10.12818/P.0304-2340.2013v62p139

CRIMES CIBERNÉTICOS: O DESCOMPASSO DO ESTADO E A REALIDADE

CYBERCRIME: THE MISMATCH STATE AND REALITY

David Augusto Fernandes[*]

RESUMO

O presente artigo tem por objetivo traçar o desenvolvimento da internet, apresentando os grandes benefícios deste avanço tecnológico, que se constitui num excelente meio de comunicação de massas. Por outro lado, também propicia a ação criminosa, pois o conhecimento apurado de informática facilita a prática de infrações penais, causando danos de grande monta a terceiros que, não tendo a precaução necessária, tornam-se vítimas dessas pessoas. Oportunamente, são também delineadas as soluções apresentadas no Direito Comparado, como os projetos existentes em nosso País para coibir este novo tipo de ação criminosa.

PALAVRAS-CHAVE: Internet. Crimes cibernéticos. Direito Comparado. Convenção de Budapeste.

ABSTRACT

This article aims to trace the development of the internet, showing the great benefits of this technological advancement, it is an excellent means of mass communication. On the other hand, it also provides criminal activity because of improved knowledge of informatics facilitates the practice of criminal offenses, causing large amounts of damage to a third party who is not a necessary precaution, they become victims of these people. In due course, are also outlined the solutions presented in comparative law, as existing projects in our country to curb this new type of criminal activity.

KEYWORDS: *Internet. Cyber crimes. Comparative Law. Budapest Convention.*

[*] Mestre e Doutor em Direito pela Universidade Gama Filho. Professor de Direito Internacional, Direito Processual Penal e Direito Penal. Professor em cursos de graduação e de pós-graduação do Centro Universitário Moacyr Sreder Bastos e em cursos de graduação do Centro Universitário de Barra Mansa.

E-mail: fernandes.ddaf@gmail.com.

AUTORIZADA DE SISTEMAS DE INFORMAÇÃO; 1.1.4 - VIOLAÇÃO DE SIGILO FUNCIONAL; 1.1.5 - LEIS EXTRAVAGANTES; 1.1.5.1 - ESTATUTO DA CRIANÇA E DO ADOLESCENTE (ECA) – PORNOGRAFIA INFANTIL; 1.1.5.2 - CRIMES CONTRA A ORDEM TRIBUTÁRIA, ECONÔMICA E CONTRA AS RELAÇÕES DE CONSUMO; 1.1.5.3 - LEI DE INTERCEPTAÇÃO DE COMUNICAÇÕES TELEFÔNICAS; 1.1.5.4 - CÓDIGO ELEITORAL; 1.1.5.5 - LEI DE PROPRIEDADE INTELECTUAL DE PROGRAMA DE COMPUTADOR; 1.1.6 - SUBSUNÇÃO DE CONDUTAS CRIMINAIS; 1.1.6.1 - CRIME DE DANO; 1.1.6.2 - FRAUDE ELETRÔNICA: ESTELIONATO E FURTO; 1.1.6.3 - PLÁGIO PRODUZIDO VIA INTERNET; CONSIDERAÇÕES FINAIS; REFERÊNCIAS.

INTRODUÇÃO

No período da guerra fria, mais especificamente durante o ano de 1962, pesquisadores americanos começaram a imaginar um sistema imune a ataques aéreos, que fosse capaz de interligar muitos computadores, permitindo o compartilhamento de dados entre eles. Passados sete anos, a primeira versão desse sistema ficou pronta, recebendo a denominação de *Advanced Research Projects Agency* ou Agência de Projetos de Pesquisa Avançada (ARPAnet). Sua principal característica era não possuir um comando central, de modo que, em caso de destruição de um ou mais computadores, todos os outros equipamentos ligados ao sistema continuariam operando.

Décadas mais tarde, com o desenvolvimento tecnológico, o sistema veio a ser utilizado na interligação de universidades americanas, e depois também em institutos de pesquisa sediados em outros países. A ideia central, porém, permaneceu intacta, ou

seja, uma espécie de associação mundial de computadores, todos interligados por meio de um conjunto de regras padronizadas que especificam o formato, a sincronização e a verificação de erros em comunicação de dados.

Na década de 1990 a exploração comercial do serviço começou, tendo se desenvolvido, em face da invenção da *world wide web* (www), um enorme pacote de informações, em formato de texto ou mídia (imagens e arquivos de áudio e vídeo), organizadas de forma a que o usuário pudesse percorrer as páginas na rede, isto é, "navegar", a partir de sequências associativas (*links*) entre blocos vinculados por remissões[1].

1 COMITÊ Gestor da Internet no Brasil. **Manual prático de investigação de crimes cibernéticos**. São Paulo, 2006. Disponível em: <http://www.prsp.mpf.gov.br.html>. Acesso em: 26 dez. 2011.
Para efeito de comparação com outro extraordinário invento tecnológico, que é o telefone, o PhD Lori Valigra ressalta, em sua mais famosa citação, que o telefone levou 75 anos para chegar à marca de 50 milhões de usuários, enquanto que a internet levou apenas quatro para fazer o mesmo. Portanto, a internet passa, desde os últimos anos do século XX, a fazer parte dos hábitos populares, do Ocidente ao Oriente, de Norte a Sul. Como uma grande explosão, ela invade o lar, a academia e a indústria, e reivindica autonomia para se manter em constante expansão. Com isso, novos cenários surgem, novos atores se apresentam e novas perspectivas são postas para os contratos sociais. Emerge, entre outros efeitos colaterais desta revolução técnico-social, o cibercrime e, com ele, indagações sobre como combatê-lo num espaço totalmente desfigurado daquele conhecido pelo Estado Moderno, o qual, por sua vez, foi engendrado essencialmente na base territorial.
No final dos anos 1980 e início dos 1990, o pesquisador britânico do *Conseil Européen pour la Recherche Nucléaire* (CERN) [Conselho Europeu para a Pesquisa Nuclear], *Sir* Tim Berners-Lee, escreve sobre uma possível e viável proposta de interconectar redes de computadores numa única e gigantesca rede: a rede mundial de computadores. Surgia, assim, teórica e empiricamente, a internet.
Também na década de 1980, o ex-programador do *Massachussets Institute of Technology* (MIT), Richard Stallman, consolidava as instituições filosóficas, técnicas e jurídicas do Movimento Software Livre, as quais serviram de base para muitas das grandes invenções e programas que ajudariam a popularizar a internet anos à frente: a licença GNU, o sistema operacional GNU/Linux, o servidor *web* Apache, o navegador Firefox, dentre outros.
Berners-Lee projetara a internet para funcionar de forma descentralizada e o mais universal possível, afinal, os protocolos de transmissão e linguagens que a suportavam (TCP/IP10, HTTP11, HTML12) também eram/são livres e abertos à sociedade, acadêmica ou não. Logo, é possível acessar uma página HTML hospedada numa máquina X a partir de um terminal Y, não importando o tipo/marca deste. Uma espécie de *ciberisonomia* se constituíra. Conforme acentuam SOUZA, Gills Lopes Macêdo;

A denominação "internet" somente surgiu na década de 1980, com a seguinte definição:

> [...] um conjunto de redes de computadores interligadas pelo mundo inteiro, que têm em comum um conjunto de protocolos e serviços, possuindo a peculiaridade de funcionar pelo sistema de trocas de pacotes e cada pacote pode seguir uma rota distinta para chegar ao mesmo ponto[2].

Desde o início da implementação da internet, o número de usuários aumentou exponencialmente. Em 1990, havia cerca de dois milhões de pessoas conectadas à rede em todo o mundo. Depois de uma década, esse número passou para 604 milhões. Conforme Bogo, a internet surgiu no Brasil em 1991, trazida pela Rede Nacional de Pesquisas (RNP), com o objetivo de conectar redes de universidades e centros de pesquisas, indo posteriormente para as esferas federal e estadual. Somente em 1995, o Ministério de Comunicações e de Ciência e Tecnologia autorizou sua abertura para a comercialização, através da RNP, e depois com a Embratel[3].

Já sua regulamentação foi feita pelo Comitê Gestor da Internet, criado por meio da Portaria Interministerial nº 147, e alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003, que tinha como funções integrar todas as iniciativas de serviços de internet no país e promover a qualidade técnica, a inovação e a disseminação dos serviços ofertados[4].

Conforme constata Diego Beas, a internet atua como novo agente de organização de massas e também influencia as

---

PEREIRA, Dalliana Vilas. A Convenção de Budapeste e as leis brasileiras. Disponível em: < www.charlieoscartango.com.br/.../A%20convencao%20de%20**Budapeste**%20e%20as%20**leis**%20bra...>. *Acesso em: 29 dez. 2011.*

2 Conforme ROSA, Fabrízio. **Crimes de informática**. 3. ed. Campinas: Bookseller, 2007, p. 35.

3 BOGO, Kellen Cristina. A história da internet: como tudo começou... 2000. Disponível em: <http://www.kplus.com.br>. Acesso em: 2 jan. 2012.

4 *Idem.*

esferas de poder do Estado, pois este deixa de ter a hegemonia do controle sobre as pessoas. A invejável condição desfrutada pela internet em conectar milhões de pessoas e mobilizá-las de maneira imediata é um recurso efetivo para provocar ações políticas importantes no cenário contemporâneo, haja vista os fatos ocorridos recentemente no Oriente Médio, quando a população se manifestou para apear do poder líderes políticos que não angariavam mais sua confiança[5].

Com esse desenvolvimento tecnológico, entra em cena uma nova modalidade criminosa. Infelizmente o Estado, tal como ocorre na mobilização popular, não tem a competência de antever a ação criminosa e, na maior parte das vezes, age reativamente após sua ocorrência.

