UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
CENTRO DE CIÊNCIAS SOCIAIS E JURÍDICAS - CEJURPS
CURSO DE DIREITO

CRIMES DE INFORMÁTICA

PEDRO AMÉRICO DE SOUZA NETO

Itajaí, novembro de 2009

UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
CENTRO DE CIÊNCIAS SOCIAIS E JURÍDICAS - CEJURPS
CURSO DE DIREITO

CRIMES DE INFORMÁTICA

PEDRO AMÉRICO DE SOUZA NETO

Monografia submetida à Universidade do Vale do Itajaí – UNIVALI, como requisito parcial à obtenção do grau de Bacharel em Direito.

Orientador: Professor Guilherme Augusto Correa Rehder

Itajaí. novembro de 2009

TERMO DE ISENÇÃO DE RESPONSABILIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando a Universidade do Vale do Itajaí, a coordenação do Curso de Direito, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Itajaí [SC], novembro de 2009

Pedro Américo de Souza Neto
Graduando

PÁGINA DE APROVAÇÃO

A presente monografia de conclusão do Curso de Direito da Universidade do Vale do Itajaí – UNIVALI, elaborada pelo graduando Pedro Américo de Souza Neto, sob o título Crimes de Informática, foi submetida em 20 de novembro de 2009 à banca examinadora composta pelos seguintes professores: Guilherme Augusto Correa Rehder e Wellington César de Souza(membro), e aprovada com a nota _____.

Itajaí [SC], novembro de 2009

Guilherme Augusto Correa Rehder
Orientador e Presidente da Banca

MSc. Antônio Augusto Lapa
Coordenação da Monografia

ROL DE ABREVIATURAS E SIGLAS

Ampl.	Ampliada
Art.	Artigo
Atual.	Atualizada
CP	Código Penal
CRFB	Constituição da República Federativa do Brasil de 1988
Ed.	Edição
Min.	Ministro
MSc.	Mestre
n.	Número
p.	Página
Rel.	Relator
Rev.	Revista
v.	Volume

ROL DE CATEGORIAS

Rol de categorias que o Autor considera estratégicas à compreensão do seu trabalho, com seus respectivos conceitos operacionais.

Cracker

"são pessoas especializadas em quebrar senhas. Ao contrário dos *hackers*, os *crackers* têm intenção criminosa (o cometimento de fraudes, espionagem etc..)".[1]

Crime de Informática

"É a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar".[2]

Hacker

"Este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver quem consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual. [...]".[3]

Hardware (Equipamento de informática)

"O equipamento é a base que permite a operação informática e compreende: a unidade central de processamento (CPU), com a memória Rom e a memória Ram, aos quais somam-se todos os diversos aparelhos periféricos que servem

---

[1] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2.ed. Rio de Janeiro: Lumen Juris, 2003. p. 219.

[2] ROSA, Fabrízio. **Crimes de Informática** .2.ed. Campinas: Bookseller, 2006. p. 55.

[3] NOGUEIRA, Sandro D'Amato. **Crimes de Informática.** São Paulo: BH Editora, 2008. p. 61

para introduzir informação (*input*), o teclado (*keyboard*) e o *disk drive* e para dar saída (output) os monitores e as impressoras. [...]".[4]

Informática

"É uma ciência cujo objecto de estudo relaciona com o tratamento lógico de conjunto de dados, utilizando técnicas e equipamentos que possibilitam o seu processamento de modo a obter informação que depois poderá ser armazenada e/ou transmitida".[5]

Internet

"A Internet consiste num conjunto de tecnologias para acesso, distribuição e disseminação de informação em redes de computadores". [6]

IP – Internet Protocol

"Versão numérica do nome do hospedeiro. Todo computador de rede tem um endereço IP".[7]

Site

"Conjunto de documentos apresentados ou disponibilizados na Web por um indivíduo, instituição ou empresa, e que pode ser fisicamente acessado por um computador e em endereço específico na rede".[8]

Software (programa de computador)

"Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de

---

[4] LORENZETTI,Ricardo Luis. Informática, Cyberlaw, E-Commerce. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. São Paulo: Quartier Latin, 2005. p. 494.

[5] MOREIRA, Rui. **Introdução à informática.** Disponível em: <http://www2.ufp.pt/~rmoreira/MTC/Aula3_II.pdf>. Acesso em: 02 de outubro de 2009.

[6] ROSA, Fabrízio. **Crimes de Informática.** 2.ed. Campinas: Bookseller, 2006. p. 35.

[7] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003. p. 222.

[8] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003. p. 223.

qualquer natureza, de emprego necessário em máquinas automáticas de tratamento de informação, dispositivos, instrumentos ou equipamentos periféricos, baseadas em técnica digital ou análoga, para fazê-los funcionar de modo e fins determinados".[9]

Vírus

"[...] programa de computador escrito em linguagem de programação, que faz a contaminação de outros programas do computador através de sua modificação de forma a incluir uma cópia de si mesmo. [...]".[10]

Web

"Também se usa a sigla WWW: World Wide Web. É o recurso ou serviço oferecido na Internet e que consiste num sistema distribuído de acesso à informações, as quais são apresentadas na forma de hipertexto, com elos entre os documentos e outros objetos (menus, índices), localizados em pontos diversos da rede".[11]

---

[9] BRASIL. Lei nº 9.609 de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L9609.htm>. Acesso em; 23 de julho de 2009.

[10] CONCERINO, Arthur José. Internet e Segurança são Compatíveis? *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. São Paulo: Quartier Latin, 2005. p. 157.

[11] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais.** 2 ed. Rio de Janeiro: Lumen Juris, 2003. p. 223-224.

SUMÁRIO

RESUMO

A presente monografia tem como objetivo apresentar os principais aspectos da criminalidade informática, vale dizer, dos delitos que emergiram do rápido avanço tecnológico, em especial com a popularização do computador e da Internet. Porém, este avanço tecnológico não foi acompanhado pelos poderes públicos instituídos, notadamente o brasileiro, à míngua de legislação e de agentes capacitados para combater e prevenir esses crimes. Buscou-se analisar na legislação brasileira quais condutas podem ser enquadradas como delito no ordenamento atual e aquelas que não estão previstas como tal, fazendo-se necessária a edição de lei para que estejam tipificadas. Também se realizou uma análise de como outros países têm enfrentado os problemas causados pelos crimes de informática. O presente trabalho de conclusão de curso foi subdividido em três capítulos: o primeiro trata da parte principiológica aplicada aos crimes de informática, assim como da parte histórica; o segundo capítulo faz uma análise dos sujeitos dos crimes de informática e dos crimes de informática em espécie; o terceiro capítulo, por sua vez, trata do direito comparado, analisando a legislação de outros países, assim como o atual ordenamento brasileiro.

INTRODUÇÃO

O presente trabalho tem como objeto os crimes de informática e, como objetivo geral, analisar, além dos crimes já tipificados pelo ordenamento jurídico brasileiro, as condutas danosas praticadas por meio da informática que ainda não possuem previsão legal incriminadora.

Esta pesquisa tem como *objetivos*: *institucional*, produzir monografia para obtenção do grau de bacharel em Direito, pela Universidade do Vale do Itajaí – Univali; *geral,* investigar alguns pontos acerca dos crimes de informática.

Para a investigação do objeto e como meio para se atingir os objetivos propostos adotou-se o método indutivo[12], operacionalizado com as técnicas[13] do referente[14], da categoria[15], dos conceitos operacionais[16] e da pesquisa bibliográfica, em conjunto com as técnicas propostas por Colzani[17], dividindo-se o relatório final em três capítulos.

Na presente pesquisa foram levantados os seguintes problemas:

1º) O Brasil possui leis para punir as condutas abusivas praticadas através da informática? Hipótese: em geral, não. São raros os casos em que se pode aplicar a legislação vigente para os crimes de informática.

---

[12] O método indutivo consiste em 'pesquisar e identificar as partes de um fenômeno e colecioná-las de modo a ter uma percepção ou conclusão geral'. [PASOLD, 2001, p. 87].

[13] "Técnica é um conjunto diferenciado de informações reunidas e acionadas em forma instrumental para realizar operações intelectuais ou físicas, sob o comando de uma ou mais bases lógicas investigatórias". [PASOLD, 2001, p. 88].

[14] Referente "é a explicitação prévia do motivo, objetivo e produto desejado, delimitando o seu alcance temático e de abordagem para uma atividade intelectual, especial-mente para uma pesquisa". [PASOLD, 2001, p. 63].

[15] Categoria "é a palavra ou expressão estratégica à elaboração e/ou expressão de uma idéia". [PASOLD, 2001, p. 37].

[16] Conceito Operacional é a "definição para uma palavra e/ou expressão, com o desejo de que tal definição seja aceita para os efeitos das idéias que expomos". [PASOLD, 2001, p. 51].

[17] COLZANI, Valdir Francisco. Guia para elaboração do trabalho científico.

2º) Ainda que tenha uma legislação interna aplicável, isto basta para um combate eficaz à criminalidade informática? Hipótese: não, para um combate efetivo é necessária a cooperação entre os países.

Subdividiu-se o presente trabalho em três capítulos. No primeiro capítulo tratará dos princípios, constitucionais e penais, aplicados aos crimes de informática. Também serão tratados: a história do computador, da Internet e dos crimes de informática.

O segundo capítulo fará uma análise dos sujeitos ativos e passivos dos crimes envolvendo a informática. Ainda identifica algumas condutas danosas praticadas através da informática, trazendo as principais características de cada uma delas

Por fim, no terceiro capítulo será feita uma análise de como os crimes de informática são tratados em outros países, assim como da atual legislação brasileira.

As considerações finais apresentarão a síntese de cada capítulo, demonstrando se as hipóteses foram ou não confirmadas.

CAPÍTULO 1

PRINCÍPIOS E HISTÓRIA DOS CRIMES DE INFORMÁTICA

1.1 PRINCÍPIOS

1.1.1. Princípio da Legalidade

O princípio da legalidade é previsto na Constituição da República Federativa do Brasil, em seu art. 5º, II[18], que determina que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei".

Alexandre de Moraes[19] comenta este importante princípio:

> O art. 5º, II, da CF preceitua que ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei. Tal princípio visa combater o poder arbitrário do Estado. Só por meio das espécies normativas (CF, art. 59) devidamente elaboradas, conforme as regras de processo legislativo constitucional, podem se criar obrigações para o indivíduo, pois são expressão da vontade geral. Com o primado da lei, cessa o privilégio da vontade caprichosa do detentor do poder em benefício da lei. [...]

Tal princípio tem muita relevância no direito penal da informática, já razão que ainda não existem leis para os crimes praticados através de meio tecnológico. Desta forma, há práticas que, apesar de causarem graves incômodos e danos à sociedade, não são puníveis. Isto acontece porque muitas das condutas realizadas na Internet ou em qualquer meio similar não têm previsão legal, sendo consideradas atípicas.

---

[18] BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constitui%C3%A7ao.htm>. Acesso em: 23 de abril de 2009.

Carla Rodrigues Araújo de Castro[20] explana sobre a falta de legislação aplicável aos crimes de informática:

> Nos crimes praticados através da informática, ou seja, tipos antigos, nos quais o agente utiliza a informática como meio de execução, como instrumento de sua empreitada, não há dificuldades. O crime é mesmo previsto em sua origem, a forma de sua execução é que inovou, por exemplo, uma ameaça feita pessoalmente não se distingue na tipicidade de uma ameaça virtual.
>
> Problema surge em relação aos crimes cometidos contra o sistema de informática, atingindo bens não tutelados pelo legislador, como dados, informações, *hardware*, *sites, home pages, e-mail* etc.. São condutas novas que se desenvolveram junto com nossa sociedade razão pela qual o legislador de 1940, época do Código Penal, não pôde prever tais tipos penais.

Portanto, não há que se falar em crime relativamente àquelas condutas que ainda não foram previstas pelo legislador como fato típico e, desta maneira, o autor não poderá ser punido nem compelido a deixar de praticá-las.

1.1.2. Princípio da Anterioridade da Lei Penal

A Constituição da República Federativa do Brasil dispôs em seu artigo 5º, XXXIX[21], que "não há crime sem lei anterior que o defina, nem pena sem cominação legal".

Pedro Lenza[22], sobre este dispositivo constitucional, faz um breve comentário:

---

[19] MORAES, Alexandre de. **Direitos Humanos Fundamentais:** Teoria Geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 8. ed. São Paulo: Saraiva, 2007. p. 97

[20] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais.** 2. ed. Rio de Janeiro, Lumen Juris, 2003. p. 217.

[21] BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constitui%C3%A7ao.htm>. Acesso em: 23 de abril de 2009.

[22] LENZA, Pedro. **Direito Constitucional Esquematizado**. 9ªed. Método: São Paulo, 2005. p. 551.

> O art. 5º, XXXIX, consagra a regra do *nullum crimen nulla poena sine praevia lege*. Assim, de uma só vez, assegura tanto o **princípio da legalidade** (ou reserva legal), na medida em que não há crime sem **lei** que o defina, nem pena sem cominação **legal**, com o **princípio da anterioridade**, visto que não há crime sem lei **anterior** que o defina, nem pena sem **prévia** cominação legal.

Na realidade este princípio tem finalidade específica de constitucionalizar o princípio da legalidade para o âmbito do direito penal, como bem afirma Uadi Lammêgo Bulos[23]:

> A Constituição de 1988 compactua-se com o art. 1º do Código Penal: "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal", semelhante ao velho aforismo latino *Nulla crimen nulla poena sine praevia legel.* Prestou homenagem à *tipicidade penal*. Típico é o fato que subsume ao comportamento delituoso, prescrito nas normas penais incriminadoras pelo legislador infraconstitucional.

Assim, tal como o princípio da legalidade, o princípio da anterioridade da lei penal traduz a garantia constitucional de que as condutas cujas previsões em abstrato não estejam previamente consignadas em lei não sejam puníveis.

É o que torna, a título de exemplo, inócua qualquer tentativa de repelir a ação dos *crackers*. De acordo com Fábio Podestá[24]:

> A situação dos "Hackers" ou "Crackers", por ser patológica, muitas vezes tem referência, com a tutela penal da Internet, matéria que se encontra ainda incipiente na legislação correlata diante da incidência do princípio da legalidade estrita diretamente associada a tipificação de crimes para possibilitar a punição de fatos considerados ilícitos pelo legislador.

Um exemplo claro desta situação tem relação com a pedofilia, quando uma pessoa repassava via e-mail para uma pessoa

---

[23] BULOS, Uadi Lammêgo. **Constituição Federal Anotada.** 7. ed. rev. e atual. até a Emenda Constitucional nº 53/2006. São Paulo: Saraiva, 2007. p. 254.

[24] PODESTÁ, Fábio. Direito à Intimidade em Ambiente da Internet. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. São Paulo: Quartier Latin, 2005. p. 519

determinada, fotos ou vídeos eróticos envolvendo crianças ou adolescentes, não praticava crime, de acordo com Carla Castro[25]: “Por outro lado, quem envia um e-mail com uma foto anexada não está tornando público e sim enviando a pessoa determinada, destarte, a conduta é, infelizmente, atípica.”

Somente em 2008 este fato passou a ser considerado como crime, uma vez que o Estatuto da Criança e do Adolescente (ECA) foi alterado através da Lei 11.829/08, com a criação do art. 241-A que prevê reclusão de três meses a seis anos e multa para aquele que “oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente”.

Fica evidente, portanto, o perigo que este tipo de situação acarreta, como no exemplo citado, ficou-se muitos anos sem poder punir aqueles que praticavam um fato tão deplorável e danoso à sociedade.

1.1.3. Inviolabilidade das Correspondências

A inviolabilidade de correspondências está prevista na Constituição da República Federativa do Brasil em seu art. 5º, XII[26] que dispõe:

> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Desta maneira, toda comunicação entre particulares deve ser mantida sob sigilo, admitindo-se a sua violação somente em relação às

---

[25] CASTRO, Carla Rodrigues Araújo. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Lumen Juris: Rio de Janeiro, 2003. p. 46.

[26] BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constitui%C3%A7ao.htm>. Acesso em: 23 de abril de 2009.

comunicações telefônicas mediante ordem judicial. Porém, Alexandre de Moraes[27] faz algumas considerações, de modo a, seguindo os mesmo requisitos, estender também aos demais meios de comunicação:

> É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. Ocorre, porém, que apesar de a exceção constitucional expressa referir-se somente à interpretação telefônica, entende-se que nenhuma liberdade individual é absoluta, [...], sendo possível, respeitados certos parâmetros, a interceptação das correspondências e comunicações sempre que as liberdades públicas estiverem sendo utilizadas como instrumento de salvaguarda de práticas ilícitas.

Assim, a garantia constitucional da inviolabilidade de correspondências deve ser estendida às mensagens privadas realizadas por meio da Internet, sejam elas emitidas via *e-mail*, *chat* (bate-papo virtual), por redes sociais ou fóruns privados, comunicadores instantâneos etc.

Na utilização da Internet, muitos usuários extrapolam em suas condutas, invadindo a privacidade alheia através de programas espiões para capturar o conteúdo da mensagem diretamente ou mesmo da senha do *email* ou similar para ter acesso aos dados contidos nas mensagens armazenadas pela vítima. Sobre a inviolabilidade e a privacidade na Internet, disserta Roberto Senise Lisboa[28]:

> Entretanto, a Internet pode ser utilizada de forma indevida por algumas pessoas, impondo-se reconhecer que, nesse caso, ela proporciona “enormes riscos em matéria de concentração e controle social”. Daí porque não é suficiente a autoregulação do setor. Os direitos socialmente relevantes devem ser protegidos pelo Estado, que possui o papel de agente assegurador das liberdades públicas e do mercado de consumo.

---

[27] MORAES, Alexandre de. **Direitos Humanos Fundamentais**: Comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 8ª ed. São Paulo: Editora Atlas, 2007. p. 140.

[28] LISBOA, Roberto Senise. Quebra da Inviolabilidade de Correspondência Eletrônica por Violação da Boa-fé Objetiva. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. São Paulo: Quartier Latin, 2005. p. 519.

> Não se pode negar que as novas tecnologias constituem-se um grande benefício a humanidade, porém os meios mais avançados de comunicação representam uma séria ameaça a alguns direitos personalíssimos, dentre eles a intimidade e a privacidade.

Uadi Lammêgo Bulos[29] faz algumas anotações acerca da inviolabilidade das mensagens em *e-mails*, com base no que dispõe o art. 5º, XII da Constituição da República Federativa do Brasil[30]:

> As comunicações telemáticas, via internet, estão sujeitas ao império do art. 5º, XII, e da Lei 9.296/96 (art. 1º, parágrafo único), porque nada mais são do que comunicações realizadas via ligação telefônica. Não restam dúvidas a esse respeito. Interpretar a Constituição de outra forma é desconhecer que muitas empresas de grande porte trabalham com redes independentes valendo-se de cabos , fios, fibras óticas, satélites, parabólicas, sistemas infravermelho etc..
>
> Essas comunicações modernísimas podem ser interceptadas do mesmo modo que as convencionais. É nesse contexto que surge o problema da interceptação e uso de e-mail como prova. (..)
>
> Como o e-mail pode ser transmitido para uma malha de servidores até o seu destino, via senha "secreta", ocorrem casos de violação do seu conteúdo, depositado nas caixas postais, colocando em riso o sigilo das comunicações (art. 5º, XII).
>
> Algumas discussões jurídicas vem sendo debatidas em nível de Tribunais Superiores tais como a natureza jurídica do e-mail, a legalidade de sua interceptação, o regime jurídico a que está sujeito etc.
>
> Sem embargo, sendo o e-mail, repita-se, uma comunicação telefônica interagida com a informática, certo é que está sujeito à garantia insculpida no art. 5º, XII. Para que sirva como meio de prova é necessário, em primeiro lugar, verificar o modo de sua interceptação. Só assim é possível perquirir a verdade real ou judicial

Portanto, entende-se que as comunicações realizadas através de sistema telemático estão sob a égide da Constituição brasileira e, assim, são, a princípio, invioláveis. Somente poderá haver a interceptação dessas

---

[29] BULOS, Uadi Lammêgo. **Constituição Federal Anotada.** 7. ed. rev. e atual. até a Emenda Constitucional nº 53/2006. São Paulo: Saraiva, 2007

[30] BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constitui%C3%A7ao.htm>. Acesso em: 23 de abril de 2009.

comunicações, assim como das telefônicas, mediante mandado judicial para fins de investigação criminal ou instrução processual penal.

