**UNIVERSIDADE FEDERAL DO CEARÁ**
**FACULDADE DE DIREITO**
**CURSO DE GRADUAÇÃO EM DIREITO**

**CARLOS JEREMIAS MARQUES SOUSA**

# OS DELITOS INFORMÁTICOS NA INTERNET

**Fortaleza - Ceará**
**2008**

CARLOS JEREMIAS MARQUES SOUSA

# OS DELITOS INFORMÁTICOS NA INTERNET

Monografia apresentada ao Curso de Graduação em Direito, da Universidade Federal do Ceará (UFC/CE), como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Prof. Dr. Raimundo Hélio Leite

Fortaleza - Ceará
2008

CARLOS JEREMIAS MARQUES SOUSA

# OS DELITOS INFORMÁTICOS NA INTERNET

Monografia apresentada ao Curso de Graduação em Direito, da Universidade Federal do Ceará (UFC/CE), como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Prof. Dr., Livre Docente, Raimundo Hélio Leite

Aprovada em 20 de novembro de 2008.

BANCA EXAMINADORA

_____

Prof. Dr. Raimundo Hélio Leite (Orientador)
Universidade Federal do Ceará

_____

Prof. José Adriano Pinto
Universidade Federal do Ceará

_____

Prof. MsC. Marcos José Nogueira de Souza Filho
Faculdade Christus

*A Deus, sustentáculo de nossas vidas.*

Aos meus pais, Dalva e Messias, ao meu tio Carlos Alberto, à minha avó Gercina pelos exemplos de perseverança que são para mim e pelo apoio que sempre me deram.

## AGRADECIMENTOS

Aos meus pais, Dalva e Messias, por me ensinarem os valores da honestidade e do trabalho;

À minha avó Gercina, pelo exemplo de vida e por cultivar nobres valores em sua vida;

Aos meus tios, que sempre estiveram presentes e que muito me ensinaram;

Ao meu orientador, Prof. Dr. Raimundo Hélio Leite, pela atenção e direção do trabalho;

Aos ilustres membros da banca examinadora, Adriano Pinto e Marcos Filho, pela gentileza em aceitar o convite;

Ao meus grandes amigos, Ernando, Cidade e Renato, pela ajuda e incentivo a mim dispensados;

À minha namorada e amiga, Tatyana, pelo apoio, cumplicidade e companheirismo em todas as horas;

A todos aqueles que contribuíram de forma direta e indireta à concretização desta monografia.

A invenção da pólvora não
reclamou redefinição do
homicídio para tornar
explícito que nela se
compreendia a morte
dada a outrem mediante
arma de fogo

HC 76.689-0-PB

## RESUMO

Esta monografia faz um estudo dos principais tipos de delitos informáticos, bem como eles são punidos no Brasil. A grande problemática de se criar ou adequar a legislação brasileira para tratar dos crimes em ambientes virtuais será mostrada e discutida. O estudo da nomenclatura a ser adotada é também abordado, por ser de extrema utilidade para a fixação do objeto deste trabalho. O mito de que esses crimes através da Internet não deixam vestígios e de que os criminosos não podem ser identificados serão analisados. Uma das principais características da Internet, a transnacionalização, pode ser o grande problema enfrentado pelos operadores de direito de todo o mundo para punir as pessoas que cometem crimes cibernéticos em razão de este possuir o poder de atingir vários países. O estudo de como devem ser punidos torna-se necessário. Para a isso, levar-se-ão, cumulativa ou isoladamente, em conta o país de origem do crime, a residência física do autor ou onde se produziu o resultado da ação do criminoso. Classificam-se normalmente os delitos informáticos em próprios e impróprios. Fica evidente que o código penal brasileiro não pode acompanhar em sua totalidade os crimes cometidos na Internet ou através dela já que ele data de 1940. Tratados internacionais ou acordos devem ser uma boa solução para regulamentar e punir os delitos informáticos que atinjam várias jurisdições nacionais



Palavras-chave: Delitos Informáticos Próprios e Impróprios, Internet, Legislação sobre Informática.

## ABSTRACT

This monography makes a study of the main types of cybernetic crimes, as well as how they are punished in Brazil. The greatest problem in creating or adequating our legislation to treat cybernetic crimes will be shown and discussed. This work looks to analyze the denomination that will be adopted to study main object of this work. The myth that these internet crimes don´t leave vestiges and the agents can´t be identified will be discussed. One of the main characteristics of the Internet, the transnacionalization, can be the greatest problem faced by law operators of the entire world to punish people that commit cybernetic crimes since cybernetic crimes can affect several countries. It´s necessary studies how to punish them. For that, it´s taken in consideration the country of origin of the crime or the physical residence of the author or where it was produced the action of the criminal. Normally computer crimes are characterized by proper and improper. It is evident tha the Brazilian penal code can not accompany in its totality the crimes committed on the Internet or through it since the code was established in 1940. International treaty or agreements may be a good solution to regulate and punish cybernetic crimes that affect several national jurisdictions



Keywords: Crimes on Internet, Proper and Improper Crimes, Computer Legislation.

**SUMÁRIO**

# 1 INTRODUÇÃO

O estudo interdisciplinar da Informática e do Direito apresenta-se como tarefa bastante árdua, visto que envolve dois ramos do conhecimento humano distintos. De um lado, estão o positivismo, os números, a exatidão, a máquina, a tecnologia; do outro, o humanismo, a dialética, o homem, o Direito.

Cada um encerra um campo hermético de conhecimentos, somente acessível àqueles que se dispuserem a dedicar a vida inteira ao seu estudo exclusivo.

Porém, se é verdade que não se pode exigir do homem moderno o conhecimento eclético que detinham Platão e Aristóteles, também é certo que as ciências humanas, em especial o Direito, devem acompanhar as evoluções tecnológicas. Principalmente, porque o Direito, como instrumento regulador dos fatos sociais juridicamente relevantes, não pode deixar de acompanhar as profundas mudanças ocorridas no meio social em decorrência do surgimento da Internet, tendo como conseqüência importante o surgimento de uma Sociedade da Informação.

A relação entre direito e realidade sempre foi um tema central no pensamento jurídico. Com o desenvolvimento tecnológico, essa relação tornou-se ainda mais importante, na medida em que a rápida mudança que se presencia no plano dos fatos traz consigo o germe da transformação no plano do direito. Essa transformação se dá de duas formas: de modo indireto, quando as instituições jurídicas permanecem imutáveis ainda que os fatos subjacentes a elas se alterem profundamente; ou de modo direto, quando o direito se modifica efetivamente perante a mudança na realidade, em um esforço de promover novas soluções para os novos problemas.

A Internet revolucionou o mundo dos computadores e das comunicações como nenhuma invenção foi capaz de fazer antes. As invenções do telégrafo, do telefone, do rádio e do computador prepararam o terreno para esta nunca antes havida integração de meios de comunicação. A Internet é, de uma vez e ao mesmo tempo, um mecanismo de disseminação da informação e

divulgação mundial e um meio para colaboração e interação entre indivíduos e seus computadores, independentemente de suas localizações geográficas.

É notório a todos que, com o advento da Internet, ocorreu uma exponencial ampliação no acesso às informações, possibilitada pela maior rapidez com que uma obra pode ser copiada e pelo vertiginoso aumento da velocidade de divulgação das informações.

Dessa forma, através de suas infinitas facetas e utilidades, a Internet trouxe diversas possibilidades para seu usuário, o que criou, por sua vez, inúmeros fatos novos e novas relações para o Direito tutelar. Para o Direito, assim, as mudanças geradas pela informática repercutiram em todos os seus ramos, que sofreram, direta ou indiretamente, seus reflexos na maneira de ser ou de agir.

Este ensaio monográfico tem como objetivo investigar os desafios propostos ao direito em decorrência do advento da Internet e da tecnologia digital.

Não se pode deixar de reconhecer que o espantoso crescimento da informática nas últimas décadas, trouxe grandes benfeitorias para a sociedade como um todo, mas também trouxe questionamentos nunca antes enfrentados. Os diversos segmentos da sociedade moderna. Dentre estes vale destacar os que englobam os profissionais do Direito, os quais demonstram clara preocupação do homem moderno com os rumos da rede mundial de computadores (Internet), que apesar de ser, inegavelmente, um marco na divisão da história da humanidade, ao lado de tantos benefícios que propicia, tem também o seu lado nefasto: pode ser um instrumento para a prática de crimes.

Os denominados “cybercrimes” ou crimes virtuais são aqueles delitos praticados utilizando-se como meio a Internet. Devido ao anonimato que a rede mundial de computadores proporciona, aliada à falta de legislação específica sobre o assunto, tal modalidade de delito aumenta consideravelmente no mundo contemporâneo, de forma a obrigar a população e as autoridades a buscarem mecanismos de prevenção contra os criminosos.

Tais crimes apresentam-se de várias formas, destacando-se dentre elas a violação dos direitos autorais sobre *softwares* e o dano causado pelos famosos vírus de computador. Como lembra Maria Helena Junqueira Reis:

> A gama de delitos que podem ser perpetrados pela Internet é quase infinita. A lista inclui o mau uso dos cartões de crédito, ofensas contra a honra, apologia de crimes, como racismo, ou incentivo ao uso de drogas, ameaças e extorsão, acesso não autorizado a arquivos confidenciais, destruição e falsificação de arquivos, programas copiados ilegalmente e até crime eleitoral (propaganda não autorizada, por exemplo) dentre outros[1].

Não se desconhece, portanto, conforme mencionado, que o advento dessa nova mídia, mesmo ao trazer incontáveis benefícios ao irreversível processo de globalização vivido pela sociedade neste final de Século, conduz em seu ventre o germe de uma nova delinqüência, intimamente unida ao que chamamos de macrocriminalidade, dado o refinamento que norteia a ação dos seus praticantes.

Surge também o problema de aliar o 'jus puniendi' do Estado com a universalidade da rede mundial de computadores, conforme leciona Marcel Leonardi:

> Como representa uma conjunto Global de redes de computadores interconectadas, não existe nenhum governo,organismo internacional ou entidade que exerça controle ou domínio absoluto sobre a Internet. A regulamentação da rede é efetuada dentro de cada país, que é livre para estabelecer regras de utilização, hipóteses de responsabilidade e requisitos para acesso, atingindo somente usuários sujeitos à soberania daquele Estado.[2]

Assim, a sociedade necessita de mecanismos reguladores eficientes que disciplinem os crimes cometidos por meio de computadores, a fim de que se consiga acompanhar a velocidade das inovações tecnológicas, coibindo devidamente a prática crescente de tais delitos.

---

1 REIS. Maria Helena Junqueira. *Computer Crimes*: a criminalidade na era dos computadores. Belo Horizonte: Del Rey, 1996. p.53.

2 LEONARDI, Marcel. *Responsabilidade Civil dos Provedores de Serviços de Internet*. São Paulo: Editora Juarez de Oliveira, 2005. p.48.

Ao Direito, portanto, caberá criar normas que disciplinem esse novo poder que surge travestido de máquina. Para isso, Informática e Direito terão que se abrir um para o outro, pois, caso contrário, a sociedade estagnar-se-á, arraigando-se na segurança fornecida pelo Direito ou caminhará para o caos na velocidade estonteante da evolução tecnológica.

Dessa forma, passar-se-á a um estudo, nos tópicos seguintes, dos aspectos relevantes do Direito Penal Informático, dando-se relevância às necessárias mudanças no Direito Penal, assim como do estudo da Internet, seu surgimento, consolidação e funcionamento. Em seguida, abordar-se-ão os crimes mais comuns praticados através da Internet.

Assim, esta monografia tem por objetivo mapear os problemas jurídicos na área penal advindos do avanço tecnológico e do uso generalizado da Internet, para aprofundar, criticamente, alguns desses problemas. Dentre esses, destacam-se os impactos para as estruturas normativas tradicionais, ressaltando a necessidade de conhecer como o sistema normativo funciona e demonstrando as alternativas reguladoras e institucionais que um pensamento estratégico brasileiro sobre o assunto deve considerar.

# 2 A SOCIEDADE DA INFORMAÇÃO

A denominada sociedade da informação merece o aprofundamento da ciência jurídica, pois dadas as suas características, alberga em seu interior toda a análise técnico-jurídica de uma gama de fatos jurídicos diretos e indiretos advindos da utilização da tecnologia da informação e da Internet. Daí o seu estudo neste trabalho, com relação ao seu surgimento, características e projeções na seara jurídico-penal.

## 2.1 Surgimento e Características

Uma das principais características do homem ante a natureza é a utilização de instrumentos diferentes dos seus próprios membros para dela tirar o maior proveito. Aliás, até mesmo antes de se tornar "homem", os primatas já se utilizavam de paus e pedras para obter, com maior rapidez e menor esforço, aquilo de que necessitavam para a sobrevivência. As "máquinas" se inserem nesta incessante busca de satisfazer, com menor gasto de energias, as necessidades mais elementares.

Nesse contexto, a informática nasceu da idéia de beneficiar e auxiliar o homem nos trabalhos do cotidiano e naqueles realizados repetitivamente. Tem-se por definição mais comum que a Informática é a ciência que estuda o tratamento automático e racional da informação. Entre as funções da informática há o desenvolvimento de novas máquinas, a criação de novos métodos de trabalho, a construção de aplicações automáticas e a melhoria dos métodos e aplicações existentes. O elemento físico que permite o tratamento de dados e o alcance de informação é o computador. O termo computador vem do latim *computadore* e significa "aquele que faz cômputos, que calcula"[3].

---

[3] FERREIRA, Aurélio Buarque de Holanda. ***Novo Dicionário da Língua Portuguesa***. 2. ed. Rio de Janeiro : Nova Fronteira, 1986. p. 443.

A necessidade de instrumentos que auxiliassem o homem a processar informações, em apoio a suas funções mentais naturais, não é recente. Os homens primitivos fizeram os primeiros cálculos[4] com o uso dos dedos. Posteriormente, os antigos pastores passaram a utilizar pedras para contabilizar seu rebanho.

Desde a saída das árvores, na condição de australopiteco, até os tempos hodiernos, as ferramentas com as quais o homem agia se modificaram e se tornaram mais elaboradas e eficientes. A sociedade humana vive em constante mudança: mudou-se da pedra talhada ao papel, da pena com tinta ao tipógrafo, do código Morse à localização por *Global Positioning System* (GPS), da carta ao *e-mail*, do telegrama à videoconferência.

Contudo, não se pode prescindir da idéia de que a humanidade não teria alcançado o estado de evolução que apresenta hoje se não tivesse desenvolvido a capacidade intelectual de elaborar e transmitir informações. A primeira forma estruturada de transmitir informações se deu quando o homem adquiriu a capacidade de falar.

Em outro nível, as tribos primitivas usavam, como meios de comunicação à distância, sinais de fumaça ou sons de tambores, que podiam ser retransmitidos várias vezes, formando verdadeiras redes de comunicação que cobriam grandes áreas das florestas.

Com o advento da eletricidade, surgiu o telégrafo e, posteriormente, a telefonia. Paralelamente a esses desenvolvimentos, também ocorria o surgimento das primeiras máquinas eletrônicas, que depois passaram a ser conhecidas como um dos primeiros computadores. Com a conjugação dessas tecnologias, é que pessoas, grupos ou mesmo comunidades inteiras localizadas em quaisquer regiões da Terra podem se relacionar, atualmente, como se estivessem frente a frente de fato.

O desenvolvimento vertiginoso das tecnologias da informação e comunicações não está apenas transformando a nossa realidade; está criando

---

[4] A palavra cálculo vem do latim *calculus,* que significa pequena pedra.

uma nova realidade, um novo universo onde as dimensões do espaço são suprimidas e as leis da física são substituídas pelas leis da computabilidade.

Alvin Tofler[5] destacou, nos anos 70, a emergência de uma sociedade da informação. A sociedade da informação seria regida, segundo ele, por dois relógios: um analógico e um digital. O relógio analógico seria aquele cuja agenda segue um tempo físico. O relógio digital seria aquele cuja agenda segue um tempo virtual, acumulando uma série de ações que devem ser realizadas simultaneamente.

A sociedade da informação citada por Tofler tem suas origens na expansão dos veículos de comunicação. A evolução da humanidade, segundo ele, poderia ser dividida em três ondas. A primeira delas teve início quando a espécie humana deixou o nomadismo e passou a cultivar a terra. Essa Era Agrícola tinha por base a propriedade da terra como instrumento de riqueza e poder. A Segunda Onda tem início com a Revolução Industrial, em que a riqueza passa a ser uma combinação de propriedade, trabalho e capital. Seu ápice se dá com a Segunda Guerra Mundial, em que o modelo de produção em massa mostra a sua face mais aterradora: a morte em grande escala, causada pelo poderia industrial das nações envolvidas.

Como dito anteriormente, a chegada da Terceira Onda, a Era da Informação, começou a dar seus primeiros sinais ainda antes do apogeu da Segunda Onda, com a invenção dos grandes veículos de comunicação, como o telefone, o cinema, o rádio e a TV. Esses veículos, nos quais trafegam volumes crescentes de informação – a característica central da Terceira Onda -, conheceram sua expansão ainda a serviço do modelo de produção em grande escala, de massificação, centralização do poder e estandardização ditado pela Era Industrial.

A Era da Informação, a terceira revolução, caracterizou-se pela paulatina chegada dos computadores ao cotidiano das pessoas. Nessa fase, houve radicais mudanças de cultura e comportamento. Nos mais variados setores, tais máquinas se imiscuíram, em especial no de serviços. Seria

---

[5] TOFLER, Alvin. *A terceira onda*. Trad. João Távora. 28. ed. Rio de Janeiro: Record, 2005.

demasiado enumerar todos os exemplos de como a vida das pessoas foi substancialmente alterada com a chegada dos computadores; mas que se tratou de uma importante revolução, disso não se tem dúvida.

A Era Digital, quarta e última revolução que interessa neste trabalho, iniciou-se com a interligação dos computadores e ainda está em curso. Caracteriza-se pela introdução de um novo conceito de espaço (Ciberespaço) e pela efetiva utilização de uma nova ferramenta, a Internet.

É o surgimento da tecnologia digital, culminando na criação da Internet, que permite a consolidação da Era Digital, pela inclusão de dois novos elementos: a velocidade, cada vez maior na transmissão de informações, e a origem descentralizada destas.

Neste contexto, o grande computador é a Internet que, inquestionavelmente, se insere na vida das pessoas e a revoluciona, podendo-se compará-la à revolução que se operou na humanidade com a descoberta de Gutemberg, o livro impresso.

Nos tempos atuais, a humanidade, portanto, se vê diante da incrível velocidade das mudanças. A primeira (Revolução Agrícola) levou um pouco mais de 9.000 anos; a segunda (Revolução Industrial) cerca de três séculos; a terceira pouco mais de 25 anos e agora pouco mais de 15 anos. A Humanidade está frente a uma nova mudança, tão profunda, que alguns estudiosos arriscam afirmar que se encontram diante de uma nova civilização; a civilização da Revolução Digital, tendo a América do Norte como o palco principal deste novo período, chamado, por muitos, de Sociedade Pós-Industrial.

É importante frisar que essas revoluções se caracterizaram, principalmente, por estarem embasadas num sistema distinto de geração de riquezas. Mas todas, indistintamente, produziram efeitos e conseqüências que interferiram de forma marcante, causando mudanças nos diferentes sistemas político, social, cultural, filosófico, jurídico, ético e institucionais, entre outros.

O Homem na Sociedade da Informação (Sociedade Digital - no seu aspecto mais recente) passeia por milhares de informações distribuídas em seu

dia, até chegar ao sono que o ajuda a renová-las. A partir daí, o homem deste século não é mais o homem que sobreviveu no século passado, e assim por diante, necessita sobremaneira não mais da visão individualista como, aliás, concebiam os Sofistas[6], a qual se reduzia a seu ambiente próximo; mas da visão de mundo. Em virtude disso, hoje, para se estudar um fenômeno jurídico o intérprete não deve se ocupar apenas com o fato em si, mas também, com os outros fatos conexos, para que, através de várias visões do vínculo, absorva o real significado do todo que o envolve e assim possa especular sobre as realidades que são propostas.

Esse quadro evidencia de que maneira as novas tecnologias afetam o cotidiano das gentes, e o Direito, especialmente o penal, não pode ficar alheio a tão gritantes transformações. Essa exigência decorre do fato de que a criminalidade se amolda e também utiliza todo o ferramental tecnológico para a prática de condutas já historicamente tipificadas e outras a serem tipificadas.

## 2.2 A Sociedade da Informação e o Direito Penal

O fortalecimento da Sociedade da Informação veio proporcionar também a disseminação de mais uma forma de criminalidade, denominada de criminalidade digital. A exemplo do que ocorreu com a criminalidade econômica, ambiental, consumerista e financeira, todas caracterizadas pela enorme complexidade como se apresentam e todas com um ponto em comum, esse novo tipo traz consigo a ofensa a bens jurídicos de caráter coletivo ou até mesmo difuso.

Pensou-se inicialmente que o próprio mercado conseguiria impedir o mau uso da Internet por pessoas inescrupulosas. Imaginou-se, sinceramente, que

---

[6] Segundo CASTRO, José Carlos. **A Utopia Política Positivista e outros ensaios**, Belém : Cejup, 1999, p. 35, "Os Sofistas eram individualistas e subjetivistas. Ensinavam que cada homem possui seu modo próprio de ver e de conhecer as coisas. Daqui a tese, segundo a qual não é possível uma ciência autêntica, de caráter objetivo e universalmente válida, mas tão só opiniões individuais."

o Estado não teria a necessidade de interferir na Rede Mundial de Computadores, pois os próprios usuários já o fariam.