Com o desenvolvimento tecnológico, o ser humano passou a utilizar-se amplamente do sistema informatizado para se comunicar, resolver seus problemas, pagar suas contas, inscrever-se em concursos, interagir com outros seres humanos nas várias redes pessoais existentes na internet. Mas, de outro lado a percepção criminosa visualizou que este meio tecnológico seria muito rentável para seus objetivos, aproveitando da ingenuidade e do despreparo de quem acessa a rede, tanto pessoa física como jurídica, ao não providenciar meios seguros para o acesso à internet.

Diante desta constatação, o presente artigo pretende apresentar o acompanhamento do Estado e as providências colocadas em prática por este Estado para anular as ações criminosas, a fim de estes criminosos serem responsabilizados penalmente por seus atos.

5 BEAS, Diego. A rua conectada com a rede. *O Globo*, Rio de Janeiro, 12 fev. 2001. Caderno A Revolução do Nilo, p. 6.

1. CRIMES CIBERNÉTICOS

A Convenção de Budapeste[6] foi o resultado de um trabalho desenvolvido pelo Conselho da Europa, na qual estava sendo priorizada a proteção da sociedade contra a criminalidade no ciberespaço. Propunha-se a escolha de uma legislação comum que objetivasse uma maior cooperação entre os Estados da União Europeia, sendo que tal tarefa já vinha sendo desenvolvida desde a década de 1990.

Com a efetivação da Convenção de Budapeste, adotada em 2002 pelo Conselho da Europa, e a abertura à assinatura por todos os países que a desejarem[7], ficou demonstrada a atualidade desta nova modalidade de crime e a necessidade de ele ser combatido por toda a sociedade mundial, visto que não só atinge a Europa, mas todo o mundo. Tal visão encontra eco nas palavras

6 A Convenção de Budapeste, celebrada na Hungria em 23 de novembro de 2001 pelo Conselho da Europa, teve como signatários 43 países, europeus, em sua maioria (Albânia, Andorra, Armênia, Áustria, Azerbaijão, Bélgica, Bósnia e Herzegovina, Bulgária, Croácia, República Checa, Dinamarca, Estônia, Finlândia, França, Geórgia, Alemanha, Grécia, Hungria, Islândia, Irlanda, Itália, Liechtenstein, Malta, Moldova, Mônaco, Noruega, Polônia, Portugal, Romênia, Rússia, Servia, Eslovênia, Eslováquia, Espanha, São Marino, Suíça, Suécia, antiga República Iugoslava da Macedônia, Turquia, Ucrânia, Reino Unido) e ainda Canadá, Costa Rica, Japão, México, Montenegro, África do Sul e Estados Unidos. Cada Estado signatário deve ratificar as disposições constantes da Convenção no seu ordenamento jurídico interno. Disponível em: <http://conventions.coe.int>. Acesso em: 3 jan. 2012.

7 Art. 37 – Adesão a Convenção
1. Após a entrada em vigor da presente Convenção, o Comitê de Ministros do Conselho da Europa pode, depois de ter consultado os Estados contratantes da Convenção e de ter obtido o acordo unânime, convidar qualquer Estado não membro do Conselho e que não tenha participado de sua elaboração, a aderir à presente Convenção. A decisão é tomada pela maioria prevista no art. 20, alínea d, dos Estatutos do Conselho da Europa e por unanimidade dos Estados contratantes com direito de voto no Conselho de Ministros.
2. Em relação a qualquer Estado aderente a Convenção, em conformidade com o nº 1, a Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data do depósito do instrumento de adesão junto ao Secretário Geral do Conselho da Europa. Disponível em: <www.charlieoscartango.com.br/.../A%20convencao%20de%20Budapeste%20e%20as%20leis%20bra...>. *Acesso em: 29 dez. 2011.*

de Medeiros, quando afirma que "não há fronteiras demarcadas no ambiente cibernético. Isso derruba um dos principais pilares do Estado Moderno" [8]. Também Castells[9] testifica que:

> O Estado não desaparece. Porém. É apenas redimensionado na Era da Informação. Prolifera sob a forma de governos locais e regionais que se espalham pelo mundo com seus projetos, formam eleitorados e negociam com governos nacionais, empresas multinacionais e órgãos internacionais. [...] O que os governos locais e regionais não têm em termos de poder e recursos é compensado pela flexibilidade e atuação em redes. Onde [...] a prática do crime é tão antiga quanto à própria humanidade. Mas o crime global, a formação de redes entre poderosas organizações criminosas e seus associados, com atividades compartilhadas em todo o planeta, constitui um novo fenômeno que afeta profundamente a economia no âmbito internacional e nacional, a política, a segurança e, em última análise, as sociedades em geral.

A Convenção de Budapeste veio a tipificar as seguintes condutas:

1) Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos:
   a) acesso doloso e ilegal a um sistema de informática;
   b) interceptação ilegal de dados ou comunicações telemáticas;
   c) atentado à integridade dos dados (conduta própria de um subgrupo *hacker*, conhecido como *cracket*[10]);
   d) atentado à integridade de um sistema;

8 MEDEIROS, Assis. **Hackers:** entre a ética e a criminalização. Florianópolis: Visual Books, 2002, p. 147.

9 CASTELLS, Manuel. **Fim do Milênio**. 4. ed. Tradução de Klaus Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 2007, p. 203.

10 *Cracker* é o especialista na engenharia de *software* ou *hardware* que pratica o *cracking* para quebrar a segurança de um sistema, danificando programas do usuário, como por exemplo, a clonagem ou adulteração de cartões magnéticos que acarretam a vulnerabilidade das páginas da internet. O *cracker* é conhecido como pichador digital, porque em geral gosta de deixar mensagens, deliciando-se com o prazer de causar estragos à vítima.

e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados.

2) Infrações informáticas:

a) falsificação de dados;
b) estelionatos eletrônicos (v.g., os *phishing scams*[11]).

3) Infrações relativas ao conteúdo:

a) pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens

11 É uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso de páginas fraudulentas na internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros, conforme o Manual Prático de Investigação de Crimes Cibernéticos do COMITÊ Gestor da Internet no Brasil, *op. cit.*
Os *sites* com *phishing* hospedam um *malware* (ou código malicioso – *malicius software*) é um termo genérico que abrange os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador. Na literatura de segurança o termo *malware* também é conhecido por "*software* malicioso". Alguns exemplos de *malware:* vírus*; worms e bots; backdoors;* cavalos de troia*; keyloggers* e outros programas *spyware; rootkits*. que subtraem senhas e *logins* dos usuários à medida que esses navegam pela internet, ou através de *downloads* feitos, que monitoram o computador infectado e furtam qualquer tipo de dados.
Com base em estudo procedido pela Trend Micro, fornecedora de antivírus, o Brasil só perde para os Estados Unidos da América e o Japão, no *ranking* de ataques de *phishing*, conforme descrição disponível em: <html://www.ebah.com.br/content/ABAAABQKAI/crimes-ciberneticos-dep-federal-julio-semeghini.hml>. Acesso em: 26 dez. 2011.
Verifica-se que a legislação brasileira é desprovida de instrumentos próprios para poder reprimir de forma eficaz a ação daqueles que possuem um conhecimento de informática e o utilizam para a prática criminosa. Como exemplo de tal atuação, situam-se aqueles que se utilizam de *sites* de difusão de *softwares* daninhos para ludibriar o incauto que navega na internet, a fim de conseguir sua senha bancária ou até aqueles que se utilizam de aparelhos copiadores de cartões de crédito ou bancários, denominados de "chupa-cabras", fazendo então um clone dos mesmos para suas empreitadas criminosas. Portanto, trata-se o *phishing* de uma fraude eletrônica, por meio da qual o agente obtém informações da vítima (senhas e dados pessoais), levando-a a erro, fazendo-se passar por terceiro, como por um banco ou um estabelecimento comercial ou levando o lesado a confiar em arquivos informáticos infectados por *softwares* daninhos, que capturam ou copiam dados. Constata-se que o objetivo do agente é a obtenção de vantagem patrimonial ilícita.

realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito);

b) racismo e xenofobia (difusão de imagens, ideias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e ameaças qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade);

4) Atentado à propriedade intelectual e aos direitos que lhe são conexos[12].

1.1 TIPOS PENAIS EXISTENTES NA LEGISLAÇÃO NACIONAL

Observa-se na legislação nacional a existência de pouca flexibilidade na matéria em comento, havendo tipos penais esporádicos, específicos, relativos aos crimes cibernéticos[13] descritos no Código Penal[14]. Estes tipos são abordados ao longo deste tópico, mediante o qual se faz um pequeno estudo sobre os mesmos.

12 Disponível em: < http://www.wirelessbrasil.org/wirelessbr/secoes/crimes_digitais/texto_convencao.pdf>. Acesso em: 27 dez. 2011.

13 COMITÊ Gestor da Internet no Brasil, *op. cit*.

14 Os delitos mais comuns praticados por meio do computador são os de intolerância religiosa, crimes contra o patrimônio, pornografia infanto-juvenil, crimes contra a honra, violação de segredo profissional, violação de direitos autorais e racismo, já tipifcados pelo nosso ordenamento, ou seja, são os velhos crimes, porém com um novo *modus operandi*. Conforme SAFERNET Brasil. Disponível em: <http://www.safernet.org.br/site/indicadores>. Acesso em: 2 jan. 2012.

1.1.1 DIVULGAÇÃO DE SEGREDO

O tipo descrito no artigo 153 do Código Penal, divulgação de segredo, expressa em seu § 1º-A que "divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública" [15]. Verifica-se que o tipo apresenta elementos de divulgação de caráter criminoso: a) divulgação de conteúdo de documento particular ou de correspondência confidencial; b) ausência de justa causa para essa divulgação; c) divulgação levada a efeito pelo destinatário ou detentor do documento particular ou de correspondência confidencial; d) potencialidade de dano a outrem.