1.1.4. Propriedade Intelectual e Direitos do Autor

Os direitos de propriedade intelectual, assim como os direitos do autor estão garantidos pela Constituição da República Federativa do Brasil, em seu art. 5º, incisos XXVII, XXVIII e XXIX[31].

Além da Constituição, no Brasil os direitos autorais são protegidos pela Lei 9.610/1998 e também pelo Código Penal que tipifica como crime com pena de detenção de 3 (três) meses a 1 (um) ano, ou multa para aquele que violar direitos de autor e os que lhe são conexos.

Orlando Soares[32] conceitua direito autoral ou autorial como sendo:

> Conjunto de princípios e teorias, que inspiram a elaboração das normas jurídicas, reguladoras do direito atribuído ao autor de obra literária, científica e artística, no sentido de reproduzi-las e explorá-las economicamente, enquanto viver, transmitindo-se aos seus herdeiros e sucessores, observados determinados prazos e condições legais.

A Internet, hoje, proporciona a seus usuários o acesso a uma quantidade gigantesca de dados, tais dados são acessados com facilidade, bastando, por exemplo, digitar a obra de um livro em um site de busca para que se tenha acesso gratuito ao conteúdo na íntegra. Porém, a maioria das obras que circulam livremente na rede é protegida pelos direitos autorais, conforme explica Helenara Braga Avancini[33]

---

[31] BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constitui%C3%A7ao.htm>. Acesso em: 23 de abril de 2009.

[32] SOARES, Orlando. **Comentários à Constituição da República Federativa do Brasil.** 12ª Ed. Rio de Janeiro: Editora Forense, 2006. P. 215.

[33] AVANCINI, Helenara Braga. O Paradoxo da Sociedade da Informação e os Limites dos Direitos Autorais. *In*: ROVER, Aires José (Org.). **Direito e Informática**. Barueri: Manole, 2004. P. 355.

> A Internet facilitou o fluxo da informação a custos baixos e em grande velocidade, tendo como paradigma o livre acesso à informação, contudo, observa-se que grande parte da informação veiculada nessa rede digital está constituída por obras protegidas pelos direitos autorais.

Ocorre que os direitos autorais, após a revolução trazida pela Internet, vem sofrendo críticas de modo que muitos acreditam que o conceito de direito autoral deve ser alterado, eis que vem de encontro com o direito à informação, conforme Avancini[34]:

> Os direitos autorais sofreram um forte impacto no que diz respeito às limitações e exceções no ambiente digital, observando-se uma tendência da comunidade internacional em torná-los cada vez mais taxativos, ao estabelecer uma enorme lista de exceções, mas permitindo na prática a supressão de muitos desses mediante o emprego de dispositivos tecnológicos, o que vai contra o dinamismo exigido pela Era do Conhecimento.
>
> Os limites dos direitos autorais constituem um dos maiores desafios da Sociedade da Informação, implicam mudanças de conceitos do próprio direito autoral, desafiando o operador do direito a compreender e buscar os limites desse paradoxo por intermédio de uma interpretação sistêmica da problemática apresentada.

Porém, a idéia de que os direitos autorais devem sofrer restrições não é totalmente aceito em países como os Estados Unidos que vem criando uma série de leis para combater o compartilhamento de arquivos em que não foram respeitados os direitos do autor, sobre o assunto fala Silvia Simões Soares[35]:

> Nos Estados Unidos a questão é flagrante. Tendo produzido nos últimos anos uma infinidade de leis para aumentar a proteção do *copyright* e ampliar a responsabilidade de quem participa mesmo que indiretamente de infrações, o país é pioneiro não apenas no tocante ao desenvolvimento tecnológico, mas também no que diz respeito à normatização do meio eletrônico frente às novas tecnologias.

---

[34] AVANCINI, Helenara Braga. O Paradoxo da Sociedade da Informação e os Limites dos Direitos Autorais. *In*: Rover, Aires José (Org.). **Direito e Informática**. Barueri: Manole, 2004. P. 356.

[35] SOARES, Silvia Simões. Aspectos Jurídicos do Compartilhamento de Arquivos MP3 PSP via Internet: A experiência do Napster e as Novas Tendências da Legislação de Copyright dos Estados Unidos. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. v. 2. São Paulo: Quartier Latin, 2008. p. 614.

Esse assunto tem gerado uma grande discussão no mundo todo, eis que, muitas vezes, na busca de proteger os direitos autorais, as leis acabam por ferir outros direitos fundamentais, como o da privacidade, por exemplo. Silvia Simões[36] faz uma ressalva quanto a forma repressiva de combater os crimes de violação dos direitos do autor:

> Tais tentativas de normatização são por vezes uma esperança, mas outras uma grave ameaça a direitos fundamentais. Assustados com os inúmeros problemas trazidos de súbito pela informatização, legisladores pressionados por interesses divergentes e fortes *lobbies* empresariais procuram encontrar saídas através de novas legislações rígidas, que suprimem direitos fundamentais na tentativa de inibir ou punir abusos na rede.
>
> A sensação de que a impunidade na internet exige medidas enérgicas já levou países a restringir a privacidade dos usuários na rede, estender a responsabilização a terceiros e estabelecer sanções penais para a quebra de sistemas de controle de cópias. Tais medidas, contudo, vem mostrando-se ineficazes contra os problemas que se dispuseram a resolver; sem por isso deixar de significar grandes perdas em termos de liberdades individuais ou econômicas. Normas como DADVSI, o EUCD e o DMCA tornam-se cada vez mais comuns, sem que a pirataria eletrônica tenha cedido.

Ainda não pacífico o entendimento, os direitos autorais requerem uma análise aprofundada em relação ao "mundo virtual", para que haja um equilíbrio, protegendo os direitos do autor e ao mesmo tempo garantindo a todos acesso à informação e à cultura da forma menos onerosa possível.

1.1.5. Liberdade de Pensamento

No texto do art. 5º, VI e V da Carta Magna brasileira[37] é assegurada a livre manifestação do pensamento, porém, assegura-se direito à resposta, assim como indenização por dano material, moral ou à imagem:

---

[36] SOARES, Silvia Simões. Aspectos Jurídicos do Compartilhamento de Arquivos MP3 PSP via Internet: A experiência do Napster e as Novas Tendências da Legislação de Copyright dos Estados Unidos. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. v. 2. São Paulo: Quartier Latin, 2008. p. 614.

[37] BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constitui%C3%A7ao.htm>. Acesso em: 23 de abril de 2009.

> IV – é livre a manifestação do pensamento, sendo vedado o anonimato;
>
> V – é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;

Pedro Lenza[38] comenta os dispositivos constitucionais pertinentes à manifestação do pensamento:

> A Constituição assegurou a liberdade de manifestação do pensamento, vedado o anonimato. Caso durante a manifestação do pensamento se cause dano material, moral ou à imagem, assegura-se o direito de resposta, proporcional ao agravo, além da indenização.

A manifestação do pensamento é garantida pela Lei-maior brasileira, porém os abusos podem ser apreciados pelo Judiciário, conforme explica Alexandre de Moraes[39]:

> A manifestação do pensamento é livre e garantida em nível constitucional, não aludindo a censura prévia em diversões e espetáculos públicos. Os abusos porventura ocorridos no exercício indevido na manifestação do pensamento são passíveis de exame e apreciação pelo Poder Judiciário com a conseqüente responsabilidade civil e penal de seus autores, decorrentes inclusive de publicações injuriosas na imprensa, que deve exercer vigilância e controle da matéria que divulga.

Da mesma forma, entende o doutrinador português Guilherme da Fonseca[40] ao falar sobre a liberdade de expressão e informação na Constituição de Portugal:

> Por seu turno, os meios de comunicação social devem responsabilizar-se pela afronta aos direitos pessoais, como sejam, nomeadamente, o direito ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar, consagrados no artigo 26º da Constituição, num quadro de protecção mais vasta da dignidade da pessoa humana proclamada no artigo 1º, suportando as conseqüências

---

[38] LENZA, Pedro. **Direito Constitucional Esquematizado**. 9. ed. São Paulo: Método, 2005. p. 526.

[39] MORAES, Alexandre de. **Direito Constitucional**. 13 ed. Atlas: São Paulo, 2003.

[40] FONSECA, Guilherme da. A liberdade de expressão e informação – jurisdição criminal, para quê?. *In:* ALMEIDA FILHO, Agassiz; CRUZ, Danielle da Rocha. **Estado de direito e direitos fundamentais**. São Paulo: Forense, 2005. p. 264.

> advenientes de tal afronta, desde logo o direito a uma indemnização devida às pessoas vitimadas pelos danos sofridos.
>
> Conciliar sempre a eficácia da Justiça com as liberdades é a meta a atingir e, conseguida a conjugação de esforços entre todos os interessados, poderá então concluir-se que afinal são indispensáveis os juízes criminais.

Sobre o direito de resposta, previsto no art. 5º, V, da Carta Magna, Uadi Lammêgo Bulos[41] faz alguns comentários:

> Pela Constituição de 1988 ficou garantido o direito de resposta, permitindo a defesa de quem se ache ofendido por notícia capciosa, inverídica, incorreta, atentadora da dignidade humana, através da imputação de fatos prejudiciais, não cometidos pelo ofendido, seja pela imprensa televisionada, escrita ou falada, seja por uma assembléia, entidade, associação ou grupo de pessoas etc.

Assim, a liberdade de pensamento é protegida pela Constituição Federal, porém, com algumas limitações, limitações estas que visam que não haja exagero por parte de quem expõe seu pensamentos. Uma destas limitações é a proibição ao anonimato.

Celso Ribeiro Bastos[42] faz algumas considerações acerca da expressão do pensamento anônimo:

> Proíbe-se o anonimato. Com efeito esta é a forma mais torpe e vil de emitir-se o pensamento.
>
> A pessoa que o exprime não o assume. Isto revela terrível vício moral consistente na falta de coragem. Mas este fenômeno é ainda mais grave. Estimula as opiniões fúteis, as meras sacadilhas, sem que o colhido por estas maldades tenha possibilidade de insurgir-se contra o seu autor, inclusive demonstrando a baixeza moral e a falta de autoridade de quem emitiu estes atos.

Sem dúvida, a Internet proporciona a seus usuários facilidades na manifestação do pensamento, eis que qualquer pessoa pode criar

---

[41] BULOS, Uadi Lammêgo. **Constituição Federal Anotada**. 5. ed. São Paulo: Saraiva, 2003. p. 133

[42] BASTOS, Celso Ribeiro; MARTINS, Ives Granda. **Comentários à Constituição do Brasil**. São Paulo: Saraiva, 1989. p. 43-44.

um *site* ou *blog* e manifestar sua opinião sobre qualquer assunto, assim como participar de fóruns, redes sociais, *chats* etc..

Mas, como visto, também deve ser vedado o anonimato, aspecto este que não é muito comum no campo virtual, além do que aos abusos será dado direito de resposta, podendo até mesmo, conforme o caso, o autor das manifestações abusivas ser responsabilizado civil e penalmente.

1.1.6. Princípio da Intervenção Mínima

O Direito penal somente deverá ser aplicado quando não houver outros meios para combater certa prática considerada danosa, conforme explica Sandro D'Amato Nogueira[43], com base na doutrina de Alice Bianchini:

> [...], ele (o Direito penal) só deve atuar como *ultima ratio* respeitando o princípio da fragmentariedade e da subsidiariedade, e quando outras sanções que não penais já tenham atuado neste controle, aí sim justifica-se. Como poderemos constatar nas considerações seguintes: Nesse sentido, trazemos novamente o ensinamento de Alice Bianchini, que assim discorre: 'somente podem ser ingeridas à categoria de crime, condutas que efetivamente obstruam o satisfatório conviver da sociedade'. Desta forma, o princípio da intervenção mínima 'pode significar tanto a abstenção do direito penal de intervir em certas situações (seja em função do bem jurídico atingido, seja pela maneira como que veio a ser atacado

Seguindo a mesma linha de raciocínio, explica Fernando Capez[44] que, pelo princípio da intervenção mínima, o Direito penal deve atuar não somente quando os demais ramos do Direito tenham perdido eficácia, mas também quando os controles sociais e formais não surtirem efeito:

> Da intervenção mínima decorre, como colorário indestacável, a característica da subsidiariedade. Com efeito, o ramo penal só deve atuar quando os demais campos do Direito, os controles formais e sociais tenham perdido a eficácia e não sejam capazes de exercer essa tutela. Sua intervenção só deve operar quando fracassam as demais barreiras protetoras do bem jurídico

[43] NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo: BH Editora, 2008. p. 138.

[44] CAPEZ, Fernando**. Curso de Direito penal:** parte geral. v. 1. 7. ed. rev. e atual. de acordo com as Leis nº 10.721/ 2003 (Estatuto do Idoso), 10.763/2003 e 10.826/2003. São Paulo: Saraiva, 2004. p. 22.

> predispostas por outros ramos do Direito. Pressupõe, portanto, que a intervenção repressiva do círculo jurídico dos cidadãos só tenha sentido como imperativo de necessidade, isto é, quando a pena se mostrar como único e último recurso para a proteção do bem jurídico, cedendo a ciência criminal a tutela imediata dos valores primordiais da convivência humana a outros campos do Direito, e atuando somente em último caso (*ultima ratio*).

Fernando Capez[45] apresenta ainda os dois destinatários principais da intervenção mínima do Direito penal, que são o legislador e o operador do Direito:

> Ao legislador o princípio exige cautela no momento de eleger as condutas que merecerão punição criminal, abstendo-se de incriminar qualquer comportamento. Somente aqueles que, segundo comprovada experiência anterior, não puderam ser convenientemente contidos pela aplicação de outros ramos do direito deverão ser catalogados como crimes em modelos descritivos legais.
>
> Ao operador do Direito recomenda-se não proceder ao enquadramento típico, quando notar que aquela pendência pode ser satisfatoriamente resolvida com a atuação de outros ramos menos agressivos do ordenamento jurídico. Assim, se a demissão com justa causa pacifica o conflito gerado pelo pequeno furto cometido pelo empregado, o direito trabalhista tornou inoportuno o ingresso do penal. Se o furto de um chocolate em um supermercado já foi solucionado com o pagamento do débito e a expulsão do inconveniente freguês, não há necessidade de movimentar a máquina persecutória do Estado, tão assoberbada com a criminalidade violenta, a organizada, o narcotráfico e as dilapidações ao erário.

O princípio da intervenção mínima é de grande importância no Direito de Informática, já que as condutas são muito diversas do “mundo físico” e não há ainda legislação, pelo menos no Brasil, que descreva quais dessas condutas devem ser incriminadas e punidas e quais devem ser resolvidas pelos outros ramos do Direito. Desse modo, quando o legislador resolver criar tipificações para os comportamentos praticados através da informática, deve analisar atentamente quais desses comportamentos realmente trazem prejuízos à sociedade e ao Estado e se não há possibilidade de se aplicar outro campo do Direito senão o do Direito penal.

1.2. HISTÓRIA

1.2.1. História do Computador

Carla Rodrigues de Araújo de Castro[46] trata da conceituação do computador:

> Computador é conceituado como sendo um processador de dados que pode efetuar cálculos importantes, incluindo numerosas operações aritméticas e lógicas, sem a intervenção do operador humano durante a execução. É a máquina ou sistema que armazena e transforma informações, sob o controle de instruções predeterminadas. Normalmente consiste em equipamento de entrada e saída, equipamento de armazenamento ou memória, unidade aritmética e lógica e unidade de controle. Em um último sentido, pode ser considerado como uma máquina que manipula informações sob diversas formas, podendo receber, comunicar, arquivar e recuperar dados digitais ou analógicos, bem como efetuar operações sobre lei.

A primeira máquina que possuía essas características foi criada na Renascença, esta máquina fazia cálculos de soma, subtração, multiplicação e divisão, conforme informam Arlete Figueiredo Muoio e Malu Aguiar[47]:

> Através dos tempos, uma grande número de cientistas pesquisou a possibilidade de se criar uma máquina para se operar os cálculos. Como resultado disso, a primeira calculadora, do modo como hoje conhecemos, surgiu na Renascença, criada por Wilhelm Schickard (1592 - 1635). Tratava-se de uma máquina que operava soma, subtração, multiplicação e divisão, mas que foi perdida durante a Guerra dos Trinta Anos. E o seu inventor faleceu, acometida pela peste, sem ter podido defender sua criação. Deste modo, atribui-se geralmente a Blaise Pascal (1623 – 1662) a construção da primeira calculadora. Porém, sua PASCALINE somente fazia somas e subtrações.

---

[45] CAPEZ, Fernando. **Curso de Direito penal**: parte geral. v. 1. 7. ed. rev. e atual. de acordo com as Leis nº 10.721/ 2003 (Estatuto do Idoso), 10.763/2003 e 10.826/2003. São Paulo: Saraiva, 2004. p. 21.

[46] CASTRO, Carla Rodrigues Araújo. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Lumen Juris: Rio de Janeiro, 2003. p. 1.

[47] MUOIO, Arlete Figueiredo; AGUIAR, Malu. **Crimes na Rede:** o perigo que se esconde no computador. São Paulo: Companhia Limitada, 2006. P. 230.

Porém, estas máquinas eram muito simples, não era possível “ler” instruções. Tal problema foi solucionado por Joseph Marie Jacquard que construiu um tear mecânico que possuía uma leitora de cartões perfurados[48]:

> Era preciso criar uma forma de “ler” instruções, aprimorar um dispositivo de “entrada”. Isto só veio a ser solucionado em 1801, durante a Revolução Industrial, quando o cientista francês Joseph Marie Jacquard inventou um tear mecânico com uma leitora de cartões automática, que lia cartões perfurados, transformando um desenho abstrato num padrão de cores, determinado através de voltas de cada fio colorido no lugar certo. A máquina de Jacquard trabalhava tão bem que milhares de tecelões desempregados se revoltaram e quase mataram o inventor.

