CRIMES DIGITAIS

Cândido Aurélio da Silva[42]
Diego Romero[43]

RESUMO

Este trabalho trata das ações humanas, perpetradas através de dispositivos eletrônicos ou de informática, contrárias à legislação pátria, ou seja, dos crimes digitais. A inovação tecnológica através dos computadores, sistemas e a internet proporcionam novos meios ou formas de comunicação ou interação. Neste sentido, o Direito, que tem por finalidade regular as relações entre os indivíduos, necessita adequar-se às novas formas de interação social. A pesquisa busca identificar as condutas criminosas que se enquadram na figura dos crimes digitais e, para tanto, utilizou o método lógico dedutivo, analisando a doutrina, as leis e os Princípios Constitucionais e Penais aplicáveis à espécie.

Palavras-chave: Direito. Crimes digitais. Informática. Computacional.

1. CONSIDERAÇÕES INICIAIS

A informática foi precedida de conceitos e avanços tecnológicos que remontam ao período compreendido entre o ano aproximado de 4000 a.C até os dias de hoje. Dentre os tantos conceitos e tecnologias precedentes e fundamentais ao advento da informática, são citados alguns, conforme Fonseca Filho (2007): o ábaco

42 Bacharel em Direito pela Universidade de Santa Cruz do Sul - UNISC-RS. Bacharel em Sistemas de Informação pela Universidade Luterana do Brasil - ULBRA-RS. Policial Militar da Brigada Militar do Estado do Rio Grande do Sul. E-mail: candidosi@hotmail.com

43 Mestre em Ciências Criminais pela Pontifícia Universidade Católica – PUCRS. Especialista em Direito penal Empresarial pela mesma instituição. Professor na Universidade de Santa Cruz do Sul – UNISC. Advogado Criminalista. e-mail: romerodiego@terra.com.br

com fios (Egito, 500 a.C); o início da ciência lógica por Aristóteles (384 a.C); eletricidade (Benjamin Franklin, 1780); sistema de telégrafo (Samuel Morse e Alfred Vail, em 1838); o computador ENIAC (Electronic Numerical Integrator and Computer), em 1946, composto por 18 mil válvulas, capaz de realizar cinco mil adições e 360 multiplicações por segundo; o 1º computador pessoal, o Kenbak I em 1971; o 1º browser (Netscape) possibilitando rápido crescimento de usuários da internet em 1994; dentre outros.

Diante desta realidade, "pode-se apontar a Segunda Guerra Mundial como um marco inicial, quando efetivamente construíram-se os primeiros computadores digitais" (FONSECA FILHO, 2007, p. 23).

Após a década de 40, houve um surpreendente avanço no segmento informático, nesta seara, "o avanço da Computação foi exponencial, abrindo-se um grande leque de tecnologias, conceitos, ideias, transformando-se em uma figura quase irreconhecível" (FONSECA FILHO, 2007, p. 23).

No entanto, "a partir de 1950, com a proliferação das pesquisas nas universidades, nos grandes laboratórios, nas indústrias – privadas ou estatais, observou-se um desenvolvimento acelerado da informática" (FONSECA FILHO, 2007, p. 22).

Contudo, se "comparada com outras áreas, a Ciência da Computação é muito recente" (FONSECA FILHO, 2007, p. 23), o que dificulta de certa forma a imediata compreensão deste fenômeno, que vem modificado intensamente a sociedade e os seus costumes.

O uso da informática através de redes de computadores tem cada vez mais se intensificado, destacando-se o uso da internet, sejam nas atividades empresariais, atividades comerciais, nas pesquisas científicas, no uso doméstico, no lazer ou recreação.

Atualmente, vive-se num mundo no qual grande parte dos acontecimentos dá-se quase ou de forma instantânea. Um bom exemplo é a transmissão da informação pelos meios computadorizados. Neste ponto, não se destaca só a velocidade da transmissão, como também a quantidade de informação que é transmitida quase que de forma instantânea.

Apenas a título de informação, se tal fenômeno de desenvolvimento tecnológico ocorresse com o ser humano, seria o mesmo que bilhões de neurônios se tivessem multiplicado, aumentando e distribuindo nossa capacidade de agrupar e analisar informações. Dentro dessa relação, nosso raciocínio trabalharia mil vezes mais rápido (CORREA, 2002, 01).