Na visão de Anibal Bruno, a expressão caráter sigiloso, escrito é aquele que deva ser mantido secreto e possa servir de prova em fato de importância jurídica. Continua o autor lecionando que a correspondência deve ser confidencial, ter um conteúdo realmente secreto, devendo ser aquilo que se diz só para chegar ao conhecimento de determinada pessoa ou a limitado número de pessoas, a coisa deve ser mantida em sigilo, posto que isto corresponda à vontade e ao interesse legítimo de alguém[16].

Constata-se que, na mesma esteira, Bitencourt afirma que sigiloso

> é algo que não deve ser revelado, confidencial, limitado ao conhecimento restrito, não podendo sair da esfera de privacidade de quem o detém. Verifica-se, também, ser indispensável que a natureza

15 Conforme GRECO, Rogério. Código Penal comentado. 5. ed. Rio de Janeiro: Ímpetus, 2011, p. 405. No Direito Comparado há o art. 621 do Código Penal Italiano que pune os crimes contra a inviolabilidade dos segredos praticados através da informática, conforme ARDIZZONE, Salvatore. A legislação penal italiana em matéria de *computer* crimes entre direito e política criminal. Revista da Faculdade de Direito das Faculdades Metropolitanas Unidas. Série Internacional v.5, ano 10, n. 15, p.103-125, jan./jun. 1996.

16 BRUNO, Anibal. **Crimes contra pessoa**. 4. ed. Rio de Janeiro: Editora Rio, 1976, p. 407.

> sigilosa ou reservada das informações divulgadas indevidamente seja objeto de lei e lei em sentido estrito, sendo inadmissível sua equiparação a resoluções, portarias, regulamentos, entre outros.[17]

Observa-se que, em havendo justa causa na divulgação do segredo e estando o agente amparado por uma causa de justificação, conforme a descrita no artigo 24 do Código Penal, Estado de necessidade, fica imune o agente da conduta no tipo do artigo 153, § 1º-A do Código Penal.

O tipo descrito neste parágrafo é uma norma penal em branco, em função de que somente se configurará a modalidade qualificada se as informações, em tese, consideradas como sigilosas ou reservadas forem aquelas apontadas como tal pela lei, estejam elas contidas ou não nos sistemas de informação ou banco de dados da Administração Pública.

1.1.2 INSERÇÃO DE DADOS FALSOS EM SISTEMA DE INFORMAÇÕES

No capítulo relativo aos crimes contra a Administração Pública, o art. 313-A do Código Penal - Inserção de dados falsos em sistema de informações – prescreve o seguinte:

Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados[18] ou bancos de dados[19] da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.

---

17 BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. São Paulo: Saraiva, 2012. v. 2, p. 492.

18 Sistema informatizado é o conjunto de elementos, materiais ou não, coordenados entre si, que funcionam como uma estrutura organizada, tendo a finalidade de armazenar e transmitir dados, através de computadores, conforme descrição de NUCCI, Guilherme de Souza. **Código Penal comentado**. 5. ed. São Paulo: Editora Revista dos Tribunais, 2005, p. 982.

19 Banco de dados é aquele que pode ter como base arquivos, fichas e papéis não relacionados à informática.

Existe aqui uma forma de peculato eletrônico, criado pela Lei nº 9.983, de 14 de julho de 2000, na qual se apresenta em duas formas criminosas: a) o próprio funcionário autorizado é quem insere dados falsos, ou seja, é ele quem introduz, inclui, coloca ou venha a facilitar para que terceira pessoa leve a efeito de inserção; b) a segunda modalidade de comportamento previsto pelo tipo a conduta do funcionário autorizado é dirigida no sentido de alterar (mudar, modificar) ou excluir (remover, afastar, eliminar), indevidamente, dados verdadeiros. Este tipo é uma norma penal em branco, visto que a definição de funcionário público encontra-se descrita no artigo 327[20], do Código Penal. Observa-se que, se a inserção for procedida com fim eleitoral, poderá o tipo ser aquele descrito no art. 72 da Lei nº 9.504, de 30 de setembro de 1997, ou seja, Código Eleitoral[21].

No Direito Comparado, verifica-se estar previsto no artigo 8º - Burla Informática, da Convenção de Budapeste, o seguinte: "trata: a) da introdução, da alteração, da eliminação, ou da supressão de dados informáticos; b) de qualquer intervenção no funcionamento de um sistema informático com a intenção de obter um benefício econômico ilegítimo para si ou para terceiros". Tipo que se apresenta de forma similar ao descrito no Código Penal brasileiro, mas que se apresenta de forma mais ampla, pois tem aplicabilidade na União Europeia [22].

20 Art. 327 - Funcionário Público - Considera-se funcionário público, para os efeitos penais, quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública.
§ 1º - Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública.
§ 2º - A pena será aumentada da terça parte quando os autores dos crimes previstos neste Capítulo forem ocupantes de cargos em comissão ou de função de direção ou assessoramento de órgão da administração direta, sociedade de economia mista, empresa pública ou fundação instituída pelo poder público. Código Penal (Decreto-Lei nº 2.848, de 7 de dezembro de 1940). Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

21 Conforme GRECO, Rogério, *op. cit.*, p. 884.

22 Disponível em: <http://www.wirelessbrasil.org/wirelessbr/secoes/crimes_

1.1.3 MODIFICAÇÃO OU ALTERAÇÃO NÃO AUTORIZADA DE SISTEMAS DE INFORMAÇÃO

A modificação ou alteração não autorizada de sistemas de informações, descritas no artigo 313-B do Código Penal, aborda a hipótese de "modificar ou alterar, o funcionário, sistema de informações[23] ou programa de informática[24] sem autorização ou solicitação de autoridade competente" [25].

O tipo ora descrito não exige que o funcionário seja aquele autorizado na utilização do sistema de informação ou programa de informática, havendo simplesmente a exigência de que seja funcionário, consumando-se o tipo quando aquele funcionário que modifica ou altera o sistema ou programa não possuía a devida autorização. Este tipo também é uma norma penal em branco, visto que a definição de funcionário público encontra-se descrita no artigo 327, do Código Penal.

1.1.4 VIOLAÇÃO DE SIGILO FUNCIONAL

A violação de sigilo funcional, tipo do art. 325 do Código Penal, aborda a ação do servidor que fere o dispositivo específico

---

digitais/texto_convencao.pdf>. Acesso em: 27 dez. 2011.

23 Sistemas de informação são aqueles que manipulam informações se utilizando de banco de dados.

24 Programa de informática é o *software,* conforme o Manual Prático de Investigação de Crimes Cibernéticos do COMITÊ Gestor da Internet no Brasil, *op. cit.*

25 Conforme GRECO, Rogério, *op. cit.,* p. 405. No Direito Comparado, especificamente no art. 221 do Código Penal português, há um tipo similar que pune com pena de prisão de até três anos ou multa aquele que interferir no resultado de tratamento de dados ou mediante estruturação incorreta de programa de dados ou interferir de qualquer outro modo no processamento com a intenção de obter para si ou para outrem enriquecimento ilegítimo, causando prejuízo alheio. Ressalte-se que o tipo em comento não aplica especificamente a funcionário, conforme o art. 313-B do CPB. Assim como o tipo do Código Penal italiano que prevê em seu art. 640, a fraude informática consistente na alteração do funcionamento de um sistema telemático ou informático com o objetivo de obter proveito indevido para si ou para outrem.

aos sistemas de informação, conforme o assinalado em seu § 1º: "Nas mesmas penas deste artigo incorre quem: I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública"[26].

1.1.5 LEIS EXTRAVAGANTES

No ordenamento jurídico esparso, também, existem tipos cibernéticos que ensejaram a preocupação do legislador pátrio.

1.1.5.1 ESTATUTO DA CRIANÇA E DO ADOLESCENTE (ECA) – PORNOGRAFIA INFANTIL

Com a modificação implementada no art. 241[27] do Estatuto da Criança e do Adolescente, por força da Lei n° 10.764, de 12 de novembro de 2003, sobreveio a criminalização da pornografia infanto-juvenil praticada pela rede mundial de computadores, penalizando, também, aquele que assegura os meios ou serviços para armazenamento das fotografias, cenas ou imagens produzidas ou que assegure, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens de pedofilia[28].

---

26 Este tipo é uma norma penal em branco, visto que a definição de funcionário público encontra-se descrita no artigo 327, do Código Penal.

27 O art. 241 do ECA apresenta a seguinte redação : "Vender ou expor à venda fotografia, vídeo ou outro registro que tenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. Pena: reclusão, de 4 (quatro) a 8 (oito) anos e multa". Conforme o art. 2º, da Lei nº 8.069, de 13 de julho de 1990, ***criança*** para os efeitos desta Lei, a pessoa até 12 (doze) anos de idade incompletos, e ***adolescente*** aquele entre 12 (doze) e 18 (dezoito) anos de idade (grifos deste trabalho). Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em 2 jan. 2012.