A idéia de um tear mecânico que funcionava através de instruções contidas em cartões perfurados, proporcionou, com Charles Babbage, em evoluir bastante na construção de novas máquinas para cálculos[49]:

> Com a idéia do cartão perfurado de Jacquard, Babbage criou então o “calculador analítico”, a estrutura básica de um computador como o conhecemos atualmente. Entre os seus componentes estava o “moinho”, uma roda dentada que se encontrava no coração da máquina e que seria uma enorme mastigadora de números, uma máquina de somar com precisão de 50 casas decimais. As “instruções” seriam lidas em cartões perfurados, isto é, os cartões perfurados transportariam não só os números, mas o padrão de moagem também. Portanto, a máquina precisaria de um dispositivo de ENTRADA para ler os cartões. Babbage idealizou uma unidade de memória ou “armazém” para guardar os números para referências futuras. Esta unidade seia um banco de 1000 “registradores”, cada um deles capaz de armazenar um número de 50 dígitos. Estes números poderiam ser ou um número dado nos cartões de entrada ou o resultado das operações do moinho. E finalmente a SAÍDA: Babbage desenhou a primeira máquina automática de impressão para mostrar o resultado dos cálculos.

Somente em 1946 foi criado o primeiro computador eletrônico, com fins militares, conforme explica Carla Rodrigues Araújo de Castro[50]:

---

[48] MUOIO, Arlete Figueiredo; AGUIAR, Malu. **Crimes na Rede:** o perigo que se esconde no computador. São Paulo: Companhia Limitada, 2006. P. 230.

[49] MUOIO, Arlete Figueiredo; AGUIAR, Malu. **Crimes na Rede:** o perigo que se esconde no computador. São Paulo: Companhia Limitada, 2006. P. 231.

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

Apesar de o computador não se o único meio para se cometer crimes de informática, podendo ser praticados também com o telefone, com cartões de crédito, celulares etc., porém é a ferramenta mais utilizada já que é utilizado por um número cada vez maior de pessoas, de todas as classes sociais.

1.2.2. História da Internet

Internet no conceito de Carla Rodrigues de Araújo de Castro[51]:

> Internet é uma grande rede de comunicação mundial, onde estão interligados milhões de computadores, sejam eles universitários, militares, comerciais, científicos ou pessoais, todos interconectados. É um rede de redes, que pode ser conectada por linhas telefônicas, satélites, ligações por microondas ou por fibra ótica.

Analisando a Internet percebe-se que é uma tecnologia de informação totalmente diferente do que havia até então. Em geral, o usuário dos meios de comunicações tradicionais recebe a informação sem ter grande autonomia sobre o conteúdo. Já na Internet, o *internauta* é que irá buscar a informação que supra as suas necessidades, de acordo com as observações feitas por Edison Fontes[52]:

> A Internet é uma nova forma de acessar informações. Apesar de ter se tornado comercial apenas nos meados dos anos 1990, sem

---

[50] CASTRO, Carla Rodrigues de Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003. p. 2.

[51] CASTRO, Carla Rodrigues de Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003. p. 3.

[52] FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. São Paulo: Saraiva, 2006. p.73.

> sombra de dúvida, a Internet já contém uma quantidade muito grande de informações de divertimento, de pesquisa, de educação e de assuntos profissionais. Da mesma forma que consultamos jornais e revistas, a Internet permite que tenhamos acesso a essas mesmas informações de maneira mais rápida. É uma grande biblioteca!
>
> [...]
>
> Diferentemente da televisão e de outros meios de comunicação, na Internet é o usuário que busca a informação – ou seja, ela só se torna acessível se procuramos por ela. [...]

O objetivo para a criação da Internet é controvertido, muitos acreditam que o seu surgimento tinha objetivos militares, como uma ferramenta segura para a comunicação entre bases militares. Para outros, a Internet teve como objetivo principal a pesquisa científica, conforme Maria Eugênia Finkelstein[53]:

> Sua predecessora chamava-se ARPANET, tendo sido desenvolvida em 1969. Sem dúvida há boatos de que a ARPANET foi desenvolvida para fins militares, mas a tese dominantes é a de que a Internet surgiu com o objetivo de pesquisa de um projeto da agência norte-americana ARPA. A conexão teve início ao interligarem-se os computadores de quatro universidades, passando, a partir disso, a ser conhecida como ARPANET. Em 1970, esse projeto foi intensamente estudado por pesquisadores, o que resultou na concepção de um conjunto de protocolos que é a base da Internet. Depois, o ARPA integrou redes de computadores de vários centros de pesquisa. Em 1986, a NSFNET, da entidade americana NSF, interligou-se a ARPANET, o que deu finalmente origem às bases da atual Internet.

Porém, a Internet só obteve a forma como é conhecida atualmente em 1989, com o surgimento da World Wide Web (WWW), o que popularizou o seu uso, diante da facilidade que tal ferramenta trouxe para o acesso as informações[54]:

> Com o advento da WWW (ou Web), a Internet se transformou num instrumento de comunicação de massa. A WWW foi criada em

---

[53] FINKELSTEIN, Maria Eugênia. Fraude Eletrônica. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes.2 v.. São Paulo: Quartier Latin, 2008. p. 407.

[54] CASTRO, Carla Rodrigues Araújo. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Lumen Juris: Rio de Janeiro, 2003. p. 3.

> Genebra, no ano de 1989, sendo formada por hipertextos, o que facilita a navegação.

No Brasil, a Internet surgiu primeiramente com o objetivo de interligar informações de universidades brasileiras com as universidades de fora do país[55]:

> Foi em 1988 que a Internet finalmente chegou ao Brasil. Ela foi apresentada por estudantes de cursos nos Estados Unidos que, ao retornar ao Brasil, sentiam a falta de intercambio mantido no exterior com outras instituições científicas. Foi assim que a Fundação do Amparo à Pesquisa no Estado de São Paulo (FAPESP), ligada à Secretaria Estadual de Ciência e Tecnologia, iniciou diversos contatos e que a troca de dados começou a ser feita. O serviço foi inaugurado, oficialmente, em abril de 1989.

A Internet é a forma mais utilizada de cometer os crimes virtuais, já que através dela pode-se acessar qualquer outro computador que esteja conectado e, por exemplo, copiar dados bancários, danificar dados, ou em relação às ferramentas de bate-papo e redes sociais praticar os crimes contra a honra, ameaça, racismo etc., dando sempre ao criminoso a ilusão de estar agindo anonimamente.

1.2.3. História dos Crimes de Informática

Como será visto adiante, são muitos os tipos de crimes de informática, sendo que a prática mais corriqueira é a da fraude, principalmente envolvendo a Internet. Portanto, é difícil precisar quando houve a sua primeira ocorrência, conforme observa Edison Fontes[56]:

> A fraude é uma ação tão velha quando a história da humanidade. A própria Bíblia relata a fraude em que Jacó enganou seu pai Isaque, quando se fez passar por Esaú, seu irmão. [...]
>
> Trata-se de velhos golpes utilizando novas tecnologias. Cada vez que uma nova tecnologia surge, já existe alguém pesquisando e

---

[55] FINKELSTEIN, Maria Eugênia. Fraude Eletrônica. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes.2 v.. São Paulo: Quartier Latin, 2008. p. 408.

[56] FONTES, Edison. **Segurança da Informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006. p.97.

> pensando na melhor forma de utilizar esses conceitos para os velhos golpes. O presente é uma sofisticação do passado.
>
> O mundo eletrônico não foge dessa situação. Precisamos estar mais atentos porque atualmente existe uma parafernália de novos recursos tecnológicos.

Antes mesmo da criação da Internet e do uso popular do computador pessoal, já existiam condutas que poderiam ser consideradas, hoje, como crime de informática, conforme Marco Assunção[57]:

> Em novembro de 1961 , desenvolvedores do MIT (Instituto de Tecnologia de Massachussets) demonstravam o seu sistema experimental compatível com gerenciamento de tempo, o que permitia quatro usuários trabalhando em terminais rodar programas de outros usuários. No final dos anos 60, terminais conectados por modem poderiam ser facilmente invadidos, já que, na época, ninguém se preocupava em colocar senhas.

Ivette Senise Ferreira[58], também afirma que os crimes virtuais iniciaram-se na década de 60, mas o exame criminológico dessas condutas só foram realizadas a partir da década seguinte:

> Ulrich Sieber, professor da Universidade de Würzburg e grande especialista no assunto, afirma que o surgimento dessa espécie de criminalidade remonta à década de 1960, época em que aparecem na imprensa e na literatura científica os primeiros casos do uso do computador para a prática de delitos, constituídos sobretudo por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados sobretudo em matérias jornalísticas. Somente na década seguinte é que iriam iniciar-se os estudos sistemáticos e científicos sobre essa matéria, com o emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial, sabendo-se porém da existência de uma grande *cifra negra* não considerada nas estatísticas.

A partir dos anos 80 as ação criminosas virtuais aumentaram consideravelmente, além de se diversificarem, conforme Ivette Ferreira[59]:

---

[57] ASSUNÇÃO, Marco Flávio Araújo. **Segredos do Hacker Ético.** 2ª ed. Visual Books: Florianópolis, 2008.

[58] FERREIRA, Ivette Senise. A Criminalidade Informática. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. 2. ed. São Paulo: Quartier Latin, 2005. p. 239.

> A evolução das técnicas nessa área, e a sua expansão, foi acompanhada por aumento e diversificação das ações criminosas, que passaram a incidir, a partir dos anos 80, em manipulações de caixas bancárias, pirataria de programas de computador, abusos nas telecomunicações, etc.., revelando uma vulnerabilidade que os criadores desses processos não haviam previsto e que carecia de uma proteção imediata, não somente através de novas estratégias de segurança no seu emprego mas também de novas formas de controle e incriminação das condutas lesivas.

No ano de 1986 surge, nos Estados Unidos, a primeira lei penal específica para os crimes de informática, tal lei foi chamada de Lei de Fraude e Abuso de Computadores, sendo que em 1988 houve a primeira prisão por crime de informática. Robert Tappan Morris Junior, um estudante, foi condenado a cinco anos de cadeia por ter transmitido um vírus (*worm*), atingindo cerca de 50.000 computadores[60]:

De acordo com Henrique Cesar Ulbrich e James Della Valle[61], um dos criminosos virtuais mais famosos foi Kevin Mitnick, que se especializou em burlar os sistemas das empresas de telefonia, causando a elas grandes prejuízos. Mitnick, além de grande conhecimento em informática, utilizava a engenharia social, que nada mais é do que a "tática para levar alguém a instalar programas ou fornecer dados"[62]. Em 1989 já era procurado pelo FBI por ter furtado um *software* secreto de uma empresa e desde essa época a Corte americana já o considerava como risco à comunidade. No ano de 1992 também foi acusado de *crackear* sistemas de informática do próprio FBI. Finalmente em 1995 foi preso, acusado por invadir empresas como Nokia e Motorola, passou cinco anos preso.

---

[59] FERREIRA, Ivette Senise. A Criminalidade Informática. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. 2. ed. São Paulo: Quartier Latin, 2005. p. 239.

[60] SHIMIZU, Heitor; SETTI, Ricardo. Tem boi na linha: hackers os espiões cibernéticos. **Super Interessante**, São Paulo, out. 1995. Disponível em: <http://super.abril.com.br/tecnologia/tem-boi-linha-hackers-espioes-ciberneticos-441127.shtml>. Acesso em: 10 de abril de 2009.

[61] ULBRICH, Henrique Cesar; VALLE, James Della. **Universo Hacker**. 4. ed. São Paulo: Digerati Books, 2004. p. 124.

[62] COLEÇÃO Info 2007: Segurança: tudo o que você precisa saber para manter os invasores longe do micro. Revista Info, São Paulo, abr. 2007. Edição Especial. p. 108.

Segundo Sandro D'Amato Nogueira[63], o primeiro caso esclarecido de crime de informática no Brasil foi em 1997, em que uma jornalista passou a receber centenas de *e-mails* de cunho erótico-sexual, juntamente com mensagens de ameaça a sua integridade física. O crime foi investigado e conseguiu-se chegar ao autor das mensagens, um analista de sistemas que foi condenado a prestar serviços junto a Academia de Polícia Civil, dando aulas de informática para novos policiais.

Porém, em 1988 *"hackers"* atuavam no país, sistemas do governo como do Banco Central e do Serviço Nacional de informação foram atingidos, assim como um grupo de jovens conseguiu fazer com que as contas telefônicas fossem apagadas dos sistemas da TELESP (Companhia Telefônica do Estado de São Paulo)[64].

Atualmente, os crimes de informática tem tido uma grande repercussão já que o combate a este tipo de criminalidade é difícil, devido a uma série de particularidades em relação aos "crimes reais".

[63] NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo: BH Editora, 2008. p. 29.

[64] SHIMIZU, Heitor; SETTI, Ricardo. Tem boi na linha: hackers os espiões cibernéticos. **Super Interessante**, São Paulo, out. 1995. Disponível em: <http://super.abril.com.br/tecnologia/tem-boi-linha-hackers-espioes-ciberneticos-441127.shtml>. Acesso em: 10 de abril de 2009.

CAPÍTULO 2

TERMINOLOGIA, SUJEITOS DOS CRIMES DE INFORMÁTICA E OS CRIMES DE INFORMÁTICA EM ESPÉCIE

2.1. TERMINOLOGIA

A terminologia utilizada para os crimes de informática variam bastante de doutrinador para doutrinador. Não há consenso na nomenclatura a ser adotada para aqueles crimes cometidos através da informática, conforme a análise de Fabrízio Rosa[65]:

> Klaus Tiedmann fala em "criminalidade de Informática", para designar todas as formas de comportamentos ilegais ou, de outro modo, prejudiciais à sociedade, que se realizam pela utilização de um computador. [...]. Kohn utiliza computer criminals para designar seus praticantes. Jean Pradel e Cristian Feuliard referem-se a "infrações cometidas por meio de computador". Há ainda quem prefira a expressão "crimes de computador", "cybercrimes", "computer crimes", "computing crimes", "delito informático", "crimes virtuais", "crimes eletrônicos" ou, ainda, "crimes digitais", "crimes cibernéticos", "infocrimes", "crimes perpetrados pela Internet", denominações distintas, mas, que, no fundo, acabam por significar basicamente a mesma coisa."

No mesmo sentido, reconhece Ivette Senise Ferreira[66] ao identificar as áreas e meios de atuação dos criminosos na informática:

> As várias possibilidades de ação criminosa na área da informática, assim entendida no seu sentido lato, abrangendo todas as tecnologias de informação, do processamento e da transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os quais lhe fornecem um

---

[65] ROSA, Fabrízio. **Crimes de Informática**. 2. ed. Campinas: Bookseller, 2005. p. 53.

[66] FERREIRA, Ivette Senise. A Criminalidade Informática. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes.2 ed. São Paulo: Quartier Latin, 2005. p. 237.

> denominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores.

Alexandre Daoun e Gisele Truzzi de Lima apresentam[67] o conceito de crimes de informáticos utilizados pela doutrina penal, assim como nos tribunais brasileiros e na Organização para Cooperação Econômica e Desenvolvimento da Organização das Nações Unidas:

> Pode-se afirmar que a doutrina penal e os tribunais brasileiros tem adotado o conceito de crimes informáticos como ação típica, antijurídica, e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão, definição esta, similar a que foi cunhada pela Organização para Cooperação Econômica e Desenvolvimento da ONU (Organização das Nações Unidas): "é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados.

Portanto, por enquanto, não há unanimidade na utilização de um termo para a criminalidade envolvendo informática, podendo utilizar-se de qualquer um temos acima citados.

2.2. SUJEITOS DOS CRIMES DE INFORMÁTICA

2.2.1. Sujeito Ativo

2.2.1.1 Hacker (White Hat)

Comumente os criminosos da informática são chamados de *hackers*, porém esta nomenclatura não é a mais adequada. Os doutrinadores, assim como os profissionais ligados à Informática, preferem chamar os criminosos de *crackers.*

Em geral os *hackers* detem, assim como os crackers, um vasto conhecimento de informática, sabem encontrar com facilidade qualquer brecha de segurança nos sistemas, porém, não altera nem danifica nada. Os

[67] DAOUN, Alexandre Jean; LIMA, Gisele Truzzi de. **Crimes Informáticos**: o Direito penal na Era da Informação. Disponível em: <http://www.truzzi.com.br/pdf/artigo-crimes-informativos-gisele-truzzi-alexandre-daoun.pdf>. Acesso em 20 de março de 2009.

hackers muitas vezes são contratados por empresas que pretendem testar os seus sistemas de segurança, de modo a procurar por eventuais falhas que comprometam seus dados sigilosos ou o próprio funcionamento da empresa.

Sandro D'Amato Nogueira[68] discorre sobre o conceito de *hacker*:

> HACKER – Este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver que consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual. Várias empresas estão contratando há tempos os Hacker's para proteção de seus sistemas, banco de dados, seus segredos profissionais, fraudes eletrônicas, etc.

Outro termo bem comum associado aos hackers é o "White Hat". Esse termo é designado para àqueles que apesar do conhecimento das brechas e falhas dos sistemas não cometem, em tese, nenhum crime.

Para Marcos Flávio Araújo Assunção[69] os "White Hat" são os "hackers do bem":

> Hacker White-Hat: Seria o "hacker do bem", chamado de "hacker chapéu branco". É aquela pessoa que se destaca nas empresas e instituições por ter um conhecimento mais elevado que seus colegas, devido ao autodidatismo e à paixão pelo que faz. Não chega a invadir sistemas e causar estragos, exceto ao realizar testes de intrusão. Resumindo: tem um vasto conhecimento, mas não o usa de forma banal e irresponsável.

Com base nos conceitos acima transcritos, pode-se afirmar que os *hackers* ou *White hats* não procuram causar danos, porém, isto não significa que não cometem crimes. O fato de invadir, por exemplo, um sistema ou computador sem autorização, ainda que sem alterar ou danificar nada, pode caracterizar um crime.

2.1.1.2 Cracker

---

[68] NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo: BH Editora, 2008. p. 61.

[69] ASSUNÇÃO, Marco Flávio Araújo. **Segredos do Hacker Ético.** 2ª ed. Visual Books: Florianópolis, 2008.p. 13.

Os *crackers* são os criminosos que possuem um vasto conhecimento de informática e utilizam deste conhecimento para encontrar brechas no ciberespaço de modo a causar danos a terceiros ou obter alguma informação confidencial.

Ao contrário dos *hackers* que são chamados de “White Hat”, os *crackers* tem como sinônimo a expressão em inglês “Black Hat”, conforme aponta Marcos Flávio Araújo Assunção[70]:

> Hacker Black-Hat: “Hacker do Mal” ou “chapéu negro”. Esse, sim, usa seus conhecimentos para roubar senhas, documentos, causar danos ou mesmo realizar espionagem industrial. Geralmente tem seus alvos bem definidos e podem passar semanas antes de conseguir acesso onde deseja, se o sistema for bem protegido.

É comum a confusão entre os dois termos, sendo associado ao criminoso virtual sempre a expressão *hacker*, expressão na qual sua utilização inicial era de associar à pessoa com grande habilidade ou apreço por computação, conforme observa Nelson Murilo de Oliveira Rufino[71]:

> Desde que apareceu nos meios de comunicação, o termo *hacker* perdeu a conotação romântica de outros tempos, pois se antes significava aficionado por computadores (a origem é ainda anterior) agora indica piratas eletrônicos ligados a crimes utilizando computadores. Bem que se tentou (e alguns ainda tentam) associar a esses últimos o termo *cracker*: “aqueles que quebram sistemas”, mas acredito que seja uma causa perdida.
>
> Visto que o termo ganhou uma carga pejorativa, os vendedores de serviço de segurança criaram a figura do “*hacker ético*”, para tentar minimizar o impacto que o termo *hacker* causa ao cliente, e é justamente a palavra “ética” que acaba fazendo toda a diferença.