Contudo, com a sistemática invasão de *hackers* e *crackers* a grandes computadores de empresas e com a disseminação da pedofilia etc., fizeram com que a crença na auto-regulamentação caísse por terra, de forma que o ramo do Direito chamado de *ultima ratio*, não outro senão o Direito Penal, fosse instado a interferir. O fato é que o Estado teve que dirigir seus olhos para esse problema a fim de garantir a proteção a bens jurídicos preciosos para a sociedade.

Alguns aspectos propiciaram que o ambiente de Internet e redes se tornasse adequado aos criminosos, que vão desde inúmeras oportunidades e tentações de delitos existente nos sistemas até uma certa predisposição romântica para o crime, passando pela sensação de anonimato, certeza da falta de legislação, dificuldade em se investigar, coibir e julgar, além de uma série de ferramentas e facilidades para se cometerem tais atos criminosos

Importante ressaltar que tal busca por soluções mais drásticas, típicas do Direito Penal, ocorreu de modo uniforme pelo mundo; possivelmente em decorrência dessa universalização da Informação, com a conseqüente universalização da problemática dos crimes no ciberespaço. A preocupação, que inicialmente circunscrevia-se aos Estados Unidos da América, passou a ser de todos os países em que a Internet é uma realidade e onde, invariavelmente, há uma gama de delitos praticados no âmbito desta rede.

No Brasil, observa-se o pensamento de que o Direito está totalmente desatualizado com as atuais transformações. Alegam tais estudiosos que, pelo princípio constitucional do '*nullum crimen, nulla poena sine lege'* (que proíbe expressamente que se criem crimes por analogia), algumas condutas ficariam impuníveis pela atipicidade do fato, pois ausente é no ordenamento jurídico brasileiro uma legislação penal específica para o ambiente virtual.

É sabido que, infelizmente, os criminosos são mais rápidos que os legisladores, onde quer que se esteja. Ainda mais em se tratando de Internet, que, apesar do recente largo emprego, possui características ímpares, incomuns aos outros meios de comunicação.

Ao Contrário, o Direito Penal atualmente alberga muito das condutas delitivas cometidas nos ambientes virtuais, pois se pode aproveitar a maior parte da legislação em vigor. A principal mudança está, isso sim, na postura de quem a interpreta e faz sua aplicação. É errado, portanto, pensar que a tecnologia cria um grande buraco negro, no qual a sociedade fica à margem do Direito, uma vez que as leis em vigor são aplicáveis à matéria, desde que com sua devida interpretação. Mas é também equivocado o pensamento de que se pode prescindir de uma legislação penal específica, com o argumento de que a maioria das condutas são típicas no ordenamento jurídico brasileiro.

No combate aos crimes virtuais, a Justiça brasileira vem utilizando o Código Penal, capitulando a grande maioria das infrações penais cometidas através da Internet. Contudo, não se pode deixar de salientar que a edição de normas específicas para tipificação de tais condutas é bastante salutar; pois com isso criar-se-á no âmago da sociedade um efeito coercitivo e preventivo de tais condutas; além de oferecer segurança jurídica a todos os usuários escrupulosos.

Assim, os crimes praticados através da Internet, também denominados crimes de informática, crimes de computador, delitos computacionais, crimes telemáticos, crimes eletrônicos, cibercrimes, ciberdelitos ou crimes informacionais, por suas peculiaridades apresentam os seguintes problemas: de início, a falta de uma legislação penal e processual penal especiais, para a proteção de bens jurídicos informáticos em geral e de outros, como é o caso dos crime contra a honra, que possam ser violados através da Internet. Em seguida, vêm as questões de tipicidade, autoria, competência e territorialidade. Em momento oportuno, tais questões e outras - o bem jurídico a ser tutelado e a macrocriminalidade - serão enfrentadas neste trabalho.

Contudo, preliminarmente, pode-se antever a premente necessidade de uma legislação penal própria para os crimes praticados através da Internet. Concluindo, temos que, enquanto tal legislação não se fizer presente, conforme se verá, as Normas Penais vigentes podem e devem ser utilizadas para o combate a tais tipos de delitos. Assim, nessa seara, temos de início, que o Código Penal e as leis especiais – de Imprensa, Lei de Proteção aos Direitos Autorais, Lei

da Propriedade Industrial – são aplicáveis às condutas praticadas através do mundo virtual.

# 3 INTERNET

Neste capítulo é que se começa a navegar pela Internet, desvendando as suas nuances, abordando os seus ângulos mais importantes, a saber: surgimento e consolidação, conceito, funcionamento. Apresentará a história da Internet desde o tempo que ela ainda não era chamada por esse nome até o seu aparecimento no Brasil. Além disso, o funcionamento do *browser* e os tipos de componentes da Web também serão explanados. Dessa forma, poder-se-á entender como tal meio está sendo utilizado constantemente para o cometimento de crimes virtuais.

## 3.1 Surgimento e consolidação

Os primeiros registros de interações sociais que poderiam ser realizadas através de redes foi uma série de memorandos escritos por J.C.R. Licklider, do *MIT (Massachussets Institute of Technology)*, em agosto de 1962, discutindo o conceito da "Rede Galáxica". Ele previa vários computadores interconectados globalmente, por meio dos quais, poder-se-iam acessar dados e programas de qualquer local rapidamente. Em essência, o conceito foi muito parecido com a Internet de hoje.

Com o desenvolvimento dessa idéia de interação em nível global, ocorreram pesquisas no sentido de ser concretizável uma rede de grandes proporções, a fim de se promover uma rápida e eficiente comunicação, além do compartilhamento de recursos. Assim surgiu a ARPANET (*Advanced Research Projects Agency Network*), que foi um programa militar mantido pelo Departamento de Defesa dos Estados Unidos.

Essa rede possuía quatro nós, ligando três universidades e um instituto de pesquisa, e não era de acesso liberado ao público. Tal programa, criado em 1969, tinha por objetivo possibilitar a comunicação e transferência de

dados entre seus usuários através de canais redundantes, de forma que, mesmo na hipótese de destruição de partes da rede em uma eventual guerra, o funcionamento do sistema não restaria prejudicado.

O projeto consistia na criação de uma rede sem um centro estratégico, que não pudesse ser destruída por bombardeios e que fosse capaz de interligar pontos estratégicos, como centros de pesquisa e tecnologia. Uma outra motivação do governo americano para investir no desenvolvimento desta rede foi a Guerra Fria, pois tal rede possibilitaria a comunicação entre as bases militares, mesmo em caso de um ataque.

Em 1973, surgiu o Protocolo de Controle de Transmissão (*Transfer Control Protocol / Internet Protocol*), o Protocolo Internet, que é um código. Com isso, conseguiu-se permitir que diferentes *networks,* incompatíveis entre si, pelos seus programas e sistemas, pudessem se comunicar. Dessa forma a ARPANET começou a comunicar-se com outras redes, incluindo as existentes em outros países.

A utilidade das redes computadorizadas - especialmente o correio eletrônico - demonstrada por DARPA e pelo Departamento de Defesa dos Estados Unidos não foi perdida em outras comunidades, e, ainda na década de 1970, redes começaram a aparecer em qualquer lugar que dispusesse de fundos e recursos para isso.

Ao mesmo tempo em que a tecnologia Internet estava sendo experimentalmente validada e largamente utilizada por um conjunto de pesquisadores da ciência da computação, outras redes e tecnologias de rede estavam sendo criadas.

A ARPAnet se dividiu em duas categorias no ano de 1980. Uma categoria se destinava para fins civis, continuando com a denominação original; a outra, exclusiva para fins militares, foi nomeada de MILnet.

Em 1985, os Estados Unidos queriam ampliar o tamanho da sua rede, interligando todos os grandes centros. Não satisfeitos somente com os quatro nós iniciais da ARPAnet, fundaram a NSFnet (National Science Foundation).

O termo Internet utilizado atualmente teve sua origem em 1986 decorrente da fusão da rede NSFnet e ARPAnet. Somente um ano depois, em 1987, a Internet teve seu acesso liberado para uso comercial, não sendo mais restrito aos grandes centros de pesquisas norte-americano.

Em 1986, a Internet já estava bem estabelecida como uma larga comunidade de suporte de pesquisadores e desenvolvedores e começava a ser usada por outras comunidades para comunicações diárias pelo computador. O correio eletrônico já estava sendo usado por muitas comunidades, frequentemente com sistemas diferentes, mas a interconexão entre os diferentes sistemas de correio foi demonstrando a utilidade de comunicação eletrônica entre as pessoas.

Em 1989, em Genebra, foi criado o *World Wide Web* (Rede Mundial de Computadores), que conhecemos como *WWW* ou *Web*. São documentos onde os textos, as imagens e sons, são transmitidos de forma especial, denominada hipertextos e que podem ser relacionados com outros documentos. Com esse código a Internet invadiu o mundo. Assim também destaca, dentre os fatores que para a rápida aceitação da Internet, CORRÊA:

> A popularização da Internet aconteceu devido à criação da *World Wide Web*, ao desenvolvimento dois navegadores Netscape e Internet Explorer e ao barateamento e avanço das tecnologias empregadas no acesso à rede. A *World Wide Web*, possibilitou inovações no *layout* das páginas eletrônicas, uma vez que disponibilizou aos usuários, que se utiliza da Internet para navegar pela *www*, a utilização da imagem, som e movimento. Foi a integração entre imagem som, texto e movimento que levou a Internet ao desenvolvimento experimentado atualmente.

De acordo com VASCONCELOS, a Internet surgiu no Brasil em 1988, tendo logo uma rápida implantação e desenvolvimento. Seu desenvolvimento coube à Rede Nacional de Pesquisa (RNP), que foi uma iniciativa do Ministério da Ciência e tecnologia, que pretendia implementar uma infra-estrutura de serviços de Internet com abrangência nacional. A RNP possibilitou o desenvolvimento de muitas redes regionais em vários Estados do Brasil, facilitando a comunicação de dados através de uma estrutura nacional. Até hoje a RNP é o *backbone* principal

e envolve instituições e centros de pesquisa (FAPESP, FAPEPJ, FAPEMIG, etc.), universidades, laboratórios, etc.

Em 1993, surgiram os primeiros provedores de acesso à Internet no mundo, mas somente em 1995 a figura do provedor de acesso apareceu no Brasil.

Em 1994, no dia 20 de dezembro é que a EMBRATEL lança o serviço experimental a fim de conhecer melhor a Internet. Somente em 1995 é que foi possível, pela iniciativa do Ministério das Telecomunicações e Ministério da Ciência e Tecnologia, ser usada para outros fins além do educacional, abrindo as portas para o setor privado da Internet para exploração comercial, ocorrendo a partir daí uma grande expansão da Internet no Brasil. Assim, em maio de 1995, esta rede internacional deixa de se restringir às áreas de interesse da comunidade de educação e pesquisa; ocorrendo, dessa forma, a abertura da Internet comercial no país.

Vale salientar que, inicialmente, diferentemente do que ocorre atualmente, a Internet não era uma rede comercial; inclusive, antes do desenvolvimento da *World Wide Web*, os seus usuários seguiam regras de conduta que proibiam expressamente o uso da rede para estes fins. O uso comercial da Internet tornou a rede lenta e sobrecarregada. Surgiu, então, no seio da comunidade acadêmica, o projeto de criar uma rede de alto desempenho. A iniciativa em questão, uma verdadeira nova geração da Internet, caracterizada pela alta velocidade e pelas tecnologias multimídias em tempo real, sendo batizada de Internet 2.

Esta abertura deveu-se à Portaria 13, iniciativa conjunta dos Ministérios das Comunicações e da Ciência e Tecnologia, que possibilitou a operação comercial da rede no país ao criar a figura do provedor de acesso privado. Após a abertura da Internet comercial, o governo brasileiro procurou deixar a cargo da iniciativa privada a exploração dois serviços de Internet no país, não interferindo nas relações usuário-provedor; o que se observa claramente da análise dos itens 1.2 a 1.4 abaixo discriminados da Portaria em estudo.

> 1.2 O provimento de serviços comerciais na Internet ao público em geral deve ser realizado, preferencialmente, pela iniciativa privada.
> 1.3 O Governo estimulará o surgimento no País de provedores privados de serviços Internet, de portes variados, ofertando ampla gama de opções e facilidades, visando ao atendimento das necessidades dos diversos segmentos da Sociedade.
> 1.4 A participação das empresas e órgãos públicos no provimento de serviços Internet dar-se-á de forma complementar à participação da iniciativa privada, e limitar-se-á às situações onde seja necessária a presença do setor público para estimular ou induzir o surgimento de provedores e usuários.

Fazendo-se um resumo cronológico, destacam-se:

1969: Criação da ARPAnet;

1970: Começo da utilização dos emails;

1980: ARPAnet para fins civis e MILnet para fins militares;

1985: Criação NSFnet para interligar grandes centros;

1986: NSFnet se funde com a ARPAnet resultando na Internet;

1987: Internet para uso comercial;

1988: Primeiras conexões no Brasil;

1993: Primeiros provedores de acesso à Internet;

1995: Utilização comercial da Internet no Brasil.

## 3.2 Conceito

É gigantesco o universo que a Internet alcança. Pode-se consultar banco de dados em todos os países do mundo, visitar museus, faculdades e universidades, efetuar transações de compra e venda bancárias, enfim, uma gama infindável de serviços.

O avanço tecnológico, que provoca mudança nos hábitos sociais, tem como conseqüência gerar mudanças nas regras jurídicas. O crescente uso da rede, seja para consultar um saldo bancário, seja para comprar um livro, envolve envio ou recepção de informações, que devem ser protegidas. A rede é aberta a todos que se conectarem a ela; visita-se uma página, sobre qualquer assunto, à hora que quiser, porém, como ferramenta de comunicação fabulosa que é não deve sofrer censura. O que não se pode aceitar é que criminosos usem essa ferramenta.

A Internet é uma rede mundial de computadores interligados que permite o intercâmbio de arquivos entre usuários de quaisquer partes do mundo, constituindo-se em um poderoso meio de comunicação.

A supracitada Nota Conjunta de 1995 traz a definição de Internet em seu item 2.1, enumerando, ainda, serviços disponíveis na Net, à época de sua publicação.

> 2.1 A Internet é um conjunto de redes interligadas, de abrangência mundial. Através da Internet estão disponíveis serviços como correio eletrônico, transferência de arquivos, acesso remoto a computadores, acesso a base de dados e diversos tipos de serviços de informação, cobrindo praticamente todas as áreas de interesse da Sociedade.

O Grande Dicionário Larousse traz a seguinte definição:

> Internet – s.f. (ingl.) Rede internacional de computadores que, por meio de diferentes tecnologias de comunicação e informática, permite a realização de atividades como correio eletrônico, grupos de discussão, computação de longa distância, transferência de arquivos, lazer, compras, etc.

Como observa Marcel Leonardi:

> A Internet não é uma entidade física ou tangível, mas sim uma rede gigante que interconecta inúmeros pequenos grupos de redes de usuários conectados por sua vez entre si. É, portanto, uma rede de redes. Algumas das redes são fechadas, isto é, não interconectadas com outras redes ou usuários. A maior parte das redes, no entanto, está conectada através de redes que, por sua vez, estão conectadas a outras redes, de maneira que permitam a cada um dos usuários de qualquer delas comunicar-se com

> usuários de quaisquer outras redes do sistema. Esta rede global de usuários e redes de usuários vinculados é conhecida como Internet.

Também esclarecedor é o conceito de Internet dado por Gustavo Testa Corrêa:

> É um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento.

Além desses conceitos, Ivete Senise Ferreita conceitua a rede mundial da seguinte maneira:

> Podemos definir Internet como uma gigantesca rede mundial de computadores, interligados por linhas comuns de telefone, linhas de comunicação privadas, cabos submarinos, canais de satélite e diversos outros meios de telecomunicação.

Assim, a Internet é um conjunto de redes de computadores interligados que têm em comum um conjunto de protocolos e serviços, de forma que os usuários conectados possam usufruir os serviços de informação e comunicação.

É como se as pessoas estivessem em uma cidade eletrônica, já que na Internet podem-se encontrar bibliotecas, bancos, museus, previsões do tempo e ainda acessar a bolsa de valores, conversar com outras pessoas, pedir uma pizza, comprar livros ou CDs, ouvir música, ler jornais e revistas, ter acesso a banco de dados, ir ao *Shopping Center* e muito mais. É um verdadeiro mundo *on-line*.

Portanto, a Internet é, ao mesmo tempo: a união de um enorme número de redes ao redor do mundo que se comunicam através do protocolo TCP/IP; uma comunidade de pessoas que usam e desenvolvem estas redes; uma coleção de recursos que podem ser alcançados através destas redes.

## 3.3 Funcionamento

Como visto, a Internet é uma grande rede das redes, o que significa dizer que ela representa inúmeros computadores interligados através de redes, sendo a conexão a esta rede possibilitada através da banda larga (*cable-modem*, ADSL-*modem*, radio-modem) ou por um *modem* normal.

A mencionada Nota Conjunta (1995) enumerou as características básicas do funcionamento da Internet:

> 2.2 A Internet é organizada na forma de espinhas dorsais *backbones,* que são estruturas de rede capazes de manipular grandes volumes de informações, constituídas basicamente por roteadores de tráfego interligados por circuitos de alta velocidade.
> 2.3 Interligadas às espinhas dorsais de âmbito nacional, haverá espinhas dorsais de abrangência regional, estadual ou metropolitana, que possibilitarão a interiorização da Internet no País.
> 2.4 Conectados às espinhas dorsais, estão os provedores de acesso ou de informações, que são os efetivos prestadores de serviços aos usuários finais da Internet, que os acessam tipicamente através do serviço telefônico.
> 2.5 Poderão existir no País várias espinhas dorsais Internet independentes, de âmbito nacional ou não, sob a responsabilidade de diversas entidades, inclusive sob controle da iniciativa privada.

Mais simplificadamente, cada computador conectado à Internet é parte dessa rede. Quando um usuário doméstico utiliza a rede, através de seu provedor de acesso, seu computador conecta-se à rede daquele provedor. Este, por sua vez, conecta-se a uma rede ainda maior e passa a fazer parte desta, e assim sucessivamente; possibilitando o acesso, dentro de certas condições, a qualquer outro computador conectado à Internet.

Dentro do funcionamento dessa imensa rede de comunicação, pode-se afirmar que cada país participante da Internet possui estruturas principais de rede, chamadas de *backbones*, com conectividade através do protocolo TCP/IP (*Transmission Control Protocol / Internet Protocol*), aos quais se interligam centenas ou milhares de outras redes. Os *backbones* nacionais, por sua vez, são

conectados entre si aos backbones de outros países, compondo, assim uma gigantesca rede mundial

O ato de o usuário conectar-se a diferentes computadores é chamado de navegação na Internet. O usuário, uma vez conectado, explora o mundo virtual, também chamado de ciberespaço. Já o site ou sítio corresponde ao local onde estão armazenadas as páginas pertencentes a um endereço ou domínio da Internet. No mesmo raciocínio, tem-se que o servidor é o computador responsável por administrar, fornecer programas e repassar informações para os computadores conectados.

O funcionamento da navegação pela WEB ocorre da seguinte forma: cada pedido solicitado via http *(Hyper Text Transfer Protocol*) é enviado a um servidor que procura a solicitação e, quando encontra o domínio solicitado, envia uma resposta ao usuário. O caminho dos dados começa, então, na máquina do internauta; segue para o provedor de acesso, que processa o pedido e envia a resposta para o computador que solicitou a informação. Neste caminho, o trabalho do provedor é encontrar os dados que o usuário pede, e o da companhia que oferece o serviço em banda larga é propiciar o canal para que esse conteúdo possa fluir.

Assim, observa-se que o funcionamento da Internet se dá, basicamente, pela transferência de informações, através de uma linguagem comum ou protocolo, que possibilita aos usuários individuais interagirem com qualquer outra rede ou usuário individual que seja também parte do sistema. Com isto, se quer dizer que na Internet várias barreiras são rompidas por um simples motivo, todos falam a mesma linguagem, qual seja, o protocolo IP.

Tudo que é transmitido pela Internet é transformado, se faz por meio de pacotes que são identificados em seu ponto de origem, por meio do endereço do solicitante e pelas instruções de destino. Estes pacotes são enviados através de redes interligadas, para serem remontados no ponto de destino.

Observa-se assim que a Internet não tem dono, não pertence a nenhum país ou empresa, o que faz com que a rede não seja de ninguém, não possua um poder central. Quanto a este aspecto, diferencia-se de uma rede

menor; que, mesmo conectada à Internet, pode pertencer a uma empresa, a uma universidade ou a qualquer outra organização

O usuário, para ingressar na rede e poder usufruir de toda a gama de serviços que ela oferece, necessita ter um computador, um modem, um programa denominado de *browser* e, geralmente, uma linha telefônica; pois hoje já existem meios que dispensam o uso da linha convencional, como as ligações via cabos de fibra óptica e via rádio. Além disso, são necessários os chamados provedores de acesso que fornecem os recursos técnicos e materiais, que efetivamente concretizam a entrada dos usuários na Grande Rede. Dessa forma, é salutar um estudo superficial do funcionamento do *browser* e do Provedor.