28 Palavra de origem grega, pedofilia é a "qualidade ou sentimento de quem é pedófilo",

Existe substitutivo do Senador Eduardo Azeredo propondo a modificação do artigo 241 do Estatuto da Criança e do Adolescente, que teria a seguinte redação:

> Art. 20. O *caput* do art. 241 da Lei nº 8.069, de 13 de julho de 1990, passa a vigorar com a seguinte redação:
> "Art. 241. Apresentar, produzir, vender, receptar, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:
> ....." (NR)[29]

---

e este adjetivo designa a pessoa que "gosta de crianças". Qual seja: todo pai, toda mãe, e demais parentes que gostem de crianças são pedófilos, mas não são criminosos. Porém, o substantivo pedofilia e o adjetivo pedófilo, por uso irregular dos meios de comunicação, vêm se tornando costumeiros na acepção de infrações penais contra crianças, particularmente ligadas a questões de sexo e outros abusos nessa área. De tanto serem lidas, ouvidas e/ou assistidas nesse sentido, acabam tais palavras por serem assimiladas, pelas pessoas comuns, como verdadeiras. Fala-se de pedofilia como "crime" praticado por pedófilo, conforme MORAES, Bismael B. Pedofilia não é crime. **Boletim IBCCRIM**, São Paulo, v. 12, nº 143, p. 3, out. 2004.
O termo pedofilia possui variadas conotações, é bastante problemático e raramente usado com alguma consistência, a começar pela sua etimologia grega que o define como "o amor pelas crianças". O termo está também associado a caricaturas grosseiras, porém não há algo como um pedófilo típico. A Associação Americana de Psiquiatria define a pedofilia como: "fantasias sexuais intensas envolvendo atividade sexual com pré-adolescentes ou crianças, durante um período de ao menos seis meses". A Organização Mundial de Saúde diz que "são comportamentos sexuais que um adulto (acima de dezesseis anos), essencialmente do sexo masculino, tem em relação às crianças (menor de treze anos)". A definição clínica é bastante diferente da sua definição legal, a qual é, por sua vez, diferente da interpretação do público em geral. A pedofilia é o ato de "abusar" de crianças e adolescentes, os quais com o acesso de novas tecnologias e a internet tem vindo a crescer e a propagar-se via internet consequentemente devido à fiscalização ser ainda insuficiente. Assim tem existido a dificuldade de deter os infratores e vetar principalmente, o grande número de interessados neste assunto. É preciso que se conheça como acontece a pedofilia, qual o cenário atual e como ajudar no seu combate não só via internet, mas na nossa sociedade igualmente. **Disponível em: <**http://content.worldgroups.com/groups/Custom/P/PortugalCompanhiaOnline/naoapedofilia.htm**>. Acesso em: 30 dez. 2011.**

29 Este substitutivo foi aprovado em 18 de junho de 2008. Disponível em: <http://legis.senado.gov.br/mate-pdf/13674.pdf>. Acesso em: 2 jan. 2012.

O substitutivo ao projeto de lei acima referido tenta ampliar a forma de repressão àquele que se utiliza dessa forma criminosa para expor o menor, sendo viável toda a proposta que venha a inibir de forma eficaz esta prática criminosa tão revoltante.

A criminalização do acesso e do *download* de imagens contendo pornografia infanto-juvenil não se encontram configuradas como tipo penal, o que inibe a ação persecutória no que tange a determinados atos preparatórios, mas de outro lado quando o agente conclui o *download* ele transforma em posse, não havendo imediata destruição, concretiza-se o tipo descrito no art. 241-A do Estatuto da Criança e do Adolescente[30].

Existe reportagem da revista IstoÉ de outubro de 2004, cujo título é "Perigo Digital", na qual se traça o panorama da incidência da pedofilia na sociedade atual. A mesma reportagem alerta para o perigo que a internet se tornou para as crianças, pois os pedófilos ou predadores se utilizam de tal meio para saciar sua perversão, aproximando-se de crianças na rede mundial[31].

Ponto interessante é o processo de estabelecimento de confiança entre o pedófilo e a criança ou adolescente, chamado

30 Art. 241-A, do ECA: 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 explicito ou registro que contenha criança ou adolescente. Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.
Nada obsta que existam acessos por atos de imperícia ou imprudência, sem que daí se manifeste interesse em perpetuar a pornografia infantil, conforme descrito por VIDAL, Leila Quintanilha de Souza *et al*. **Cartilha da Divisão de Direitos Humanos**. Brasília: Departamento de Polícia Federal; ANP, 2009, p. 104.

31 RODRIGUES, Alan; SIMAS FILHO, Mario. Perigo Digital. **Revista IstoÉ**, Rio de Janeiro, n. 1829, p. 50-55, 27 out. 2004.

de *grooming*[32], não abrange o fato descrito no art. 241-D[33], do Estatuto da Criança e do Adolescente, visto que este se restringe especificamente à criança, assim aqueles com mais de doze anos de idade, os quais poderiam continuar sendo objeto de aliciamento por meio de programas de comunicação remota e redes sociais, sem que as autoridades responsáveis pela investigação possam tomar qualquer providência, salvo se a conduta também seja tipificada no Código Penal ou em legislação penal extravagante[34].

O termo "imagens contendo pornografia infanto-juvenil" pode ser entendido como sendo: desenhos, imagens realísticas (*morphing*[35]), montagens, utilização de maiores caracterizadas como menores.

Com a edição da Lei nº 11.829 de 25 de novembro de 2008 não havia definição específica para estes procedimentos,

32 Internet *grooming* é a expressão inglesa usada para definir genericamente o processo utilizado por predadores sexuais na internet e que vai do contato inicial à exploração sexual de crianças e jovens. Trata-se de um processo complexo, cuidadosamente individualizado, pacientemente desenvolvido através de contactos assíduos e regulares desenvolvidos ao longo do tempo e que pode envolver a lisonja, a simpatia, a oferta de presentes, dinheiro ou supostos trabalhos de modelo, mas também a chantagem e a intimidação. MORAIS, Tito de. *Grooming*: aliciamento e sedução de menores. Disponível em: <http://www.miudossegurosna.net/artigos/2007-03-29.html>. Acesso em: 30 dez. 2011.

33 Art. 241-D: Aliciar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso. Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

34 VIDAL, Leila Quintanilha de Souza, *op. cit.*, p. 105.

35 *Morphing* é um efeito especial em filmes e animações que muda (ou *morphs*) uma imagem para outra através de uma transição sem problemas. Na maioria das vezes ele é usado para descrever uma pessoa se transformar em outra através de meios tecnológicos ou como parte de uma fantasia ou uma sequência surreal.
As novas tecnologias modificaram a natureza da pornografia. Câmeras e filmadoras digitais tornaram a produção fácil e barata. Há menos risco de que outra pessoa descubra a operação, haja vista que não é necessário revelar as fotos, qual a fotografia convencional. A reprodução do material não acarreta perda de qualidade. A distribuição tornou-se fácil, barata e rápida com o advento da internet. Investigação e persecução penal tornaram-se mais difíceis, dado o caráter internacional da internet. Com o uso dos programas de computação gráfica é possível combinar duas

mas o art. 241-E do Estatuto da Criança e do Adolescente[36], que é uma norma explicativa, quando descreve "cena de sexo explícito ou pornografia", abrange quaisquer situações que venham a envolver criança ou adolescente em atividades sexuais específicas, tanto reais como simuladas.

Constata-se que ficam excluídos da tipificação legal os desenhos e imagens realísticas (*morphing*), assim como as simulações de *maiores* caracterizadas como menores, uma vez que não se enquadram no descrito no Estatuto da Criança e do Adolescente. Assim como as imagens sensuais de crianças, ainda que produzidas e utilizadas para fins especificamente sexuais, desde que não exibam os órgãos sexuais, não foram incluídas no conceito legal, abrindo-se um espaço para a atuação de pedófilos nessa seara. Quanto às montagens de fotografias de crianças em corpos de adultos encontram-se tipificadas, uma vez que um dos bens protegidos é a dignidade da pessoa humana[37]. (Grifo deste trabalho).

Abrindo um parêntese ao foco deste artigo, é salutar uma abordagem ao tema dignidade da pessoa humana apresentado em vários documentos do Direito Internacional. Quando se referem à dignidade, fazem uso de várias locuções, como no preâmbulo da Declaração Universal dos Direitos do Homem, de 10 de dezembro de 1948, alude-se à dignidade dos "membros da família humana"

---

imagens em uma, ou distorcê-las criando outra totalmente nova (*morphing*). Imagens reais não-pornográficas de crianças podem ser transformadas em pornográficas, e imagens pornográficas de "crianças virtuais" podem ser produzidas. Disponível em: <http://content.worldgroups.com/groups/Custom/P/PortugalCompanhiaOnline/naoapedofilia.htm**>. Acesso em: 30 dez. 2011.**

36 Art. 241-E – ECA: Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explicito ou pornografia" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais, explícitas, reais ou simuladas, ou exibição de órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais. Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

37 VIDAL, Leila Quintanilha de Souza *et al.*, *op. cit.*, p. 105.

e em seu primeiro artigo liga esta noção com os "seres humanos" [38]. Os preâmbulos de ambos os pactos internacionais dos direitos (civis, políticos, bem como econômicos, sociais e culturais) de 16 de dezembro de 1966, ao referir-se também aos integrantes da família humana, conectam a dignidade à "pessoa humana".

A Convenção Europeia para a Salvaguarda dos Direitos do Homem e das Liberdades Fundamentais, de 4 de novembro de 1950, não menciona a dignidade. Com ela se relacionam, porém, dois outros diplomas jurídicos regionais versando sobre o *status* pessoal: o art. 5º da Convenção Americana sobre os Direitos Humanos, de 4 de novembro de 1969, cita a dignidade da "pessoa humana"; o art. 5º da Carta Africana dos Direitos do Homem e dos Povos, de 28 de junho de 1981, articula a dignidade com o "ser humano"[39].

Complak cita Emmanuel Kant, quando este afirma ser a dignidade o valor de que se reveste tudo aquilo que não tem preço, ou seja, não é passível de substituição por equivalente. Entretanto, Complak discorda da afirmação kantiana, quando define a dignidade humana como algo privativo do ser humano: a dignidade é destinada exclusivamente ao indivíduo em particular representado pelo ser humano[40].

