos crimes digitais.

REFERÊNCIAS

ARAS, Vladimir. **Crimes de informática.** Uma nova criminalidade. Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: <http://jus.uol.com.br/revista/texto/2250>. Acesso em: 10 set. 2010.

BRASIL. **Lei nº 9.983, de 14 de julho de 2000**. Altera o Decreto-lei n.º 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências. Disponível em: <http://www.senado.gov.br>. Acesso em: 15 set. 2010.

_____. **Lei nº 8.137, de 27 de dezembro de 1990**. Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. Disponível em: <http://www.senado.gov.br>. Acesso em: 15 set. 2010.

_____. **Lei nº 9.504, de 30 de setembro de 1997**. Estabelece normas para as eleições. Disponível em: <http://www.senado.gov.br>. Acesso em: 15 set. 2010.

_____. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: <http://www.senado.gov.br>. Acesso em: 15 set. 2010.

_____. **Projeto de Lei da Câmara n° 89 de 2003**. Modifica alguns arts. do Código Penal e de outras leis, para tipificar e regulamentar crimes digitais. Disponível em: <http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=63967>. Acessado em: 05 de nov. 2010.

_____. **Decreto-lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Disponível em:<http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del2848.htm>. Acesso em: 10 set. 2010.

_____. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Disponível em:<http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm>. Acesso em: 10 set. 2010.

_____. **Constituição (1988). Constituição da República Federativa do Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm>. Acesso em: 15 set. 2010.

_____. **Tribunal de Justiça de Santa Catarina**. Apelação criminal n. 2007.006842-9. Segunda Câmara Criminal. Relator: Irineu João da Silva. Julgado em 22/05/2007. Disponível em <http://app.tjsc.jus.br/jurisprudencia/acnaintegra!html.action?qTodas=busca+e+apreens%E3o+computador&qFrase=&qUma=&qNao=&qDataIni=&qDataFim=&qProcesso=&qEmenta=&qClasse=&qRelator=&qForo=&qOrgaoJulgador=&qCor=FF0000&qTipoOrdem=relevancia&pageCount=10&qID=AAAGxaAALAAAVWWAAA>. Acesso em: 23 out. 2010.

_____. CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet** - parte I: conceitos de Segurança. Disponível em: <http://cartilha.cert.br/conceitos/sec8.html#sec8>. Acesso em: 20 out. 2010

CAVALCANTI, Leonardo; GÓES, Dalila; ALVES, Renato. **Conexão perigosa**. 6 dez. 2000. Disponível em:<http://www.cgi.br/infoteca/clipping/2000/midia-dez02.htm>. Acesso em: 16 set. 2010.

CAPEZ, Fernando. **Curso de processo penal.** 16 ed, São Paulo: Saraiva, 2009.

COIMBRA, Márcio C. **A inviolabilidade dos e-mails**. 27 out. 2000. Disponível em: <http://www.widebiz.com.br/gente/marcio/email.html>. Acesso em: 10 out. 2010.

DICIONÁRIO Michaelis. Disponível em: <www.uol.com.br/michaelis>. Acesso em: 10 nov. 2010.

ELIAS, Paulo Sá. **A questão da reserva legal no Direito Penal e as condutas lesivas na área da informática e da tecnologia**. Jus Navigandi, Ed. 12, out. 2001. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2038>. Acesso em: 15 set. 2010.

FERREIRA, Érica Lourenço de Lima. **Internet: Macrocriminalidade e Jurisdição Internacional**. 1ª ed. Curitiba: Juruá, 2007.

FERREIRA, Ivette Senise **A criminalidade informática. In Direito & internet:** aspectos jurídicos relevantes. 1ª ed. Bauru: Edipro, 2000.

FOINA, Ariel G.; REIS, Igor de V. Cavalcante**. Das provas de crimes na internet:** as questões do cibercrime e da rede para o Direito Penal e seu processo. n. 10. Brasília: Universitas Jus, 2004.

FRAGOMENTI, Ana Helena. **Dicionário enciclopédico de informática**. v. 1.Rio de Janeiro: Campus, 1986.

JESUS, Damásio Evangelista de. **Direito penal.** v. 1, 25ª ed. São Paulo. Saraiva, 2002.

LAUDON, K. C.; LAUDON, J. P. **Gerenciamento de sistemas de informação**. 3ª ed. Rio de Janeiro: LTC, 2001.

LIBERATI. Wilson Donizeti. **Comentários ao Estatuto da Criança e do Adolescente**. 1ª. ed. São Paulo: Malheiros Editora, 2008.

LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.). **Direito e internet:** aspectos jurídicos relevantes. 1ª ed. Bauru: Edipro, 2000.

MIRABETE, Júlio Fabrini. **Processo penal.** 18ª. ed. São Paulo: Atlas, 2006.

MONTEIRO NETO. João Araújo. **Crimes informáticos,** uma abordagem dinâmica ao direito penal informático. 1ª. ed. Fortaleza, Pensar, 2003.

MONTEIRO NETO. João Araújo; FREITAS DA SILVA. Francisca Jordânia. **Crimes eletrônicos no Ordenamento jurídico brasileiro**. São Paulo. 2009. Disponível em: <http://www.publicadireito.com.br/conpedi/manaus/arquivos/Anais/sao_paulo/2319.pdf>. Acessado em: 25 de set. 2010.

NOGUEIRA. Sandro D´Amato. **Crimes de Informática**. 1ª. ed. São Paulo: BH Editora, 2008.

PAESANI, Liliane Minardi. **Direito e Internet**. 1ª. ed. São Paulo: Atlas, 2003.

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: 10 de set. 2010.

ROSA, Fabrizio. **Crimes de Informática**. 2ª edição. Campinas: Bookseller. 2005.

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

SANTOS, Ana Mara Hoffmam dos. **Crimes contra a honra na internet**. Disponível em:<http://www.buscalegis.ufsc.br/arquivos/Artigo%20%20Crimes%20contra%20honra%20na%20internet%20-%20Ana%20Mara.htm> Acesso em: 20 set. 2010.

VALLIM, Celso Henrique de C. Baptista. **Crimes contra a honra na internet.** Santa Catarina. Disponível em: <www.buscalegis.ufsc.br/arquivos/mono-crimescahni.pdf> Acesso em: 10 out. 2010.

VIANA. Túlio Lima. **Hackers:** um estudo criminológico da subcultura cyberpunk**.** Disponível em <http://www.infojur.ccj.ufsc.br>. Acesso em: 15 set. 2010.