Os cracker ainda são subdivididos conforme a área de atuação ou nível de conhecimento: *phreaker*; *spammers*; *defacer ou* pichador virtual; *lammer*; carders

---

[70] ASSUNÇÃO, Marco Flávio Araújo. **Segredos do Hacker Ético.** 2ª ed. Visual Books: Florianópolis, 2008.p. 13.

[71] RUFINO, Nelson Murilo de O. **Segurança Nacional:** Técnicas e Ferramentas de Ataque e Defesa de Redes de Computadores. São Paulo: Novatec, 2002. P. 16.

Os *phreakers* são os chamados *hackers* de telefonia, eis que se especializam em burlar os sistemas das operadoras de telefonia. Os crimes mais comuns são a clonagem de celulares, fazer escutas telefônicas sem autorização e alterar os sistemas de cobrança dos telefones, etc..

Fabrízio Rosa[72] conceitua *phreaker* como sendo aquele que é:

> Especializado em telefonia, atua na obtenção de ligações telefônicas gratuitas e instalação de escutas, facilitando o ataque a sistemas a partir de acesso exterior, tornando-se invisíveis ao rastreamento ou colocando a responsabilidade em terceiros;

Defacer é todo aquele que faz uma "pichação virtual", que consiste no conceito de Fabrizio Roza[73] "colocar, de forma indevida, textos ou figuras em sites de terceiros sem a devida autorização". Porém, o autor do fato somente poderá ser incriminado caso provoque ao dono do *site* algum prejuízo patrimonial. O mero fato de colocar na página um desenho ou assinatura, por exemplo, não acarreta em qualquer crime visto que não provoca qualquer prejuízo de ordem patrimonial, e esta conduta no Brasil ainda não é considerada como crime.

Nelson Murilo de Oliveira Rufino[74] subdivide os *hackers* por "facções" e afirma que existem, além de *Phraker e cracking,* os *Virii, Warez, Carding e Coders*:

> Virii – programadores e colecionadores de vírus.
>
> Warez –Pirataria de software, [...].
>
> Carding – manipulação de cartões magnéticos (clonagem, leitura, programação de chips) e telefônicos.
>
> Coders – codificadores , conhecedores de uma ou mais linguagens de programação, que permitem escrever programas, exploits e ferramentas de invasão e segurança e também

[72] ROSA, Fabrízio. **Crimes de Informática**. 2.ed. Campinas: BookSeller, 2006. p. 62.

[73] ROSA, Fabrízio. **Crimes de Informática**. 2. ed. Campinas: BookSeller, 2006. p. 65.

[74] RUFINO, Nelson Murilo de Oliveira. **Segurança Nacional:** Técnicas e Ferramentas de Ataque e Defesa de Redes de Computadores. São Paulo: Novatec, 2002. p. 19.

> examinar programas-fonte à procura de vulnerabilidades que possam ser exploradas.

Nota-se que são vastas as modalidades de *crackers*, variando a sua nomenclatura conforme a área em que atuam, não impedindo, porém, que um mesmo *hacker* possa ter conhecimento em duas ou mais áreas, como por exemplo, um mesmo indivíduo ter habilidade em *phreaker e carding*.

2.2.1.3 Outros Sujeitos

É importante ressaltar que nem todo criminoso virtual possui um grande conhecimento de computação. Alguns crimes de informática podem ser praticados por usuários comuns, bastando saber usar o computador e acessar a Internet. Podem-se citar como exemplos os crimes contra a honra (calúnia, difamação e injúria); pedofilia (no que se refere a adquirir, repassar conteúdo pornográfico envolvendo crianças e adolescentes).

2.2.2. Sujeito Passivo

Podem ser sujeitos passivos nos crimes de informática todas as pessoas que utilizam de um computador ou qualquer tecnologia informática (smartphone, Pager, caixa eletrônico etc.), estejam conectados à Internet ou não. Conforme observa Sandro D'Amato Nogueira[75]: "qualquer um de nós pode ser vítima, todos nós que temos acesso a rede mundial de computadores estamos arriscados a sermos vítimas dos delitos informáticos".

2.3. CLASSIFICAÇÃO DOS CRIMES

Ivette Senise Ferreira[76] sugere a seguinte classificação dos crimes de informática: "Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou

[75] NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo: BH Editora, 2008. p.63.

[76] FERREIRA, Ivette Senise. A Criminalidade Informática. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. 2. ed. São Paulo: Quartier Latin, 2005. p. 261.

programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial".

2.4. CRIMES EM ESPÉCIE

2.4.1. Crimes contra a Honra

Os crimes contra a honra estão previstos nos artigos 138 ao 145 do Código Penal, sendo que são três as espécies de crimes contra a honra: Calúnia (art. 138 do CP); Difamação (art. 139 do CP) e; Injúria (art. 140)[77].

Julio Fabbrini Mirabete[78] comenta o crime de calúnia dizendo que:

> Pratica o crime quem imputa, atribui a alguém, a prática de crime, ou seja, é afirmar, falsamente, que o sujeito passivo praticou determinado delito. É necessário, portanto, para a configuração da calúnia, que a imputação verse sobre fato determinado, concreto, específico, embora não se exija que o sujeito ativo descreva suas circunstâncias, suas minúcias, seus pormenores. Trata-se de crime de ação livre que pode ser cometido por meio da palavra escrita ou oral, por gestos e até meios simbólicos. Pode ela ser explícita (inequívoca) ou implícita (equívoca) ou reflexa (atingindo também terceiro). A imputação da prática de uma contravenção não constitui calúnia, mas pode caracterizar o delito da difamação. Como a honra, objetiva e subjetiva, é um bem jurídico disponível, o consentimento anterior ou concomitante com o fato exclui o crime.

Sobre o crime de difamação, explica Ney Moura Teles[79], fazendo a análise dos elementos objetivos deste tipo penal:

---

[77] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848compilado.htm>. Acesso em: 06 de setembro de 2009.

[78] MIRABETE, Julio Fabbrini. **Código Penal Interpretado**. 3. ed. São Paulo: Atlas, 2003.

[79] TELES, Ney Moura. **Direito penal:** Parte Especial: arts. 121 a 212, v. 2. São Paulo: Atlas, 2004. p. 271.

> A difamação é a imputação de um fato certo, determinado, capaz de macular a honra objetiva da pessoa. Não pode ser um fato típico de crime, pois aí haverá calúnia, mas, imputada a prática de um outro ilícito, uma contravenção penal ou um ilícito civil, poderá constituir difamação desde que tal fato seja ofensivo.
>
> Não é necessário que o fato seja ilícito, todavia deve ser daqueles que martirizam a reputação da vítima. Dizer que determinada pessoa dá-se a práticas homossexuais com seu motorista é, evidentemente, um fato ilícito mas que ofende a honra até do homossexual que mantém, perante o seu meio social, uma imagem de heterossexual.

Por fim, resta o crime de injúria, que o nobre doutrinador Julio Fabbrini Mirabete[80] considera que:

> A conduta típica é ofender a honra subjetiva do sujeito passivo, atingindo seus atributos morais (dignidade) ou físicos, intelectuais, sociais (decoro). Não há na injúria imputação de fatos precisos e determinados, como na calúnia ou difamação, mas apenas de fatos genéricos desonrosos ou de qualidades negativas da vítima, como menosprezo, depreciação etc.

Os crimes contra a honra são praticados na maioria das vezes de forma oral, apesar de admitida a forma escrita, esta não é muito comum. Ocorre que no mundo virtual, há um agravamento no impacto provocado por esses crimes, já que se dão de forma escrita ou gráfica e podem ser vistos por qualquer pessoa que possua acesso à rede, além de muitas vezes ser difícil a identificação do criminoso e a retirada do conteúdo ofensivo.

Todos esses crimes estão se tornando comuns na Internet, já que esta proporciona a seus usuários a sensação de que estão protegidos pelo anonimato. Os usuários utilizam de ferramentas como as redes sociais, *chats*, *blogs* etc., para ofender a honra de seus desafetos, seja imputando a este falsamente um crime, um fato ofensivo a reputação ou mesmo ofendendo a dignidade e o decoro.

Sobre os crimes contra a honra utilizando de sistema informático colaciona-se de Carla Rodrigues Araújo de Castro[81]:

---

[80] MIRABETE, Julio Fabbrini. **Código Penal Interpretado**. 3. ed. São Paulo: Atlas, 2003.

> Tanto a calunia como a difamação protegem a honra objetiva e para a sua consumação é necessário que terceira pessoa tome conhecimento do fato. Se só o ofendido souber das agressões, não se consumará o crime. Diante disso, podemos afirmar que estes crimes podem ser praticados através de uma homepage ou em salas de bate-papo, nas conhecidas conversas on line. As ofensas proferidas em conversas on line podem ser conhecidas dos integrantes do canal ou das salas, ou dirigidas particularmente ao ofendido. Quando a ofensa puder ser conhecida por outrem além do próprio ofendido, resta consumada a infração. Todavia, quando a ofensa é dirigida só para o ofendido e ninguém toma conhecimento do seu conteúdo, não há crime de calunia e difamação. O mesmo raciocínio pode ser utilizado para as ofensas enviadas por e-mails. Se só a vítima utiliza, difícil é a configuração do crime. Todavia, se o e-mail é conjunto e o agente sabia desta condição, é possível a consumação. [...].
>
> O crime de injúria tutela honra subjetiva, sendo suficiente para sua configuração que o ofendido tome conhecimento do fato. Assim, este delito pode ser praticado por email, nas salas de conversa, nas homepages, nos sites, etc.

Ao falar sobre as redes sociais, Maristela Basso e Fabrício Polido[82]o apontam que um dos ilícitos praticados através desta ferramenta é a violação aos direitos à honra. Ainda, observam que há uma dificuldade para o Judiciário entender como se dá as violações à honra no ambiente virtual:

> Em geral, os litígios relacionados aos direitos da personalidade na *internet* referem-se à violação dos direitos ao nome, à imagem, à honra e privacidade dos usuários. Nesses casos, o jurista encontra dificuldade em entender as armadilhas relacionadas ao armazenamento e circulação de informações no ambiente digital. O caso das redes de relacionamento social aponta para as hipóteses de apropriação injustificada de dados armazenados nos perfis de usuários, as quais servem de ponto de partida para a prática de ilícitos de violação de direitos da personalidade (*e.g. sites* ofensivos, intercâmbio e disseminação de mensagens difamatórias, utilização de fotos para endossar correspondência e interação com usuários de *internet* sem qualquer correspondência efetiva com o titular dos direitos de imagem associados, criação de perfis utilizando nome da pessoa sem autorização etc..) [...].

---

[81] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2.ed. Rio de Janeiro: Lumen Juris, 2003. p. 16.

[82] BASSO, Maristela; POLIDO, Fabrício. Jurisdição e Lei Aplicável na Internet: Adjudicando litígios de violação de direitos da personalidade e as redes de relacionamento social. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. v. 2. São Paulo: Quartier Latin, 2008. p. 462.

Portanto, nota-se que a informática, especialmente através da Internet, contribuiu para o aumento do número de ocorrência de crimes contra a honra uma vez que o volume de dados que trafegam pela rede é enorme, sendo dificultoso o seu controle. Ainda, uma das causas para esse aumento se deve, como já visto, ao anonimato que a Internet proporciona a seus usuários.

2.4.2. Racismo e Injúria Qualificada pelo Uso de Elemento Racial

Racismo, no conceito de Uadi Lammêgo Bulos[83] é:

> Todo e qualquer tratamento discriminador da condição humana em que o agente dilacera a auto-estima e o patrimônio moral de uma pessoa ou de um grupo de pessoas, tomando por critérios raça ou cor da pele, sexo, condição econômica, origem etc.

A Constituição da República Federativa do Brasil traz alguns dispositivos para coibir a prática do racismo. Dispõe os artigos 3º, IV; 4º, VIII; e 5º, XLII da CRFB[84]:

> Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil:
>
> IV – promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.
>
> Art. 4º A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios:
>
> VIII – repúdio ao terrorismo e ao racismo;
>
> Art. 5º.
>
> XLII – a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei;

Para por em prática os dispositivos constitucionais, a lei nº 7.716 de 05 de janeiro de 2009 definiu os crimes resultantes de preconceito racial,

---

[83] BULOS, Uadi Lammego. **Constituição Federal anotada.** 5. ed. São Paulo: Saraiva, 2003. p. 255.

[84] BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constitui%C3%A7ao.htm>. Acesso em: 08 de agosto de 2009.

assim como de descriminação ou preconceito de etnia, religião ou procedência nacional. Esta lei traz uma série de condutas que são consideradas como crime.

Conforme observa Alexandre de Moraes[85], para dar maior eficácia ao dispositivo constitucional, o Código Penal brasileiro prevê a injúria qualificada pelo uso de elemento racial:

> Acrescente-se, por fim, que o legislador ordinário, para garantir maior eficácia do preceito constitucional, protetor de igualdade e inimigo das discriminações, estabeleceu como figura típica diferenciada a injúria consistente na utilização de elementos referentes a raça, cor, etnia, religião ou origem, apenando-a com reclusão de um a três anos e multa (CP, art. 140, §3º)

No caso da injúria qualificada pelo uso de elemento racial ofende-se a honra da vítima, com palavras, termos ou gestos referentes à raça. Diferente do racismo, que para sua consumação o agente deve "praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional". Assim, o racismo, conforme os dispositivos da Lei 7.716/89, caracteriza-se em impedir alguém de exercer algum direito em função de sua raça, cor, etnia religião ou procedência nacional, como por exemplo, alguém que nega atendimento a outrem em função da raça deste. É comum que haja, até mesmo pela doutrina, a confusão entre a Lei 7.716/89 e o dispositivo do §3º do Código Penal[86].

Importante destacar, sobre o art. 140, §3º do Código Penal, que houve uma modificação através da Lei nº 12.033, de 29 de setembro de 2009 tornando ação penal pública condicionada à representação do ofendido os crimes de injúria em razão de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência.

Também é possível a ocorrência de preconceito racial no campo virtual que se dá de modo similar aos crimes contra a honra, em que são

---

[85] MORAES, Alexandre de. **Direitos Humanos Fundamentais**: teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 8. ed. São Paulo: Atlas, 2007. p. 230.

[86] BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 18.620-PR (2005/0187497-1), Sexta Turma, Brasília, DF, 14 de outubro de 2009.

publicados textos, imagens ou vídeos de conteúdo ofensivo na Internet. Neste caso o crime está previsto no artigo 20 da Lei nº 7.716[87]:

> Art. 20 Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
>
> Pena: reclusão de um a três anos e multa.

Sandro D'Amato Nogueira[88], apresenta o primeiro processo aberto em decorrência de racismo praticado através da Internet:

> O primeiro processo aberto no Brasil, acusando pessoas da prática de racismo na internet foi em janeiro de 2006. Os acusados são 2 estudantes de Brasília que utilizaram o ORKUT para praticar o crime. O processo está tramitando no Tribunal de Justiça do Distrito Federal.

Ainda com toda a repressão legal, o racismo e a injúria qualificada pelo uso de elemento racial continuam a ocorrer, sendo que a internet tornou-se uma ferramenta a mais para a prática desse tipo de crimes. Há nesses crimes, assim como em muitos outros crimes virtuais, uma enorme dificuldade em seu combate, já que a quantidade de dados que circulam pela internet todos os dias é muito grande.

2.4.3. Pedofilia

A pedofilia causa uma grande repulsa à sociedade, sendo que no entendimento de Sandro D'Amato Nogueira[89], não é propriamente um crime, mas sim um desvio sexual, porém passa a ser punido quem, em razão de sua atração sexual, pratica alguma conduta sexual envolvendo crianças ou adolescente, proibidas por lei.

> Uma parafilia na qual a atração sexual de um indivíduo adulto está dirigida primariamente para crianças pré-púberes ou ao redor da puberdade. [...]. A pedofilia por si só, não é um crime, mas sim,

---

[87] BRASIL. Lei nº 7.716 de 5 de janeiro de 1989. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L7716.htm>. Acesso em: 14 de agosto de 2009.

[88] NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo: BH Editora, 2008. p. 41.

[89] NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo: BH Editora, 2008. p. 97.

> um estado psicológico, e um desvio sexual. A pessoa pedófila passa a cometer um crime quando, baseado em seus desejos sexuais, comete atos criminosos como abusar sexualmente de crianças ou divulgar ou produzir pornografia infantil.

No caso do Brasil, tanto o Código Penal quanto a Lei nº 8.069, de 13 de julho de 1990, protegem a criança e o adolescente contra os indivíduos com esse desvio sexual. A Lei nº 8.069/90, conhecida como Estatuto da Criança e do Adolescente, pune mais a divulgação de material pornográfico que envolva crianças e adolescentes.

A pedofilia pode ser um crime de informática quando os pedófilos trocam entre si materiais pornográficos envolvendo adolescentes e/ou crianças. Esse crime, não necessita necessariamente de um conhecimento profundo em informática, bastando conhecer algumas ferramentas como *e-mail*, programas mensageiros ou redes sociais etc., para cometer o ilícito penal.

O Código Penal, em seu artigo 224, *a*, considera como violência presumida nos crimes contra a liberdade sexual, quando a vítima é menor de 14 (quatorze) anos. Luiz Regis Prado[90] comenta tal dispositivo:

> O legislador presume a violência quando a vítima não é maior de quatorze anos (art. 224, a), estendendo-se a proteção legal até a data em que atinge essa idade. A razão da tutela reside na innocentia consilli do sujeito passivo, ou seja, "a sua completa inconsciência em relação aos fatos sexuais de modo que não se pode dar valor algum ao seu consentimento" (Exposição de Motivos do Código Penal, n. 70).

O Estatuto da Criança e do Adolescente também procura combater ao máximo a pedofilia, sendo que no ano de 2008 houve algumas alterações, já que não havia punição para aquele que mandava um email, com fotos ou qualquer outro tipo de arquivo envolvendo sexo com crianças e/ou adolescentes, para uma única pessoa.

2.4.4. Pichação Virtual

---

[90] PRADO, Luiz Regis. **Direito penal Parte Especial** – Arts. 197 a 288. 2.ed. reform., atual. e ampl. São Paulo: Revista dos Tribunais, 2008. p. 43.

Também chamada de *defacement,* a pichação virtual se dá quando um *cracker* consegue invadir qualquer *site* fazendo alterações na sua estrutura, como por exemplo, deixando o seu nome no *layout* da *homepage*. No conceito de Fabrizio Rosa[91] pichação virtual consiste em "Colocar, de forma indevida, textos ou figuras em sites de terceiros sem a devida autorização".

Sandro D'Amanto[92] trata dos objetivos principais dos pichadores virtuais:

> Estes adoram violar algum site, a maioria do poder público, como do FBI, Pentágono, Supremo Tribunal Federal, INSS e lá deixar sua marca, as vezes acontece algum tipo de protesto político ou religioso com esse tipo de invasão, ou podermos chamar de 'manifesto', normalmente não causam danos.

A pichação virtual também não tem previsão legal no Brasil, a única possibilidade de ocasionar a abertura de um processo criminal se dá quando o *cracker* provoca ao proprietário do *site* algum tipo de dano, tipificado no artigo 163 do Código Penal, com pena de detenção, de um a seis meses, e multa. Este dano, porém, deve ter valor patrimonial[93].