Como argumenta CORREA (2002, 12), "esse fascinante desenvolvimento tecnológico resultou no advento de uma nova era para humanidade, a denominada 'Era da Informação'". Pela primeira vez na história, somos capazes de organizar e dominar a informação como nunca, por meio da utilização de computadores, da

internet e de outras tecnologias relacionadas. Sabemos o quanto é importante, pois a troca e a difusão de informações, no decorrer do tempo, sempre foi responsável pelo desenvolvimento dos mecanismos de transformação social, já que onde houve revoluções houve necessariamente a disseminação de ideais, ou seja, comunicação.

A rapidez desse salto qualitativo e quantitativo de tecnologia, porém é incompatível com os conceitos e padrões contemporâneos, contribuindo assim com o aparecimento de conflitos entre as novas tecnologias e a sociedade. Talvez por estarmos cercados por tecnologias com as quais não podemos negar interação seja nosso dever estudá-las e entendê-las, sob pena de ficarmos isolados e esquecidos.

Não pairam dúvidas que a existência da telemática, tecnologia eletrônica de informática em rede de computadores, representa inexorável mudança nos hábitos cotidianos dos que a utilizam, promovendo sua inclusão definitiva em um mundo cada vez mais dinâmico. A presença cada vez mais forte dos computadores em nossas vidas, a capacidade de coletar e analisar dados pelas empresas e pelo Estado, e de disseminá-los através das vias rápidas das telecomunicações, nos têm proporcionado benefícios, mas, na, mesma proporção, também malefícios ao representar um formidável marco para prática de novos crimes.

Os crimes realizados com o uso ou através das redes de computadores tem como motivação a possibilidade de anonimato e a alta complexidade técnica para a apuração e verificação de autoria por parte de agentes estatais.

Desta forma, faz-se necessária uma reflexão e análise dos crimes de informática (crimes digitais), sob a visão da Constituição Federal, do Código Penal e da Lei n.º 12.737/2012. Assim, objetiva-se neste trabalho apresentar informações consistentes referentes à definição legal dos tipos penais e, ainda, elencar e compreender os Crimes de Informática vigentes no sistema penal brasileiro.

O recente empenho do Congresso Nacional em aprovar o Projeto de Lei n.º 2.793/11, que deu origem à Lei n.º 12.737/2012, com a finalidade de tipificar e regulamentar crimes realizados através da internet, também foi consequência do Projeto de Lei inicialmente apresentado sob o n.º 84/99.

Considerando, ainda, que as condutas criminosas relacionadas aos crimes de informática possuem um grande alcance e que, na atualidade, tais crimes são de grande incidência ("Segundo a Norton/Symantec, 75% dos brasileiros que usam a internet já foram vítimas de alguma forma de cibercrime" [44]), reforça-se ainda mais a relevância do tema.

---

44 CUSTO anual do cibercrime no Brasil é de R$ 16 bilhões, diz estudo. Disponível em: <http://www1.folha.uol.com.br/tec/1163431-custo-anual-do-cibercrime-no-brasil-e-de-r-16-bilhoes-diz-estudo.shtml>.

2. DOS CRIMES DE INFORMÁTICA (CRIMES DIGITAIS)

Os crimes informáticos ou crimes digitais podem ser definidos como toda conduta realizada com a utilização de equipamento eletrônico capaz de processamento, armazenamento ou transmissão de dados que seja típica, antijurídica e culpável. Assim, o crime de informática é "toda ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão" (FERREIRA, 2000, p. 210).

Quanto à classificação, os crimes de informática são classificados como puros (próprios) e impuros (impróprios ou comuns).

Os crimes de informática puros podem ser definidos como as ações ou condutas realizadas contra um ou mais sistemas de informática -neste caso o bem jurídico protegido é o sistema de informática-, já os crimes de informática impuros são definidos como as condutas em que a informática é meio ou instrumento de execução contra bens outros bens jurídicos. Ou seja, nas condutas contra sistemas ou dados temos os crimes informáticos puros, já nas condutas perpetradas a outros bens jurídicos temos os crimes informáticos impuros.

3. DOS CRIMES DIGITAIS PRÓPRIOS EM ESPÉCIE

Os crimes de informática que pertencem à categoria dos Crimes Digitais próprios são os seguintes:

Invasão de dispositivo informático: o art. 154-A do Código Penal criminaliza a conduta de invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. A conduta foi tipificada recentemente pela Lei n.º 12.737/2012, que alterou o Código Penal.

O crime foi denominado como invasão de dispositivo informático e tem a finalidade de proteger dados ou informações armazenadas desses equipamentos. Porém, o alcance do tipo é limitado, pois para configurar o delito é necessário a violação de mecanismo de segurança, assim como o invasor deverá ter o objetivo de obter, adulterar ou destruir dados.