Sarlet entende por dignidade da pessoa humana o seguinte:

> [...] a qualidade intrínseca e distintiva de cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como

38 "Art. 1. Todos os seres humanos nascem livres e iguais em dignidade e direitos. Dotados de razão e consciência, devem agir uns para com os outros em espírito e fraternidade."

39 Conforme COMPLAK, Krystian. Cinco teses sobre a dignidade da pessoa humana como conceito jurídico. Disponível em: < http://www.estig.ipbeja.pt/~ac_direito/Complak.pdf>. Acesso em: 5 jan. 2012.

40 *Idem.*

> venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e co-responsável nos destinos da própria existência e da vida em comunhão com os demais seres humanos[41].

Tal definição encontra eco no tema em desenvolvimento, no entendimento de que o ser humano não pode padecer de um tratamento em desacordo com a dignidade da pessoa humana, mais especificamente nos tipos penais referenciados à pedofilia.

No Direito Comparado, especificamente na Convenção de Budapeste, em seu Titulo 3 – Infrações relacionadas com o conteúdo, e no artigo 9º – Infrações relacionadas com pornografia infantil, no qual considera como tal as seguintes condutas:

> (1): a) produzir pornografia infantil com o objetivo da sua difusão através de um sistema informático; b) oferecer ou disponibilizar pornografia infantil através de um sistema informático; c) difundir ou transmitir pornografia infantil através de um sistema informático; d) obter pornografia infantil através de um sistema informático para si ou para terceiros; e) possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos. (2) Para efeitos do número 1, a expressão "pornografia infantil" inclui qualquer material pornográfico que represente visualmente: a) um menor envolvido num comportamento sexualmente explícito; b) uma pessoa que aparente ser menor em um comportamento sexualmente explícito; c) imagens realísticas que representem um menor envolvido em um comportamento sexualmente explicito. (3) Para efeitos do número 2, a expressão "menor" inclui qualquer pessoa com idade inferior a 18 anos. Uma parte pode, no entanto, exigir um limite de idade inferior, que não será menor de 16 anos. (4) (Cada parte pode reservar-se o direito de não aplicar, no todo ou em parte, nos números 1, alínea d, e 2, alíneas b e c [42].

41 SARLET, Ingo Wolfgang. **O princípio da dignidade da pessoa humana e os direitos fundamentais**. 2. ed. Porto Alegre: Livraria do Advogado, 2002, p. 62.

42 Disponível em: < http://www.wirelessbrasil.org/wirelessbr/secoes/crimes_digitais/texto_convencao.pdf>. Acesso em: 27 dez. 2011.
Há, também, no Direito italiano com a Lei nº 547, de 23 de dezembro de 1993, a introdução de novas figuras em seu Código Penal, penalizando as condutas criminosas ligadas ao computador. Naquele diploma legal estão incriminadas as condutas de

Observa-se que a Convenção de Budapeste, apesar de apresentar-se de forma genérica, aparenta ter mais praticidade, pois fixa os limites de idade, que vão abranger tanto a criança como o adolescente, descritos no corpo da Convenção. Já no texto do Estatuto da Criança e do Adolescente, conforme descrito acima, o legislador não teve o cuidado de abordar casos específicos que poderiam ocorrer, tanto com a criança quanto com o adolescente, deixando uma brecha mediante a qual o pedófilo fica isento de pena (art. 241-D, do ECA).

1.1.5.2 CRIMES CONTRA A ORDEM TRIBUTÁRIA, ECONÔMICA E CONTRA AS RELAÇÕES DE CONSUMO

Na lei contra a ordem tributária verificamos a preocupação do legislador no sentido de punir a conduta de "utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública", mas dando uma sanção considerada de menor potencial ofensivo[43].

---

danos de sistemas informáticos e telemáticos (destruição, deterioração, que torne inutilizável, total ou parcialmente sistemas informáticos ou telemáticos alheios; atentados a equipamentos de utilidade pública; alteração, falsificação ou supressão do conteúdo de comunicações informáticas ou telemáticas; difusão de programas que visem a danificar ou interromper o funcionamento de um sistema informático), conforme ARDIZZONE, Salvatore, *op. cit*.

43 Lei n° 8.137, de 27 de dezembro de 1990. Art. 2°: Constitui crime da mesma natureza (vide Lei nº 9.964, de 10 de abril de 2000):
I - fazer declaração falsa ou omitir declaração sobre rendas, bens ou fatos, ou empregar outra fraude, para eximir-se, total ou parcialmente, de pagamento de tributo;
II - deixar de recolher, no prazo legal, valor de tributo ou de contribuição social, descontado ou cobrado, na qualidade de sujeito passivo de obrigação e que deveria recolher aos cofres públicos;
III - exigir, pagar ou receber, para si ou para o contribuinte beneficiário, qualquer percentagem sobre a parcela dedutível ou deduzida de imposto ou de contribuição como incentivo fiscal;

1.1.5.3 LEI DE INTERCEPTAÇÃO DE COMUNICAÇÕES TELEFÔNICAS

Conforme disposição legal da lei de interceptação de comunicações telefônicas, será punida a interceptação de informática, sendo tal conduta punida com pena de reclusão devido à sua gravidade, visto que o bem tutelado é esta inviolabilidade[44].

1.1.5.4 CÓDIGO ELEITORAL

O artigo 72 da Lei eleitoral apresenta três verbos: obter, desenvolver e causar, sendo que estão ligados em sequência às ações executadas pelo autor da infração penal, posto que primeiramente ele obtém o acesso com o fim de alterar a apuração ou a contagem de votos e, atingindo este objetivo, estará incurso no inciso I do artigo em comento. Caso obtenha acesso, mas, em vez de executar a ação descrita no inciso I, venha a "desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral", responderá pelo inciso II. Por último, se vier a causar dano (...) na totalização

---

IV - deixar de aplicar, ou aplicar em desacordo com o estatuído, incentivo fiscal ou parcelas de imposto liberadas por órgão ou entidade de desenvolvimento;
V – **utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública**. (Grifo deste trabalho).
Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa. Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

44 Lei nº 9.296, de 24 de julho de 1996. Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa. Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

de votos ou a suas partes, responderá pelo contido no inciso III, sendo certo que os tipos aqui descritos são punidos a título de dolo.[45]

1.1.5.5 LEI DE PROPRIEDADE INTELECTUAL DE PROGRAMA DE COMPUTADOR

A Lei de propriedade intelectual de programa de computador traz em seu artigo 12 o preceito que inibe a violação de direitos de autor de programa de computador, sendo punido com uma pena de menor potencial ofensivo. Ressalvado que, se a violação consistir em reproduzir, por qualquer meio, de programa de computador, para fins de comércio, a pena torna-se de reclusão de um a quatro anos, conforme seu parágrafo primeiro e, em seu parágrafo segundo, está previsto que aquele que vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador produzido com violação de direito autoral, responderá tendo a mesma pena do parágrafo anterior.[46]

---

45 Lei nº 9.504, de 30 de setembro de 1997. Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:
I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;
II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;
III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes. Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

46 Lei nº 9.609, de 19 de fevereiro de 1998. Art. 12. Violar direitos de autor de programa de computador:
Pena - Detenção de seis meses a dois anos ou multa.
§ 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
Pena - Reclusão de um a quatro anos e multa.
§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda,

Nos crimes previstos neste artigo, somente se procede mediante queixa, ressalvado se os lesados forem entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público, conforme inciso I, do parágrafo terceiro; e quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo, conforme inciso II do mesmo parágrafo.

1.1.6 SUBSUNÇÃO DE CONDUTAS CRIMINAIS

No panorama nacional, existem tipos penais com a possibilidade de subsunção de condutas criminais realizadas via internet, contidas no Código Penal e leis extravagantes, tais como: o *cracker*[47], que pode estar incurso no crime de dano, descrito no art. 163 do Código Penal; a prática ou incitação do

introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
§ 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.
§ 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação. Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

47 *Hackers* e *crackers* possuem conhecimentos que podem ser usados legalmente ou ilegalmente, porém trabalham de forma diferente. O *hacker* invade, se aproveita de vulnerabilidades para ter acesso a uma determinada estação de trabalho ou rede. Já o *cracker* modifica, altera as propriedades de um *software* ou sistema para obter outro comportamento do "programa". *Cracker* é o termo usado para designar quem pratica a quebra (ou *cracking*) de um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 por *hackers* em defesa contra o uso jornalístico do termo *hacker*. O uso deste termo reflete a forte revolta dos *hackers* contra o roubo e vandalismo praticado pelo *cracking*. Disponível em: < http://www.hardware.com.br/termos/cracker>. Acesso em: 30 dez. 2011.

racismo é reprimida pelo art. 20, *caput*, e § 2°, descritos na Lei n° 7.716, de 5 de janeiro de 1989[48]; o *phishing scam* subsume-se perfeitamente ao delito de furto.

1.1.6.1 CRIME DE DANO

Com o advento do substitutivo ao PLS nº 76/2000 foi proposta a inserção do artigo 163-A, ao Código Penal, com a seguinte redação:

> **Dano por difusão de código malicioso eletrônico ou digital ou similar**
> Art. 163-A. Criar, inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.
> Pena: reclusão, de 1 (um) a 3 (três) anos, e multa[49].