2.4.5. Dano

O crime de dano está previsto no artigo 163 do Código Penal[94], sendo que no Parágrafo Único trata do dano qualificado, que assim dispõe:

> Art. 163 – Destruir, inutilizar ou deteriorar coisa alheia:
>
> Pena – detenção, de um a seis meses e multa
>
> Dano qualificado

---

[91] ROSA, Fabrízio. **Crimes de Informática**. 2. ed. Campinas: Bookseller, 2006. p.

[92] NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo: BH Editora, 2008. p. 62.

[93] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus aspectos processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003. p. 77.

[94] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848compilado.htm>. Acesso em: 01 de outubro de 2009.

> Parágrafo Único – se o crime é cometido:
>
> I – com violência à pessoa ou grave ameaça;
>
> II – com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave
>
> III – contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista;
>
> IV – por motivo egoístico ou com prejuízo considerável para a vítima:
>
> Pena – detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.

Acerca deste crime, Celso Delmanto[95] tece alguns comentários em relação ao seu tipo objetivo:

> Tipo objetivo: a figura contém três núcleos alternativos: destruir (eliminar, extinguir), inutilizar (tornar inútil, imprestável) ou deteriorar (arruinar, estragar). A deterioração não se confunde com a conspurcação, pois nesta não fica afetada a individualidade ou substância da coisa. Quanto ao desaparecimento, a opinião mais acertada é a de que não configura o crime de dano. [...]. A conduta pode ser comissiva ou omissiva. O objeto material é a coisa (imóvel ou móvel), que deve ser alheia. Em face dos próprios verbos que o art. 163 emprega, não se perfaz o delito de dano sem que a coisa fique prejudicada no seu valor ou utilidade.

No âmbito do Direito de Informática, vem sendo discutida a possibilidade de aplicar o crime do artigo 163 do Código Penal para os casos de destruição ou inutilização de arquivos digitais de terceiros.

Na opinião de Túlio Lima Viana[96], é totalmente possível a aplicação do art. 163 do Código Penal, ainda que o arquivo não tenha valor patrimonial, sendo que desta forma não seria necessária a criação de um novo tipo penal para o dano ocasionado através da Informática:

> O crime de dano previsto no art. 163 do CP brasileiro é perfeitamente aplicável à tutela dos dados informáticos, sendo completamente prescindível a criação de um novo tipo penal para

---

[95] DELMANTO, Celso; et al. **Código Penal Comentado** 4. ed. São Paulo: Renovar, 1998. p. 326.

[96] VIANA, Túlio Lima. **Do delito de dano e de sua aplicação ao direito penal informático**. Revista dos Tribunais, São Paulo, a. 92, v. 807, p. 491, janeiro de 2003.

> tal fim. Trata-se de interpretação extensiva da palavra “coisa”, elemento objetivo do tipo penal.
>
> A proteção patrimonial dos dados não se limita a seu valor econômico, pois a *intentio legis* é proteger todo o patrimônio da vítima, compreendido não só como tutela de valores econômicos, mas também do valor utilidade e do valor afetivo que porventura tenha a coisa.

De modo diverso, entende Carla Rodrigues Araújo de Castro[97] que não pode ser aplicado o crime previsto no art. 163 do Código Penal para a destruição, inutilização ou deterioração de arquivos digitais, já que o capítulo dos crimes de dano está incluso dentro da parte referente aos Crimes contra o patrimônio, e, assim, só se poderia aplicar o citado artigo quando o arquivo tiver algum valor material:

> Para a configuração do crime de dano como previsto no CP é necessário que provoque prejuízo econômico. Assim, se o agente envia vírus e destrói apenas os email de outro usuário e estes tratam de assunto sentimental ou mensagens de amizade, não haverá crime.

No mesmo sentido, Ivette Senise Ferreira[98] entende que o atual dispositivo de proteção ao dano não se enquadra às condutas ofensivas praticadas no ambiente virtual:

> Certas condutas ofensivas aos sistemas informáticos ou telemáticos ou ao uso do computador, na verdade não se adaptam às figuras penais existentes na nossa legislação, seja as que constituem crimes informáticos propriamente ditos, seja as que constituem como crimes de legislação comum ou especial praticados por intermédio da informática ou dos computadores. Isso vale também para o delito de dano, que nessa matéria ultrapassa em muito os limites próprios do art. 163 do Código Penal, [...].
>
> Parece então ser apropriada a criação de um novo tipo penal, o do *dano informático*, consistente na destruição, alteração ou supressão de dados informáticos com o fim de produzir prejuízo

---

[97] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus aspectos processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003. p. 28

[98] FERREIRA, Ivette Senise. A Criminalidade Informática. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. 2. ed. São Paulo: Quartier Latin, 2005. p. 261.

> ao usuário ou a terceiros, o que viria resolver inúmeros problemas existentes, atualmente sem uma resposta penal.

E, ainda, Guilherme de Souza Nucci[99] ao dar o conceito de coisa na redação do art. 163 do Código Penal:

> Conceito de coisa: é tudo aquilo que existe, podendo tratar-se de objetos inanimados ou de semoventes. No contexto dos delitos contra o patrimônio (conjunto de bens suscetíveis de apreciação econômica), cremos que imprescindível que a coisa tenha para o seu dono ou possuidor, algum valor econômico.

Desta forma, percebe-se que a maioria dos doutrinadores entende que não é possível a aplicação do dispositivo penal aos danos causados às coisas que não possuem valor econômico. Assim, somente estará praticando crime aquele que destruir, inutilizar ou deteriorar os arquivos digitais que possuam algum valor econômico, não podendo ser aplicado o art. 163 do Código Penal para arquivos que tenham meramente valores sentimentais, por exemplo.

2.4.6. Disseminação de Vírus, Worms e Similares

Primeiramente, importante trazer o conceito de vírus. Os vírus, no conceito de Flávio Tamega[100], são:

> Programas desenvolvidos para alterar nociva e clandestinamente softwares instalados em um computador, têm comportamento semelhante ao vírus biológico: multiplicam-se, precisam de um hospedeiro, esperam o momento certo para o ataque e tentam se esconder para não serem exterminados.

Fabrízio Rosa[101], de forma semelhante, também trata do conceito de vírus: “Vírus é o segmento de programa de computador capaz de mudar a estrutura do *software* do sistema e destruir ou alterar dados ou programas ou outras ações nocivas, com ou sem o conhecimento do autor”.

Já os *worms* são espécies de vírus, porém se auto reproduzem sem alterar o conteúdo dos arquivos infectados e se alocam no

---

[99] NUCCI, Guilherme de Souza. **Código Penal Comentado.** 7. ed. São Paulo: Editora Revista dos Tribunais, 2007. p. 708.

[100] TAMEGA, Flávio. **Hacker Inside**. v.1 . Goiania: Editora Terra, 2003. p. 40

sistema operacional de difícil acesso. Também, se caracterizam por serem imperceptíveis ao usuário do sistema e por trocarem constantemente de nome[102].

A mera disseminação ou contaminação dos vírus em computadores ou similares não tem são considerados como crime pelo ordenamento jurídico brasileiro, é um fato atípico. Desta forma, somente será punido, em razão da disseminação de vírus ou similar, aquele que ocasionar um dano patrimonial a terceiro, aplicando-se, assim, o crime do art. 163 do Código Penal brasileiro.[103]

2.4.7. Violação dos Direitos do Autor

As violações aos direitos do autor são comumente associadas ao termo pirataria virtual, como bem observa Henrique Galdemann[104]:

> Chama-se vulgarmente de pirataria à atividade de *copiar* ou reproduzir, *bem como utilizar indevidamente* – isto é, sem a expressa autorização dos respectivos titulares – livros ou outros impressos em geral, gravações de sons e/ ou imagens, *software* de computadores, ou, ainda, qualquer outro suporte físico que contenha obras intelectuais legalmente protegidas.

É um crime que vem dividindo opiniões, para alguns a conduta de colocar arquivos sem que tenham sido respeitados os direitos autorais deve ser duramente punida. Para outros, só se configura o crime quando há a intenção lucrativa no compartilhamento dos arquivos.

Na realidade, mesmo que se confirme que a pirataria virtual realmente é um crime e, como tal, deve punir aqueles que infringirem a lei, é uma conduta de difícil controle, eis que uma parcela muito grande dos usuários da Internet faz *downloads* ilegais.

---

[101] ROSA, Fabrízio. **Crimes de Informática**. Campinas: Bookseller, 2005. p. 69.

[102] TAMEGA, Flávio. **Hacker Inside**. v.1 . Goiania: Editora Terra, 2003. p. 39.

[103] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. Rio de Janeiro: Lumen Juris, 2003. p. 28.

[104] GALDEMANN, Henrique. **De Gutemberg à Internet**: Direitos autorais na era digital. 4. ed. Rio de Janeiro: Record, 2001. p. 86.

Os Estados Unidos, pressionado pelas gravadoras, vem sendo firme no combate a pirataria. Criou leis rígidas sobre o assunto e ante o enorme número de infratores, tem processado e condenado somente alguns deles, na tentativa de amedrontar o restante dos usuários para que parem de desobedecer aos direitos autorais.

O Professor José de Oliveira Ascensão (Direito & Internet II) relata como é realizado o controle das violações de *copyright* nos Estados Unidos:

> O sistema é conhecido por *notice and take down*. Aplica-se apenas às violações de *copyright*. Este procedimento é minuciosamente regulado. Consiste, basicamente, no seguinte:
>
> 1. O titular alegadamente ofendido notifica do conteúdo que considera violador o provedor intermediário de serviços de armazenagem;
>
> 2. O provedor retira prontamente o material ou bloqueia o acesso;
>
> 3. O provedor notifica imediatamente o destinatário do serviço
>
> 4. Este pode, por contra-notificação, sustentar a legalidade do conteúdo;
>
> 5. O provedor avisa então o reclamante que o material ou o acesso serão repostos num prazo de 10 a 14 dias, se o reclamante não intentar uma ação tendente a impor a remoção ou o bloqueio do acesso ao material;
>
> 6. Se a ação for intentada, o material ou acesso só serão repostos por decisão judicial.

Um exemplo da rigidez no combate a pirataria foi o julgamento de Jammie Thomas Rasset, condenada pela justiça americana a pagar U$ 1.92 milhão a seis gravadoras por ter feito ilegalmente o *download* de vinte e quatro músicas[105].

Mesmo sendo, conforme visto, bem rígida em suas normas para combater a violação a *copyright*, existe nos Estados Unidos uma exceção a essas regras. É o chamado *Fair Use*, que permite a cópia de obras literárias,

---

[105] MULHER pagará US$ 1,9 milhão por baixar música da internet. **G1**. Disponível em: <http://g1.globo.com/Noticias/PopArte/0,,MUL1199972-7084,00-MULHER+PAGARA+US+MILHAO+POR+BAIXAR+MUSICA+DA+INTERNET.html>. Acesso em: 21 de junho de 2009

devendo, porém, obedecer a alguns requisitos.

Sobre o *Fair Use*, comenta Silvia Simões Soares:

> Uma das mais importantes limitações dos direitos autorais nos Estados Unidos é o instituto do *fair use* (ou uso legítimo), adicionado pela última grande revisão na legislação, o *Copyright Act* de 1976. Embora não estivesse anteriormente expresso no texto da legislação do *copyright*, a doutrina do *fair use* já vinha sendo aplica em diversas decisões judiciais, tendo sido desenvolvida justamente a partir da experiência das Cortes. A seção 107 do primeiro capítulo do Título 17 do Código dos Estados Unidos é inteiramente dedicada ao *fair use*, e prevê a possibilidade de utilização e mesmo da produção de cópias de obras protegidas independente de autorização do autor ou detentor de direitos, desde que para finalidades como crítica, produção de notícias, estudo, pesquisa ou ensino (incluindo a distribuição de cópias para alunos em sala de aula), se observadas algumas condições.

Não tão repressiva, a França também procura acabar com a pirataria. Aprovou um projeto de lei[106] antipirataria em que ordena a suspensão do acesso à Internet para aqueles que fizerem *downloads* de filmes e músicas sem autorização. Demonstrando que a pirataria é um assunto polêmico, pouco tempo após a publicação da lei o mais alto tribunal francês limitou a aplicação da lei, admitindo somente a notificação dos infratores, sendo que a decisão de cortar o acesso à *web* deve ser dada somente através de um magistrado[107].

Outro caso famoso foi o do site PirateBay responsável por compartilhar milhares de arquivos *torrent* de filmes, jogos, programas, músicas ilegalmente. Os donos do site foram condenados pela Justiça sueca em um ano de prisão e a pagar o valor equivalente a R$ 7,6 milhões pelos danos causados

---

[106] SENADO francês aprova lei contra download ilegal. G1. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1124705-6174,00.html> . Acesso em: 13 de junho de 2009.

[107] TRIBUNAL francês limita poder de lei antipirataria na internet. **G1.** Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1190164-6174,00-TRIBUNAL+FRANCES+LIMITA+PODER+DE+LEI+ANTIPIRATARIA+NA+INTERNET.html>. Acesso em: 20 de junho de 2009.

as grandes indústrias audiovisuais[108].

O magistrado Demócrito Reinaldo Filho[109] comenta sobre a repercussão deste caso no futuro dos direitos autorais na Internet:

> Uma das primeiras consequências que podem ser observadas como resultado do julgamento sueco é a acertada estratégia processual de mirar nos fabricantes e dirigentes de empresas que facilitam a troca de arquivos digitais. A indústria fonográfica e grandes estúdios de filmes tem tomado medidas judiciais também contra os usuários que compartilham arquivos pirateados. Essa iniciativa, no entanto, tem se mostrado pouco eficaz, além de angariar a antipatia e aversão dos internautas e grupos e entidades civis ligados à defesa de liberdades civis.
>
> [...]
>
> Portanto, a tendência parece ser que as cortes judiciárias vão considerar responsáveis solidários, no cometimento das infrações a direitos autorais, que de qualquer forma auxilie, incentive ou assista aos internautas a baixarem, embora por seus próprios meios, arquivos ou obras protegidos pelo direito autoral. A disseminação de novos tipos de arquitetura descentralizada para compartilhamento de arquivos não livrará os disseminadores desse tipo de tecnologia da responsabilização.

Da mesma forma, o jornalista Bruno Garattoni na Revista Superinteressante do mês de junho de 2009 demonstra que não adianta responsabilizar os internautas para acabar com a pirataria:

> É por isso que, mesmo depois de processar 50 mil internautas, a indústria do entretenimento não consegue frear a pirataria. Está tentando criminalizar práticas que já se tornaram corriqueiras. "Cada vez mais a conduta normal está sendo reconhecida como ilegal. Isso desmoraliza a lei, porque as pessoas se vêem como criminosas e começam a se acostumar à idéia", diz Lawrence Lessig, professor de direito da Universidade de Stanford, em seu livro Remix (ainda sem tradução em português).
>
> No Brasil,o crime de violação aos direitos autorais tem

---

[108] JUSTIÇA sueca condena diretores do site Pirate Bay à prisão. G1. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1088598-6174,00.html>. Acesso em: 17 de maio de 2009.

[109] REINALDO FILHO, Demócrito. **A decisão contra o Pirate Bay e sua Repercussão sobre o Futuro do Direito Autoral na Internet**. Disponível em: <http://www.ibdi.org.br/site/artigos.php?id=225>. Acesso em: 20 de junho de 2009.

previsão no Código Penal no art. 184[110]:

> Art. 184. Violar direitos de autor e os que lhe são conexos:
>
> Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa
>
> §1º Se a violação constituir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação ou execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:
>
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
>
> §2º Na mesma pena do §1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
>
> §3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:
>
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
>
> §4º O disposto nos §§1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei n. 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto.

Sobre o *caput* do art. 184 do Código Penal, doutrina Luiz Regis Prado[111]:

> A conduta insculpida no artigo 184, *caput* consiste em violar

---

[110] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848compilado.htm>. Acesso em: 06 de setembro de 2009.

[111] PRADO, Luiz Regis. **Direito penal:** Parte Especial – arts. 121 a 196. 2. ed. reform., atual. e ampl. São Paulo: Revista dos Tribunais, 2008. p. 133-134.

> (infringir, ofender, transgredir) direitos de autor (interesses patrimoniais e morais) e os que lhe são conexos (direitos correlatos aos de autor – dos artistas intérpretes ou executantes – arts. 90 a 92, produtores fonográficos – arts. 93 e 94 – e das empresas de radiodifusão – art. 95 -, constantes da Lei 9.610/1998). Trata-se de norma penal em branco que precisa ser complementada por outra norma; no caso em apreço, pela Lei 9.610/1998.

Porém, relativos à pirataria virtual, o Brasil não tem agido eficazmente para combatê-la, em geral a repressão está voltada para aqueles que colocam ou facilitam o compartilhamento de arquivos que não foram respeitados os direitos autorais na Internet, e não para os que adquirem (“baixam”) esses arquivos. Em recente decisão, no Agravo de Instrumento nº 561.551-4, o Tribunal de Justiça do Estado do Paraná impediu que a empresa Cadari Tecnologia da Informação Ltda disponibilizasse o programa “K-Lite Nitro”, programa este que possibilitava o compartilhamento de arquivos digitais entre os internautas:

> AGRAVO DE INSTRUMENTO. TUTELA INIBITÓRIA. PRETENDIDA ANTECIPAÇÃO LIMINAR DOS SEUS EFEITOS. DISPONIBILIZAÇÃO PÚBLICA DE "SOFTWARE", DENOMINADO "K-LITE NITRO", PARA CONEXÃO ÀS REDES "PEER-TO-PEER" (P2P) POSSIBILITANDO O "DOWNLOAD" DE MÚSICAS PELA "INTERNET". PLAUSIBILIDADE DA OCORRÊNCIA DE CONDUTA ANTIJURÍDICA (CIVIL E CRIMINAL). RISCO NA DEMORA PRESENTE. PRETENSÃO NO SENTIDO DE SER REMOVIDO O ILÍCITO MEDIANTE ORDEM QUE IMPEÇA A CONTINUAÇÃO DESSA ATIVIDADE. DECISÃO DO JUIZ DA CAUSA APENAS DETERMINANDO A INSERÇÃO DE "BANNERS" NOS "SITES" COMUNICANDO AOS INTERNAUTAS A NATUREZA ILÍCITA DESSA OPERAÇÃO SEM O PAGAMENTO DE DIREITOS AUTORAIS. MEDIDA QUE NÃO SE MOSTRA APTA A TORNAR EFETIVA A TUTELA JURISDICIONAL ALMEJADA. RECURSO PROVIDO PARCIALMENTE PARA DETERMINAR A INSTALAÇÃO, EM PRINCÍPIO, COMO PROVIDÊNCIA VISANDO A OBTENÇÃO DO RESULTADO PRÁTICO EQUIVALENTE AO DO ADIMPLEMENTO, DE DISPOSITIVO (FILTRO) NO REFERIDO PROGRAMA DE COMPUTADOR, SOB PENA DE MULTA DIÁRIA, PARA IMPEDIR O COMPARTILHAMENTO DE ARQUIVOS E/OU FONOGRAMAS MUSICAIS PROTEGIDOS PELA LEI FEDERAL Nº 9.610/1998. REMESSA, OUTROSSIM, DE PEÇAS DOS AUTOS AO EXCELENTÍSSIMO SENHOR PROCURADOR GERAL DE JUSTIÇA.