### 3.3.1 Funcionamento do *browser*

A navegação na Internet ocorre através de programas chamados *Browser*[7]. A *web* possui três componentes de *softwares* principais, são eles: o cliente, o *proxy* e servidor. O usuário final tem mais contato com o cliente, que é o *browser*. Tecnicamente, são denominados de *browsers* os *softwares* que realizam a interface entre usuário e a *web*.

Atualmente, os clientes realizam operações são complexas, tais como: ativar programas para interpretar e exibir respostas, capacidade de fazer cachê das páginas visitadas para diminuir o tempo de resposta em um pedido futuro, etc.

Hoje em dia, o *browser* é conhecido também como agente de usuário, pois ele que inicia um pedido da *web*. Os *browsers* modernos também aprimoraram e modernizaram o mecanismo de *hyperlinks*, permitindo que usuários navegassem sem emendas. Assim surgiram o Netscape e o Internet *Explorer*.

---

[7] É a palavra em inglês para designar os programas de navegação na Internet.

Nesse sentido, um *browser* típico é um cliente da *web* que realiza basicamente as seguintes tarefas: *constrói* e envia o pedido feito pelo usuário, recebe no destino, analisa e apresenta a resposta para o usuário.

A série de pedidos enviados pelo usuário com base nas respostas do servidor é chamada de sessão, ela pode durar poucos minutos como também bem mais. Antes do envio do pedido com a URL[8] desejada, o cliente cria uma conexão com o servidor e no final da sessão a conexão é encerrada.

Oportunamente, exemplifica-se que, ao digitar o endereço http://www.cade.com.br o *browser* analisa primeiramente o conteúdo que vem antes do ":", que é o tipo de protocolo[9]. O protocolo será usado para buscar o recurso e no caso acima é o protocolo HTTP[10], mas poderia ser outro tipo como o FTP[11], etc.

### 3.3.2 Funcionamento do Provedor

Outro elemento essencial para que o usuário doméstico usufrua da rede é a interferência de um provedor. O vocábulo 'provedor' de prover, do latim '*providere'* (olhar por, providenciar acerca de), na linguagem da Informática, designa instituição que tem computador (es) conectado (s) a uma grande rede (p. ex., a Internet) e que oferece acesso a essa rede para outros computadores.

Por sua vez, leciona a professora Liliana Minardi Paesani:

> Os provedores são sujeitos privados, empresários ou entidades acadêmicas que viabilizam ao usuário, consumidor ou empresário,

---

8 A sigla URL significa Uniform Resource Location, ou seja, localização uniforme de recursos. Pode ser obtida de diversos meios como clicando em um link, digitando o endereço em um campo espeífico no browser ou então por meio do histórico de navegação do usuário, chamado de Bookmarks.

9 Tipo de código que possibilita a comunicação entre computadores diversos.

10 É a sigla para 'Hyper Text Transfer Protocol' (Protocolo de Transferência *de* Hipertexto), que é um protocolo que permite o funcionamento da interface gráfica na Internet.

11 Sigla de File Transfer Protocol (Protocolo de Transferência de Arquivos), que é um dos protocolos que permite a transferência de arquivos de um computador para outro pela Internet.

> a conexão com a Internet e, eventualmente, outros serviços, por período determinado, mediante remuneração ou de forma gratuita.

O conceito supracitado é o de provedor de acesso ou conexão, que é a instituição que serve obrigatoriamente de elemento de ligação entre o usuário e a Internet, por oferecerem estrutura técnica garantidora do acesso à rede. É, assim, a Instituição que se liga à Internet, partindo de um "ponto-de-presença" ou outro provedor, para obter conectividade IP e repassá-la a outros indivíduos e instituições, em caráter comercial ou não.

A função de um provedor de Internet é caracterizada por diversos fatores, dentre eles a possibilidade de possuir a conexão *full time* à rede mundial através de um *backbone.* Essas conexões são feitas através de circuitos de comunicação ponto a ponto, conhecidas como *links.* Geralmente, um provedor de grande porte faz a ligação com os provedores menores, através dos quais os usuários de computadores se conectam à rede mundial. Dessa forma ocorre o acesso à Internet.

Além deste, existem outros tipos de provedor: o provedor de conteúdo e informação, e o de hospedagem. O provedor de informação é o organismo cuja finalidade principal é coletar, manter ou organizar informações on-line para acesso através da Internet por parte de assinantes da rede.

Já o Provedor de serviço (*Internet Service Provider*) engloba tanto o provedor de acesso, quanto o de informação. É a união do provedor de acesso com o de conteúdo. Existe também o provedor de hospedagem ou *hosting*, que tem como principal função alojar páginas e sites.

Cabível é esclarecer que algumas empresas provedoras podem prestar conjuntamente os serviços de *Internet Service Providers* (ISP), *Hosting Service Providers* (HSP) e *Access Service Providers* (ASP), tornando-se um complexo fornecedor de serviços no mercado de consumo da rede mundial de computadores.

# 4 INTERNET E A MACROCRIMINALIDADE

Com o advento das redes, houve considerável diminuição das distâncias, corolário da velocidade com que as informações transitam pelo mundo. Portanto, o vetor espaço merece reavaliação, especialmente do operador do Direito, que, em permanente exercício de construção, deve adaptar essa nova realidade ao ordenamento jurídico existente. Dessa forma, tal reavaliação será realizada neste tópico através da construção doutrinária do tema.

## 4.1 O Fenômeno da Macrocriminalidade

Conforme mencionado, a Internet é um poderoso meio de comunicação, uma vez que trouxe maiores possibilidades de relacionamentos entre as pessoas do que qualquer outro meio já existente. Com a popularização da Internet, a distância entre duas pessoas tornou-se quase irrelevante, já que quaisquer usuários, independentemente do país onde se encontrem, passaram a trocar dados e informações instantaneamente.

Com a mitigação da distância, ocorreu um aumento significativo nas possibilidades de interações entre os usuários. Tais interações passaram a ser reguladas no ordenamento jurídico de diversos países. Assim, ante a essa crescente profusão de novas relações jurídicas criadas na Internet, leis foram adotadas em diversos países, visando à proteção dos indivíduos que estão inseridos nesta nova comunidade virtual.

Contudo, as novas tendências na área econômica internacional, decorrentes, principalmente, dessa revolução informacional, na qual a distância passou a ser mitigada pelas relações quase diretas, trouxeram à tona a incapacidade de o Estado Nacional e do Direito, em regular estas novas atividades e relações, que romperam com a tradicional concepção de Estado -

Nação, como associação soberana reguladora e como instrumento de controle estatal.

Na seara do Direito Penal, observa-se, assim, o aparecimento de uma nova figura conhecida como macrocriminalidade, que rompe os limites territoriais, criando uma rede de criminalidade mundial, sem respeito à soberania ou qualquer sistema de acordo internacional realizado entre os Estados. É o caso dos crimes cometidos por meio da Internet, considerando o avanço da macrocriminalidade e a dependência do sistema informático entre os Estados, em virtude da globalização das informações e comunicações

Nas palavras do então Ministro do Superior Tribunal de Justiça Antônio de Pádua Ribeiro "a crise do judiciário é um aspecto da crise do próprio Estado. Sem se organizar e dar eficiência ao Estado administrador e ao Estado legislador, deficiente continuará o Estado justiça"[12]. Isto tudo, numa visão micro de todo um sistema macro, isto é, se for analisada a crise interna pela qual passam os Estados, é possível entender o crescimento da crise internacional, seja no âmbito social, econômico ou criminal.

Desta forma, os últimos anos demonstraram claramente a nova visão e característica da criminalidade mundial; uma criminalidade transnacional com interesses à superação dos limites territoriais, possibilidade cada vez mais tranqüila com o desenvolvimento da Internet; acarretando a desconstituição dos Estados-Nações, o que impede ou dificulta a detecção, o processamento e a punição de tais crimes que integram esta macrocriminalidade.

Podem-se citar como exemplos de crimes da macrocriminalidade, os delitos informáticos, econômicos, tributários, ambientais, criminalidade no comércio exterior, contrabando internacional de armas, drogas, órgãos, entre outros; todos permeados por características comuns, sendo que as principais são: geralmente a ausência de vítimas individualizadas; pouca visibilidade dos danos causados; bens jurídicos supra-individuais, universais ou vagos; novo e específico *modus operandi*; ausência de violência física e muita organização.

---

[12] PADUA RIBEIRO, A. de. O judiciário como poder político no século XXI, p.42.

Em síntese, “criminalidade organizada, criminalidade internacional e criminalidade dos poderosos são, provavelmente, as expressões que melhor definem os traços gerais da delinqüência da globalização”[13]

Estas novas dificuldades obrigam o Direito a rever conceitos, alargando interpretações que até então eram restritas e controladas através da soberania, jurisdição e competência (determinação territorial, extradição, princípio da extraterritorialidade da justiça universal). A macrocriminalidade, incluindo, portanto, os crimes informáticos ou crimes digitais, suscitou problemas sérios para a comunidade jurídica, eis que os crimes informáticos estão no ápice da criminalidade contemporânea.

A grande questão pontuada pela evolução tecnológica, no intuito de uma premente necessidade de intensificação para a internacionalização de um Direito Penal e Processual comuns, é saber como se deve reger, de modo uniforme, a comunicação eletrônica, a partir de regramentos jurídicos pertinentes a cada nação ou, ainda, como aplicar os acordos, tratados e convênios internacionais assinados sobre a informática, quando os pontos de transmissão e recepção se encontram fora dos países signatários.

Em relação aos crimes informáticos, que são o maior exemplo da evolução da criminalidade decorrente dos avanços tecnológicos, Gustavo Testa Corrêa prevê que os “criminosos investirão em alta tecnologia e conhecimento, e, assim, como historicamente extorquiram policiais, políticos, médicos, advogados, etc. passarão a extorquir cientistas e programadores”[14].

## 4.2 O ciberespaço

Observa-se que a Internet não tem dono, nacionalidade nem território, permitindo que o internauta se relacione com pessoas das mais diversas nacionalidades, sem necessitar de saber onde elas estão e, muito menos, sob

---

13 SILVA SANCHEZ, J-M. A expansão do direito penal, p. 80.

14 CORRÊA, G. T. Aspectos jurídicos da Internet, p. 56.

qual jurisdição estão subordinadas. Estas características possibilitam que os crimes praticados através da Internet possam atingir várias pessoas em territórios diversos, com leis distintas.

Por isso, o ciberespaço é, e continuará sendo, nas palavras de Santiago Muñoz Machado[15], "*um fertilíssimo caldo de cultivo para a transformação não só da economia e da sociedade, como também do Direito nas próximas décadas"*, fato novo trazido pela era da globalização. E, no que concerne à globalização jurídica, far-se-á necessária a criação de instituições legislativas, executivas e judiciais mundiais para atender os problemas dela decorrentes; pois qualquer regulação, para que não reste inócua, deve ser feita numa escala de referência globalizada.

No ciberespaço, cada indivíduo é, potencialmente, um emissor e um receptor de um meio qualificadamente e, quantificadamente diferenciado, uma vez que todos se comunicam com todos. Os internautas não se localizam principalmente por seus nomes, posição social, localização geográfica, senão a partir de centros ou sites de interesses mútuos, uma comunicação recíproca, interativa e ininterrupta.

O filósofo Pierre Lévy, apontado como o ícone na análise dos territórios real e virtual, nome respeitado no mundo das tecnologias da informação, materializa da seguinte forma sua compreensão sobre o ciberespaço:

> O ponto fundamental é que o ciberespaço, conexão de computadores do planeta e dispositivo de comunicação ao mesmo tempo coletivo e interativo, não é uma infra-estrutura: é uma forma de usar as infra-estruturas existentes e de extrapolar os seus recursos por meio de uma inventividade distribuída e incessante que é indissociavelmente social e técnica. [...] o ciberespaço não é uma infra-estrutura territorial e industrial clássica, mas um processo técnico-social auto-organizador, finalizado a curto prazo por um imperativo categórico de conexão (a interconexão é um fim em si) visando de forma mais ou menos clara um ideal de inteligência coletiva que já está amplamente em prática[16].

---

15 *Apud* ROSSINI, A. E. S. Informática, telemática e Direito Penal, p. 165.

16 Idem.

Mais adiante, o mesmo autor traça interessante paralelo entre os territórios físico e virtual:

> O território é definido por seus limites e seu centro. É organizado por sistemas e proximidades física ou geográfica. Em contrapartida, cada ponto do ciberespaço é em princípio copresente a qualquer outro, e os deslocamentos podem ser feitos à velocidade da luz. Mas a diferença entre os dois espaços não se deve apenas a propriedades físicas e topológicas. São também qualidades de processos sociais que se opõem. As instituições territoriais são antes hierárquicas e rígidas, enquanto as práticas dos cibernautas têm tendência a privilegiar os modos transversais de relação e fluidez das estruturas. As organizações políticas territoriais repousam sobre a representação e a delegação, enquanto as possibilidades técnicas do ciberespaço tornariam facilmente praticáveis formas inéditas de democracia direta em grande escala etc.

E arremata, dizendo que os dois espaços, ao contrário de se excluírem, se complementam:

> Articular os dois espaços não consiste em 'eliminar' as formas territoriais para 'substituí-las' por um estilo de funcionamento ciberespacial. Visa antes compensar, no que for possível, a lentidão, a inércia, a rigidez indelével do território por sua exposição em tempo real no ciberespaço. Visa também permitir a solução e, sobretudo, a elaboração dos problemas da cidade por meio da colocação em comum das competências, dos recursos e das idéias.
> (...)A perspectiva aqui traçada não incita de forma alguma a deixar o território para perder-se no 'virtual', nem que um deles 'imite' o outro, mas antes a utilizar o virtual para habitar ainda melhor o território, para tornar-se seu cidadão por inteiro.

O panorama apresentado por Gustavo Testa Correa esclarece o que denomina de comunidade virtual:

> O conjunto de pessoas interligadas eletronicamente, comunicando-se por meio de uma nova linguagem, representava a transformação do mundo linear, especializado e visual, criado pela mídia impressa num mundo simultâneo, holístico e multissensorial, propiciado pela mídia eletrônica. Antes, era uma coisa atrás da outra, uma de cada vez. Hoje, é tudo ao mesmo

> tempo, em todo lugar. Na aldeia global, tudo se fala, tudo se ouve[17].

As principais características deste "Direito do Espaço Virtual", denominação apresentada por Newton De Lucca[18], são a multidisciplinariedade (principalmente com a engenharia eletrônica), o cosmopolitismo (que está a exigir os códigos Deontológicos, de Ética ou de boa conduta) e a tecnicalidade (marcado por conceitos técnicos). Tal espaço é híbrido e possibilita um fórum heterogêneo, permitindo que o sujeito viva a possibilidade de inúmeras ambivalências.

Nestes novos espaços sociais nascem mecanismos de participação nunca antes imaginados, novas formas de democracia, de decisão, de negociação, de cooperação, de sociabilidade envolvendo o local e o global, entre o eu e o anonimato, promovendo o encontro entre o ser produtor e consumidor de conhecimentos à escala global, entre a nacionalidade e o cosmopolitismo.

Assim, o Ciberespaço é um novo ambiente humano e tecnológico de expressão, informação e transações econômicas. Consiste em pessoas de todos os países, de todas as culturas e linguagens, de todas as idades e profissões fornecendo e requisitando informações; uma rede mundial de computadores interconectada pela infraestrutura de telecomunicações que permite à informação em trânsito ser processada e transmitida digitalmente.

Evidencia-se por tudo o que foi transcrito que o Ciberespaço é uma realidade que já faz parte da vida humana moderna, mesmo porque a Rede Mundial (Internet) é utilizada por milhões de viventes que se comunicam, compram, vendem, conversam, exprimem os seus sentimentos por meio dela. Resta saber se o ordenamento jurídico está habilitado a resolver os problemas advindos desta potencializada e virtual interconexão.

---

[17] CORRÊA, G. T. *Aspectos jurídicos da Internet*, p. 46.

[18] PAESANI, Liliana Minardi. *Direito de informática: comercialização e desenvolvimento internacional do Software*. São Paulo: Atlas, 2005.

Respondendo a tal questionamento, Vicente Greco Filho defende que a Internet não é diferente de outras conquistas tecnológicas, e critica a tentativa de se ver uma dicotomia entre o real e o virtual, afirmando a inexistência desta última realidade: "a realidade não comporta qualificativos. "A realidade é, e pronto. Não existe a menor razão para bajular os meios eletrônicos, atribuindo-lhes o poder de ter criado uma realidade diferente[19]". Para o autor, a Internet não passa de mais uma pequena faceta da criatividade do espírito humano e como tal deve ser tratada pelo Direito, especialmente o Penal, concluindo que:

> Evoluir, sim, mas sem correr atrás, sem se precipitar e, desde logo, afastando a errônea idéia de que a ordem jurídica desconhece ou não está apta a disciplinar o novo aspecto da realidade. E pode fazê-lo no maior número de aspectos, independentemente de qualquer modificação. [...] Como se vê, as ditas situações modernas não são tão modernas assim. Podem as circunstâncias torná-las mais importantes, mais danosas e, até, mais interessantes, mas não cabe ao Direito Penal entendê-las como um fenômeno diferente do comportamento irregular na humanidade. A conclusão, portanto, salvo demonstração em contrário, é a de que devemos deixar o Direito Penal em paz, porque está ele perfeitamente apto a atender à proteção dos direitos básicos das pessoas, e se houver alguma modificação a fazer, deve ser feita dentro de uma perspectiva de proteção genérica de um bem jurídico[20].

Assim, esta nova realidade não é perniciosa ao ser humano, muito ao contrário, pois as virtudes, os dons, enfim, todas as potencialidades podem ser exercidas de forma exponencial neste novo universo que se descortina. E não seria demais afirmar que nesta seara a proteção de tantos interesses legítimos também é tarefa do Direito.

Nessa mesma linha é a análise de Augusto Eduardo de Souza Rossini, que acredita ser possível, com algumas poucas adaptações legislativas, além de esforço interpretativo, o atual ordenamento jurídico resolver os problemas advindos do ciberespaço:

---

[19] GRECO FILHO, V. Algumas observações sobre o direito penal e a Internet.
[20] Idem.

> Em verdade, onde o humano age e interage, o Direito existirá, sob o risco de estabelecer o caos, que, por óbvio, é autofágico e limitador. Não permitir que regras jurídicas atuem também neste novo espaço é convir que o Ciberespaço não existe, ou não merece existir, o que não é verdade[21].

Pode-se concluir que o ordenamento jurídico está apto a enfrentar eficientemente tal realidade, bastando algumas poucas adaptações legislativas, além de esforço interpretativo. Dessa forma, a Internet e os espaços criados por ela não trazem nada de intrinsecamente novo: praticamente tudo o que podemos fazer através deles, poderíamos fazer de outra forma, sem o auxílio do computador, este em ambiente telemático ou não. O que eles modificam é a velocidade e a escala em que as trocas de informações ocorrem.

Por conseguinte, quanto à questão da jurisdição e competência no ciberespaço, tal tema será tratado em tópico próprio. Concluindo-se com a análise sobre a necessidade de uma *ciberjusticia*[22] com extraterritorialidade internacional ou uma jurisdição internacional para crimes cometidos no ciberespaço, tal questão será tratada no tópico seguinte.

## 4.3 A Macrocriminalidade e o Universalismo Jurídico

Sobre seu território o Estado exerce jurisdição, o que vale dizer que detém uma série de competências para atuar com autoridade; é o Estado soberano com jurisdição geral e exclusiva. Esta generalidade da jurisdição significa que o Estado exerce no seu domínio territorial todas as competências de ordem legislativa, administrativa e jurisdicional. Tal exclusividade permite que o Estado local não enfrente a concorrência de qualquer outra soberania, detentor que é do monopólio do uso legítimo da força.

---

[21] ROSSINI, A. E. S. Informática, telemática e Direito Penal, p. 166 e 170.
[22] Termo de MUÑOZ MACHADO. *Apud* ROSSINI, A. E. S. Informática, telemática e Direito Penal, p. 169.

Na sociedade internacional, as cortes internacionais não têm sobre os Estados soberanos aquela autoridade congênita que os juízes e tribunais de qualquer país exercem sobre pessoas e instituições encontráveis em seu território de impor o cumprimento das decisões. Enquanto a jurisdição nacional impõe-se pela ação cogente do Estado a indivíduos, empresas e entidades de direito público, a jurisdição internacional só se exerce, equacionando conflitos entre soberanias, quando estas previamente deliberam submeter-se à autoridade das cortes.

José Francisco Rezek ressalta, numa perspectiva do Estado - Nação não integrado, que "a mais notável dentre as características da soberania do Estado é exatamente a prerrogativa de negar ou pôr em dúvida a estabilidade de seus pares, sem que qualquer poder supranacional lhe imponha, a respeito, uma definição irrecusável"[23].

Com as crescentes mudanças no âmbito supranacional, será necessária uma nova concepção de soberania por parte dos Estados, mesmo porque, atualmente, vários são os fenômenos que limitam substancialmente a soberania de um Estado, pode-se destacar, entre outros: a crescente interdependência no plano econômico, social, ecológico e cultural; o desenvolvimento de novas formas de integração e comércio entre os Estados; a existência das grandes empresas transnacionais, que, apesar de não gozarem de soberania, são capazes de influenciarem fortemente e direcionarem a política de governo dos países , no que se refere aos aspectos econômicos da produção e circulação de riquezas.