Contudo, quando da passagem pelo Senado, houve alteração do texto fazendo-se inserir ao texto do artigo 163 do Código Penal[50] a expressão "ou dado eletrônico alheio", ficando assim constituído:

---

48 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.
§ 2º Se qualquer dos crimes previstos no caput ***é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza*** (grifos deste trabalho):
Pena: reclusão de dois a cinco anos e multa. Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

49 Substitutivo (ao PLS n° 76/2000, PLS n° 137/2000 e PLC n° 89/2003). Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), fica acrescido do art. 163-A. Disponível em: <http://andreum.blog.br/pt/wp-content/uploads/2007/12/substitutivo_cct.pdf>. Acesso em: 2 jan. 2012.

50 **Art. 163** - Destruir, inutilizar ou deteriorar coisa alheia:
Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.
Dano qualificado
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:

> Art. 4º O *caput* do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:
> **"Dano**
> Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio[51]:
> ....."(NR)

O mesmo dispositivo também propôs a inserção ao Código Penal do artigo 163-A, com a seguinte redação:

> Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:
>
> **Inserção ou difusão de código malicioso**
> Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> **Inserção ou difusão de código malicioso seguido de dano**
> **§ 1º** Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> **§ 2º** Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte[52].

Pena - detenção, de 6 (seis) meses a 3 (três) anos, e multa, além da pena correspondente à violência. Código Penal (Decreto-Lei nº 2.848, de 7 de dezembro de 1940). Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

51 Este substitutivo foi aprovado em 18 de julho de 2008. Disponível em: <http://legis.senado.gov.br/mate-pdf/13674.pdf>. Acesso em: 2 jan. 2012.

52 No mesmo substitutivo aprovado, houve a apresentação de proposta de modificação e inserção de artigo no Código Penal Militar, conforme segue: Art. 11. O *caput* do art. 259 e o *caput* do art. 262 do Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:
"**Dano Simples**
Art. 259. Destruir, inutilizar, deteriorar ou fazer desaparecer coisa alheia ou dado eletrônico alheio, desde que este esteja sob administração militar:

Considerando que a proposta inicial do crime *dano por difusão de código malicioso eletrônico ou digital ou similar,* art. 163-A, em comento, tratava de três formas de atuação do agente (criar, inserir ou difundir), em que, para sua consumação, deva ter ocorrido o dano em dispositivo de comunicação, rede de computadores, ou sistema informatizado, caso contrário, o fato será atípico. Na nova proposta, aprovada em 18 de julho de 2008, somente foram aproveitados os dois últimos verbos, sendo que o conteúdo permaneceu similar. (Grifos deste trabalho).

A redação proposta neste substitutivo aprovado ao *status* de projeto de lei vem fornecer, mesmo que de forma singela, uma adequação à realidade do mundo atual, atendendo a proposta na Convenção de Budapeste, que *trata das fraudes em sistemas informatizados com ou sem ganho econômico*, mesmo o Brasil não sendo signatário da mesma, constata-se uma evolução que poderá alcançar determinadas condutas antes consideradas atípicas (grifos deste trabalho). Neste substitutivo aprovado pelo Senado, existe uma norma explicativa, contida no artigo 16, na qual são definidos os termos: dispositivo de comunicação, sistema informatizado, rede de computadores, código malicioso e dados informáticos, conforme transcrito a seguir:

> Art. 16. Para os efeitos penais considera-se, dentre outros:
> I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;
> II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

....." (NR)
"**Dano em material ou aparelhamento de guerra ou dado eletrônico**
Art. 262. Praticar dano em material ou aparelhamento de guerra ou dado eletrônico de utilidade militar, ainda que em construção ou fabricação, ou em efeitos recolhidos a depósito, pertencentes ou não às forças armadas:
....." (NR)
Este substitutivo foi aprovado em 18 de julho de 2008. Disponível em: <http://legis.senado.gov.br/mate-pdf/13674.pdf>. Acesso em: 2 jan. 2012.

> III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;
> IV – código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;
> V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado[53].

53 Disponível em: <http://legis.senado.gov.br/mate-pdf/13674.pdf>. Acesso em: 2 jan. 2012.
Anteriormente, no substitutivo apresentado pelo Senador Eduardo Azeredo, esta norma explicativa estava inserida no artigo 154-C para, caso aprovada, ser adicionada ao Código Penal, conforme anexo:
Dispositivo de comunicação, sistema informatizado, rede de computadores e defesa digital
Art. 154-C. **Para os efeitos penais considera-se:**
I – dispositivo de comunicação: o computador, o telefone celular, o processador de dados, os instrumentos de armazenamento de dados eletrônicos ou digitais ou similares, os instrumentos de captura de dados, os receptores e os conversores de sinais de rádio ou televisão digital ou qualquer outro meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar;
II – sistema informatizado: o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;
III – rede de computadores: os instrumentos físicos e lógicos através dos quais é possível trocar dados e informações, compartilhar recursos, entre máquinas, representada pelo conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem de comum acordo a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial;
IV - código malicioso: o conjunto de instruções e tabelas de informações ou programa de computador ou qualquer outro sistema capaz de executar uma sequência de operações que resultem em ação de dano ou de obtenção indevida de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal. Substitutivo (ao PLS n° 76/2000, PLS n° 137/2000 e PLC n° 89/2003). Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A. Disponível em: <http://andreum.blog.br/pt/wp-content/uploads/2007/12/substitutivo_cct.pdf>. Acesso em: 2 jan. 2012.

A proposta apresentada no projeto de lei encontra-se quase que idêntica a contida na Convenção de Budapeste, que fornece, também, uma norma explicativa, conforme segue:

Artigo 1º - Definições:

> Para fins da presente Convenção:
> a) Sistema informático: significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados;
> b) Dados informáticos: significa qualquer representação de fatos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático.

1.1.6.2 FRAUDE ELETRÔNICA: ESTELIONATO E FURTO

Tratando-se o *phishing* de uma fraude eletrônica, através do qual o agente obtém informações da vítima, senhas e dados pessoais, levando-a a erro, fazendo-se passar por terceiro, como por um banco ou um estabelecimento comercial ou levando o lesado a confiar em arquivos informáticos infectados por *softwares* daninhos, que capturam ou copiam dados. Verifica-se que o objetivo do agente é a obtenção de vantagem patrimonial ilícita.

O tipo descrito no artigo 171 do Código Penal – Estelionato[54]: "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". Neste caso o artifício e o ardil encontram-se circunscritos ao

54 Palavra originária de *stellio*, que significa camaleão, justamente pela qualidade que tem esse animal para mudar de cor, confundindo sua presa, facilitando, assim o bote fatal, bem como para poder fugir, também, dos seus predadores, que não conseguem, em facilidades mutacionais, perceber a sua presença, tal como ocorre com o estelionatário que, em razão de seus disfarces, engana a vítima com sua fraude, que visa à obtenção de êxito em sua ação criminosa, conforme GRECO, Rogério, *op. cit.*, p. 515.

gênero da fraude, ou seja, o engodo, o engano, a artimanha do agente, no sentido de fazer com que o lesado incorra em erro e ali, por vezes, permanecendo. De outra monta, a conduta em que o agente se utilizando de meios ardilosos, insidiosos, fazendo com que o lesado incorra, ou seja, mantida em erro, a fim de que o próprio agente pratique a subtração, está situada no disposto no artigo 155, § 4º, inciso II, segunda figura (fraude), do Código Penal, que é utilizada pelo agente, a fim de facilitar a subtração por ele levada a efeito[55].

Já considerava Nelson Hungria que o "meio fraudulento é também, qualquer ardil no sentido de provocar a ausência momentânea do *dominus* ou distraindo-lhe a atenção, para mais fácil proceder a perpetração do furto"[56]. Ante ao aludido, constata-se que, no estelionato, o agente mantém o lesado em erro, fazendo com que este lhe entregue o bem; enquanto no furto, mediante fraude, verifica-se que o agente leva o lesado a incorrer em erro, a fim de o próprio agente praticar a subtração. Tal posicionamento é compartilhado pelo Superior Tribunal de Justiça (STJ) que, ao examinar em um processo a questão da cópia de senhas bancárias para a obtenção de vantagem patrimonial ilícita, entendeu que esta conduta caracteriza crime de furto qualificado pela fraude, previsto no art. 155, § 4º, inciso II, segunda figura do Código Penal, afastando o enquadramento no art. 171 do Código Penal, pelo delito de estelionato[57].

55 Conforme GRECO, Rogério, *op. cit.*, p. 419.

56 HUNGRIA, Nelson. **Comentários ao Código Penal**, Rio de Janeiro: Forense, 1956. v. 7, p. 44.

57 A questão foi decidida no conflito negativo de competência 67.343/GO, o que por si só revela que a falta de dispositivos penais, mesmo nos casos de crimes informáticos impróprios, realmente pode tumultuar a persecução criminal. Destaca-se: "Conflito negativo de competência. Penal e processo penal. Fraude eletrônica na Internet. Transferência de numerário de conta da Caixa Econômica Federal. Furto mediante fraude que não se confunde com estelionato" (CC 67343/GO, rel. ministra Laurita Vaz, 3ª Seção, j. 28.03.2007).
Em outro exemplo, surge o entendimento do Tribunal do Estado de Minas Gerais ao julgar um caso de estelionato praticado pela internet, em que a vítima foi induzida a

No substitutivo ao PLS n° 76/2000 verifica-se a existência do art. 171-A, com a seguinte redação:

> **Difusão de código malicioso**
> Art. 171-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por qualquer forma indevida, induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, à rede de computadores, dispositivo de comunicação ou a sistema informatizado, com obtenção de vantagem ilícita, em prejuízo alheio:
> Pena – reclusão, de um a três anos.
> § 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de difusão de código malicioso[58].