> O Código Penal, porém, prevê no próprio art. 184, em seu

parágrafo §4º a possibilidade de não se aplicar o crime. Luiz Regis Prado[112] traz qual a aplicação do referido dispositivo:

> O art. 184, §4º restringe o âmbito de abrangência da tipicidade ao prescrever que não se aplicará o disposto nos parágrafos anteriores quando "se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei 9.610, de 19 de fevereiro de 1998, nem a cópia da obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto". As exceções ou limitações apontadas no parágrafo em análise são as constantes dos artigos 46, 47 e 48 da Lei 9.610/1998, de modo que ocorrendo qualquer das hipóteses ali previstas não caracterizará ofensa aos direitos autorais e a conduta será atípica.

Um caso específico de violação a direitos autorais é quanto aos *softwares*. Há uma lei específica - Lei 9.609 de 19 de fevereiro de 1998 - para proteger a propriedade intelectual do *software*, Sandro D'Amato Nogueira[113] traz o conceito de pirataria de *software*:

> Ao contrário de outros itens que você adquire, os aplicativos de software e as fontes que você compra não lhe pertencem. Você se torna um usuário licenciado – você adquire o direito de usar o software em um único computador, mas não pode inserir cópias em outras máquinas nem passar o software adiante para colegas. A pirataria de software é a distribuição e/ou a reprodução ilegais de aplicativos de softwares ou fontes da Adobe para uso comercial ou pessoal. Seja a pirataria de software deliberada ou não, ela é ilegal e pode ser punida por lei.

Conforme explica Marcos Wachovicz[114], aos programas de computador (*software*) se aplica o Direito Autoral e não os Direitos Industriais, pois enquanto linguagem de programação não tem existência física, é um bem :

> O programa de computador em si desprende-se de todo e qualquer meio físico (*hardware*) que possa lhe servir de suporte. Dessa maneira, é possível classificá-lo enquanto linguagem de programação como um bem jurídico incorpóreo, também chamado de imaterial, pois não possui existência física, mas abstrata. E dessa forma o *software* é considerado pela doutrina dominante

---

[112] PRADO, Luiz Regis. **Direito penal:** Parte Especial – arts. 121 a 196. 2. ed. reform., atual. e ampl. São Paulo: Revista dos Tribunais, 2008. p. 136.

[113] NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo: BH Editora, 2008. p. 165.

[114] WACHOWICZ, Marcos. O Programa de Computador como Objeto do Direito Informático. *In*: ROVER, Aires José **Direito e Informática**. Barueri: Manole, 2004. p. 339-340.

> como afeto e tutelado pelo Direito Autoral, e não pelo Direito Industrial.
>
> [...].
>
> O regime de proteção à propriedade intelectual de programa de computador é conferido às obras literárias pela legislação de direitos autorais.

Carlos Motta[115] ainda traça as principais aplicações da Lei do Software:

> O regime de proteção à propriedade intelectual do software está determinada pelo artigo 2º da Lei do Software. É o mesmo conferido às obras literárias pela Lei da Propriedade Intelectual. Entretanto, exceto com relação ao direito do autor do software de reivindicar a autoria do programa de computador e o direito do autor de opor-se a alterações não autorizadas, nos termos da lei, não se aplicam aos softwares as disposições relativas aos direitos morais, nos termos do §1º do artigo 2º da Lei do Software.
>
> Pelo §2º do artigo 2º também verificamos que ao autor do software é garantida a tutela dos direitos relativos ao software pelo prazo de 50 anos, contados a partir de 1º de janeiro do ano subsequente ao de sua publicação ou, na ausência desta, da sua criação. De acordo com o §3º do artigo 2º, da mesma forma que trata para qualquer propriedade intelectual, a proteção aos direitos de que trata a Lei do Software independe de registro.

No que tange a parte criminal, a Lei 9.609/1998 prevê a pena de detenção de seis meses a dois anos ou multa para quem violar direitos de autor no *software*. Caso da violação seja a reprodução, ainda que parcial do programa para atividades de comércio não autorizado a pena é de reclusão de um a quatro anos e multa.

2.4.8. Cyberterrorismo

Para entender melhor o cyberterrorismo é importante primeiramente fazer algumas análises quanto ao terrorismo. Jaime de Carvalho

---

[115] MOTTA, Carlos. Princípios da Proteção Negocial e Jurídica para Empreendedores em Tecnologia. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. v. 2. São Paulo: Quartier Latin, 2008. p. 222.

Leite Filho[116] traz algumas considerações sobre terrorismo que ajudam em sua definição:

> Definir terrorismo não é uma tarefa fácil porque, em vista da relatividade do termo e da possibilidade de este assumir diversas acepções, é difícil alcançar um conceito universal que explique sua verdadeira natureza. Jimenez de Asúa define terrorismo como sendo um crime ou uma série de crimes que se tipificam pelo alarme que produzem, ordinariamente motivado pelos meios de estrado que o terrorista costuma usar. Neste ponto reside um dos principais problemas que encontramos ao tentar definir a prática do terrorismo. Para uma parte da doutrina, o terrorismo é um crime comum como outro qualquer, enquanto para outra, trata-se de crime eminentemente político.

Para Jaime de Carvalho Leite Filho[117], utilizando do conceito de Pollitt, *cyberterrorismo* é:

> O ataque premeditado, com motivação política contra o sistema de informações de um computador, programas de computador ou arquivos armazenados em sistemas de inteligência artificial resultando danos consideráveis a pessoas ou a coisas patrocinados por grupos descontentes com o sistema político vigente na sociedade.

Desta forma, o *cyberterrorismo* se caracteriza por provocar pânico através de meios tecnológicos. Em geral, as atitudes dos *crackers* que praticam esse tipo de crime são de causar confusão ou danos aos sistemas, principalmente, de órgãos governamentais.

Sandro D'Amato Nogueira tratando do tema, estabelecendo algumas outras condutas praticadas pelos terroristas na Internet:

> Constatamos que os terroristas estão usando a *web* para:
>
> - Planejamento de ataques em massa. [...]
> - Divulgação de manuais de guerrilha
> - Ensinar como preparar bombas

---

[116] LEITE FILHO, Jaime de Carvalho. Ciberterrorismo – O Terrorismo na Era da Informação. *In*: ROVER, Aires José **Direito e Informática**. Barueri: Manole, 2004. p. 46.

[117] LEITE FILHO, Jaime de Carvalho. Ciberterrorismo – O Terrorismo na Era da Informação. *In*: ROVER, Aires José **Direito e Informática**. Barueri: Manole, 2004. p. 50.

- Como realizar e organizar atentados em massa
- Envio de mensagens de ódio
- Propaganda com a divulgação de vídeos com mensagens terroristas
- Divulgação de boatos para aterrorizar algum país ou população específica
- Como realizar ataques terroristas, entre outros

Pode-se citar como exemplo de *cyberterrorismo* o ocorrido no ano de 2007 na Estônia, país declarado como o mais conectado do mundo, onde um grupo de *crackers* deixou a maioria das páginas oficiais fora do ar. Este ataque foi considerado o maior *cyberataque* até agora. As autoridades estonianas declararam que foi detectado, através do IP, que os ataques partiram de computadores governamentais russos[118]. Se considerar a afirmação de Jaime de Carvalho de que o terrorismo é um crime de caráter político, este ataque a Estônia pode sim ser considerado como *cyberterrorismo* tendo em vista que os dois países envolvidos encontram-se em crime diplomática[119].

Os ataques cibernéticos têm preocupado as autoridades do mundo inteiro, inclusive da Organização do Tratado do Atlântico Norte – OTAN, organização internacional de colaboração militar, que após o ataque a Estônia tem tomado algumas medidas de modo a evitar novos ataques nos países pertencentes a esta aliança. A OTAN iniciou um programa de atividades com a criação do NATO Computer Incident Response Capability (NCIRC) responsável por criar medidas de segurança para seus próprios sistemas assim como para os aliados[120].

---

[118] Info Online. **Estônia acusa Rússia de ataque hacker**. Disponível em: <http://info.abril.uol.com.br/aberto/infonews/052007/18052007-4.shl>. Acesso em: 13 de julho de 2009.

[119] G1. **Presidente russo usa festa para criticar Estônia e Polônia**. Disponível em: <http://g1.globo.com/Noticias/Mundo/0,,MUL34061-5602,00-PRESIDENTE+RUSSO+USA+FESTA+PARA+CRITICAR+ESTONIA+E+POLONIA.html>. Acesso em 13 de julho de 2009.

[120] NORTH ATLANTIC TREATY ORGANIZATION. Disponível em: <http://www.nato.int/cps/en/SID-67FA1DF4-6367D7B7/natolive/topics_49193.htm?selectedLocale=en>. Acessado em 13 de julho.

Outro país que tem despendido medidas para o combate aos *cyberataques* são os Estados Unidos, que por ter serviços como o fornecimento de água, eletricidade, controle de vôos conectados à Rede Mundial teme um ataque de terroristas através da internet.

Esta preocupação se intensificou após os ataques de 11 setembro, conforme afirma Maria Eugênia Finkelstein[121]:

> Após os ataques terroristas de 11 de setembro de 2001, os estados Unidos passaram a se preocupar intensamente com a ocorrência de crimes informáticos, uma vez que foi amplamente noticiado pela imprensa que os terroristas utilizaram-se dos meios eletrônicos para se comunicar e arquitetar os ataques que chocaram o mundo.

Recentemente, visando uma maior proteção a esses ataques o presidente Barack Obama anunciou, em maio de 2009, um plano para proteger os sistemas americanos contra ataques cibernéticos[122].

Desta forma, fica evidente que o *cyberterrorismo* acarreta quase tantos problemas quanto um ataque terrorista 'tradicional', pois os terroristas tem utilizado a informática tanto para arquitetar os ataques físicos, quanto para atacar os sistemas informático de órgãos governamentais.

2.4.9. Interceptação Informática

A Constituição brasileira protege a inviolabilidade da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, em seu art. 5º, XII:

> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no

---

[121] FINKELSTEIN, Maria Eugênia. Fraude Eletrônica . *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. v. 2. São Paulo: Quartier Latin, 2008. p. 431.

[122] G1. **Obama lança plano para proteger os computadores dos EUA**. Disponível em: <http://g1.globo.com/jornaldaglobo/0,,MUL1176517-16021,00-OBAMA+LANCA+PLANO+PARA+PROTEGER+OS+COMPUTADORES+DOS+EUA.html>. Acesso em: 13 de julho.

> último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução penal;

A Lei nº 9.296/96[123], que regulamenta a parte final do inciso XII da Constituição Federal, fez uma extensão para a informática, em seu art. 1º, Parágrafo Único:

> Art. 1º. A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
>
> Parágrafo Único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Prevê ainda a Lei nº 9.296/96[124], no art. 10, que será punido aquele que interceptar comunicações de informática com reclusão, de dois a quatro anos e multa:

> Art. 10. Constitui crime realizar interceptações de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
>
> Pena: reclusão, de dois a quatro anos, e multa.

Ivette Senise Ferreira[125] entende que este artigo somente pode ser aplicado quando se tratar do fim visado pela lei, que é a obtenção de prova para fins policiais ou judiciais:

> Nos termos em que foi estabelecido esse tipo penal, a conduta criminosa fica limitada aos fins visados pela lei em que se insere, ou seja, a obtenção de provas para fins policiais ou processuais, o

---

[123] BRASIL. Lei nº 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm>. Acesso em: 25 de junho de 2009.

[124] BRASIL. Lei nº 9.296 de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm>. Acesso em: 25 de junho de 2009.

[125] FERREIRA, Ivette Senise. A Criminalidade Informática. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. 2. ed. São Paulo: Quartier Latin, 2005. p. 260.

> que limita bastante a incriminação, pois se a interceptação informática não adequar-se ao modelo proposto o autor incidirá apenas no delito de violação de comunicação, previsto no art. 151, §1º do Código Penal, punido mais brandamente.

Dispõe o art. 151 do Código Penal[126]:

> Art. 151. Devassar indevidamente o conteúdo de correspondência fechada dirigida a outrem:
>
> Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa
>
> §1º Na mesma pena incorre:
>
> I – quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói

Porém, Guilherme de Souza Nucci[127], afirma que o art. 151, assim como seu §1º, foi derrogado pela Lei nº 6.538/78:

> Derrogação do art. 151: as figuras típicas previstas no *caput* e no §1º foram substituídas pela lei que rege os serviços postais – especial e mais nova -, o que se pode constatar pela leitura do art. 40: 'Devassar indevidamente o conteúdo de correspondência fechada dirigida a outrem: Pena – detenção, até seis meses, ou pagamento não excedente a vinte dias-multa. §1º Incorre nas mesmas penas que se apossa indevidamente de correspondência alheia, embora não fechada, para sonegá-la ou destruí-la, no todo ou em parte. §2º As penas aumentam-se da metade se há dano para outrem'.

Na análise do núcleo dos tipos, Guilherme de Souza Nucci entende que devassar[128] significa descobrir o conteúdo da correspondência, não necessariamente abrindo-a e, no caso do §1º, apossar[129] é pegar para si correspondência de outrem.

---

[126] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848compilado.htm>. Acesso em: 10 de setembro de 2009.

[127] NUCCI, Guilherme de Souza. **Código Penal Comentado**. 7. ed. São Paulo: Revista dos Tribunais, 2007. p. 649.

[128] NUCCI, Guilherme de Souza. **Código Penal Comentado**. 7. ed. São Paulo: Revista dos Tribunais, 2007. p. 649.

[129] NUCCI, Guilherme de Souza. **Código Penal Comentado**. 7. ed. São Paulo: Revista dos Tribunais, 2007. p. 652.

Portanto, há dois caminhos para os crimes de interceptação informática. Caso a conduta tenha finalidade de instruir investigação policial ou processual penal, sem que haja uma autorização judicial para tal, será aplicada a Lei 9.296/96 com a pena um pouco mais grave do que para os demais casos, onde será aplicada a Lei nº 6.538/78 que trata também dos crimes de violação de correspondência.

2.4.10. Fraude Eletrônica ou Informática

Fabrízio Rosa[130] traz o conceito e as principais características da fraude eletrônica ou informática:

> Fraude/ falsidade informática: entrada, alteração/ modificação, apagamento ou supressão de dados ou programas, ou qualquer outra ingerência num sistema de processamento de dados, que, de acordo com o Direito nacional, constitua uma falsificação nos moldes tradicionais. O delito de fraude informática surge para preencher uma lacuna, para caso da obtenção de injusto proveito patrimonial, mediante uso ilícito do sistema informático ou telemático, devido à impossibilidade de aplicar o modelo tradicional do estelionato, tendo-se em conta a 'não humanidade' do destinatário da manobra enganadora. É punido quem quer que, alterando de qualquer modo o funcionamento de um sistema informático ou telemático ou intervindo sem direito, mediante não importa qual modalidade sobre dados, informações ou a eles pertencente, busque para si ou para outrem um injusto proveito com prejuízo a terceiro.

Este conceito, porém, não procura trazer a aplicação prática considerando o atual ordenamento jurídico penal brasileiro, e, sim, como deveria ser aplicado.

Conforme o conceito deste doutrinador, não poderia ser aplicado o crime de estelionato, previsto no art. 171 do Código Penal[131], porém, há entendimentos contrários como se verá adiante. Assim, primeiramente, importante trazer o que dispõe o crime de estelionato:

---

[130] ROSA, Fabrízio. **Crimes de Informática**. Campinas: BookSeller, 2006. p. 65.

[131] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848compilado.htm>. Acesso em: 10 de setembro de 2009.

> Art. 171 – Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
>
> Pena – reclusão, de um a cinco anos, e multa

Julio Fabbrini Mirabete[132] comenta o citado artigo:

> A conduta do estelionato consiste no emprego de meio fraudulento para conseguir vantagem econômica ilícita. A fraude pode consistir em artifício, que é a utilização de uma aparato que modifica, aparentemente, o aspecto material da coisa ou da situação etc., em ardil, que é a conversa enganosa, em astúcia, ou mesmo em simples mentira, ou em qualquer outro meio para iludir a vítima [...]

No que tange ao estelionato praticado através de sistemas informáticos, entende Ivette Senise Ferreira[133]:

> A figura do *estelionato*, prevista no art. 171 do Código Penal brasileiro de 1940, que consiste no emprego de meios fraudulentos para a obtenção de ilícita vantagem, abrange os exemplos mais conhecidos e mais freqüentes dessas atuações criminosas, tanto no Brasil quanto nos demais países. Compreende tanto o caso das transferências fraudulentas de fundos nas contas bancárias quantos os casos de frações de quantias, ou contas "arredondadas", nos cálculos de clientes ou da empresa, acumulando-se o dinheiro lentamente na conta pessoal do agente. Ou ainda o uso de cartão personalizado, fornecido pelos bancos para permitir o acesso às contas eletrônicas através de um código pessoal, abusivamente utilizado por alguém que o tenha furtado, encontrado ou falsificado.

Porém, deve-se analisar caso a caso para que se estabeleça que o crime a ser aplicado é o de estelionato. No caso das transações bancárias fraudulentas, um dos exemplos de fraude trazidos por Ivette Senise Ferreira, no chamado *Internet Banking*, não se pode aplicar o crime do art. 171 do CP, mas sim o crime de furto previsto no art. 155 do Código Penal.

O STF já decidiu sobre o tema, no Conflito de Competência nº 72.738-RS , que no caso das fraudes em relações bancárias se aplica o Art.

---

[132] MIRABETE, Julio Fabbrini. **Código Penal Interpretado**. 3 ed. São Paulo: Atlas, 2003. p. 1350.

155, §4º, II do Código Penal, ou seja, furto qualificado. Isto porque no caso do estelionato tem-se como característica a entrega do bem de forma espontânea através de fraude, já no furto não há concordância por parte do sujeito passivo, conforme bem explica a Ministra Relatora Thereza de Assis Moura em seu voto:

> O furto mediante fraude, escalada ou destreza não se confunde com o estelionato. No primeiro, a fraude visa a diminuir a vigilância da vítima, sem que esta perceba que está desapossada; há a discordância expressa ou presumida do titular do direito patrimonial em relação à conduta do agente. No segundo, a fraude visa a fazer com que a vítima incida em erro e, espontaneamente, entregue o bem ao agente; o consentimento da vítima integra a própria figura delituosa.

Tal entendimento acerca da fraude eletrônica não quer dizer que não possa ser cometido o crime de estelionato através da Internet. Carla Rodrigues Araújo de Castro[134] fala sobre algumas possibilidades da prática deste crime na informática:

> O crime de estelionato pressupõe dois resultados: vantagem ilícita e prejuízo alheio. Este resultado deve ser obtido mediante artifício, ardil ou qualquer outro meio fraudulento. É exatamente aqui que entra a informática. O agente pode utilizar *homepages*, *sites,* conversas *on line* e *e-mails* para induzir o lesado a erro, seja mediante ardil, artifício ou qualquer meio.

Sandro D'Amato Nogueira[135] cita alguns exemplos comuns na Internet em que se procura enganar os *internautas*:

> Muitas pessoas receberam e-mail pedindo para se que recadastrarem na Receita Federal, pois seu CPF iria ser cancelado. Outro e-mail muito conhecido, foi sobre o recadastramento no Tribunal Superior Eleitoral, avisando a pessoa da necessidade imediata de enviar seus dados completos, pois eu título de eleitor seria cancelado. Este tipo de e-mail é enviado aos milhões e as pessoas com medo acabam respondendo, e seus dados vão para nas mãos de crackers e serão usados para fins ilícitos, como na compra de alguma mercadoria, financiamentos e falsificação de algum documento para cometerem alguns crimes.