Dessa forma, parece mais condizente com a conjuntura mundial o pensamento de desenvolvimento de um Direito Positivo Universal, onde o conceito de soberania é repensado e estudado levando-se em conta os vários fatores de interdependência entre os Estados. Por isso o entendimento de Norberto Bobbio:

> O universalismo jurídico ressurge hoje não mais como crença num eterno Direito Natural, mas como vontade de constituir um Direito positivo único, que recolhe em unidade todos os Direitos positivos

---

23 REZEK, J. F. Direito internacional público, p. 87.

existentes e que seja produto não da natureza, mas da história, e esteja não no início do desenvolvimento social e histórico (como o Direito natural e o estado de natureza), mas no fim. A idéia do Estado mundial único é a idéia limite do universalismo jurídico contemporâneo[24].

[24] BOBBIO, N. Teoria do ordenamento jurídico, p. 164.

# 5 DO DELITO INFORMÁTICO

Após as imprescindíveis digressões supracitadas, passar-se-á propriamente ao estudo dos delitos informáticos. Neste tópico serão enfrentados alguns pontos relevantes, senão vejamos: O conceito, a classificação e o bem jurídico dos delitos informáticos. Nesse tópico serão analisados também os sujeitos ativo e passivo do delito informático.

## 5.1 Conceito

Sem definir o conceito, não sabemos bem onde começa e onde termina uma coisa. O conceito nos dá a forma, o sentido das coisas. Daí a necessidade de pelo menos tentar encontrar um conceito que dê forma e sentido ao que aqui se denomina “Delito Informático”.

Na Literatura hodierna, várias denominações são encontradas: “crime informático”, “crime por computador”, “crime de informática”, “abuso de informática”, “abuso de computador”, “crime de computação”, “delinqüência informática”, “fraude informática”, “crimes virtuais”, “crime de computador”, “crime eletrônico”, “crime digital”, “crime cibernético”, “infocrime”.

Cláudio Líbano Manzur, secretário executivo da Associação de Direito e Informática do Chile, define “crimes cibernéticos” como sendo:

> Todas aquelas ações ou omissões típicas, antijurídicas e dolosas, trate-se de fatos isolados ou de uma série deles, cometidos contra pessoas naturais ou jurídicas, realizadas em uso de um sistema de tratamento da informação e destinadas a produzir um prejuízo na vítima através de atentados à sã técnica informática, o qual, geralmente, produzirá de maneira colateral lesões a distintos valores jurídicos, reportando-se, muitas vezes, um benefício ilícito

> no agente, seja ou não de caráter patrimonial, atue com ou sem ânimo de lucro[25].

Reginaldo César Pinheiro lança seu conceito de crime informático como sendo: *toda conduta positiva ou negativa (ação ou omissão), praticada total ou parcialmente no ambiente informático e que venha causar algum prejuízo à vítima, seja ele patrimonial ou não*[26].

Maria de La Luz Lima assevera que:

> Em um sentido amplo é qualquer conduta criminógena ou criminal que em sua realização faz uso da tecnologia eletrônica seja como método, meio ou fim e que, em um sentido estrito, o delito informático é qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel seja como método, meio ou fim[27].

A Faculdade de Direito da Universidade Nacional Autônoma do México – UNAN, ao elaborar o Estudo "Delitos Informáticos: proposta para o tratamento da problemática no México"[28], definiu os delitos informáticos como *todas aquelas condutas ilícitas suscetíveis de ser sancionadas pelo direito penal, que fazem uso indevido de qualquer meio informático*.

Otto Banho Licks e João Marcelo de Araújo Júnior definem "crime de informática" como sendo:

> A conduta que atenta, imediatamente, contra o estado natural dos dados e recursos oferecidos por um sistema de processamento, armazenagem ou transmissão de dados, seja em sua forma, apenas compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenamento de dados, seja na

---

25 LÍBANO MANZUR, Cláudio. Chile: Los delictos de hacing em sus diversas manifestaciones. In: Revista Electrónica de Derecho Informático, n.21, abr.2000. Disponível em: <http://publicaciones.derecho.org/redi>, apud Reginaldo César Pinheiro. Os crimes virtuais na esfera jurídica brasileira. Boletim IBCCRIM – Publicação Oficial do Instituto Brasileiro de Ciências Criminais. São Paulo, ano 8, n.101, p. 18-19.

26 Os crimes virtuais na esfera jurídica brasileira. Boletim IBCCRIM – Publicação Oficial do Instituto Brasileiro de Ciências Criminais. São Paulo, ano 8, n.101, p. 18-19.

27 Delitos electrónicos. In: Criminalia. Academia Mexicana de Ciencias Penales. N. 1-6, año L, Enero-Junio. México: Ed. Porrúa. 1984. P.100, Apud Reginaldo César Pinheiro, op. cit., p.26.

28 Disponível em <http://tiny.uasnet.mx/prof/cls/der/silvia/index.htm>, apud Reginaldo César Pinheiro, op. Cit., p.27.

> sua forma compreensível pelo homem(...). Em segundo lugar, o crime de informática é aquele que atentando contra estes dados, o faz de forma também compreensível por um sistema de tratamento, transmissão ou armazenamento de dados[29].

Em outra obra[30], Araújo Júnior assevera que:

> (...)No atual estágio do desenvolvimento científico, o conceito de criminalidade informática deverá girar em torno da idéia de direito de informação e de direito de informática, nos quais a informação, o ambiente e a relevância econômica serão fatores fundamentais. A Informação há de ser considerada como um bem de valor econômico, cultural e político, além de se haver transformado num potencial de risco específico. O ambiente há de ser tratado como um elemento gerador de confiabilidade e segurança da informação, a despeito de sua vulnerabilidade. Esse novo modo de ver as coisas, torna evidente que os bens intangíveis devem ser tratados de forma inteiramente diferente daquela pela qual são tratados os crimes tradicionais, de caráter material. Diante disso, é, a nosso juízo, indispensável a mudança de paradigmas.

E traz a seguinte definição de *computer crime*:

> (...)caracteriza-se por ser uma conduta lesiva, dolosa, à qual pode corresponder ou não a obtenção de uma indevida vantagem, porém cometida, sempre, com a utilização de dispositivos de sistemas de processamento ou comunicação de dados.

Neil Barret assevera que crime digital é *a* "(...) utilização de computadores para ajuda em atividades ilegais, subvertendo a segurança de sistemas, ou usando a Internet ou redes bancárias de maneira ilícita"[31]. Nesta mesma seara, Gustavo Testa Corrêa aduz que:

> Crimes digitais seriam todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados,

---

29 LICKS, Otto Banho; ARAÚJO JÚNIOR, João Marcelo de. Aspectos penais dos crimes de informática no Brasil. *Revista dos Tribunais*, São Paulo, p. 82-103.

30 ARAÚJO JÚNIOR, João Marcelo de. *Dos crimes contra a ordem econômica*. São Paulo: RT, 1995. p.127 e 133.

31 BARRET, Neil. Digital Crime. Londres: Kogan Page, 1997, p.31, *apud* Gustavo Testa Corrêa. *Aspectos jurídicos da Internet*. São Paulo: Saraiva, 2000.

> acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico[32].

Sérgio Marcos Roque também oferece o conceito de crime de informática como *"*conduta definida em lei como crime em que o computador tiver sido utilizado como instrumento para a sua perpetração ou consistir em seu objeto material"[33].

Dessa forma, observa-se que não há consenso acerca de um conceito para o crime informático. Muitas vezes, a falta de um rigor técnico fez surgir diversas nomenclaturas para um mesmo fato. Diante disso, é necessário ser fixado um conceito de delito informático para a correta delimitação do tema aqui exposto.

Deve-se primeiramente analisar o destinatário de tal conceito. Para o penalista, preocupado em estudar os tipos novos surgidos com o uso do computador e que deles necessitam para existirem e,ainda, os tipos antes existentes e com vida própria, independente do computador, a denominação "delito informático" é aconselhável, com a conseqüente separação do delito informático em 'puro' (o delito da primeira espécie) e delito informático 'impuro' (o delito da segunda espécie).

Já para quem almeja examinar, de forma mais ampla, tais crimes, principalmente no que se refere à sua descoberta e à sua persecução, a denominação 'crimes por computador' se apresenta bastante ajustada. Interessa aí o estudo de qualquer crime informático, puro ou impuro, desde que cometido pelo computador, aproveitando-se das facilidades decorrentes de seu uso e, principalmente, das dificuldades impostas pelas soberanias dos Estados à persecução penal além do território nacional (dificuldade bastante presente numa sociedade da informação em que a Internet encontra-se como meio universalizador das informações e das interações sociais).

---

32 CORRÊA, Gustavo Testa, op. Cit., p.43.

33 Crimes de informática e investigação policial. In: PENTEADO, Jaques de Camargo (Coord.) et al. Justiça penal, 7: críticas e sugestões: justiça criminal moderna: proteção à vítima e à testemunha...São Paulo: Revista dos Tribunais, 2000. (Centro de Extensão Universitária, v.7), p.317.

Neste trabalho, por se buscar um estudo de conduta com enfoque eminentemente penal, apesar de considerarmos também os crimes informáticos impuros, analisando alguns aspectos da persecução penal, usar-se-á predominantemente a denominação de delito informático. Outro fator que vem embasar tal decisão é que a denominação escolhida alberga não somente os crimes, mas também as contravenções; mesmo porque no Brasil o delito é gênero, do qual são espécies o crime e a contravenção. Assim passemos ao conceito de delito informático.

Pelo lado fenomenológico, podemos considerá-lo como um recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais (crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware, software, redes, etc.).

Por outro lado temos um conceito cunhado pela Organização para a Cooperação Econômica e Desenvolvimento da ONU que é o de que o delito informático é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados.

Apesar da propriedade de tal conceito, uma crítica há de ser-lhe dirigida. A expressão “conduta ilícita não-ética” é incompatível com a cultura jurídica brasileira, mesmo porque se parte do pressuposto de que toda norma penal incriminadora é eticamente indesejável. Aliás é de todo incongruente que tipos penais não tenham por fundamento a repulsa moral da sociedade. Dessa forma, parece mais acertada a concepção fenomenológica de delito informático.

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

Assim, a denominação delitos informáticos alcança não somente aquelas condutas praticadas no âmbito da Internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de

modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível conexão à Rede Mundial de Computadores, ou qualquer outro ambiente telemático. Desta maneira, “delito informático” é gênero, do qual o “delito telemático” é espécie.

Apesar de o enfoque principal deste trabalho ser o delito telemático, aprofundar-se-á o estudo com base no delito informático de modo a se ter uma visão mais ampla de tal fenômeno social, que é o crescente uso dos computadores em práticas delitivas.

Por derradeiro, mas não menos importante, não é muito lembrar que a Convenção de Budapeste (Convenção sobre Cibercrime) encerra somente as condutas praticadas em ambiente de rede, abarcando somente os fatos típicos ocorridos exclusivamente no ciberespaço**.**

## 5.2 Classificação

A busca por uma classificação guarda enorme complexidade, à exemplo do que se viu no tópico concernente ao conceito de delito informático. Sem embargo dessa indecisão doutrinária, uma coisa parece certe nesse terreno tão tormentoso: existem dois grandes blocos de teóricos da criminalidade informática. De um lado, posicionam-se os que consideram o delito informático como um qualquer outro crime tradicional e, por isso, subsumível nos tipos legais de crime já existentes. O computador seria mero instrumento do crime. O segundo bloco seria composto por aqueles que entendem que, além dos crimes tradicionais, existem delitos de informática puros e, por isso, reclamam a urgente adaptação da legislação penal vigente e a criação de normas específicas.

Um embrião de classificação já havia desde meados da década de oitenta. No entanto, tal classificação tinha como elementos a classificar delitos praticados em sua quase totalidade em ambiente exclusivamente informático. Após isto, substancial modificação se operou em decorrência do avanço das tecnologias, retratado principalmente no advento e massificação das

comunicações realizadas através das redes de computadores; em conseqüência do que a delinqüência passou, em sua maioria, para o plano telemático, com a prática de ilícitos à distância, determinando-se, pois, a reclassificação dos delitos informáticos.

A Classificação dos crimes praticados por meio da Internet é de grande valia para melhor visualização do assunto. A doutrina tem proposto diversas classificações. Nenhuma, porém, inteiramente satisfatória, mas todas de grande valia para esclarecimento e delimitação do tema em análise.

O Professor Ulrich Sieber dividiu os crimes por computador em três grupos:

> a) crimes econômicos, que por seu turno se subdividem em a1) fraude por manipulação de dados em sistemas de processamento de dados; a2) espionagem de dados e pirataria de programas; a3) sabotagem; a4) furto de serviço ou furto de tempo; a5) acesso não autorizado a sistemas de processamento de dados; a6) uso do computador para crimes empresariais;
> b) ofensas contra direitos individuais, que se subdividem em: b1) uso incorreto de informação; b2) obtenção ilegal de dados e posterior arquivo das informações; b3) revelação ilegal e mau uso da informação; b4) dificuldade de se distinguir entre obtenção, arquivamento ou revelação de informações; e
> c)ofensas contra direitos supraindividuais, divididas em c1) ofensas contra interesses estaduais e políticos e c2) a extensão desta categoria para crimes contra a integridade humana[34].

Marc Jeager, citado por Ivette Senise[35], propõe outra classificação, da forma abaixo:

> a) fraudes propriamente ditas, que se subdividem em a1) fraudes no nível da matéria corporal ou hardware (contra a integridade física do próprio computador); a2) fraudes no nível do input (modificação dos dados), fraudes no nível do tratamento (modificação apenas dos programas), deixando intactos os dados); fraudes no nível do output (intervenção no resultado

---

[34] The internacional handbook on computer crime. New York: John Wiley Sons, 1986, *apud* Sandra Gouvêa. *O Direito na Era Digital*: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997, (Série Jurídica, v. 1), p. 62-65.

[35] JEAGER, *apud* FERREIRA, Ivette Senise. Os Crimes da Informática. In: BARRA, Rubens Prestes (Coord.); ANDREUCCI, Ricardo Antunes (Coord.) Estudos Jurídicos em Homenagem a Manoel Pedro Pimentel. São Paulo: RT, 1992. p. 145.

> obtido a partir de dados corretos, corretamente tratados); e b) atentados à vida privada.

Jean Pradel, citado por Ivette Senise[36], propõe a seguinte classificação: "a) manipulações para obtenção de dinheiro; e b) manipulações para obtenção de informação".

Hervé Croze e Yves Bismuth, citados por Ivette Senise[37], propõem uma outra classificação: "a)atos dirigidos contra um sistema de informática, por qualquer motivo; e b) atos que atentam contra outros valores sociais ou outros bens jurídicos, cometidos através de um sistema de informática".

Sérgio Marcos Roque aduz que duas são as categorias de crimes de informática:

> Aqueles praticados através do uso do computador e os perpetrados contra os dados ou sistemas informáticos. Nos primeiros o computador será o instrumento; no segundo, o objeto material. Assim, quando o computador for utilizado apenas como instrumento de escolha pelo agente ativo para a consecução do crime, este será crime de informática comum; mas, quando a ação do criminoso se dirigir contra os dados contidos no sistema, será definido como crime de informática autêntico, porque nesse último o computador é essencial para a existência do delito[38].

João Marcelo de Araújo Júnior oferece sua própria classificação para os delitos informáticos assentada na natureza do dano causado:

> a) prejuízos econômicos diretos: o agente obtém vantagem indevida sobre patrimônio alheio através da utilização de sistemas de informática;
> b) prejuízos econômicos indiretos: o agente obtém vantagem indevida reflexa, sem se apropriar dos bens ou valores, mas captando informações contidas em arquivos;
> c) prejuízos intangíveis: são valores que representam prejuízos intangíveis relativos a valores impalpáveis, como a imagem de um

---

[36] A Criminalidade Informática. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.) et al. *Direito & Internet*: aspectos jurídicos relevantes. Bauru: EDIPRO, 2000. p. 209-215.

[37] Idem.

[38] Crimes de informática e investigação policial. In: PENTEADO, Jaques de Camargo (Coord.) et al. Justiça penal, 7: críticas e sugestões: justiça criminal moderna: proteção à vítima e à testemunha...São Paulo: Revista dos Tribunais, 2000. (Centro de Extensão Universitária, v.7), p.317-318.

> banco perante seus clientes ao ter seu sistema de informatização sabotado.[39]

Túlio Lima Vianna, por seu turno, acredita que os delitos informáticos se dividem em quatro grupos:

> 1) Delitos informáticos impróprios: são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados).
> 2) Delitos informáticos próprios: são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).
> 3) Delitos informáticos mistos: são crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa.
> 4) Delito informático mediato ou indireto: é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação40.

Apesar de tal classificação não ser a adotada diretamente neste trabalho, discorrer sobre tal classificação será de fundamental importância para a construção dialética do tema aqui enfrentado. Em virtude de sua brilhante contribuição para o tema, a classificação de VIANNA[41] será exposta em tópico próprio.

### 5.2.1 Classificação de Túlio Lima Vianna[42]

Conforme visto, para o estudioso o delito informático se dividiria em quatro grupos: próprios, impróprios, mistos e mediatos.

---

39 ARAÚJO JÚNIOR, João Marcello de. Computer-crime. In: CONFERÊNCIA INTERNACIONAL DE DIREITO PENAL, 1988. Anais. Rio de Janeiro: Procuradoria Geral da Defensoria Pública, 1988. p.461.

40 *Fundamentos de direito penal informático*. Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003, p. 13-26.

41 *Fundamentos de direito penal informático*. Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003, p. 13-26.

42 Idem.

5.2.1.1- Delitos informáticos impróprios

A boa técnica manda que se Conforme exposto acima, para Vianna[43] delitos informáticos impróprios “são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados)”.

Sua popularidade é grande e, na maioria das vezes, para sua prática não há necessidade de que o agente detenha grandes conhecimentos técnicos. Hipótese clássica são os crimes contra a honra – calúnia, injúria, difamação – cometidos pelo simples envio de um email. Tal ação não exige conhecimento especializado e permite não só a execução de delitos contra a honra, mas também o empreendimento dos crimes de induzimento, instigação ou auxílio ao suicídio (art.112 CP), ameaça (art.147 CP), violação de segredo profissional (art.154 CP), incitação ao crime (art.286 CP) e apologia de crime ou criminoso (art.287 CP).

Um outro exemplo é a criação e publicação de uma página simples na Internet para veiculação de material ilícito. A simplicidade, aliada à facilidade da publicação em servidores gratuitos, é responsável por uma expressiva quantidade de casos de publicação de fotos pornográficas de crianças na Internet, o que em nossa legislação é crime de pedofilia, previsto no art. 241 do Estatuto da Criança e do Adolescente (ECA – Lei nº 8.069 de 13 de julho de 1990).

Outros delitos informáticos impróprios estão previstos na legislação penal extravagante, senão vejamos: concorrência desleal (art.195 da Lei nº 9.279 de 14 de maio de 1996), violação de direito autoral (art.12 da Lei nº 9.609 de 19 de fevereiro de 1998) e uma série de crimes eleitorais (art.337 da Lei nº 4.737 de 15 de julho de 1965).

Outro exemplo de tal classificação é o uso de falsas páginas de comércio eletrônico nas quais o agente efetua o pagamento mas nunca recebe o

---

43 Idem.

produto comprado caracterizam o crime de estelionato na Internet, em que o tipo penal está disposto no artigo 171 do Código Penal.

A prostituição também é muito explorada através de páginas na Internet, nos quais há anúncios de serviços de 'profissionais do sexo'. O que, em tese, pode caracterizar os delitos de favorecimento da prostituição (art.228 CP) – já que as páginas facilitam o acesso com os clientes – ou rufianismo (art. 230 CP) – uma vez que o responsável pela página recebe comissão pelos contatos bem-sucedidos.

O tráfico de drogas e tráfico de armas também podem ser realizados com a simples criação de uma página na Internet. Tanto é possível que há registro de casos de indivíduos que tentaram vender substância entorpecente, órgãos humanos e fetos em populares *sites* de leilões pela Internet[44].

É importante notar que em nenhum destes delitos há qualquer ofensa ao bem jurídico inviolabilidade das informações automatizadas. Pode-se notar também que o computador é usado como instrumento da consecução do crime, sendo apenas um dos meios dos quais pode dispor o delinqüente para praticar a conduta almejada. Dessa forma, tais crimes são classificados como delitos informáticos impróprios.

#### 5.2.1.2 Delitos Informáticos Próprios

Segundo VIANNA, são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).

---

[44] Em 24 de setembro de 1999, três vendedores anunciaram, na página de leilões pela Internet *Ebay*, a venda de maconha de um anúncio com o título de "o melhor da Holanda" no qual constava uma foto dos agentes junto a pacotes plásticos com a droga. Sete pessoas se ofereceram para comprar o produto, em ofertas que chegaram a 10 (dez) milhões de dólares até que o anúncio fosse tirado do ar. Naquele mesmo mês foram encontrados casos de venda de órgãos humanos e de um feto na mesma página. Cf. FUOCO, Taís. Maconha é oferecida em leilões da *Ebay*. *Plantão Info*. Disponível em: <http://www2.uol.com.br/info/infonews/091999/24091999-2.shl>. Acesso em: 25 de setembro de 1999.

A Interferência em dados informatizados é uma modalidade de crime informático próprio. A Lei nº 9.983/2000 acrescentou dois tipos penais ao Código Penal Brasileiro prevendo a hipótese da interferência em dados informatizados unicamente quando praticada por funcionário público no exercício de suas funções.