Existe projeto de lei que pretende tipificar o furto eletrônico, sendo que uma das versões do substitutivo ao PLS n° 76/2000 apresentava o furto eletrônico com a seguinte redação:

> Art. 155. .
> § 4º .....
> V - mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra

---

erro, caindo no golpe do estelionatário, que acabou sendo condenado em 1ª Instância, porém recorreu ao Tribunal por meio da apelação criminal nº 1.0024.02.875258-2/001/BH, cujo relator foi o desembargador William Silvestrini, o que demonstra que os julgadores não têm encontrado dificuldades em decidir os casos que envolvem o estelionato cometido por meio da internet, conforme descrito em seguida: Tratando-se de estelionato cometido via internet, provado o uso de *home page* grátis com o nome de fantasia de determinada empresa, sem a sua autorização, induzindo pessoas em erro, mediante falsa promessa de emprego no exterior, com a indicação, inclusive por *e-mail* enviado a terceiro, de conta bancária da titularidade do agente, em cujo nome restou provada a efetivação de depósito pela vítima, deve ser mantida a condenação aplicada em 1ª instância. ACR nº 1.0024.02.875258-2/001/ BH – BELO HORIZONTE. APELAÇÃO CRIMINAL. Relator: Des. WILLIAM SILVESTRINI. Julgamento: 07/03/2007. Órgão Julgador: Quarta Câmara. DJ 21/03/2007.

58 Substitutivo (ao PLS n° 76/2000, PLS n° 137/2000 e PLC n° 89/2003). **Art. 6º** O Capitulo VI do Título II do Código Penal passa a vigorar acrescido do seguinte artigo, conforme, Disponível em: <http://andreum.blog.br/pt/wp-content/uploads/2007/12/substitutivo_cct.pdf>. Acesso em: 2 jan. 2012.

> rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares"[59].

Após a apresentação do substitutivo acima descrito, o aprovado em julho de 2008 abandonou o tratamento do furto eletrônico (art. 155 § 5º, V do CP) e do crime de estelionato eletrônico (art. 171-A do CP, com o nome de "difusão de código malicioso"). Agora, conforme o substitutivo, o estelionato informático (*phishing)* será tipificado no inciso VII do § 2º do art. 171 do CP[60], e não se cuidará do furto eletrônico, crime informático impróprio perfeitamente compatível aos esquemas típicos das formas qualificadas de furto, seja com fraude ou mediante destreza[61].

---

59 Substitutivo (ao PLS n° 76/2000, PLS n° 137/2000 e PLC n° 89/2003). **Art. 4º** O § 4º do art. 155 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).
Aproveitou-se neste substitutivo para produzir alteração no Código Penal Militar, fazendo uma inserção em seu artigo 240, que trata do furto, conforme segue: Art. 11. O § 6º do art. 240 do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar acrescido do seguinte inciso V:
Art. 240.
Furto qualificado
§ 6º
V – mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra rede de computadores, dispositivos de comunicação ou sistema. Disponível em: <http://andreum.blog.br/pt/wp-content/uploads/2007/12/substitutivo_cct.pdf>. Acesso em: 2 jan. 2012.

60 Substitutivo aprovado pelo Senador Eduardo Azeredo:
Art. 6º O art. 171 do Código Penal passa a vigorar acrescido dos seguintes dispositivos:
Art. 171
§ 2º Nas mesmas penas incorre quem:
Estelionato Eletrônico
VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado:
§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime do inciso VII do § 2º deste artigo, a pena é aumentada de sexta parte.
Este substitutivo foi aprovado em 18 de julho de 2008. Disponível em: <http://legis.senado.gov.br/mate-pdf/13674.pdf>. Acesso em: 2 jan. 2012.

61 Conforme ARAS, Vladimir. Crimes de informática: uma nova criminalidade. **Jus Navigandi**, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus2.uol.com.

Por outro lado, colocou-se o crime de estelionato com *phishing* no lugar devido, o que permitiu adequar sua pena ao padrão normativo do Código Penal, já que na proposta anterior a sanção era de um a três anos. Assim, procedeu com maior tecnicidade o legislador, ao manter a estrutura do estelionato simples, prevendo no inciso VII do § 2º do art. 171, do Código Penal, outro meio fraudulento de obtenção de vantagem ilícita, em prejuízo alheio, tendo como agente quem "difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado", sendo este o estelionato eletrônico[62].

1.1.6.3 PLÁGIO PRODUZIDO VIA INTERNET

No Direito brasileiro, tanto na Lei nº 9.610, de 19 de fevereiro de 1998[63], assim como no art. 184 do Código Penal, ainda não abordam de forma clara, específica, a figura do plágio via internet, necessitando a intervenção do legislador pátrio para sanar esta falha e acompanhar o desenvolvimento tecnológico,

br/doutrina/texto.asp?id=2250>. Acesso em: 29 dez. 2011.

62 Conforme ARAS, Vladimir, *op. cit.*

63 A criação intelectual, da qual nasce a obra audiovisual, é tutelada pelos direitos autorais através da Lei nº 9610/1998, sendo que internacionalmente, é regida pela Convenção de Berna, em seu Artigo 25, alínea 1, 3 e 6. A Convenção Universal que foi internalizada pelo Decreto nº 76.905, de 24 de dezembro de 1975, em seu artigo III, também dispõe sobre a tutela, não o gênero audiovisual, mas à espécie de obra cinematográfica.
A obra audiovisual submete-se a um dos dois sistemas de proteção aos direitos autorais. O sistema anglo-saxônico, denominado *copyright* (em 1710, surge na Inglaterra a primeira Lei a reconhecer o direito exclusivo dos autores a imprimir ou dispor de cópias de qualquer livro seu. A Lei reconhecia o direito dos autores e de seus cessionários sobre qualquer obra, durante 14 anos a contar a data da primeira publicação, prorrogável por mais 14 anos, se o autor ainda estivesse vivo. Esta Lei era intitulada de C*opyright Act*, e foi instituída pela rainha Ana em proteção as obras literárias, conforme COSTA NETO, José Carlos. **Direito Autoral no Brasil**. São Paulo: FTD,1998, p. 247) e o sistema francês, denominado *droit d'auteur*, este último norteia o Direito brasileiro.

sendo que este último trata dos crimes contra propriedade intelectual.

No tipo sob comento não se permite a aplicação do princípio da insignificância, em face de o bem tutelado ser a propriedade intelectual dos artistas[64]. Convém lembrar que a Lei de Direito Autoral[65] não considera como conduta ilícita aquela em que a pessoa atua em conformidade com o especificado no art. 46:

> Art. 46. Não constitui ofensa aos direitos autorais:
> I - a reprodução:
> a) na imprensa diária ou periódica, de notícia ou de artigo informativo, publicado em diários ou periódicos, com a menção do nome do autor, se assinados, e da publicação de onde foram transcritos;
> b) em diários ou periódicos, de discursos pronunciados em reuniões públicas de qualquer natureza;
> c) de retratos, ou de outra forma de representação da imagem, feitos sob encomenda, quando realizada pelo proprietário do objeto encomendado, não havendo a oposição da pessoa neles representada ou de seus herdeiros;
> d) de obras literárias, artísticas ou científicas, para uso exclusivo de deficientes visuais, sempre que a reprodução, sem fins comerciais, seja feita mediante o sistema Braille ou outro procedimento em qualquer suporte para esses destinatários;
> II - a reprodução, em um só exemplar de pequenos trechos, para uso privado do copista, desde que feita por este, sem intuito de lucro;
> III - a citação em livros, jornais, revistas ou qualquer outro meio de comunicação, de passagens de qualquer obra, para fins de estudo, crítica ou polêmica, na medida justificada para o fim a atingir,

64 O crime de violação de direito autoral não permite a aplicação do princípio da insignificância, tendo em vista que tutela a propriedade intelectual dos artistas. A prática delitiva não se mostra justificada, tampouco como a única forma alternativa de reverter sua situação financeira, restando inaplicável a excludente da ilicitude do estado de necessidade. Conforme TRF 4ª Região, ACr 2007.70.08.000211-8, PR, 8ª T, Rel. Juiz Fed. Sebastião Ogê Muniz, j. 04/08/ 2010, DEJF 18/8/2010, p. 633.

65 Art. 3º - Os direitos autorais reputam-se, para os efeitos legais, bens móveis, Lei nº 9.610, de 19 de fevereiro de 1998. Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

> indicando-se o nome do autor e a origem da obra;
> IV - o apanhado de lições em estabelecimentos de ensino por aqueles a quem elas se dirigem, vedada sua publicação, integral ou parcial, sem autorização prévia e expressa de quem as ministrou;
> V - a utilização de obras literárias, artísticas ou científicas, fonogramas e transmissão de rádio e televisão em estabelecimentos comerciais, exclusivamente para demonstração à clientela, desde que esses estabelecimentos comercializem os suportes ou equipamentos que permitam a sua utilização;
> VI - a representação teatral e a execução musical, quando realizadas no recesso familiar ou, para fins exclusivamente didáticos, nos estabelecimentos de ensino, não havendo em qualquer caso intuito de lucro;
> VII - a utilização de obras literárias, artísticas ou científicas para produzir prova judiciária ou administrativa;
> VIII - a reprodução, em quaisquer obras, de pequenos trechos de obras preexistentes, de qualquer natureza, ou de obra integral, quando de artes plásticas, sempre que a reprodução em si não seja o objetivo principal da obra nova e que não prejudique a exploração normal da obra reproduzida nem cause um prejuízo injustificado aos legítimos interesses dos autores[66].

Assim como as paráfrases e paródias que não forem verdadeiras reproduções da obra original, conforme mencionado no artigo 47 da Lei n° 9.610, de 19 de fevereiro de 1998: "Art. 47. São livres as paráfrases e paródias que não forem verdadeiras reproduções da obra originária nem lhe implicarem descrédito" [67].