---

[133] FERREIRA, Ivette Senise. A Criminalidade Informática. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. 2. ed. São Paulo: Quartier Latin, 2005. p. 250.

[134] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003. p. 31.

[135] NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. São Paulo: BH Editora, 2008. p. 180.

Conclui-se, então, que na ocorrência de fraude informática, apesar de não ter uma previsão expressa na legislação penal brasileira, pode ser aplicado, conforme o caso, o crime de estelionato (art. 171 do CP) ou o crime de furto qualificado (Art. 155, §4º, II do CP).

CAPÍTULO 3

LEGISLAÇÃO APLICÁVEL

3.1 PRINCÍPIO DA TERRITORIALIDADE

Um dos maiores desafios para acabar com os crimes de informática é a questão da territorialidade. A Internet, por possuir um caráter global, permite que um crime seja praticado, por exemplo, no Japão sem que o criminoso nunca tenha saído do Brasil. Por este motivo, importante primeiramente saber acerca do princípio da territorialidade no âmbito do direito penal.

Acerca da territorialidade para efeitos criminais, dispõe o artigo 5º do Código Penal brasileiro[136]:

> Art. 5º Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
>
> §1º Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.
>
> §2º É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aqueles em pouso no território nacional ou em vôo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil.

---

[136] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848compilado.htm>. Acesso em: 23 de setembro de 2009.

Julio Fabbrini Mirabete[137] traz o conceito de territorialidade e sua aplicação e abrangência na legislação criminal brasileira:

> Para definir a possibilidade de aplicação da lei nacional a fatos que ocorram no país ou fora dele ou que violem interesses nacionais embora cometidos no exterior, estabelece a lei os princípios de aplicação penal no espaço, adotando como base o *princípio da territorialidade*, decorrente da soberania, segundo o qual se aplica a lei brasileira ao crime cometido no território nacional. Em sentido estrito, material, o território abrange o solo (e subsolo), sem solução de continuidade e com limites reconhecidos, as águas interiores, o mar territorial, a plataforma continental e o espaço aéreo. [...].

Quanto a extraterritorialidade, regula o art. 7º do Código Penal brasileiro[138]:

> Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:
>
> I – os crimes:
>
> a) contra a vida ou 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.

---

[137] MIRABETE, Julio Fabbrini. **Código Penal Interpretado**. 3. ed. São Paulo: Atlas, 2003. p. 119

[138] BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848compilado.htm>. Acesso em: 23 de setembro de 2009.

> § 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.

No caso dos crimes de informática, quando o crime é praticado através de *site* brasileiro aplica-se a legislação brasileira, porém, nos casos em que o crime se dá em *sites* estrangeiros, o entendimento era de que deveria ser aplicado, por analogia, o art. 42 da Lei de Imprensa (Lei 5.250/1967). Dispõe o art. 42 da Lei de Imprensa[139]:

> Art. 42. Lugar do delito, para a determinação da competência territorial, será aquele em que for impresso o jornal ou periódico, e o local do estúdio do permissionário ou concessionário do serviço de radiodifusão, bem como o da administração principal da agência noticiosa.

Sobre a aplicação do art. 42 para os crimes de informática, entende Rebeca Novaes Aguiar[140]:

---

[139] BRASIL. Lei nº 5.250 de 9 de fevereiro de 1967. Regula a liberdade de manifestação do pensamento e de informação. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L5250.htm>. Acesso em: 02 de outubro de 2009.

[140] AGUIAR, Rebeca Novaes. **Competência Territorial para Apurar os Crimes de Informática**. Disponível em: <http://www.buscalegis.ufsc.br/revistas/files/journals/2/articles/6043/public/6043-6035-1-PB.pdf>. Acesso em 20 de agosto de 2009.

> Sendo assim, o crime praticado no Brasil por brasileiro ou estrangeiro, através de um *site* hospedado no Brasil, a competência seria do Brasil, pois utilizar-se-ia o Princípio da Territorialidade. Nesse caso seria, ainda, Estadual, ou seja, do Estado onde se encontra situado a sede do Site no Brasil. Porém, supondo que o resultado do crime tenha se dado no exterior, aplicar-se-ia o art. 42 da lei de imprensa, porém, para punir o infrator deve-se utilizar as regras estabelecidas pelo artigo 7º do Código Penal Brasileiro.

Porém, importante destacar que este entendimento deverá se modificar, já que recentemente o Supremo Tribunal Federal entendeu que a Lei de Imprensa não foi recepcionada pela Constituição Federal de 1988 e, desta forma, não tem eficácia.

Independente do entendimento de que norma deverá ser aplicada, para que seja eficiente o combate aos crimes de informática é necessária a cooperação entre os Estados para uma melhor eficiência na aplicação das leis. Como bem observa Maria Eugênia Finkelstein[141], diante do alcance internacional que caracteriza a Internet, deve haver a uniformização das leis por todos os países:

> O caráter global da *Internet* e a possibilidade de crimes informáticos internacionais são pontos que devem ser considerados. Em face desse caráter, qualquer mudança legislativa deveria ser implementada por vários países no sentido de uniformizar as leis por meio de esforços internacionais no sentido de harmonizar as práticas. O maior erro que poderíamos cometer seria o de tentar resolver os problemas gerados pela Internet pensando individual e regionalmente, sem a inserção no contexto internacional. Afinal, a *Internet* não é um assunto de âmbito meramente local, mas, sim, global em face da diluição de fronteiras ocasionada.

Da mesma forma, ao analisar os problemas no comércio eletrônico, Carlos Alberto Soto Coaguila[142] espera uma uniformização dos princípios e regras:

---

[141] FINKELSTEIN, Maria Eugênia. Fraude Eletrônica. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes.2 v.. São Paulo: Quartier Latin, 2008. p. 411.

[142] COAGUILA, Carlos Alberto Soto. A Criminalidade Informática. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. v. 2. São Paulo: Quartier Latin, 2008. p. 203.

> Fazemos votos para que a América Latina e o mundo entrem em acordo no sentido de contemplar regras e princípios uniformes orientados para promover e viabilizar o comércio eletrônico, com o que resolver-se-ão outros tantos problemas, como o da legislação aplicável e a jurisdição competente em caso de conflitos resultantes da contratação eletrônica.

Da forma como é hoje fica difícil de determinar a lei de qual país deve ser aplicada aos crimes de informática, sobre esta dificuldade, em especial sobre a violação de direitos de personalidade, comentam Maristela Basso e Fabrício Polido[143]:

> Violação de direitos da personalidade praticados no domínio do espaço virtual trazem dificuldades ao jurista com relação à determinação do direito aplicável. Essa questão, como se examinará, não é um problema novo no Direito Internacional Privado e sempre foi, de certa forma, negligenciada pela doutrina jusprivatista internacional. Para o caso analisado, haveria necessidade de se reconsiderar a relevância prática de regras de conexão adequadas para a solução dos conflitos de lei no espaço envolvendo os atos de violação de direitos de personalidade. Nos sistemas de conexão adequadas para a solução de conflitos de lei no espaço envolvendo os atos de violação de direitos da personalidade. Nos sistemas de tradição do *common law*, a doutrina desenvolve a concepção do *cybertort* – disciplina jurídica da responsabilidade civil relativamente a ilícitos praticados no espaço virtual. É tarefa do Direito Internacional Privado justamente a de estabelecer um conjunto de normas e princípios que possam auxiliar na melhor 'localização' dos fatos e relações jurídicas mistas no domínio do espaço virtual e igualmente designar a lei aplicável às obrigações delituais com conexão internacional decorrentes de atos de violação de direitos praticados no espaço virtual.

O posicionamento acima citado demonstra bem toda a dificuldade encontrada para estabelecer qual lei deve ser aplicada aos ilícitos civis. Porém, não só no Direito Civil há dificuldades de se coibir as práticas abusivas na Informática, da mesma forma há muitas discussões para aplicação do Direito penal para os crimes envolvendo sistemas de informática ou telemático, em especial quando relacionada à Internet, já que esta abrange o mundo inteiro. Por este motivo, os já citados autores Maria Eugênia Finkelstein e Carlos Soto

---

[143] BASSO, Maristela; POLIDO, Fabrício. Jurisdição e Lei Aplicável na Internet: Adjudicando litígios de violação de direitos da personalidade e as redes de relacionamento social. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes.2 v.. São Paulo: Quartier Latin, 2008. p. 470.

Coaguila tem se posicionado a favor de uma uniformização para os princípios e leis a serem aplicados para a Informática.

3.2. LEGISLAÇÃO INTERNACIONAL

3.2.1. Convenção de Budapeste – Conselho da Europa

A Convenção de Budapeste[144], assinada entre os países membros do Conselho da Europa em 2001, é um exemplo de cooperação entre Estados para o combate a *cybercriminalidade*. O próprio preâmbulo fala acerca da necessidade desta cooperação entre Estados, conforme segue: “Acreditando que uma luta efictiva contra o cibercrime requer uma acrescida, rápida e eficaz cooperação internacional em matéria penal;”

A Convenção de Budapeste propõe aos países membros quais os fatos típicos que deverão ser tomadas as medidas legislativas e/ou outras medidas que se façam necessárias.

Os crimes de informática estão assim classificados na Convenção de Budapeste[145]:

> Infracções penais contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos: Acesso ilegítimo; interceptação ilegítima; interferência em dados; interferência em sistemas e uso indevido de dispositivos.
>
> Infracções penais relacionadas com computadores: Falsidade Informática, Burla informática.
>
> Infracções penais relacionadas com o conteúdo: infrações penais relacionadas a pornografia infantil
>
> Infracções penais relacionadas com a violação do direito do autor e direitos conexos.

---

[144] PROCURADORIA DA REPÚBLICA EM PERNAMBUCO. Disponível em: <http://www.prpe.mpf.gov.br/internet/content/download/2770/22203/file/CONVEN%C3%87%C3%83O%20DE%20BUDAPESTE.pdf>. Acesso em: 01 de outubro de 2009

[145] PROCURADORIA DA REPÚBLICA EM PERNAMBUCO. Disponível em: <http://www.prpe.mpf.gov.br/internet/content/download/2770/22203/file/CONVEN%C3%87%C3%83O%20DE%20BUDAPESTE.pdf>. Acesso em: 01 de outubro de 2009

Também é previsto na Convenção de Budapeste[146] que os países membros do Conselho da Europa deverão legislar sobre as sanções a serem impostas a cada infração, sendo admitida até mesmo a pena privativa de liberdade; sobre a possibilidade de tentativa; sobre a parte processual adotadas aos crimes; a competência para o julgamento dos crimes.

Por fim, estabeleceu alguns princípios de cooperação internacional e auxílio mútuo para resolver o problema da criminalidade na informática.

Do modo que foi estabelecido a Convenção em comento, fica mais fácil para conseguir punir os "infratores virtuais", ainda que cada país tenha sua própria legislação. Mesmo que o crime seja praticado de um país pro outro, com o auxílio mútuo dos países envolvidos, ambos poderão fazer a investigação e, se for o caso, prender o criminoso.

3.2.2. Peru

Os principais dispositivos de coerção aos crimes de informática no Peru estão previstos no Código Penal, introduzidos pela Lei n. 27.309 de 17 de julho de 2009, que assim dispõem:

> *Artículo 207 a)*[147]
>
> *El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar ejecutar o alterar un esquema, u otro similar, o para interferir, interceptar, acceder ó copiar información en tránsito contenida en una base de datos, será reprimido con pena privativa*

---

[146] PROCURADORIA DA REPÚBLICA EM PERNAMBUCO. Disponível em: <http://www.prpe.mpf.gov.br/internet/content/download/2770/22203/file/CONVEN%C3%87%C3%83O%20DE%20BUDAPESTE.pdf>. Acesso em: 01 de outubro de 2009

[147] Aquele que utiliza ou ingressa indevidamente em uma base de dados, sistema ou rede de computadores ou qualquer parte da mesma, para executar ou alterar um arquivo, ou outro similar, ou para interferir, interceptar, acessar ou copiar informação em trânsito contida em uma base de dados, será punido com pena privativa de liberdade de no máximo dois anos ou com prestação de serviços a comunidade de cinqüenta e dois a cinqüenta e quatro jornadas.

de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.[148]

Artículo 207 b) [149]

El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multe.

Artículo 207 c) [150]

En los casos de los Artículos 207 a) y 207 b), la pena será privativa de libertad no menor de cinco ni mayor de siete años,

cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.

2. El agente pone en peligro la seguridad nacional.

CAPITULO XI. DISPOSICIÓN COMÚN

Artículo 208. [151]

---

[148] Se o agente atuou com a finalidade de obter um beneficio econômico, será punido com pena privativa de liberdade de no máximo três anos ou com prestação de serviços a comunidade de no mínimo cinqüenta e quatro jornadas.

[149] O que utiliza, ingressa ou interfere indevidamente em uma base de dados, sistema, rede ou programa de computadores ou qualquer parte da mesma com o fim de alterá-los, danificá-los ou destruí-los, será punido com pena privativa de liberdade de no mínimo três e no máximo de cinco anos e com setenta a noventa dias multa.

[150] Nos casos dos artigos 207 a e 207 b, a pena será privativa de liberdade de no mínimo cinco e no máximo sete anos, quando:1. o agente acessar uma rede de dados, sistema ou rede de computador, fazendo uso de informação privilegiada, obtida em razão do seu cargo.2. o agente põe em risco a segurança nacional.

[151] Não são punidos, sem prejuízo da indenização civil, os furtos, apropriações, fraudes ou danos que se causem: 1.Aos cônjuges, concubinos, ascendentes, descendentes e afins em linha reta; 2. O consorte viúvo, a respeito dos bens de seu cônjuge falecido, salvo quando tenha passado ao poder de terceiro; Os irmãos e cunhados, se viverem juntos.

> *No son reprimibles, sin perjuicio de la reparación civil, los hurtos, apropiaciones, defraudaciones o daños que se causen:*
>
> *1. Los cónyuges, concubinos, ascendientes, descendientes y afines en línea recta.*
>
> *2. El consorte viudo, respecto de los bienes de su difunto cónyuge, mientras no hayan pasado a poder de tercero.*
>
> *3. Los hermanos y cuñados, si viviesen juntos.*

O legislador peruano decidiu proteger os interesses dos usuários da Internet mediante a penalização das condutas que provocam danos à propriedade privada, assim como o ingresso indevido aos sistemas ou redes informáticas. Por este motivo, em 17 de julho de 2000, foi publicada a lei n. 27.309, que alterou o código penal peruano, incluindo os chamados delitos informáticos.

Essa alteração ao Código Penal peruano contempla duas hipóteses de crimes de informática, previstos no *artículo 207-A* e *artículo 207-B*. Carlos Alberto Soto Coaguila[152] diferencia os dois tipos penais:

> A diferença entre as hipóteses de ambos os artigos se apresenta no objetivo do cometimento do delito, já que enquanto na primeira (207-A) se faz referência ao ingresso indevido ou à alteração (mediante planejamento, execução ou cópia) de informação, na segunda (207-B) alude-se ao efeito de produzir dano e, inclusive, destruição de um determinado programa ou base de dados, sendo tais efeitos os determinantes para a aplicação da pena prevista.

Desta maneira, nota-se que o Peru, a exemplo dos Estados Unidos, Portugal, Chile etc., tem se preocupado com a questão criminal na Informática. Assim, fez alterações em seu Código Penal de modo a punir aqueles que agem com o intuito de causar danos a outrem.

3.2.3. Chile

[152] COAGUILA, Carlos Alberto Soto. A Criminalidade Informática. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes. v. 2. São Paulo: Quartier Latin, 2008. p. 201.

Um dos poucos países da América Latina que possui uma legislação específica para os crimes de informática é o Chile[153]. A lei que trata acerca deste tema é a de nº 19.223, onde em quatro artigos pune as condutas realizadas através ou contra um sistema informático.

O primeiro artigo da Lei nº 19.223 trata da destruição ou inutilização de um sistema de informática; o segundo artigo pune quem intercepte ou interfira sem autorização em um sistema; já o artigo terceiro tem o escopo de punir quem alterar, danificar ou destruir dados em um sistema de tratamento de informação; por fim o artigo quarto pune o que maliciosamente difundir dados contidos em um sistema de informação. [154]

Por se tratar de uma lei muito sucinta, acaba deixando de prever todas as possibilidades de crimes em um sistema de informática, desta forma acaba sendo criticada neste ponto, conforme explica Cristian Andrés Meneses Diaz[155]:

> Por último, se crítica la ley nº 19.223 por dejar fuera de regulación ciertos delitos informáticos. Al respecto , existe consenso en la doctrina en cuanto a que nuestra normativa, contempla sólo dos modalidades delictivas: el *sabotaje informático* (artículos 1º y 3º) y *el espionaje informático* (artículos 2º y 4º) dejando de lado las figuras del fraude informático, la del acceso no autorizado o hacking directo y la piratería de programas.

Assim, nota-se que apesar de o Chile ser o país pioneiro na América Latina a fazer uma lei para tratar sobre a criminalidade na informática, deixou muitas práticas, que poderiam ser consideradas como crime, de fora, dando prioridade somente ao combate a sabotagem informática aos sistemas de tratamento de informação e a espionagem informática[156].

---

[153] ROSA, Fabrízio. **Crimes de Informática.** 2. ed. Campinas: Bookseller, 2006. p. 84.

[154] INFORMATICA JURIDICA. Disponível em: <http://www.informatica-juridica.com/anexos/19223.pdf> . Acesso em: 22 de julho de 2009.

[155] DIAZ, Cristian Andés Meneses. **Delitos Informáticos y Nuevas Formas de Resolución del Conflicto Penal.** Disponível em: <http://www.alfa-redi.org/rdi-articulo.shtml?x=1428>. Acesso em 23 de julho de 2009.

[156] ROSA, Fabrízio. **Crimes de Informática.** 2. ed. Campinas: Bookseller, 2006. p. 85.

3.2.4. Estados Unidos

Os Estados Unidos é um dos pioneiros na questão de legislação aplicável aos crimes de informática. No fim da década de 1970, iniciou a legislar sobre o tema e em 1986 criou o *Computer Fraud anda Abuse Act – CFAA,* criminalizando alguns tipos de condutas realizadas através de sistema de informática, conforme ensina Fabrízio Rosa[157]:

> Os EUA começaram a legislar sobre os crimes de informática no fim da década de 1970; a primeira lei federal sobre crimes de Informática foi a *Computer Fraud anda Abuse Act – CFAA*, de 1986, que criminalizava condutas como, por exemplo, o acesso não autorizado, seja para obtenção de segredos nacionais com intenção de prejudicar os EUA, seja para obter informações financeiras e de créditos, ou, ainda, o simples acesso não-autorizado a computador do Governo Federal.

Segundo Carla Rodrigues Araújo de Castro[158], os Estados Unidos possuem várias leis na área de crimes de informática, citando as principais delas e seus objetivos:

> Os Estados Unidos possuem várias leis sobre a informática. A Lei 18 U.S.C. 1030 disciplina a fraude e atividades relacionadas a computadores, tipificando algumas condutas e conceituando computador, dentre outras expressões, prevendo penas de multa e de encarceramento.
>
> [...].
>
> Outras leis existem sobre o assunto: lei 18 U.S.C. 1362 protegendo as linhas de comunicação, estações e sistemas. A lei 18 U.S.C. 2511 tutela as comunicações tipificandpo como crime a conduta de quem intercepta ou revela comunicação, oral ou eletrônica, proibida. A lei 18 U.S.C. 2701 tipifica o acesso ilícito de comunicações armazenadas. E a lei 18 U.S.C. 2702 dispõe sobre a revelação de conteúdo.