> Inserção de dados falsos em sistema de informações
> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos 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 (dois) a 12 (doze) anos, e multa.
> Modificação ou alteração não autorizada de sistema de informações
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa.
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

Em ambas as condutas previstas, não se pune a mera leitura dos dados, razão pela qual não se trata de acesso não autorizado a sistemas computacionais, mas de crime especial em relação a este, ou seja, de interferência em dados informatizados. Tal norma procura prevenir a alteração ou destruição de dados armazenados em sistemas computacionais da Administração Pública.

Já a interferência em sistemas computacionais não se confunde com a hipótese anterior. O que se protege diretamente aqui não é a integridade dos dados em si, mas o seu processamento. A inviolabilidade dos dados é protegida indiretamente. Na interferência em sistemas computacionais, a ação do agente é direcionada no sentido de impossibilitar o funcionamento do sistema, comprometendo o acesso aos dados por inoperância do sistema.

Um exemplo bem freqüente de interferência em sistemas computacionais é o ataque de recusa de serviço DoS (Denial of Service), que são

capazes de derrubar sites da Internet. A conduta isolada de interferir em sistemas computacionais privados não está tipificada no ordenamento jurídico brasileiro. Mas geralmente tal conduta pode caracterizar o crime de dano (art. 163, CP), caso algum dado seja perdido ou algo seja destruído com a invasão.

Com a interceptação ilegal, os dados são capturados durante sua transferência de um sistema computacional para outro. Ou seja, o agente não obtém acesso direto ao computador da vítima, limitando-se a interceptar os dados em trânsito. Tal conduta encontra-se tipificada no ordenamento jurídico brasileiro na Lei nº 9.296 de 24 de julho de 1996, que em seu artigo 10º dispõe:

> Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
> Pena: reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

Outro importante delito informático próprio é a falsificação informática, que consiste na adulteração de dados de computador com fins fraudulentos. Um exemplo de tal delito é a criação de pequenos programas denominados *cracks*, capazes de forjar falsos registros para habilitar diversos programas, em uma clara e direta violação aos direitos autorais.

Destacando-se, por fim, mas não menos importante, dentre os delitos informáticos próprios, a criação e divulgação de programas de computadores destrutivos, os conhecidos vírus informáticos.

A palavra vírus deriva do latim e significava originalmente 'veneno'. Os vírus de computador são programas que infectam outros programas, podendo causar variados danos aos dados armazenados no sistema e se reproduzindo a partir do hospedeiro. Na legislação brasileira não há um tipo penal específico visando à repressão dos vírus informáticos, mas é perfeitamente possível a punição por crime de dano (art.163 CP) quando a conduta destruir, deteriorar ou inutilizar os dados armazenados no sistema operacional; apesar de alguns juristas entenderem que os dados não podem ser considerados 'coisa' para fins penais.

Apesar de as condutas descritas anteriormente serem passíveis de punição, a despeito da inexistência de legislação própria e específica, observou-se também que, em alguns casos, existem condutas não tipificadas no nosso ordenamento jurídico. Portanto, melhor seria que houvesse lei específica que viesse tipificar condutas delitivas onde o computador, em meio telemático ou não, como mero acessório ou como figura essencial, fosse usado. Ou seja, apesar de a atual legislação não deixar muitas das condutas delitivas com o uso do computador impunes, não se pode prescindir de uma legislação específica e atual.

### 5.2.1.3 Delitos Informáticos Mistos

Conforme exposto por VIANNA, delitos informáticos mistos são crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa.

Como se sabe, crime simples é aquele que se identifica com um só tipo legal, enquanto que o crime complexo é aquele que representa a fusão unitária de mais de um tipo penal (ex.: roubo, estupro). Observa-se assim que são delitos derivados do acesso não autorizado a sistemas computacionais que ganharam o *status* de delitos *sui generis,* dada à importância do bem jurídico protegido diverso da inviolabilidade dos dados.

Como foi visto anteriormente, no Brasil o 'delito' de acesso não autorizado a sistemas computacionais ainda não foi tipificado, ainda aguardando regulamentação. Mas, paradoxalmente, um delito informático derivado do acesso não autorizado a sistemas computacionais já foi tipificado. Trata-se do acesso não autorizado a sistemas computacionais do sistema eleitoral, que surgiu como tipo penal no ordenamento jurídico nacional com a Lei nº 9.100/95, que em seu art. 67, VII, assim o tipificou:

> Obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos.
> Pena: reclusão, de 1(um) a 2(dois) anos, e multa.

No entanto, a Lei nº 9.504/97, em seu art. 72, I, disciplinou a matéria da seguinte forma:

> Obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, afim de alterar a apuração ou a contagem de votos.
> Pena: reclusão, de 5(cinco) a 10(dez) anos, e multa.

Nesse aparente conflito de normas, pode-se observar o considerável aumento da pena. Em uma análise superficial, pode-se concluir erroneamente que a modalidade tentada desse tipo de acesso não-autorizado deixou de ser crime. Mas, na verdade, o dispositivo não regulou completamente a matéria, não revogando tacitamente o dispositivo anterior; visto que apenas excluiu da majoração da pena a modalidade tentada do crime. Além disso, a Lei nº 9.504/97 enumerou taxativamente em seu artigo 107 os dispositivos revogados, não fazendo qualquer menção ao art. 67, VII, da Lei nº 9.100/95.

Assim, portanto, encontra-se parcialmente em vigor o art. 67, VII, da Lei nº 9.100/95, disciplinando exclusivamente os casos de tentativa do acesso não autorizado a sistemas de tratamento automático de dados do sistema eleitoral. Dessa forma, o simples tentar e a conduta invadir são figuras típicas no ordenamento jurídico brasileiro desde que o sistema a se invadir seja o de tratamento automático de dados do sistema eleitoral.

#### 5.2.1.4 Delito Informático Mediato ou Indireto

Delito Informático Mediato ou Indireto, segundo VIANNA, é o delito fim não- informático que herdou esta característica de delito-meio informático realizado para possibilitar a sua consumação.

Um exemplo dado por tal autor foi o furto de determinada quantia em dinheiro através de um acesso sem autorização ao sistema computacional de um banco. Deste modo, caso o acesso não-autorizado a sistema computacional fosse figura típica no Brasil, o indivíduo estaria cometendo dois delitos distintos: o furto e o acesso não-autorizado. O primeiro, delito patrimonial; o segundo, delito informático próprio.

Um outro bom exemplo para tal classificação pode ser vislumbrado na hipótese de um acesso não autorizado a um banco de dados de uma empresa de comércio eletrônico para a aquisição dos números dos cartões de créditos dos clientes, com sua posterior utilização em compras na Internet.

Observa-se nos dois casos que o acesso não autorizado é executado como 'delito'-meio para se executar o delito-fim que consiste na subtração da coisa alheia móvel ou na obtenção de vantagem indevida.

Atualmente, como tal acesso não é figura típica no Brasil, o agente só será punido pelo furto ou pelo estelionato, conforme o caso. Mas se o acesso não-autorizado a sistemas computacionais fosse conduta típica, haveria um conflito aparente de normas que seria resolvido pela aplicação do princípio da consunção[45].

### 5.2.2 Classificação adotada

Apesar do brilhantismo da classificação anteriormente exposta, esta não será a adotada por tal trabalho. Tal classificação foi defendida em um trabalho que abordava especificamente o acesso não-autorizado a sistemas computacionais. Portanto bastante ênfase foi dada ao tema quando da propositura de tal classificação. Pode-se observar que a classificação foi proposta

---

[45] Princípio segundo o qual um tipo descarta o outro porque consome ou exaure o seu conteúdo proibitivo, isto é, porque há um fechamento material. Sua aplicação é de grande importância quando do conflito aparente de dois tipos penais distintos, em que cada um protege um bem jurídico, a consumação do segundo exaure ou consome a consumação do primeiro, só sendo aplicada a pena daquele.

com base no bem jurídico a ser tutelado, em que o bem jurídico considerado era o da inviolabilidade das informações automatizadas (dados).

Como o objeto de estudo deste trabalho não é especificamente o acesso não-autorizado a sistemas computacionais, opta-se por adotar uma classificação mais singela e objetiva, já que o intuito de tal trabalho não é o aprofundamento no tema. Pra corroborar ainda mais essa decisão, está o fato de que no Brasil o acesso não-autorizado a sistemas computacionais ainda não é conduta tida como típica, salvo o anteriormente explicitado.

Para este trabalho, será adotada a seguinte classificação, pois se acredita que tal classificação está mais próxima da realidade dos fatos: os delitos informáticos puros e os delitos informáticos mistos.

Os delitos informáticos puros são aqueles em que o sujeito visa especificamente ao sistema de informática em todas as suas formas, sendo que a informática é composta principalmente do *software*, do *hardware* (computador e periféricos), dos dados e sistemas e dos meios de armazenamento. A conduta ou ausência dela visam exclusivamente ao sistema informático do sujeito passivo. São exemplos os atos de vandalismo contra a integridade dos dados em acessos não-autorizados. São os delitos informáticos próprios da classificação anterior.

Os delitos informáticos mistos são aqueles em que o computador é mera ferramenta para ofensa a outros bens jurídicos que não exclusivamente os do sistema informático; ou seja, a informática é um meio, um veículo para a prática de um delito claramente definido na legislação penal, estando o bem jurídico já devidamente tutelado. Alguns de seus exemplos são o estelionato, a ameaça e os crimes contra a honra, podendo imaginar-se, inclusive, homicídio por meio da Internet (mudança à distância de rotas de aviões, alterações em sistemas de gerenciamento hospitalar). São os delitos informáticos impróprios, mistos e mediatos da classificação anterior.

## 5.3 Bem Jurídico Tutelado

A criação do conceito de bem jurídico faz parte da evolução da sociedade moderna, que somente pode ver na criação de novos tipos penais o último recurso da intervenção do Estado. Em verdade, num Estado Democrático de Direito, onde está presente a intervenção mínima e o Direito Penal é a *ultima ratio*, nada mais razoável do que dar graus de importância àquilo que se pretende efetivamente proteger.

Portanto, se a defesa de determinados interesses coletivos pode ocorrer de outra forma, sem a existência de preceitos secundários (sanções penais das mais variadas naturezas), que assim se faça, com a intervenção ora do Direito Civil, ora do Direito Administrativo etc.

É justamente neste contexto que se insere a discussão acerca da necessidade, ou não, da intervenção do Direito Penal nesta seara do mais moderno, revolucionário e emblemático conhecimento humano. Ao que consta, o princípio da razoabilidade autoriza a intervenção do Direito Penal, pois de outra forma determinados bens nunca seriam protegidos ( a propriedade e a vida).

Se aqui se aponta a necessidade da intervenção do Direito Penal na telemática, há que se indagar se existe um bem jurídico permanente a autorizar a criação de um ramo autônomo dentro do Direito Penal.

Com base na classificação adotada, a indicação dos bens jurídicos nos delitos mistos não é tarefa difícil: no estelionato é o patrimônio; nos crimes de calúnia, injúria e difamação é a honra. Nos delitos puros, os bens jurídicos a se proteger também não são difíceis de apontar: invasão e destruição dos dados, patrimônio; na pirataria de software, o bem jurídico a proteger é a propriedade intelectual.

Mas há um bem jurídico absolutamente permanente – que é a Segurança Informática, que existe independentemente dos bens jurídicos individuais e coletivos que possam existir concomitantemente numa conduta típica praticada no âmbito da Internet.

Na tríplice classificação[46] proposta por Smanio e aqui admitida, trata-se de um bem jurídico-penal de natureza difusa. Isto porque, além de atingir um número indeterminado de pessoas, gera conflituosidade entre o interesse dos usuários da Internet (incontáveis), aí incluídos os usuários comuns, além dos *hackers*, *crackers* e o das grandes corporações, quer de empresas fornecedoras de bens e serviços, quer de provedores de acesso.

Essa segurança informática consiste na utilização da tecnologia informática adstrita aos limites legais e constitucionais de forma que os elementos a seguir sejam alcançados: a)Integridade: a informação deve ser fidedigna e completa e somente o usuário pode mudá-la; b)Disponibilidade: o usuário deve ter a informação no momento em que necessitar; c)Confidencialidade: ninguém, sem consentimento, deve ter acesso ou divulgar a informação.

A livre iniciativa, um dos valores fundamentais da República Federativa do Brasil, sem citar outros não menos importantes (soberania, dignidade da pessoa humana), estaria prejudicada se na Internet não houvesse a imprescindível segurança para o tráfego de dados. Sem essa segurança informática, não há que se falar em segurança jurídica, valor este do qual ninguém pode prescindir num Estado Democrático de Direito.

A organização de um sistemático ataque ao recente tipo de criminalidade que se estabeleceu no âmago da Internet representa um verdadeiro desafio a todos os países modernos; tanto que a Convenção de Budapeste, que

---

[46] Gianpaolo Poggio Smanio: "a) primeiramente, os bens jurídico-penais de natureza individual, que são os referentes aos indivíduos, dos quais estes têm disponibilidade, sem afetar os demais indivíduos. São portanto bens jurídicos divisíveis em relação ao titular. Citamos como exemplo, a vida, a integridade física, a propriedade, a honra etc.; b) os bens jurídico-penais de natureza coletiva, que se referem à coletividade, de forma que os indivíduos não têm disponibilidade sem afetar os demais titulares do bem jurídico. São, dessa forma, indivisíveis em relação aos titulares. No Direito Penal, os bens de natureza coletiva estão compreendidos dentro do interesse público. Podemos exemplificar como a tutela da incolumidade pública, da paz pública, etc.; c) os bens jurídico-penais de natureza difusa, que também se referem à sociedade em sua totalidade, de forma que os indivíduos não têm disponibilidade sem afetar a coletividade. Ocorre que os bens de natureza difusa trazem uma conflituosidade social que contrapõe diversos grupos dentro da sociedade, como na proteção do meio ambiente, que contrapõe, por exemplo, os interesses econômicos industriais e o interesse na preservação ambiental, ou na proteção das relações de consumo, em que estão contrapostos os fornecedores e os consumidores, a proteção da saúde pública, enquanto referente à produção alimentícia e de remédios, a proteção da economia popular, da infância e da juventude, dos idosos etc." (SMANIO, Gianpaolo Poggio. *Tutela penal dos direitos difusos*. São Paulo: Atlas, 2000.p.108).

encontra-se no final deste trabalho, é uma resposta inicial a essa questão, ao sugerir o estabelecimento de um sistema de leis com vista ao enfrentamento da questão, quer com a criação de novos tipos penais, quer com tratamento processual moderno e diferenciado do que até hoje existe.

Destarte, evidencia-se que há um bem jurídico permanente, autorizador da construção de uma nova dogmática penal; qual seja, a segurança informática, que pode ser considerada como a expressão da liberdade do indivíduo e que consiste no direito a utilizar lícita e livremente, com os limites constitucionais e legais, a tecnologia informática. De forma que os delitos informáticos podem ser vistos como violação dessa mesma liberdade informática e como infração das distintas liberdades que o emprego destas tecnologias pode alcançar (intimidade, domicílio, livre circulação, livre associação etc.).

## 5.4 Sujeito ativo

É um engano pensar que os delitos informáticos são cometidos somente por especialistas, principalmente, na sociedade atual, onde o acesso a computadores está cada vez maior, sendo este acesso associado ao crescimento da Internet. Com a evolução dos meios de comunicação, o aumento de equipamentos, o crescimento da tecnologia e, principalmente, da acessibilidade e dos sistemas disponíveis, uma pessoa com apenas um mínimo de conhecimentos na área pode ser um criminoso de Informática.

Tem-se assim que a Internet é um instrumento que ampliou indubitavelmente os conhecimentos dos usuários; dentre eles aqueles que descuram de respeitar os limites legais. O tempo real, a tentativa e erro, a ação e reação, enfim, a forma interativa de como as informações chegam a todos, ampliou o leque de possibilidades; daí o surgimento de um sem número de pessoas com o conhecimento necessário para a prática delitiva num ambiente telemático. Ou seja, o acesso a qualquer informação, inclusive criminosa, facilitou o aparecimento de delinqüentes telemáticos.

O anonimato também contribuiu para o cultivo desse terreno fértil para a prática delitiva. Os mais modernos programas de rastreamento (através do número IP etc.) podem até permitir que se chegue ao computador de onde partiu a prática criminosa, mas não indicam necessariamente quem efetivamente utilizou a máquina. Aliás, os estabelecimentos denominados *Cyber Cafés* fornecem a necessária estrutura para que isto ocorra, haja vista não existir qualquer regulamentação de funcionamento deste tipo de atividade, o que é absolutamente necessário.

A confirmar que o anonimato é elemento fomentador deste novo tipo de criminalidade, Newton Fernandes e Valter Fernandes trazem à colação um interessante exemplo:

> É extremamente difícil apanhar um 'cracker' habilidoso; há oito anos um deles acessa regularmente os computadores da NASA, FBI, CIA, Marinha, Casa Branca e da própria NSA (Agência Nacional de Segurança) e, até hoje não se conseguiu pegá-lo. Diga-se, a bem da verdade, que esse 'cracker' nunca danificou ou alterou nenhum dos arquivos que acessou ou mudou sequer um byte do computador. Para demonstração de seu poder, telefonou para o FBI e identificou-se; a ligação logo começou a ser rastreada. O FBI conseguiu descobrir o país, o código de área e o prefixo do telefone, mas quando estava para apurar os demais números, o computador zerava e indicava outro país, outro DDD e outro prefixo. Esta conversa durou vinte minutos e quando foi desligada, o 'cracker' não havia deixado nenhuma pista. A única coisa que se sabe sobre ele é que freqüentou a universidade de Berkeley na Califórnia, e o MIT, Instituto de Tecnologia de Massachussets.47

Um aspecto importante a ser analisado neste tópico prende-se à exata denominação dos sujeitos ativos dos delitos telemáticos. Marcelo de Luca Marzochi informa que a palavra '*hacker*' nasceu nos laboratórios de computação do MIT, e assim eram os estudantes de computação que ficavam durante as noites nos laboratórios *fuçando, pesquisando e experimentando tudo o que o*

---

47 FERNANDES, Newton; FERNANDES, Valter. Criminologia integrada. 2. ed. Rev. Atual. São Paulo: Revista dos Tribunais, 2002. p. 634-635.

*computador pudesse fazer. 'Fuçador', segundo especialistas, seria a tradução mais correta*[48].

A palavra '*hacker*', em si, é motivo de confusão, já que tem significados variados. No meio de tal confusão, está presente todo um movimento a desmitificar aquilo que se denominou hacker, que seria um curioso, nunca um criminoso. No entanto, tal entendimento romântico prescinde de uma abordagem realista do fenômeno *hacking*, onde tal termo designa o uso não-autorizado do computador e seus recursos de rede. Tal conduta pode causar dano pela simples presença e uso dos recursos de sistema.

Em tradução livre do dicionário Longman, hacker significa *alguém que está apto a usar ou mudar a informação nos sistemas de computador de outras pessoas sem seu conhecimento ou permissão*[49]. Já o dicionário de Informática e Internet de Márcia Regina Sawaya traz como significado da palavra hacker: são programadores tecnicamente sofisticados, que dedicam boa parte de seu tempo a conhecer, dominar e modificar programas e equipamentos[50].

Portanto, neste trabalho, opta-se por excluir a visão romântica de que o hacker é apenas um curioso; mas também se excluirá o uso do termo como sinônimo de agente criminoso.

### 5.4.1 Classificação existente

Superada a questão terminológica referentemente a '*hacker',* resta classificar os sujeitos ativos, no caso específico, aqueles que atuam num ambiente telemático. A classificação a seguir leva em conta a especialidade do agente, salientando-se que todos são abominados pelos usuário-padrão da rede.

---

48 *Direito.br*: aspectos jurídicos da Internet no Brasil. São Paulo: Ltr, 2000, p. 35.

49 HACKER. In: LONGMAN. (Ed.). *Longman dictionary of contemporary english*: new edition. England: Longman, 1987.p. 469.

50 HACKER. In: Dicionário de informática e Internet. São Paulo: Nobel, 1999. 544 p. p. 208.

Os *'crackers'* possuem os mesmos conhecimentos que os *'hackers'*, mas os utilizam para fins espúrios. O termo *'cracker'* é uma derivação do verbo to *'crack'*, que tem como significados quebrar, destruir. São também chamados de "*hackers do mal"*.

No Dicionário de Informática e Internet acima citado: cracker é o indivíduo que uso o computador, maliciosamente, como hobby, e obtém acesso não-autorizado a sistemas de computador, com o objetivo de derrotá-los. Pode roubar informações sobre contas bancárias e cartões de crédito ou destruir dados.

Neste trabalho, os *crackers* são considerados gênero e as demais denominações são suas espécies. Esta classificação é resumo do que foi escrito pelos brasileiros Olavo José Anchieschi Gomes[51], Antônio Celso Galdino Fraga[52], Jose Caldas Gois Junior[53], Alexandre Jean Daoun[54], Marcelo de Luca Marzochi[55], Sérgio Marcos Roque[56], Newton Fernandes e Valter Fernandes[57], e Reginaldo César Pinheiro[58]. Em ordem alfabética e não de importância, são:

a) *Anarchy*: são anarquistas que utilizam a rede para propalar sua ideologia. Preferem invadir páginas governamentais para manifestar sua preferência política.

b) *Arackers*: são a maioria absoluta do mundo cibernético. Fingem ser os mais ousados e espertos usuários de computador. Planejam ataques, e fazem ameaças em salas de bate-papo. Mas no final das contas, fazem *download* de imagens eróticas e as lançam nas salas de bate-papo.