De outro modo, a Convenção de Budapeste apresenta dispositivo legal que inibe a violação de direito autoral, via internet, conforme a seguir descrito:

> Art. 10 - Infrações relacionadas com a violação do direito do autor e direitos conexos.
> 1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer como infração penal, em conformidade com seu direito interno, a violação do direito do autor definido pela

66 Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

67 *Idem*.

> legislação desta Parte, em conformidade com as obrigações que a mesma assumiu em aplicação a Convenção Universal sobre o Direito do Autor, revista em Paris, em 24 de julho de 1971, da Convenção de Berna para a Proteção das Obras Literárias e Artísticas, do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual relacionadas ao Comércio, e do Tratado da OMPI sobre o direito do Autor, com exceção a quaisquer direitos morais conferidos por essas Convenções, quando estes atos forem praticados intencionalmente, a uma escala comercial e *por meio de sistema informático*.
> 2. Cada Parte adotará as medidas e outras que se revelem necessárias para estabelecer a infração penal, em conformidade com o seu direito interno, a violação dos direitos conexos definidos pela legislação dessa Parte, em conformidade com as obrigações assumidas, por força da Convenção Internacional para proteção dos artistas interpretes ou executantes, dos produtos dos fonogramas ou e dos organismos de radiodifusão (Convenção de Roma) do Acordo sobre Aspectos dos Direitos de Propriedade Intelectual relacionados com o Comércio, e do Tratado da OMPI sobre interpretações, execuções e fonogramas, com exceção de qualquer direito moral conferido por essas Convenções, quando esses atos forem praticados intencionalmente, a uma escala comercial e a um sistema informático.
> 3. Uma Parte, em circunstâncias bem delimitas, reserva-se o direito de não determinar a responsabilidade penal nos termos do n.ºs 1 e 2 do presente artigo, na condição de estarem disponíveis outros meios eficazes e essa reserva não prejudique as obrigações internacionais que incumbem a essa Parte, em aplicação dos instrumentos internacionais mencionados nos n.ºs 1 e 2 do presente artigo. (Grifos deste trabalho)

Tal processo evolutivo jurídico deveria ser adotado na legislação nacional, visto que a cada dia se torna mais rotineira a utilização das redes de computadores para estudos, pesquisas e aprimoramento de conhecimento, mas também, conforme referido anteriormente, para prática criminosa, devendo o Estado, na sua atividade preventiva, providenciar meios para que tais atos criminosos não venham a ocorrer e a causar prejuízo a uma parcela considerável da sociedade[68].

68 Em janeiro de 2012 tivemos conhecimento de que foi fechado, por violar direito

CONSIDERAÇÕES FINAIS

Desde o planejamento até a elaboração da Convenção de Budapeste, transcorreram aproximadamente cinco anos, sendo que, no ordenamento pátrio, o projeto de lei que trata dos crimes cibernéticos está sem definição há mais de uma década, levando à instabilidade no meio social. Por isso, verifica-se cotidianamente a invasão de sistemas informatizados, práticas criminosas, sem existir uma lei clara e precisa para inibir e punir aqueles que se utilizam de seus conhecimentos de informática para ações criminosas, no sentido de causar prejuízo a milhares de pessoas.

No Direito Internacional, existe o Direito Internacional Uniforme, sendo uma de suas subdivisões o Direito Uniforme espontâneo, que ocorre quando coincidem os direitos primários de dois ou mais ordenamentos, seja natural e casualmente, seja porque têm a mesma origem, ou porque sofreram influências idênticas, ou, ainda, quando países adotam sistemas jurídicos clássicos total ou parcialmente, de outros Estados. Quase todos os países do mundo se utilizam deste Direito. No caso em comento, o Brasil poderia aderir ou adotar a Convenção de Budapeste, haja vista que, nos projetos de leis anteriormente referidos, se encontra uma similitude entre os projetos apresentados e o conteúdo da Convenção.

O objetivo primário é a repressão dos crimes cibernéticos com a utilização de normas eficientes e práticas, mediante as quais a sociedade se sinta segura para se desenvolver, sem a interferência daqueles que procuram por meios escusos conseguir lucros, mesmo que causem prejuízos monetários e danos morais a terceiros.

---

autoral, o *site megaupload*, nos Estados Unidos da América. O Google lançou uma nova política de privacidade que entrou em vigor no dia 1º de março de 2012, sendo certo que outros sites também adotaram idêntico procedimento, conforme descrito nos Termos de Serviço em http://www.google.com/policies.

REFERÊNCIAS

ARAS, Vladimir. Crimes de informática: uma nova criminalidade. **Jus Navigandi**, Teresina, ano 5, nº 51, out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2250>. Acesso em: 29 dez. 2011.

ARDIZZONE, Salvatore. A legislação penal italiana em matéria de *computer* crimes entre direito e política criminal. **Revista da Faculdade de Direito das Faculdades Metropolitanas Unidas**. São Paulo, série internacional v. 5, ano 10, n. 15, p.103-125, jan./jun. 1996.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. São Paulo: Saraiva, 2012. v. 2.

BRASIL. Presidência da República. Lei n° 9.610, de 19 de fevereiro de 1998. Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

_____. Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em: <http://www2.planalto.gov.br/presidencia/legislacao>. Acesso em: 2 jan. 2012.

BRUNO, Anibal. **Crimes contra pessoa**. 4. ed. Rio de Janeiro: Editora Rio, 1976.

CASTELLS, Manuel. **Fim do milênio**. 4. ed. Tradução de Klaus Brandini Gerhardt; Roneide Venancio Majer. São Paulo: Paz e Terra, 2007.

COMITÊ Gestor da Internet no Brasil. **Manual prático de investigação de crimes cibernéticos**. São Paulo, 2006. Disponível em: <http://www.prsp.mpf.gov.br.html>. Acesso em: 26 dez. 2011.

COMPLAK, Krystian. Cinco teses sobre a dignidade da pessoa humana como conceito jurídico. Disponível em: < http://www.estig.ipbeja.pt/~ac_direito/Complak.pdf>. Acesso em: 5 jan. 2012.

CONVENÇÃO de Budapeste. Disponível em: <http://www.charlieoscartango.com.br/.../A%20convencao%20de%20**Budapeste**%20e%20as%20**leis**%20bra...>. *Acesso em: 29 dez. 2011.*

CONVENTIONS. Disponível em:< http://conventions.coe.int>. Acesso em: 3 jan. 2012.

COSTA NETO, José Carlos. **Direito Autoral no Brasil**. São Paulo: FTD, 1998.

EBAH. Crimes cibernéticos. Disponível em: <html://www.ebah.com.br/content/ABAAABQKAI/crimes-ciberneticos-dep-federal-julio-semeghini.hml>. Acesso em: 26 dez. 2011.

GRECO, Rogério. **Código Penal comentado**. 5. ed. Rio de Janeiro: Impetus, 2011.

HARDWARE. Disponível em: <http://www.hardware.com.br/termos/cracker>. Acesso em: 30 dez. 2011.

HUNGRIA, Nelson. **Comentários ao Código Penal**. Rio de Janeiro: Forense, 1956. v. 7.

LEGIS. Projeto de Lei PLS n° 76/2000. Disponível em: <http://legis.senado.gov.br/mate-pdf/13674.pdf>. Acesso em: 2 jan. 2012.

MEDEIROS, Assis. **Hackers:** entre a ética e a criminalização. Florianópolis: Visual Books, 2002.

MORAES, Bismael B. Pedofilia não é crime. **Boletim IBCCRIM**, São Paulo, v. 12, n. 143, p. 3-8, out. 2004.

MORAIS, Tito de. *Grooming*: aliciamento e sedução de menores. Disponível em: <http://www.miudossegurosna.net/artigos/2007-03-29.html>. Acesso em: 30 dez. 2011.

NUCCI, Guilherme de Souza. **Código Penal comentado**. 5. ed. São Paulo: Editora Revista dos Tribunais, 2005.

RODRIGUES, Alan; SIMAS FILHO, Mario. Perigo Digital. **Revista IstoÉ**, Rio de Janeiro, nº 182.927, p. 50-55, out. 2004.

ROSA, Fabrízio. **Crimes de informática**. 3. ed. Campinas: Bookseller, 2007.

SAFERNET Brasil. Disponível em: <http://www.safernet.org.br/site/indicadores>. Acesso em: 2 jan. 2012.

SARLET, Ingo Wolfgang. **O princípio da dignidade da pessoa humana e os direitos fundamentais**. 2. ed. Porto Alegre: Livraria do Advogado, 2002.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilas. A Convenção de Budapeste e as leis brasileiras. Disponível em: <http://www.charlieoscartango.com.br/.../A%20convencao%20de%20**Budapeste**%20e%20as%20**leis**%20bra...>. *Acesso em: 29 dez. 2011.*

SUBSTITUTIVO ao PLS n° 76/2000, PLS n°137/2000 e n° PLC 89/2003. Disponível em: <http://andreum.blog.br/pt/wp-content/uploads/2007/12/substitutivo_cct.pdf>. Acesso em: 2 jan. 2012.

VIDAL, Leila Quintanilha de Souza *et al*. **Cartilha da Divisão de Direitos Humanos.** Brasília: Departamento de Polícia Federal; ANP, 2009.

WIRELESSBRASIL. Crimes Digitais. Disponível em: <http://www.wirelessbrasil.org/wirelessbr/secoes/crimes_digitais/texto_convencao.pdf>. Acesso em: 27 dez. 2011.

WORLDGROUPS. Disponível em: <http://content.worldgroups.com/groups/Custom/P/PortugalCompanhiaOnline/naoapedofilia.htm**>. Acesso em: 30 dez. 2011.**

Recebido em 11/01/2013.

Aprovado em 25/02/2013.