De acordo com Maria Eugênia Finkelstein[159], depois dos ataques terroristas em 11 de setembro de 2001, os Estados Unidos se

---

[157] ROSA, Fabrízio. **Crimes de Informática.** 2. ed. Campinas: Bookseller, 2006. p. 82.

[158] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais** 2. ed. Rio de Janeiro: Quartier Latin, 2003. p. 161.

[159] FINKELSTEIN, Maria Eugênia. Fraude Eletrônica. *In*: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) **Direito & Internet**: Aspectos Jurídicos Relevantes.2 v.. São Paulo: Quartier Latin, 2008. p. 431.

preocuparam ainda mais na questão dos crimes de informática, pois os terroristas passaram a utilizar e a projetar os ataques através da informática. As principais legislações que entraram em vigor após os ataques foram:

> USAPA – *USA Patriotic Act* – lei aprovada no final de 2001 que visa a agilizar a captura e punição dos responsáveis por ataques eletrônicos. Essa lei prevê que alguns ataques de *hackers* são tratados como atos terroristas e seus responsáveis estão sujeitos a penas extremamente severas. Como condutas condenáveis encontram-se a publicação de informações que possam causar dano aos Estados Unidos, de informações técnicas que possam levar ao terrorismo e até a transmissão de informações pessoais de pessoas estranhas;
>
> FISA – *Foreign Intelligence Survaillance Act* – prevê o monitoramento de agentes especiais do exterior atuando nos Estados Unidos e facilita a atuação das autoridades em casos internacionais;
>
> CSEA – *Cybersecurity Enhancement Act* – que institui 10 anos de cadeia como pena mínima para crimes eletrônicos e punição imediata para quem acessa informações sem que tenha permissão para isso.

Os Estados Unidos, através de leis rígidas, é um dos países que mais tem se preocupado com a questão da criminalidade na informática, até quanto ao *cyberterrorismo* que ficou mais claro após os ataques terroristas em 11 de setembro de 2001.

3.2.5. Inglaterra

Na Inglaterra a principal lei de combate aos crimes de informática é o *Computer Misuse Act*, de 1990. Sobre a referida lei inglesa, explica Carla Rodrigues Araújo de Castro[160]:

> O *Computer Misuse Act*, de 1990, disciplinou várias condutas criminosas ligadas à informática, como, por exemplo, a obtenção de acesso não autorizado a programa ou informação. Dispôs a excludente de responsabilidade criminal sempre que o agente, sem saber, obtém a informação, ou seja, não houve intenção de violar o sistema alheio.

[160] CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais** 2. ed. Rio de Janeiro: Quartier Latin, 2003. p. 162.

> O acesso também é punível quando for meio para execução de outro delito. Desta forma, puniu o legislador inglês os atos preparatórios de crimes mais graves que, por circunstâncias diversas, não chegam a se consumar. Trata-se de tipo subsdiário, conhecido em nossa legislação, vide a LCP.
>
> Modificar informações armazenadas em computadores também é punível, excluindo-se, no entanto, a modalidade culposa.

Fabrízio Rosa[161] também trata sobre o *Computer Misuse Act*:

> A lei inglesa que dispõe a respeito dos "crimes de Informática" foi elaborada em 1990, quando foi introduzido, no ordenamento jurídico, o delito de acesso não-autorizado, dispondo no art. 3º, inc. 2º, que a pessoa deve ter a intenção de modificar o conteúdo de qualquer computador através dos seguintes comportamentos:
>
> * impedindo a operação de qualquer computador; ou
>
> * impedindo ou dificultando o acesso a qualquer programa, ou a confiança desses dados;
>
> * impedindo a execução de qualquer dos programas, ou a confiança desses dados.

Porém, a lei inglesa é criticada em razão da sua amplitude[162], mas ainda assim é uma importante ferramenta para o combate à criminalidade informática, punindo diversas condutas envolvendo a informática. Nota-se, também, que a Inglaterra se preocupa há bastante tempo com o combate aos crimes de informática.

3.2.6. Portugal

Portugal, desde 1991, conta com a lei nº 109/91 para combater a "criminalidade informática", tal lei tipificou seis condutas envolvendo a Informática. Fabrízio Rosa[163] explica cada uma delas:

---

[161] ROSA, Fabrízio. **Crimes de Informática.** 2. ed. Campinas: Bookseller, 2006. p. 83.

[162] ROSA, Fabrízio. **Crimes de Informática.** 2. ed. Campinas: Bookseller, 2006. p. 83.

[163] ROSA, Fabrízio. **Crimes de Informática.** 2. ed. Campinas: Bookseller, 2006. p. 86-87.

> Falsidade informática – art. 4º - este artigo penaliza a introdução, modificação ou a supressão de dados ou de programas informáticos;
>
> Dano relativo a dados ou programas informáticos – art. 5º - Este artigo penaliza a atuação não autorizada com intenção de causar prejuízo ou obter benefício ilegítimo;
>
> Sabotagem informática – art. 6º - Neste caso, é penalizado o apagamento, a alteração, a introdução ou a supressão de dados ou programas informáticos, com o objetivo de entravar ou perturbar o funcionamento informático ou de comunicação de dados à distância;
>
> Acesso ilegítimo – art. 7º - Este artigo penaliza o acesso não autorizado;
>
> Interceptação ilegítima – art. 8º - É penalizada a interceptação, sem autorização, de comunicações que se processem no interior de um sistema ou rede informática;
>
> Reprodução ilegítima de programa protegido e de topografia – art. 9º - Neste artigo é punida a reprodução, divulgação ou a comunicação ao público, sem autorização, de um programa informático protegido por lei.

Uma questão a ser destacada na legislação portuguesa é quanto à responsabilidade penal, já que o artigo 3º da Lei 109/91[164] trata justamente da "responsabilidade penal das pessoas colectivas e equiparadas":

> Art. 3º - Responsabilidade penal das pessoas colectivas e equiparadas.
>
> 1 – as pessoas colectivas, sociedades e mera associações de facto são penalmente responsáveis pelos crimes previstos na lei quando cometidos em seu nome e no interesse colectivo pelos seus órgãos ou representantes.
>
> 2 – A responsabilidade é excluída quando o agente tiver actuado contra ordens ou instruções expressas de quem de direito.
>
> 3 – A responsabilidade das entidades referidas no nº1 não exclui a responsabilidade individual dos respectivos agentes.
>
> 4 – As entidades referidas no nº1 respondem solidariamente , nos termos da lei civil, pelo pagamento das multas, indemnizações e outras prestações em que forem condenados os agentes das infracções previstas na presente lei.

---

[164] COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS. Disponível em: <http://www.cnpd.pt/bin/legis/nacional/lei_10991.htm>. Acesso em: 14 de setembro de 2009.

Este artigo demonstra que Portugal se preocupou em punir não somente as pessoas físicas, mas também as pessoas jurídicas, chamadas lá de ‘pessoas colectivas’.

Na legislação portuguesa somente pode ser aplicado o direito penal às pessoas jurídicas quando expressamente previsto. O artigo 11 do Código Penal Português determina que só as pessoas físicas podem ser responsabilizadas criminalmente, salvo quando expressamente preveja a possibilidade da incriminação das pessoas jurídicas, porém não há nenhuma hipótese prevista no Código Penal português para responsabilização das pessoas jurídicas.

Deste modo, conforme observa Paulo de Sousa Mendes[165], há alguns crimes envolvendo informática em que as pessoas jurídicas poderão ser responsabilizadas e punidas e outros que, por estarem previstos dentro do próprio Código Penal, não podem ser aplicados às pessoas jurídicas:

> A localização de certo tipo incriminador dentro ou fora do Código Penal, ‘[parecendo] ser questão menor, de mera sistemática, tem afinal importantes consequências substantivas’. Por exemplo, a burla informática foi incluída no próprio Código Penal português, no art. 221º, por se considerar que tinha o mesmo significado que burla em geral, ao passo que o dano informático aparece no art. 5º da lei de criminalidade informática. Por consequência, as pessoas colectivas respondem criminalmente pelo dano informático, mas já não respondem pela burla informática.

Por fim, importante destacar que Portugal em 15 de setembro de 2009, publicou uma nova lei (Lei nº 109/2009) de crimes de informática para adequar o direito interno às normas estabelecidas pelo Conselho da Europa, esta adequação refere-se à cooperação internacional que foi determinada na Convenção de Budapeste. Esta lei, porém, só entrará em vigor a

---

[165] MENDES, Paulo de Sousa. **A responsabilidade de pessoas colectivas no âmbito da criminalidade informática em Portugal**. Portugal, [200-?]. Disponível em: <http://www.apdi.pt/APDI/DOUTRINA/A%20responsabilidade%20de%20pessoas%20colectivas%20no%20%C3%A2mbito%20da%20criminalidade%20inform%C3%A1tica%20em%20Portugal.pdf>. Acesso em: 20 de set. 2009.

partir de 30 de outubro de 2009, já que prevê o prazo de 30 dias para entrar em vigor[166].

3.3. LEGISLAÇÃO BRASILEIRA

O Brasil carece ainda de uma legislação específica para os crimes de informática. Não somente referente aos crimes de informática, mas também há lacunas em leis do âmbito cível, trabalhista, tributário etc., no que tange as suas relações com a informática.

Para os crimes de informática utiliza-se de forma análoga o Código Penal de 1940, ano em que ainda não existiam a internet e o computador, pelo menos não da forma que conhecemos atualmente. Por este motivo, é necessário que leis identifiquem as condutas que possam trazer algum dano à sociedade e, assim como em qualquer outro crime, especifique a pena a ser aplicada para aquele que infringir tais regras.

Algumas medidas emergenciais foram tomadas, de modo a combater algumas dessas atitudes. Um exemplo claro disto, é no caso da pornografia infantil. Até o final de 2008, com a reforma do Estatuto da Criança e do Adolescente, não era considerado crime aquele armazenava conteúdo digital de cunho erótico/ pornográfico envolvendo crianças e/ou adolescentes.

Através da lei 9.983, de 14 de julho de 2000 foram feitas modificações no Código Penal envolvendo a informática, porém em relação somente à Administração Pública:

> Art. 313 – “A” do Código Penal: Inserção de dados falsos em sistemas de informações, alteração ou exclusão indevidas de dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública;
>
> Art. 313 – “B” do Código Penal: Modificação ou alteração não autorizada de sistema de informações ou programa de informática;

[166] DIARIO DA REPÚBLICA ELECTRÓNICO. Disponível em: <http://dre.pt/pdf1sdip/2009/09/17900/0631906325.pdf>. Acesso em: 01 de outubro de 2009.

> Art. 153, §1º, do Código Penal: Divulgação, sem justa causa, de informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública;
>
> Art. 325, §1º, inc. I, do Código Penal: Fornecimento e empréstimo de senha a pessoas não autorizadas, a sistemas de informações ou banco de dados da Administração Pública;
>
> Art. 325, §1º, inc. II, do Código Penal: Utilização indevida do acesso restrito.

Levando-se em conta que a internet no Brasil, como visto no primeiro capítulo, se popularizou a partir do ano de 1994, tem-se um período de 15 (quinze) anos que esta prática deplorável permaneceu impune.

Existem alguns projetos de lei para regular as práticas criminosas na informática. O principal deles é o projeto de lei 76/2000. Porém, tal projeto vem sofrendo fortes críticas, em decorrência, talvez, de envolver medidas para intensificar as ações conta a pirataria na internet, o que acabou irritando a grande parcela da população brasileira que faz *downloads* ilegais. Sobre o projeto de lei 76/2000, Fabrízio Rosa[167] cita os principais comportamentos quer poderão vir a ser punidos caso seja aprovado:

> O acesso não autorizado a computadores e sistemas eletrônicos;
>
> A destruição ou alteração de informações;
>
> A sabotagem por computadores;
>
> A intercessão de correio eletrônico;
>
> Fraude eletrônica, e;
>
> A transferência ilícita de fundos

Outro projeto de lei importante é o Projeto de Lei da Câmara dos Deputados nº 84, de 1999 que tipifica uma grande diversidade de condutas

[167] ROSA, Fabrízio. **Crimes de Informática**. 2. ed. Campinas: BookSeller, 2006. p. 92.

praticadas por meio eletrônico, tais como clonagem de celular, difusão de vírus, acesso indevido etc.[168]

[168] ROSA, Fabrízio. **Crimes de Informática**. 2. ed. Campinas: BookSeller, 2006. p. 91.

CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo investigar, os crimes de informática, considerando tanto os crimes que efetivamente estão tipificados no ordenamento jurídico penal brasileiro, quanto aquelas condutas que, mesmo não tendo tipificação, causam graves danos à sociedade.

Os crimes de informática têm ganhado destaque na mídia em razão dos enormes prejuízos que causam. Porém, mesmo causando graves danos, não há uma lei que regule a informática no âmbito penal, assim como as autoridades não estão preparadas para o combate a este tipo de criminalidade.

Para seu desenvolvimento lógico o trabalho foi dividido em três capítulos.

No primeiro capítulo tratou-se dos princípios aplicados aos crimes de informática, assim como a parte histórica, apresentando sucintamente como se deu o surgimento do computador e da Internet, ferramentas principais na informática, e, ainda, quais foram as primeiras condutas maliciosas utilizando essas tecnologias.

O segundo capítulo refere-se aos sujeitos ativos e passivos dos crimes de informática, fazendo, no caso dos sujeitos ativos, a sua classificação conforme a área de atuação. Apresentaram-se, também, algumas condutas que tem trazido danos e riscos aos usuários da informática.

E, no terceiro e último capítulo, analisou-se como se tem legislado a respeito dos crimes de informática em diversos países. Também se apresentou alguns dos crimes de informática que já possuem previsão no direito penal brasileiro e alguns projetos de lei que tratam acerca do tema.

A pesquisa foi embasada nos seguintes problemas:

1º) O Brasil possui leis para punir as condutas abusivas

praticadas através da informática? Não. São raros os casos em que se pode aplicar a legislação vigente para os crimes de informática, faltando uma legislação penal para punir os abusos na informática. Hipótese confirmada.

2º) Ainda que tenha uma legislação interna aplicável, isto basta para um combate eficaz à criminalidade informática? Não, para um combate efetivo é necessária a cooperação entre os Países, tendo em vista que, o principal meio para a prática dos crimes de informática é a Internet, sendo que esta tem abrangência caráter global. Hipótese confirmada.

Por fim, ressalte-se que o presente trabalho não tem a finalidade de exaurir a matéria, o estudo dos crimes de informática é relativamente novo, sendo que o trabalho visa apenas apresentar a gravidade de não ter ainda leis que punam e reprimam os abusos causados na informática.

REFERÊNCIA DAS FONTES CITADAS

ALMEIDA FILHO, Agassiz; CRUZ, Danielle da Rocha. **Estado de Direito e direitos fundamentais.** São Paulo: Forense, 2005.

ASSUNÇÃO, Marco Flávio Araújo. **Segredos do Hacker Ético**. 2. ed. Florianópolis: Visual Books, 2008.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. **Comentários à Constituição do Brasil**. v. 2. São Paulo: Saraiva, 1989.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constitui%C3%A7ao.htm>.

BRASIL. Decreto-Lei nº 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848compilado.htm>.

BRASIL. Lei nº 5.250 de 9 de fevereiro de 1967. Regula a liberdade de manifestação do pensamento e de informação. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L5250.htm>.

BRASIL. Lei nº 7.716 de 5 de janeiro de 1989. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L7716.htm>.

BRASIL. Lei nº 9.609 de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L9609.htm>. Acesso em; 23 de julho de 2009.

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 18.620-PR (2005/0187497-1), Sexta Turma, Brasília, DF, 14 de outubro de 2009.

BULOS, Uadi Lammêgo. **Constituição Federal Anotada**. 5. ed. São Paulo: Saraiva, 2003.

CAPEZ, Fernando**. Curso de Direito penal:** parte geral. v. 1. 7. ed. rev. e atual. de acordo com as Leis nº 10.721/ 2003 (Estatuto do Idoso), 10.763/2003 e 10.826/2003. São Paulo: Saraiva, 2004.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

DELMANTO, Celso; et al. **Código Penal Comentado**. 4. ed. Rio de Janeiro: Renovar, 1998.

FONTES, Edison. **Segurança da Informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

GALDEMANN, Henrique. **De Gutemberg à Internet**: Direitos autorais na era digital. 4 ed. Rio de Janeiro: Record, 2001.

LENZA, Pedro. **Direito Constitucional Esquematizado**. 9. ed. São Paulo: Método, 2005.

LUCCA, Newton; SIMÃO FILHO, Adalberto. **Direito & Internet**: Aspectos Jurídicos Relevantes.v.1. 2. ed. São Paulo: Quartier Latin, 2006.

LUCCA, Newton; SIMÃO FILHO, Adalberto. **Direito & Internet**: Aspectos Jurídicos Relevantes.v.2. São Paulo: Quartier Latin, 2008.

MIRABETE, Julio Fabbrini. **Código Penal Interpretado**. 3 ed. São Paulo: Atlas, 2003.

MORAES, Alexandre de. **Direito Constitucional**. 13. ed. São Paulo: Atlas, 2003.

MORAES, Alexandre de. **Direitos Humanos Fundamentais:** Teoria Geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 8 ed. São Paulo: Atlas, 2007.

MUOIO, Arlete Figueiredo; AGUIAR, Malu. **Crimes na Rede**: o perigo que se esconde no computador. São Paulo: Companhia Limitada, 2006.

NOGUEIRA, Sandro D'amato. **Crimes de Informática**. São Paulo: BH Editora, 2008.

NUCCI, Guilherme de Souza. **Código Penal comentado.** 7 ed. São Paulo: Revista dos Tribunais, 2007.

PRADO, Luiz Regis. **Direito Penal parte especial –** Arts. 197 a 288. 2 ed. refor. atual. e ampl. São Paulo: Revista dos Tribunais, 2008.

ROSA, Fabrízio. **Crimes de Informática.** 2.ed. Campinas: BookSeller, 2006.

ROVER, Aires José. **Direito e Informática**. Barueri: Manole, 2004.

RUFINO, Nelson Murilo de. **Segurança Nacional**: Técnicas e Ferramentas de Ataque e Defesa de Redes de Computador. São Paulo: Novatec, 2002.

SHIMIZU, Heitor; SETTI, Ricardo. Tem boi na linha: hackers os espiões cibernéticos. **Super Interessante**, São Paulo, out. 1995. Disponível em: <http://super.abril.com.br/tecnologia/tem-boi-linha-hackers-espioes-ciberneticos-441127.shtml>. Acesso em: 10 de abril de 2009.

SOARES, Orlando. **Comentários à Constituição da República Federativa do Brasil**. 12. ed. Rio de Janeiro: Forense, 2006.

TAMEGA, Flávio. **Hacker Inside**. v.1. Goiania: Editora Terra, 2003.

ULBRICH, Henrique César; VALLE, James Della. **Universo Hacker.** 4. ed. São Paulo: Digerati Books, 2004.

VIANA, Túlio Lima. **Do delito de dano e de sua aplicação ao direito penal informático**. Revista dos Tribunais, São Paulo, a. 92, v. 807. janeiro 2003.