---

51 *Segurança total*: protegendo-se contra os hackers. São Paulo: Makron Books, 2000.

52 Crimes de Informática: a ameaça na era da informação digital. In: SCHOUERI, Luís Eduardo (Org.). Internet: o direito na era virtual. 2. ed. Rio de Janeiro: Forense, 2001. p. 367-370.

53 O direito na era das redes: a liberdade no ciberespaço. 1. ed. Bauru: EDIPRO, 2001, p. 120-124.

54 Crimes Informáticos. In: BLUM, Renato M. S. Opice (Coord.) et al. Direito eletrônico: a Internet e os tribunais. 1. ed. Bauru: EDIPRO, 2001. p. 209-211.

55 *Direito.br*: aspectos jurídicos da Internet no Brasil. São Paulo: Ltr, 2000, p. 33-44.

56 Crimes de informática e investigação policial. In: PENTEADO, Jaques de Camargo (Coord.) et al. Justiça penal, 7: críticas e sugestões: justiça criminal moderna: proteção à vítima e à testemunha...São Paulo: Revista dos Tribunais, 2000. p.313-316.

57 Criminologia integrada. 2. ed. Rev. Atual. São Paulo: Revista dos Tribunais, 2002. 779 p. p. 634-637.

58 Os crimes virtuais na esfera jurídica brasileira. Boletim IBCCRIM – Publicação Oficial do Instituto Brasileiro de Ciências Criminais. São Paulo, ano 8, n. 101, p. 18-19, abr. 2001.

c) *Carders*: são os agentes especializados na falsificação de cartões - de crédito, telefônicos, magnéticos etc., para utilização fraudulenta junto às empresas que atuam no ambiente de rede. Por atuarem exclusivamente no ambiente de rede, diferenciam-se dos falsários e estelionatários comuns.

d) *Lammers*: da junção dos termos ingleses *'lame'* (pessoa estúpida) e '*hackers'*. São indivíduos que se auto-intitulam *'crackers*', mas não possuem conhecimentos suficientes para tanto. Aproximam-se dos 'arackers'.

e) Larvas: são os agentes que se situam entre os wannabes e os crackers. Têm capacidade suficiente para criar programas para atingir seus intentos, além de conhecimento médio para invasão em sistemas de segurança.

f) *Newbie*: Trata-se do iniciante, novato. Quando adquire os conhecimentos necessários, passa a integrar outra 'tribo'.

g) *Phreackers*: são delinqüentes especializados em burlar sistemas de comunicação com o fito de não adimplir o custo das ligações que posteriormente fazem a partir de telefones fixos ou celulares.

h) *Script Kiddies*: não têm foco certo e copiam outras formas de invasões realizadas por outros tipos de delinqüentes cibernéticos. Procuram invadir sites famosos com o fim de ganharem fama e reconhecimento.

i) *Sneakers*: são *'crackers'* que, mediante paga ou outra vantagem, quebram a proteção de sistemas. São indivíduos que utilizam seus conhecimentos para realizar pirataria empresarial. Podem ser chamados de “mercenários cibernéticos”.

j) Virii: são os indivíduos que criam os vírus eletrônicos. Possuem grande capacidade técnica e desenvolvem programas de alto poder destrutivo. Foram esses indivíduos que criaram os '*worms'* (vírus eletrônicos auto-replicantes).

k) *Wannab*e: possui grande capacidade técnica e almeja o respeito dos crackers. Utiliza-se de manuais, de programas prontos, que podem ser

obtidos na rede mundial e que permitem a quebra de segurança e a invasão de outros computadores.

l) *Warchalkers*: integrantes do movimento 'Warchalking'. Eles invadem redes wireless. Com antenas feitas com lata, a localização e gratuito uso destes pontos vulneráveis de conexão, o walchalker marca o local com símbolo próprio, assegurando informações atualizadas para os demais membros do grupo.

m) *Warez*: são os que copiam Softwares caríssimos e os distribuem gratuitamente. Atuam como verdadeira sociedade secreta, com códigos e sinais de reconhecimento.

n) *Wizards*: também chamados de mestres, magos ou gurus. São crackers que detém o máximo que se pode ter de conhecimentos na rede.

### 5.4.2 Classificação norte-americana

O FBI, no combate ao cibercrime, entende que existem três tipos de criminosos. O Primeiro é formado por aqueles que desejam chamar a atenção. São os '*hackers*' ativistas e as organizações terroristas.

Já o Segundo grupo é composto por pessoas que preferem o anonimato e utilizam-se de pseudônimos. São os '*hackers'* com motivação financeira; os patrocinados por governos interessados em sabotagem e espionagem; e criminosos organizados.

Por fim, o Terceiro grupo é formado por aqueles que estão do 'lado de dentro', quer de empresas, corporações, órgãos públicos etc que, motivados pela insatisfação, ganância ou outra razão e aproveitando-se do conhecimento das vulnerabilidades dos sistemas onde exercem suas funções, provocam mais prejuízos do que os demais criminosos.

### 5.4.3 Classificação adotada

Apesar da importância das classificações anteriores na construção dialética deste trabalho, a classificação adotada leva em conta a própria classificação da infração penal telemática. Tal decisão foi tomada com base na simplicidade e na relação com a classificação dos delitos informáticos, o que é mais consentâneo com a discussão aqui proposta.

O sujeito ativo próprio ou puro é o que age exclusivamente no ambiente de rede, sem que o 'iter criminis' em nenhum momento resvale no ambiente natural. Toda a sua conduta, ou ausência dela, ocorre no ambiente telemático. Nos itens anteriores, estão exemplos deste tipo de criminoso, destacando-se que todos ali relacionados são detentores de conhecimentos tecnológicos em maior ou menor grau. É uma nova espécie de infrator, que surgiu com as novas tecnologias, merecendo, assim, severa atenção da Criminologia.

Já o sujeito ativo impróprio ou impuro, que age tanto no ambiente telemático quanto fora dele e utiliza as ferramentas informáticas, telemáticas ou não, como usaria um revólver, uma chave mixa ou uma gazua. É o delinqüente comum, já conhecido dos estudiosos da Ciência Penal que, em razão de circunstâncias especiais e em decorrência de oportunismo, busca o fim criminoso com o uso do computador, como poderia alcançá-lo de qualquer outra forma. É o caso do estelionatário, do falsário, do sonegador etc.

Proposta mais esta classificação, a dos sujeitos ativos, segue-se a análise dos sujeitos passivos da infração telemática.

## 5.5 Sujeito Passivo

O sujeito passivo, como se sabe, é o ente sobre o qual recai a ação ou omissão realizada pelo sujeito ativo. É a pessoa ou entidade titular do bem

jurídico tutelado pelo legislador e sobre a qual recai a conduta do sujeito ativo. De qualquer modo, o sujeito passivo dos crimes de Informática pode ser qualquer pessoa, física ou jurídica, de natureza pública ou privada.

É importante destacar, entretanto, que a maioria desses delitos não chega ao conhecimento das autoridades para a devida apuração, em virtude das empresas ou instituições financeiras. Menciona-se, por exemplo, que esse tipo de delito pode trazer desprestígio e perda da credibilidade que, pois poderá dar a impressão de que esta ou aquela instituição não possuem sistemas de segurança eficazes. E é justamente essa 'lei do silêncio', que vem estimulando, de alguma forma, os criminosos a continuarem suas empreitadas ilícitas.

# 6 – JURISDIÇÃO, COMPETÊNCIA E TERRITORIALIDADE

Como dito anteriormente, a Telemática permitiu a interação de uma máquina com outra. A partir desta possibilidade, houve uma revolução denominada Era da Informação, oportunidade em que foram viabilizadas a geração, o processamento, a transmissão e a recepção de informações. Ou seja, dadas todas estas possibilidades, a Humanidade vive uma grande e irreversível transformação, com reflexos no mundo jurídico.

Essa revolução sócio-jurídica causada pelo fenômeno Internet obrigou os estudiosos a realizarem uma releitura em certos dogmas e conceitos, dentre eles, a soberania e a jurisdição internacional, os princípios reguladores da eficácia espacial da lei; matérias até então limitadas ao Direito Internacional Público, porém, hoje, foco de atenção das diversas áreas do Direito, principalmente, o Direito Penal.

Assim, iniciar-se com uma rápida análise sobre jurisdição e competência, *ratione materiae* e territorial, bem como os princípios reguladores da eficácia espacial da lei penal brasileira, ou seja, a extraterritorialidade; concluindo-se com análise sobre a necessidade de uma *ciberjusticia*[59] com extraterritorialidade internacional ou uma jurisdição internacional para crimes cometidos no ciberespaço. Dessa forma, tais questões aqui serão tratadas em conformidade com a necessidade do tema desenvolvido.

## 6.1 Jurisdição e Competência

Um estudo sobre os delitos informáticos não pode prescindir da análise da jurisdição, já que não se refere unicamente à seara penal, mas envolve as relações civis e comerciais. Isto porque, conforme Sandra Gouvêa, “a tecnologia vem reduzindo o custo das transações e dificultando a determinação

[59] Termo de MUÑOZ MACHADO.

do tempo e lugar de atos juridicamente relevantes"[60], obrigando, desta forma, um estudo mais aprofundado das leis no espaço considerando o risco de violação e lesão de diversos ordenamentos jurídicos de diferentes Estados.

Em sentido amplo, jurisdição é o poder de conhecer e decidir com autoridade dos negócios e contendas, que surgem dos diversos círculos de relações da vida social, falando-se assim em jurisdição policial, jurisdição administrativa, jurisdição militar, jurisdição eclesiástica etc. Em sentido estrito, porém, é o poder das autoridades judiciárias regularmente investidas no cargo de dizer o direito no caso concreto.

Os juízes, pelo simples fato de serem juízes, têm jurisdição, o poder de julgar, o poder de dizer o direito. Etimologicamente, a palavra *jurisdição* vem de *jurisdictio*, formada de *jus, juris* (direito), e de *dictio, dictionis* (ação de dizer, pronúncia, expressão), traduzindo, assim, a idéia de ação de dizer o direito[61]. É o poder de aplicar o direito conferido aos magistrados, que realizam com imparcialidade o ato jurisdicional. Estabeleceu-se a jurisdição como poder que toca ao Estado, entre suas atividades soberanas, de formular e impor a regra jurídica concreta por força do direito vigente.

O Estado, vedada que é a autotutela, tem o poder-dever de resolver, através do processo, os conflitos emergentes das relações sociais. O Estado se desincumbe de tal tarefa através da jurisdição, poder-dever, reflexo da sua soberania, através do qual, substituindo-se à atividade das partes, coativamente age em prol da ordem ou segurança jurídica.

Ao invés de conceituar a jurisdição como poder, Chiovenda[62] prefere considerá-la como função estatal. Jurisdição, portanto, é a função do Estado de declarar e realizar, de forma prática, o direito diante de uma situação jurídica controvertida, utilizando, para tanto, dos juízes. Assim, o Estado defende com a jurisdição sua autoridade de legislador. A priori esta jurisdição é inerte, visto que cabe ao particular provocar a movimentação do Estado exigindo a proteção jurisdicional respectiva, salvo exceções.

---

60 GOUVEA, S. O Direito na era digital, p. 89-90.

61 TOURINHO FILHO, Fernando da Costa. Processo Penal. 4. ed. São Paulo: Jalovi, v.2, p.1

62 SILVA, O. A. B. Teoria geral do processo civil, p. 62.

Sobre seu território, o Estado exerce jurisdição, o que vale dizer que detém uma série de competências para atuar com autoridade; é o Estado soberano com jurisdição geral e exclusiva. Esta generalidade da jurisdição significa que o Estado exerce no seu domínio territorial todas as competências de ordem legislativa, administrativa e jurisdicional. Tal exclusividade permite que o Estado local não enfrente a concorrência de qualquer outra soberania, detentor que é do monopólio do uso legítimo da força.

Assim, como poder soberano do Estado, a jurisdição é una e, investido no poder de julgar, o juiz exerce a atividade jurisdicional. É evidente, porém, que um juiz não pode julgar todas as causas e que a jurisdição não pode ser exercida ilimitadamente por qualquer juiz. Por isso, o poder de julgar, ou jurisdição, é distribuído por lei entre os vários órgãos do Poder Judiciário, através da competência. A competência é, assim, o limite e a medida da jurisdição, é a delimitação do poder jurisdicional. A Constituição Federal e as leis, inclusive as de organização judiciária, fixam a competência dos Juízes e dos Tribunais da nação, que se distribuem por seu território, para os casos concretos, permitindo-lhes exercer suas atribuições jurisdicionais. Essa fixação da competência se dá por meio da paulatina concretização do poder jurisdicional.

Observa-se, assim, que o estudo da Jurisdição destina-se precipuamente ao denominado direito penal internacional, ou seja, à aplicação da lei penal no espaço; ou seja, quando ocorrer um conflito, aparente ou não, entre as soberanias dos Estados envolvidos. Um exemplo disso, é o caso de um crime ter início no Brasil e terminar no exterior, ou vice-versa (é o denominado crime à distância).

Já o estudo da Competência destina-se à fixação do juízo que dirá o direito, ou seja, pressupõe a Jurisdição; pois aquela é o limite e a medida desta. Quando se passa ao estudo da Competência, não há mais que se indagar se a lei brasileira é aplicável ao caso concreto, pois tal questionamento já fora vencido em momento anterior, quando da análise da Jurisdição.

Após tal digressão, passa-se ao estudo das normas presentes no ordenamento jurídico brasileiro para a Jurisdição e a Competência, relacionando-

se tais temas com os delitos informáticos; delitos estes que, como se observou em outros tópicos, vence facilmente as barreiras territoriais existentes, fazendo surgir uma necessidade indeclinável de reavaliação das teorias jurídicas já existentes sobre o assunto.

## 6.2 Lei Penal no espaço

A lei penal é elaborada para viger dentro dos limites em que o Estado exerce a sua soberania. Como cada Estado possui sua própria soberania, com a contribuição da macrocriminalidade, surgiu o problema da delimitação espacial do âmbito de eficácia da legislação penal. Dessa forma, um crime cibernético pode violar o interesse de dois ou mais países, quando a ação é praticada no território de um Estado e a consumação dá-se em outro, rompendo fronteiras nacionais. Para que a própria soberania dos Estados não reste prejudicada, mister se faz repensar as normas e princípios sobre os quais se assentam a delimitação do alcance de determinadas normas de um ordenamento jurídico.

No ordenamento jurídico brasileiro, existem cinco princípios a respeito do âmbito de eficácia espacial da lei penal: da territorialidade; da nacionalidade; da defesa; da Justiça penal universal; e da representação. Apontam-se da seguinte forma os princípios.

### 6.2.1 Princípio da Territorialidade

Segundo o princípio territorial, a lei penal só tem aplicação no território do Estado que a determinou, sem atender à nacionalidade do sujeito ativo do delito ou do titular do bem jurídico lesado. É também denominado princípio territorial exclusivo ou absoluto, pois exclui a aplicação da lei penal de um país fora de seu território, segundo a regra '*leges non obligant extra territorium*'.

Tem por fundamento tríplice aspecto: processual, repressivo e internacional. Assim, segundo tal princípio em sua acepção absoluta, o monopólio do '*jus puniendi*' – que pertence ao Estado nos limites de seu território – exclui a interferência de outro. Tal princípio é muito rígido; rigidez esta que, pela natureza do Direito, é modulada. Daí permitirem as legislações penais, adotando a territorialidade como princípio fundamental, o temperamento de seu rigor através da aplicação dos outros princípios.

### 6.2.2 Princípio da Nacionalidade

De acordo com tal princípio, também denominado da personalidade, a lei penal do Estado é aplicável a seus cidadãos onde quer que se encontrem. O que importa é a nacionalidade do sujeito. É denominado da personalidade ou da nacionalidade porque o Estado entende pessoal a norma punitiva e a aplica ao nacional. Fundamenta-se em que o cidadão deve obediência à lei de seu país, ainda que se encontre no estrangeiro.

Tal princípio subdivide-se em dois tipos: a nacionalidade ativa e nacionalidade passiva. A primeira considera apenas a nacionalidade do autor e a segunda exige que o fato praticado pelo nacional no estrangeiro atinja um bem jurídico de seu próprio Estado ou de um concidadão.

Percebe-se que o princípio da nacionalidade passiva não é a mais indicada para punir os crimes virtuais que atingem várias nações. Pela proporção descomunal com que os delitos informáticos ocorrem no mundo, o princípio da nacionalidade ativa é mais interessante, pois bastaria conhecer a nacionalidade do autor da ação criminosa para julgá-lo.

### 6.2.3 Princípio da Proteção

É também chamado princípio real, da competência ou de defesa. Leva em conta a nacionalidade do bem jurídico lesado pelo crime, independentemente do local de sua prática ou da nacionalidade do sujeito ativo. Modernamente, enorme é o prestígio de tal princípio.

### 6.2.4 Princípio da justiça penal internacional

É também denominado princípio universal, da universalidade da justiça cosmopolita, da jurisdição mundial, da repressão universal e da universalidade do direito de punir. Preconiza o poder de cada Estado de punir qualquer crime, seja qual for a nacionalidade do delinqüente e da vítima, ou o local de sua prática. Para a imposição da pena basta encontrar-se o criminoso dentro do território de um país.

É um problema a aplicação incondicional de tal princípio, visto que existe diversidade entre as leis de cada país. Para os delitos informáticos, seria uma forma, em uma visão superficial, mais fácil para punir os criminosos onde quer que estivessem ou praticassem conduta ilícita. Mas, por outro lado, o conflito de legislações penais restaria intensamente constante, fazendo com que se criasse uma verdadeira torre de babel jurídica, o que não é salutar para o Direito Penal Internacional.

### 6.2.5 Princípio da Representação

Nos termos do sistema de interpretação, a lei penal de determinado país é também aplicável aos delitos cometidos em aeronaves e embarcações privadas, quando realizados no estrangeiro e aí não venham a ser julgados.

## 6.3 O conflito espacial no ordenamento jurídico brasileiro.

Reza o artigo 5º, caput, do CP: “Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional”.

Por aí se vê que o Código adotou o princípio da territorialidade como regra sobre a eficácia espacial da lei penal, abrindo exceção no próprio corpo da disposição às estipulações das convenções, tratados ou regras de Direito Internacional. De manifesta evidência, pois, que a lei penal brasileira permite, em determinados casos, a eficácia da norma de outros países.

Infere-se, portanto, que tal princípio não adota uma concepção absoluta do princípio da territorialidade; assim, se um brasileiro criar uma página *web* no Brasil com conteúdo ilícito e hospedar essa página em servidor situado fora do território brasileiro, esse indivíduo poderá ser julgado por leis brasileiras. Assim, adota-se no Brasil, como elemento norteador da Jurisdição, o princípio da Territorialidade temperada; pois no Código Penal a territorialidade estrita é modulada, aceitando-se, em alguns casos, os demais princípios supracitados.

A regra é a territorialidade, conforme disposto no artigo 5º do Código Penal. Ao admitir casos de Extraterritorialidade, como disposto no artigo 7º, estão sendo aceitas exceções ao princípio da territorialidade e estão sendo aceitos, ainda que em casos específicos, os demais princípios norteadores de tal tema.

> Extraterritorialidade
> Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:
> I - os crimes:
> a) contra a vida ou a liberdade do Presidente da República;
> b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público;
> c) contra a administração pública, por quem está a seu serviço;
> d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil;
> II - os crimes:
> a) que, por tratado ou convenção, o Brasil se obrigou a reprimir;
> b) praticados por brasileiro;
> c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados.
> § 1º - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro.
> § 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições:
> a) entrar o agente no território nacional;
> b) ser o fato punível também no país em que foi praticado;
> c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição;
> d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena;
> e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.
> § 3º - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior:
> a) não foi pedida ou foi negada a extradição;
> b) houve requisição do Ministro da Justiça.

Dessa forma, percebe-se que o princípio da proteção é facilmente vislumbrado no art.7º, I, e § 3º; o princípio da justiça universal, no art. 7º, II, a; o princípio da nacionalidade ativa, no art. 7º, II, b; o princípio da representação, no art. 7º, II, c.

Contudo, para que o trabalho não se esvaia em um anacrônico sofisma, outras premissas merecem ser estabelecidas. Uma delas estabelece que , para a formação de um raciocínio lógico do que seja o local das infrações penais telemáticas, não se pode prescindir de uma análise simbiótica dos institutos de Direito Penal com os de Direito Processual Penal.

Tanto é verdade que os artigos 6º e 7º do Código Penal servirão para a apreciação dos crimes à distância e os artigos 69 a 91, à exceção dos §§ 1º e 2º do art. 70, do Código de Processo Penal servirão para o estudo dos crimes

plurilocais. No estudo das infrações em ambientes telemáticos, os §§ 1º e 2º do art. 70 do CPP também assumem importância, pois disciplinam a competência do juízo, mesmo em situações em que uma fração do *'iter criminis'* é praticada no território nacional. Portanto, aqui os institutos do direito substantivo se entrelaçam e se completam com os de direito adjetivo.

Nos delitos informáticos, tal simbiose ganha importância, pois nem sempre é fácil a fixação do '*locus delicti*'; fixação esta que se subordina a questões de direito penal material e que, mesmo assim, possui capital importância para os problemas da competência penal baseada no critério '*ratione loci*'.

### 6.3.1 – Do Lugar do Crime

O exegeta hodierno depara-se com uma difícil tarefa, que é a de dizer qual o juízo natural para conhecer de uma causa penal advinda de infração a tipos penais telemáticos. Observar-se-á que a tarefa é difícil, mas não impossível, pois o sistema processual de fixação de competência é eficiente (arts. 69 e seguintes, do Código de Processo Penal, e 63, da Lei nº 9.099/95, dentre outros) e os dispositivos que tipificam as infrações informáticas puras e mistas existentes no ordenamento podem ser analisados com rigor científico.

A determinação do lugar em que o crime se considera praticado *(locus comissi delicti)* é decisiva no tocante ao direito penal internacional. Surge o problema quando o *'iter criminis'* se desenrola em lugares diferentes. Assim, cumpre ter em consideração a seguinte distinção: ou os lugares diferentes estão no mesmo país, ou em país diverso. Os crimes que se desenvolvem em diferentes lugares, dentro do território brasileiro, denominam-se delitos plurilocais; os delitos que se desenvolvem em países diferentes, são chamados de crimes à distância

Na primeira hipótese, a questão sobre a competência é solucionada pelo que se contém no artigo 70, *caput*, do CPP: 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. Isto ocorre porque não há um conflito de soberania, pois neste caso só há uma questão com relação à Competência e não com relação à Jurisdição. Na segunda hipótese, posta a questão em termos internacionais, nem sempre coincidem as legislações penais internas a respeito da matéria. E neste caso a legislação que resolverá tal conflito é a de Direito Penal, no tocante ao lugar do crime.

Portanto, é importante identificar onde ocorre o conflito; se ocorre no âmbito do território de um único país, aí será caso de fixação de competência, regida pelo Direito processual; se ocorre no âmbito territorial de mais de um país, ocorrendo um conflito de soberanias, tal conflito interessará ao Direito Penal Internacional e será resolvido conforme dispuser as leis materiais dos países envolvidos.

Diante disso, após o estudo da fixação da competência, é de suma importância o estudo do que o ordenamento jurídico dispõe para a delimitação do local do crime. Assim, passa-se ao estudo das teorias preconizadas pela doutrina acerca do local do crime: a teoria da atividade, a teoria do resultado e a teoria mista ou da ubiqüidade.

Pela teoria da atividade, lugar do crime seria o da ação ou da omissão, ainda que outro fosse o da ocorrência do resultado. Já a teoria do resultado despreza o lugar da conduta e defende a tese de que lugar do crime será, tão-somente, aquele em que ocorrer o resultado. A teoria da ubiquidade ou mista adota as duas posições anteriores e aduz que lugar do crime será o da ação ou omissão, bem como onde se produziu ou deveria produzir-se o resultado. Dessa forma, se o delito simplesmente 'tocar' o território nacional, em qualquer fase do *'iter criminis'*, na ação ou omissão, ou no resultado, será tal fato alcançado pela legislação penal brasileira.

Nosso Código Penal adotou a teoria da ubiqüidade, conforme se verifica no seu artigo 6º, assim dispondo:

> Art. 6º - 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.

A adoção da teoria da ubiqüidade resolve problemas de Direito Penal Internacional. Ela não se destina à definição de competência interna, mas, sim, à determinação do alcance das normas penais brasileiras. Embora possa, em tese, ser aplicada às normas penais brasileiras, pode acontecer que, em virtude, de convenções, tratados e regras de direito internacional, o Brasil deixe de aplicar a sua lei penal aos crimes cometidos no território nacional, conforme o princípio da territorialidade temperada.

Após tais exposições, em uma análise superficial, poder-se-ia sustentar a existência de uma contradição entre a lei penal (teoria mista) e a lei processual penal (teoria do resultado). Entretanto, tal conclusão não é a mais adequada. O artigo 6º do Código Penal destina-se exclusivamente, ao denominado direito penal internacional, ou seja, à aplicação da lei penal no espaço, quando um crime tiver início no Brasil e terminar no exterior ou vice-versa (é o denominado crime à distância). Vencida tal questão é que se passará à fixação do juízo competente para o julgamento, recorrendo-se, assim, às normas processuais de fixação de competência; normas estas que são mais percebidas nos delitos cometidos exclusivamente no território nacional.

6.3.1.1. Das infrações praticadas exclusivamente no Brasil

Como observado anteriormente, as normas processuais de fixação de competência ganham destaque quando vencido o questionamento da aplicação da lei penal brasileiro ao caso concreto, pois este fora cometido exclusivamente no Brasil. Neste caso, os artigos 69 e seguintes, do Código de Processo Penal, serão os paradigmas de fixação de competência.

O artigo 69 do CPP, através de seus incisos, hierarquiza as regras de competência:

> 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.

O primeiro inciso dispões que, de regra, será o lugar da consumação da infração que fixará a competência; o segundo inciso determina que, não se sabendo o lugar da infração, a competência será fixada inicialmente pelo domicílio e, desconhecido este, pela residência do réu; o terceiro inciso impõe que a natureza da infração é que deverá ser considerada caso as hipóteses anteriores sejam desconhecidas; a distribuição, a conexão e a continência também serão consideradas caso os incisos precedentes não fixem a competência; a prevenção, regra subsidiária de todas as outras, fixará o juízo competente caso as hipótese anteriores não tenham sido hábeis para tanto; e, por fim, mas não menos relevante, a prerrogativa de função, que vincula a distribuição à qualidade do agente, que, à evidência, é regra excepcional e autônoma, pois não está condicionada às hipóteses anteriores, fixará o juízo competente.

Ao criar este sistema, o legislador não permite que se exclua do Poder Judiciário qualquer causa criminal, pois a singela leitura do dispositivo apontado resolve eventual dúvida acerca do Juiz Natural. Dessa forma, nenhum delito será excluído da apreciação jurisdicional, muito menos aqueles conceituados como sendo delitos informáticos. Assim, se porventura as investigações não apontarem exatamente o local da infração telemática, o domicílio e a residência do réu fixarão o juízo competente; caso a autoridade incumbida das investigações também não localize o domicílio ou residência do réu, as hipóteses seguintes serão consideradas, até se chegar a última e definitiva delas, que é a prevenção.

Pode-se afirmar, sem sombra de dúvidas, que este sistema não excluirá da apreciação do Poder Judiciário qualquer causa criminal decorrente da prática de infrações no ambiente de Rede (Internet), em harmonia com o disposto no art. 5º, inciso XXXV, da Constituição Federal. De se concluir, pois, que os princípios constitucionais são respeitados pela solução legal e não há a menor

necessidade de se estabelecer novo sistema para o conhecimento de ações penais decorrentes da prática de infrações telemáticas mistas ou puras, desde que previamente tipificadas.

6.3.1.2 Dos crimes à distância

Conforme se depreende do anteriormente exposto, serão os artigos 6º do Código Penal, e 70, §§ 1º e 2º, do Código de Processo Penal, que tratarão do Direito Penal Internacional, ou seja, regularão a aplicação da lei penal no espaço quando um delito penal telemático tiver início no Brasil e terminar no exterior, ou vice-versa.

Em um primeiro momento, deverá ser observado o artigo 6º do CP. Com este artigo é que se determinará se o Brasil terá Jurisdição (entendida como expressão da soberania, como poder de dizer o direito) sobre o ocorrido. Se o delito simplesmente tocar o território nacional, pouco importa que a infração seja, de igual modo, punida no outro País; produzindo efeitos no Brasil, aplicar-se-á a Lei Penal brasileira. Basta a realização de um só fragmento da conduta punível em território pátrio para que a ela se aplique a lei brasileira, ainda que se verifique o restante da conduta e mesmo o evento no exterior, em sua forma tentada ou consumada. Vencido tal questionamento, deve-se passar ao que indaga sobre o juízo competente para proceder ao provimento jurisdicional. Tais respostas encontram-se fixadas nos §§ 1º, 2º e 3º, do art. 70, do Código de Processo Penal, assim dispostos:

> 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.

Dimana daí, que, como a lei refere-se à ação ou omissão, no todo ou em parte, omitindo-se, com relação à produção, em parte, do resultado, tal omissão não impede a aplicação da Lei Penal brasileira, já que parte do resultado é resultado.

Esses dispositivos também se aplicam a todas as espécies de infrações penais telemáticas, puras ou mistas (naturalmente se aqui tipificadas), desde que quaisquer das hipóteses legais acima estejam presentes. Assim, se o autor estiver no Brasil e o provedor no exterior, ou vice-versa, será aplicada a lei brasileira.

Ousa-se afirmar que, em qualquer fase do 'iter criminis' da infração informática, na remota hipótese de o dado passar pelo território brasileiro, mesmo através de um provedor ou roteador, independentemente do atuar humano, haverá interesse do Brasil na apuração do delito, naturalmente se aqui ele for típico, já que o país teve, mesmo que virtualmente, conspurcada sua soberania, que não desaparece pelo fato de as novas tecnologias permitirem a transnacionalização e, portanto, o considerável crescimento dos crimes à distância.

A bem da verdade, o sistema brasileiro harmoniza-se com o que existe de avançado quanto ao tema. De se concluir, pois, que também quanto às infrações telemáticas à distância a ordem jurídica brasileira é apta a dirimir qualquer conflito de competência; sendo, entretanto, de bom alvitre que sejam editas normas materiais específicas sobre o tema, face à crescente importância da Internet nas relações sociais relevantes, estas objeto do Direito.

## 7 DOS DELITOS PRATICADOS PELA INTERNET

Como se viu anteriormente, aqui se admite que as infrações penais informáticas dividem-se em puras ou próprias e mistas ou impróprias, classificação que ora é respeitada. Assim, não pode ser considerado, somente, crime de informática, aqueles que lesam um sistema de computador, por intermédio de outro, a fim de sabotar os dados pessoais ou empresariais de outrem. Atualmente, esses crimes de informática apresentam, muitas vezes, apenas novas maneiras de executar as figuras delituosas tradicionais; e em outras apresentam aspectos pouco conhecidos, que não se adaptam às incriminações convencionais e seus atores aos tipos criminosos comuns. Dessa forma, neste capítulo apresentar-se-á um breve resumo dos delitos praticados com mais freqüência na Internet.

A informática vem servindo como instrumento de realização ou preparação de crimes bem maiores. São exemplos de crimes facilitados pela Internet, como: espionagem, dos crimes contra a pessoa, dos crimes contra o patrimônio, falsificação de papel-moeda, incentivo ao racismo, a propaganda enganosa, a calúnia, a difamação, a injúria, a divulgação de receitas de fabricação de bombas.

Fraudes são praticadas com diferentes formas de manipulação de dados e programas ou utilização abusiva do computador; também, o furto, a apropriação indébita e o vandalismo são formas comuns de abuso da informática, violando a intimidade das pessoas ou sigilo das comunicações , ou os direitos do autor ou da proteção de marcas de indústria e comércio. Além disso, o aliciamento, produção e difusão em larga escala de imagens de abuso sexual de crianças e adolescentes, racismo, neonazismo, intolerância religiosa, homofobia, apologia e incitação a crimes contra a vida e maus tratos contra animais já são crimes cibernéticos atentatórios aos Direitos Humanos presentes na rede.

Assim, percebe-se que, infelizmente, os criminosos são mais rápidos que os legisladores. Isso acontece em todo o mundo e o Brasil não é exceção. Ainda mais, em se tratando de Internet, que passou a ser largamente utilizada no

Brasil. O ordenamento pátrio não possui legislação específica a respeito de crimes virtuais. Evidentemente, no combate aos crimes virtuais, a Justiça utiliza o Código Penal, que data de 1940. Fica evidente, portanto, a necessidade de uma legislação específica para regular as relações sociais, relações estas cada vez mais complexas e numerosas devido ao aumento da velocidade de comunicação entre as diversas partes do Globo terrestre.

A iniciativa pública não se preocupou, além disso, em estabelecer políticas e ações concretas e efetivas de enfrentamento a estes fenômenos complexos, que envolvessem variáveis econômicas, sociais e culturais, com desdobramentos e implicações nos campos da ética, da moral, da educação, da saúde, do direito, da segurança pública, da ciência e da tecnologia.

Ante a essa urgente necessidade de oferecer uma resposta eficiente, consistente e permanente no Brasil para os graves problemas relacionados ao uso indevido da Internet para a prática de crimes e violações contra os Direitos Humano; foi fundada, em 20 de dezembro de 2005, por um grupo de cientistas da computação, professores, pesquisadores e bacharéis em Direito, a SaferNet Brasil, que se consolidou como entidade de referência nacional no enfrentamento aos crimes e violações aos Direitos Humanos na Internet.

Assim, A SaferNet Brasil é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial, que tenta enfrentar o tema em seus vários aspectos. Dessa forma, reúne dados numéricos de ocorrência de crimes através da Internet. Observe-se, assim, a tabela abaixo, que exemplifica o número das principais condutas delituosas praticadas em ambiente de Rede.

Tabela 01 - Denúncias de 1 de Janeiro de 2008 a 1 de Julho de 2008

| **Tipo de Conteúdo** | **Período de 1-1-2008 a 1-7-2008** | | |
|---|---|---|---|
| | Domínio *Orkut* | Domínio Não-*Orkut* | **Única** |
| **Apologia e Incitação a crimes contra a Vida** | 8763 | 305 | **9068** |
| **Homofobia** | 567 | 51 | **618** |
| **Intolerância Religiosa** | 1286 | 85 | **1371** |
| **Maus Tratos Contra Animais** | 1006 | 116 | **1122** |
| **Neo Nazismo** | 1801 | 90 | **1891** |
| **Pornografia Infantil** | 24852 | 3024 | **27876** |
| **Racismo** | 1243 | 137 | **1380** |
| **Xenofobia** | 706 | 31 | **737** |
| Todos | **40224** | **3839** | **44063** |

**Fonte: http: //www..safernet.org.br/site/indicadores. Observa-se aí uma preponderância da pornografia infantil na Internet.**

### 7.1.1 Do Homicídio e das Lesões Corporais

Ao se afirmar que a prática de crimes materiais por excelência poderia ocorrer com a utilização de ferramentas telemáticas, qualquer pessoa imaginaria que tudo não passa de uma idéia ligada à literatura de ficção científica. Com a tecnologia atual, com o avanço do que se denominou Telemedicina, é crível a prática de homicídios ou lesões corporais em ambiente de Rede.

Com a Telemedicina, tornou-se possível a realização de consultas, exames, outros procedimentos e complexas cirurgias à distância. Nestas, com o uso de hardware e software próprios, além da rede de banda larga, o cirurgião fica em um lugar, enquanto o paciente em outro, tudo a permitir que, dolosa ou culposamente, o agente possa ofender a integridade corporal do operado, ou até que o mate, incorrendo, pois, nas hipóteses dos arts. 121 e 129, respectivamente, do Código Penal.

De se lembrar que tanto o homicídio quanto a lesão corporal são crimes de forma livre, podendo ser praticados por qualquer meio escolhido pelo agente, inclusive a Internet. Materiais e de dano, de maneira que a consumação acontece com a efetiva lesão ao bem jurídico tutelado, respectivamente vida e integridade física, de sorte que, pela regra geral do art. 70, caput, do Código de Processo Penal, a competência será a do lugar onde o resultado se produzir; ou seja, a competência será a do lugar onde a lesão ou homicídio ocorrer. No caso da tentativa, admissível somente nos crimes dolosos, a competência será a do lugar em que for praticado o último ato de execução, na hipótese, onde o clínico se encontra.

Outra hipótese factível de crime contra a vida é a prevista no art. 122, do Código Penal, nas modalidades de instigação ou induzimento ao suicídio, pois tanto dar a idéia, inspirar e incutir, quanto fomentar e estimular podem ser realizados através da Internet, já que o delito em apreço é de forma livre.

### 7.1.2 Dos Crimes Contra a Honra

Os crimes contra a honra são a injúria, a difamação e a calúnia e encontram-se capitulados nos arts. 138, 139 e 140, do Código Penal. Também são disciplinados no Código Eleitoral (arts. 324 a 326, da Lei nº 4737/65) e na Lei de Imprensa (arts. 20 a 22, da Lei nº 5250/67). Os preceitos primários constantes destes artigos são praticamente idênticos, havendo diferença apenas no concernente à matéria a que se aplicam, corolário do princípio da especialidade. Os crimes ora analisados violentam a honra objetiva e subjetiva da vítima. A honra objetiva é a reputação da vítima, a sua moral, perante a Sociedade. Por honra subjetiva, entende-se o sentimento da pessoa a respeito de sua conduta moral e intelectual.

Essa diferenciação é importante, pois, tanto a calúnia, quanto a difamação, atingem a honra objetiva da vítima; a injúria, ofende a honra subjetiva da vítima. Assim, na calúnia, o agente atribui à vítima, a prática de fato definido

como crime; na difamação, agente ativo atribui ao sujeito passivo a prática de fato ofensivo à reputação da vítima, maculando-lhe a reputação. Na injúria, o agente ativo propala qualidade negativa da vítima, em relação aos seus atributos morais,intelectuais ou físicos.

Com relação à calúnia e à difamação, algumas distinções devem ser estabelecidas. Com efeito, há que se perquirir se os delitos ocorreram em página aberta (site), ou através de correspondência eletrônica (email), que por sua vez pode ser direcionada a determinada pessoa ou a um grupo. Isto tem relevância pois os tipos penais visam proteger a honra objetiva da vítima, conforme o eminente jurista Guilherme de Souza Nucci:

> (...) considera-se o delito consumado quando a imputação falsa chega ao conhecimento de terceiro que não a vítima. Basta uma pessoa estranha aos sujeitos ativo e passivo para se consumarem a calúnia e a difamação. Se a atribuição falsa de fato dirigir-se direta e exclusivamente à vítima, configura-se a injúria, pois ofendeu-se somente a honra subjetiva[63].

Assim, se a falsa imputação do fato se fizer em site ou através de *e-mails* encaminhados a terceiros que não a vítima; ou através de *e-mail* dirigido à vítima, mas com cópia a terceiros, macular-se-á aí a honra objetiva da vítima. Entretanto, se o *email* for enviado exclusivamente ao ofendido, tratar-se-á de injúria, posto que somente a honra subjetiva será atingida.

Por serem a calúnia e a difamação exemplos de crime formal, não se exige a efetivação do resultado externo à conduta do agente. O foro, competente, portanto, é o da atividade, independentemente do efetivo dano, que é mero exaurimento; ou seja, o foro competente é aquele onde o agente proferiu a calúnia, independentemente de onde esteja o provedor, roteador etc., excetuando-se a regra do artigo 73 do Código de Processo Penal.

Já com relação à injúria, algumas considerações devem ser feitas. A injúria é um insulto que macula a honra subjetiva, arranhando o conceito que a vítima faz de si mesma. A consumação ocorre quando a ofensa chega ao conhecimento da vítima, independentemente de que terceiros dela tenham

---

[63] NUCCI, Guilherme de Souza. Código penal comentado. São Paulo: Revista dos Tribunais, 2000. 957 p. p. 371.

sabido, detalhe que implica diretamente na fixação do foro competente, que não se vincula não mais ao local onde agiu o ofensor, mas àquele onde o ofendido tomou conhecimento; diferentemente do que acontece nas hipóteses anteriores.

Desta forma, a injúria pode ser praticada de forma livre no ambiente de rede, quer através de sites, *e-mails* com cópia, ou até mesmo fechados (dirigidos direta e exclusivamente do agente ao ofendido), escritos ou sonoros, encriptados ou não, desde que a vítima deles tenha conhecimento. No entanto, a injúria real não pode ser praticada pela Internet, porque composta de violência ou vias de fato.

A injúria qualificada ou racial, preconizada no art. 140 § 3º do Código Penal, também pode ser praticada pela Internet. Não somente esta manifestação de preconceito pode ocorrer através da rede, mas também a todas as formas previstas no art. 20 da Lei nº 7.716/89, abaixo transcrito:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
> Pena: reclusão de 1 (um) a 3 (três) anos e multa.
> § 1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos, propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo.
> Pena: reclusão de 2 (dois) a 5 (cinco) anos e multa.
> § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza.
> Pena: reclusão de 2 (dois) a 5 (cinco) anos e multa.

Tais situações lamentavelmente vêm tomando corpo na *Web*. Muitos são os *sites* e tantos os *e-mails* que utilizam de elementos referentes a raça, cor, etnia, religião ou origem, quer direcionados a determinada pessoa, quer ao grupo. De fato, a liberdade de expressão, que atinge seu ápice através da Internet, permite que pessoas com desvio de caráter manifestem seus mais odiosos preconceitos. Isso constitui um paradoxo, pois, ao mesmo tempo em que a Rede oferece tablado para que qualquer um manifeste o seu pensamento, cria grupos reacionários dos mais variados matizes. Por este motivo é que o Direito Penal deve interferir.

## 7.3 Da Ameaça

Por ser crime formal e de forma livre, pode ser praticado através da Internet, o que ocorre com regular freqüência. Encontra-se o crime, capitulado no art. 147 do CP. Sua conduta é a de ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave. Portanto, a finalidade do delito de ameaça é atemorizar a vítima.

O momento consumativo ocorre no instante em que a vítima toma conhecimento do mal prenunciado, ainda que não se sinta intimidada; o que pode ocorrer tanto por *site*, quanto por *emails*, escritos ou sonoros, fechados ou abertos, enfim, por palavras, escritos ou gestos que possam ser transmitidos pela Internet.

## 7.4 Da Incitação ao Crime

Encontra-se esse tipo penal no artigo 286 do CP, que pune qualquer pessoa por incitar publicamente a prática de crime. Trata-se de crime contra a paz pública. Assim, quem criar um site ou enviar e-mails, para incitar os usuários a cometerem delitos, estará incorrendo no delito acima tipificado. Isso ocorre porque tanto o site, quanto o correio eletrônico, conferem publicidade à incitação. E tal incitação poderá ser para que se cometa qualquer tipo de infração penal, desde que determinada. O crime ocorre, mesmo que ninguém, devido à incitação, venha a cometer o delito em questão, já que se trata de crime formal.

Os mais comuns, encontrados na Internet, são de incitação à prática de crimes de racismo, de intolerância religiosa ou de opções sexuais. A incitação compreende, de igual modo, o induzimento e a instigação.

## 7.5 Da Apologia de Crime ou de Criminoso

O artigo 287 do CP tipifica como infração penal fazer, publicamente, apologia de fato criminoso ou de autor de crime. Fazer apologia significa exaltar, enaltecer, elogiar. O bem jurídico tutelado aqui é a paz pública. Ressalte-se que, de fato, não configura o crime em questão, a apologia de contravenção penal ou de conduta ou prática de ato imoral.

Com relação à apologia de autor de crime, o elogio, o enaltecimento deve ser a respeito de crime por ele cometido, ou seja, deve enaltecer sua conduta criminosa e não seus atributos morais ou intelectuais. Em ambiente telemático, a criação de um site ou o envio de correio eletrônico conferem publicidade à apologia de fato criminoso ou de autor de crime, configurando assim a figura delitiva de apologia de crime ou de autor de crime.

## 7.6 Do Favorecimento à Prostituição

Configura o favorecimento da prostituição, a conduta prescrita no artigo 228 do CP, consistente em induzir ou atrair alguém à prostituição, facilitá-la ou impedir que alguém a abandone. É crível que o agente, em ambiente telemático, possa praticar tal crime ao induzir, atrair ou facilitar a prostituição.

Através da Internet, poderá ser cometido o crime em tela, se o agente ativo criar uma página, com fotografias de prostitutas, ou enviar *emails* a diversos usuários, induzindo, atraindo ou facilitando, quer as meretrizes, quer os usuários, à prostituição. Nesta conformidade, constituem condutas que configuram o crime: arranjar fregueses para as prostitutas, endereçar mulheres à prostituição e encaminhar mulheres a outros lugares com o fim de prostituí-las. É importante frisar que não se trata de crime habitual, bastando, para a sua configuração, a realização única da figura típica em questão.

## 7.7 Do Rufianismo

O crime capitulado no artigo 230 do CP não só pode ser praticado através da Internet, como, infelizmente, vem se tornando assaz comum. Uma procura nos sites de busca, utilizando-se as palavras-chave sexo e classificados, demonstrará o aumento da criminalidade nesse tipo penal.

Há páginas através das quais é possível a contratação de prostitutas *on line*, que atendem em domicílio, sendo a conta debitada no cartão de crédito do usuário. Cuida-se, nesse caso, de tirar proveito da prostituição alheia, participando diretamente de seus lucros ou fazendo-se sustentar, no todo ou em parte, por quem a exerça.

## 7.8 Da Pornografia Infantil

A pornografia infantil é crime já bem definido no Estatuto da Criança e do Adolescente no seu artigo 241. O aparecimento da *web* facilitou e muito a prática da pornografia com jovens e adolescentes principalmente pela disseminação da falsa idéia de que não é possível a identificação dos agentes e o rastreamento de tal conduta em ambiente virtual.

Tal prática não é recente. Na história antiga há relatos de que o Grande Rei Persa, Dario II, realizava práticas libidinosas com seus jovens pajens. Artistas gregos, sem qualquer repressão, pintavam quadros e também faziam festinhas de orgia com jovens e crianças. A exploração de crianças e jovens esteve presente também no Império Romano, nos Feudos e na colonização das Américas. Portanto, a prática de pornografia infantil não é recente e também não apareceu por causa da Internet.

Através da Internet, a condição de anônimo é quase que totalmente alcançada, o que faz com os pedófilos tenham a falsa idéia de que podem realizar

seus desejos ilegais sem o risco de serem punidos. Os atuais e populares programas de bate-papo na Internet são meios convidativos para a prática da pedofilia. A legislação penal brasileira, no tocante à pornografia infantil, já prevê punição rigorosa. O artigo 241 do ECA reza que:

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

Percebe-se que a simples publicação de fotos pornográficas infantis já caracteriza crime, mesmo que o site onde se encontre o conteúdo não tenha sido acessado uma única vez.

## 7.9 Dos Crimes contra o Patrimônio

É sabido que os jornalistas ora usam o verbo furtar, ora roubar, ora obter com o fito de noticiarem aos leitores as condutas fraudulentas praticadas com o uso da Internet, especialmente vinculadas à rede bancária. Entretanto, tal dilema não é exclusividade do meio jornalístico. Ocorre dilema idêntico no Direito Penal quando se trata de analisar a tipicidade destes mesmos fatos.

A doutrina especializada divide-se em dois grandes grupos: o primeiro acredita que são típicas todas as condutas em que a elementar “coisa” apareça no preceito primário; o segundo defende a total impossibilidade da prática, em ambiente telemático, de qualquer infração em que figure no tipo a elementar “coisa”, pois, para eles, tal conceito se prende ao mundo físico, tangível, enquanto a Rede trabalha com conceitos intangíveis, virtuais. Para o segundo grupo, a tipicidade somente ocorrerá com a equiparação legal, a exemplo do que se fez com a energia elétrica no crime de furto.

Perfila-se neste trabalho, entretanto, uma posição não tão extremada, quanto a dos grupos supracitados. Não se pode simplesmente dizer se uma interpretação restrita vale ou não em um tema extremamente abrangente (os delitos informáticos), que compreende do acesso não-autorizado a sistemas computacionais aos delitos que hoje são praticados utilizando o computador como uma mera ferramenta.

Nos delitos informáticos próprios, é realmente forçosa a conduta de tentar equiparar a “coisa” algo que só pode ser conhecido realmente em ambiente virtual. Se assim não fosse, estar-se-ia atentando diretamente contra os princípios da legalidade e da tipicidade, visto que o tipo penal poderia ser ampliado sem nenhum cuidado ou mediante interpretações analógicas demasiadamente extensivas, causando uma tamanha insegurança jurídica; e a segurança jurídica é um dos pilares sustentadores de um Estado Democrático de Direito.

No entanto, com relação aos delitos informáticos impróprios, é perfeitamente cabível a subsunção das normas protetivas do patrimônio na esfera penal à pratica dos delitos em questão. Se assim não fosse, estar-se-ia também de uma insegurança jurídica, pois o infrator restaria impune pelo simples uso da ferramenta computacional, mesmo que sua conduta fosse punível na esfera penal; o que não é salutar para uma realidade em que o computador é uma ferramenta extremamente difundida.

A prática vem deixando tal debate doutrinário inócuo, pois, a cada dia, vêm-se tornando indissociáveis os mundos reais e virtuais. Muito difícil, na prática, que um ato praticado no mundo virtual não venha a ter repercussões no

mundo fático; o que ocorrendo faz com que o debate doutrinário acima exposto reste inócuo. Assim, praticamente todas as modalidades de infrações contra o patrimônio podem ser cometidas com a utilização de sistemas de informática. Exemplificar-se-ão abaixo os delitos de furto, dano e estelionato.

Imagine-se um indivíduo que mantém diversos objetos de valor em sua residência, protegidos por sistema informatizado de segurança, que, conectado à Internet, fornece informações ao dono dos objetos. Entretanto, um infrator, invade o sistema e faz com que as senhas de acesso sejam alteradas, facilitando o acesso e possibilitando a prática de furto dos objetos. Tem-se aí a prática do delito de furto utilizando a Internet e o computador como ferramentas de execução.

Um outro exemplo de furto, muito praticado pela Internet, é o da transferência de fundos bancários, quando o criminoso acessa o computador central de um sistema bancário e, mediante um programa especial, desvia pequenas quantias, das contas de vários clientes, para uma conta sua. Em verdade, a subtração de bens que possuam valor econômico, seja de energia, seja de dinheiro em uma conta corrente, é furto como qualquer outro; a diferença está no meio empregado.

Com relação ao delito de dano, a prática de tal delito vem se alastrando através da Internet devido à disseminação dos vírus de computador. O ato de disseminar vírus de computador pode ser enquadrado no delito de dano, já que lhes causa um dano material. O autor do delito será, sempre, a pessoa que disseminou o vírus. No entanto, a mera criação de um vírus não constitui crime, assemelhando-se a *cogitatio* (cogitação), para efeitos penais. Além disso, se o vírus não ocasionar dano efetivo ao computador, não existindo no ordenamento jurídico brasileiro tipificação penal de tal conduta, restará impune o agente na esfera penal.

De maneira geral, configura-se o crime de estelionato, quando alguém obtém, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. Mediante a fórmula genérica, penaliza qualquer espécie de fraude.

Dessarte, verifica-se que o crime de estelionato, na sua modalidade básica e em seu § 3º, também pode ser cometido através da Internet.

Nesse caso, a conduta do agente ativo consiste no emprego do meio informático, para induzir ou manter a vítima em erro, obtendo com isso vantagem ilícita. Tais condutas são as denominadas fraudes eletrônicas. Uma forma bastante utilizada na prática deste delito é a de efetuar compras, debitando-as no cartão de crédito da vítima. Um outro exemplo também ocorre quando o agente utiliza indevidamente programa de computador para obter reimpressão de cautelas de ações ao portador, mediante a utilização de senha de funcionária encarregada da emissão dos certificados, negociando-os em Bolsa de Valores.

Importante também relatar algo bastante presente na Internet, o chamado *phishing attacks*. Consiste no envio de *emails* com *links* para páginas semelhantes às páginas oficiais de bancos ou instituições financeiras. Essa semelhança tem a finalidade de induzir a erro o usuário de tais serviços, para que o mesmo forneça suas senhas de acesso. Com a obtenção dessas senhas, o criminoso visa obter vantagem indevida. Esse é um exemplo clássico de estelionato pela Internet.

Dessa forma, observa-se que é fácil a percepção de que o cometimento de crimes contra o patrimônio em ambiente telemático vem crescendo de maneira considerável. O ordenamento jurídico, de maneira geral, ainda alcança a maioria das condutas, mas isso não pode ser argumento para que se prescinda de uma legislação específica; visto que, pela magnitude que assumiu, a Internet potencializou as relações sociais e, conseqüentemente, os conflitos decorrentes de tais relações.

## 8 CONCLUSÃO

Com o uso de ferramentas o homem conseguiu atingir a hegemonia na face da Terra. Das quatro revoluções tecnológicas analisadas, que se fizeram com o efetivo uso de máquinas, quais sejam, a industrial, a elétrica, a informática e a digital, a última se destaca por ainda estar se desenvolvendo e por nela se inserir a Rede Mundial de Computadores – a Internet.

A Internet hoje é uma larga infra-estrutura de informação, o protótipo inicial do que é frequentemente chamado a Infra-Estrutura Global ou Galáxia da Informação. A história da Internet é complexa e envolve muitos aspectos - tecnológicos, organizacionais e comunitários. E sua influência atinge não somente os campos técnicos das comunicações via computadores mas toda a sociedade, na medida em que usamos cada vez mais ferramentas *on-line* para fazer comércio eletrônico, adquirir informação e operar em comunidade.

A Internet permite a prática remota de condutas não-éticas e indesejadas das mais variadas naturezas, dentre elas as infrações penais, crimes ou contravenções. Pela própria estrutura e natureza da Rede Mundial de Computadores, as condutas criminosas apresentam uma potencialidade lesiva ainda incomensurável.

O Brasil está entre os dez países que mais utilizam a Internet, num mercado promissor e crescente. O progresso tecnológico em exponencial crescimento exige o aperfeiçoamento técnico-jurídico e o aperfeiçoamento também dos meios preventivos e coercitivos da violação dos bens da vida penalmente tutelados.

Os delitos informáticos estão ficando cada vez mais sofisticados e preocupando tanto usuários da Internet como juristas de todo o mundo. No Brasil, o Código Penal ainda consegue tipificar a maioria dos delitos cometidos em ambiente de Rede, como, por exemplo, a pornografia infantil, estelionato, o furto, o rufianismo. Alem disso, em leis esparsas estão também disciplinados outros

tipos penais informáticos, tendo como exemplo o acesso não-autorizado a sistemas computacionais do sistema eleitoral.

Mas considerando-se que o rápido avanço da tecnologia da informação é assimilada rapidamente por toda a comunidade, inclusive pelos criminosos, de forma que o legislador penal não consegue acompanhar esta evolução, é conveniente que os novos tipos penais que porventura devam ser criados sejam aqueles que a doutrina denomina de abertos, de maneira que os preceitos primários sejam completados por normas de inferior hierarquia, permitindo-se que a normal penal incriminadora tenha eficiência na resposta aos crimes advindos com a modernidade.

Outra controvérsia abordada foi a própria definição do tema. Viu-se que muito se discute se os crimes praticados por meio da informática são todos aqueles em que um computador ou outros recursos da informática são usados para a prática de condutas delituosas, ou se são apenas aqueles em que os sistemas de informática são atingidos. Parece claro que a atenção deve ser voltada para ambas as espécies de conduta, pois apresentam peculiaridades que as fazem merecer um estudo à parte.

Demonstrou-se que o conceito de Delito Informático, também denominado Infração Penal Informática, abarca os crimes e as contravenções penais informáticas; e que delito Telemático, também denominado Infração Penal Telemática, é espécie do gênero Delito Informático.

Viu-se que atualmente muitas pessoas generalizam o termo *hacker* como sendo todo delinqüente virtual. A nomenclatura ideal para tais delinqüentes em ambiente de Rede seria *cracker*. No entanto, observou-se também que não se pode ter uma visão romântica de que o *hacker* é apenas um curioso. Portanto, neste trabalho, optou-se por excluir as visões românticas e a de que o *hacker* é necessariamente um criminoso; aproximando-se mais da realidade.

O bem jurídico penal tutelado nos delitos informáticos é a Segurança Informática. Este bem jurídico é de natureza difusa, pois além de atingir indeterminado número de pessoas, gera conflituosidade entre elas ou grupos, e as empresas, grandes ou pequenas, embora todos, pessoas e empresas,

possuam legítimos interesses de uso e fruição das estruturas e potencialidades da Rede Mundial de Computadores.

E tal proteção é imprescindível, pois, se a “ultima ratio” não garantí-la, apenas a utilização lúdica restará para a Rede, em prejuízo de atividades empresariais, comerciais, educacionais etc.; que, inquestionavelmente, geram empregos e tributos, enfim, legítimos dividendos das mais variadas espécies. Dessa forma, é fácil perceber que o Estado, através do Direito Penal, deve efetivamente interferir na Internet, sob pena de total destruição desta. Tal necessidade é factível, pois os demais ramos do Direito não têm se apresentado eficazes a enfrentar as condutas prejudiciais e indesejadas praticadas por pessoas e empresas inescrupulosas.

Um outro questionamento levantado foi a problemática da definição do local do crime nos delitos informáticos. Viu-se o que a legislação pátria disciplina com relação a tal matéria, ocorrendo, em seguida, a aplicação destas normas ao caso dos delitos informáticos. Observou-se, assim, que basta que o delito 'toque' o território nacional para que o Brasil, exercendo sua soberania, possa 'dizer' o direito no caso concreto. No caso, dos delitos ocorridos exclusivamente em território nacional, demonstraram-se as regras existentes para a fixação de competência para julgamento dos delitos em análise.

Assim, a definição do lugar do delito telemático se resolve como em qualquer outra espécie de crime, e se dá com a análise de sua classificação, a fim de se saber se ele é material, formal ou de mera conduta; se consumado ou tentado; de forma livre etc., tudo a depender, portanto, dos conhecimentos de direito material do intérprete.

Portanto, apesar do considerável aumento dos crimes à distância e plurilocais através da telemática, as regras de competência existentes em nosso ordenamento jurídico não necessitam de alteração, bastando para a solução dos dilemas porventura existentes o imprescindível rigor hermenêutico à vista do caso concreto.

O senso comum, muitas vezes, veicula a idéia de que o espaço cibernético é totalmente sem lei e sem regras para punir quem as transgredir.

Essa idéia contribui de certa forma para o aumento das infrações penais telemáticas que vêm sendo praticadas no Brasil. Demonstrou-se, entretanto, que as principais condutas nocivas em ambientes telemáticos ainda são alcançadas pelo ordenamento pátrio e encontram satisfatória resposta do Sistema Penal. Apesar disso, não se pode prescindir da inserção de tipos penais específicos, a fim de que tal resposta venha a ser mais efetiva.

Dessa forma, a própria tecnologia, através dos códigos de segurança, assinatura digital, registros, criptografia, números, está buscando disciplinar os novos usos gerados pela tecnologia. Esta, aliada a uma proteção jurídica globalizada e à crescente conscientização do usuário, certamente permitirá, em futuro próximo, o uso pacífico da Internet, criando um ambiente em que a segurança e a paz social possam ser concretizadas.

## REFERÊNCIAS


ALMEIDA FILHO, José Carlos de Araújo; CASTRO, Aldemario Araújo. *Manual de Informática Jurídica e Direito da Informática.* Rio de Janeiro: Forense, 2005.

ARAÚJO JÚNIOR, João Marcello. *Dos Crimes contra a ordem econômica.* São Paulo: Revista dos Tribunais, 1995.

BOBBIO, Norberto*. A Era dos Direitos*. Trad. de Carlos Nelson Coutinho. Rio de Janeiro: Campus, 1992.

BRASIL. Constituição federal, código penal, código de processo penal. Organizado por Luiz Flávio Gomes. 8. ed. rev. e ampl. São Paulo: Revista dos Tribunais, 2008.

_____. Lei nº. 9.609, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em: <www.planalto.gov.br> Acesso em: 19 set. 2008.

CABRAL, Plínio. *Direito Autoral: dúvidas e controvérsias.* São Paulo: Harbra, 2000.

CÔRREA, Gustavo Testa. *Aspectos jurídicos da Internet.* São Paulo: Saraiva, 2000.

DEMERCIAN, Pedro; MALULY, Jorge Assaf. Curso de processo penal. São Paulo: Atlas, 1999.

FERREIRA, Aurélio Buarque de Holanda. *Novo Dicionário da língua portuguesa.* 2. ed., rev. e aum., 36ª impressão, Rio de Janeiro: Editora Nova Fronteira.

FERREIRA, Ivete Senise. *Os Crimes de Informática*. In: BARRA, Rubens Prestes; ANDREUCCI, Ricardo Antunes. Estudos Jurídicos em Homenagem a Manoel Pedro Pimentel. São Paulo: Editora Revista dos Tribunais, 1992.

GANDELMAN, Henrique*. De Gutenberg à Internet: direitos autorais na era digital.* Rio de Janeiro: Record, 1997. p.36-7.

GRANDE dicionário Larousse cultural da língua portuguesa. São Paulo: Nova Cultural, 1999.

GRECO FILHO, Vicente. *Algumas observações sobre o direito penal e a Internet.* São Paulo: Saraiva, 2004.

LEONARDI, Marcel. *Responsabilidade Civil dos Provedores de Serviços de Internet*. São Paulo: Editora Juarez de Oliveira, 2005.

LICKS, Otto Banho; ARAÚJO JÚNIOR, João Marcelo. *Aspectos Penais dos Crimes de Informática no Brasil.* In: Revista do Ministério Público. São Paulo: Nova Fase, 1994, pp. 82-103.

LORENZETTI, Ricardo Luis. *Informática, Cyberlaw, E-commerce*, in *Direito & Internet – Aspectos Jurídicos Relevantes,* coordenado por Newton de Lucca e Adalberto Simão Filho, Bauru: Edipro, 2000.

MARZOCHI, Marcelo de Luca. *Direito.br: Aspectos Jurídicos da Internet no Brasil.* São Paulo: Ltr, 2000.

PAESANI, Liliana Minardi. *Direito de informática: comercialização e desenvolvimento internacional do Software*. São Paulo: Atlas, 2005.

_____. *Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil*. São Paulo, Atlas, 2006.

PINHEIRO, Reginaldo César. *Os crimes virtuais na esfera jurídica brasileira.* Boletim IBCCRIM – Publicação Oficial do Instituto Brasileiro de Ciências Criminais. São Paulo, ano 8, n.101.

REIS. Maria Helena Junqueira. *Computer Crimes: a criminalidade na era dos computadores*. Belo Horizonte: Del Rey, 1996.

ROSSINI, A. E. S. *Informática, telemática e Direito Penal.* São Paulo: Memória Jurídica, 2004.

SCORZELLI, Patrícia. *A comunidade cibernética e o Direito.* Rio de Janeiro: Lumen Juris, 1997.

SMANIO, Gianpaolo Poggio. *Tutela penal dos direitos difusos.* São Paulo: Atlas, 2000.

TOFLER, Alvin. *A terceira onda*. Trad. João Távora. 28. ed. Rio de Janeiro: Record, 2005.

UNICEF. *Pornografia Infantil.* Disponível em: <http://www.unicef.org/brazil/pt/activities_10793.htm>. Acesso em: 11 nov. 2008.

VASCONCELOS, Fernando Antônio de. *Internet: responsabilidade do provedor pelos danos praticados.* Curitiba: Juruá, 2003.

VIANNA, Túlio Lima. *Fundamentos de direito penal informático: do acesso não-autorizado a sistemas computacionais.* Rio de Janeiro: Forense, 2003.