Acessado em: 27 maio 2013.

Conforme o §1º do art. 154-A do Código Penal, igualmente incide na conduta criminosa quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador que permita a prática da conduta descrita do tipo penal. Do mesmo modo, tanto quem desenvolver software ou produzir dispositivo com finalidade de invasão computacional, como quem de alguma forma fornece a outrem, comete o crime;

Divulgação ou utilização indevida de informações: a Lei n.º 12.737/2012 acrescentou ao Código Penal o art. 154-A, § 4º, condutas que qualificam o crime de invasão de dispositivo informático. Desta sorte, as condutas que qualificam o crime são: divulgação, comercialização ou transmissão a terceiros, a qualquer título, dos dados ou informações obtidos. A qualificadora consiste no fato do agente, após obter as informações através de invasão de dispositivo, realizar a divulgação, pela internet ou por outro meio qualquer, das informações obtidas;

Inserção de dados falsos em sistema de informação: o artigo 313-A do Código Penal define como crime a conduta de inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano. No sentido de melhor explorar o tipo penal, cumpre citar:

> Trata a lei, em primeiro lugar, a conduta do funcionário público de *inserir* dados falsos nos sistemas informatizados ou bancos de dados da Administração, em que o agente acrescenta dados que não correspondem à verdade. Também comete o delito quando *altera* dados existentes, modificando a veracidade deles. Por fim, é responsável pelo crime quando exclui indevidamente dados que deviam ficar constando do sistema ou banco de dados. Em segundo lugar, comete o ilícito o funcionário que facilita a terceiro que pratique a inserção de dados falsos a alteração dos existentes ou a exclusão indevida. Nas duas modalidades está-se protegendo a regularidade dos sistemas informatizados ou bancos de dados da Administração Pública (MIRABETE, 2001, p. 1923-1924).

O crime é de mão própria, ou seja, somente pode ser perpetrado por funcionário público;

Modificação ou alteração não autorizada de sistema de informação: o artigo 313-B do Código Penal define como crime a conduta de modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente. O tipo penal incrimina a conduta de modificar um sistema (software) da Administração Pública que esteja em operação, de modo que funcionário público, sem a autorização da autoridade competente, habi-

lite um novo sistema (software) que passará a operar, assim substituindo ou desativando o primeiro. O crime é de mão própria, ou seja, somente pode ser realizado por funcionário público.

Obtenção e transferência ilegal de dados: a obtenção e a transferência de dados podem ocorrer de diversas maneiras: por invasão de sistema informático, através de programas espiões ou de vírus de computador. Nesta senda, registra a doutrina:

> O acesso a dados de um sistema informático pode se dar por muitas maneiras. Atualmente, uma forma muito simples de obtê-los é por meio dos *spywares*, termo genérico para designar espiões. Um *spyware* nada mais é que programa que rastreia informações do usuário contidas em seu computador, como, por exemplo, os sites que costuma visitar (CRESPO, 2011, p. 70).

No caso da obtenção de dados por meio de invasão, haverá a figura típica, conforme art. 154-A do Código Penal. Porém, a criminalização das condutas de obtenção de dados por um meio diverso ao da invasão de computador, apesar de ter sido proposta no PL n.º 84/99, não foi incluída na Lei n.º 12.737/2012. Diante disto, as condutas remanescentes não constituem ilícito penal.

Dano Informático: o dano informático pode ser definido como a ação que resulta em destruição de dado ou programa, ou ainda qualquer alteração em *software* que resulte em funcionamento anormal de sistema computacional. Neste ponto, Silva (2003, p. 104) infere que "a ação do agente se volta para a alteração, destruição ou inutilização do programa com a introdução de vírus, vermes e a *logic bomb*, que, como programas estranhos ao sistema informático, afetam, ou até mesmo impedem, o seu funcionamento normal". Ocorre que na legislação penal brasileira não há lei que regule especificamente todas as condutas referentes ao dano informático. Há, então, divergência doutrinária quanto à aplicação do Art. 163 do Código Penal. Para Crespo (2011, p. 72), não é admissível a aplicação do artigo 163 do Código Penal no dano informático, visto que violaria o princípio da legalidade, eis que tal princípio veda a utilização da analogia *in malam partem* em matéria criminal. Portanto, a exclusão não autorizada de um dado ou informação computacional não configuraria delito, pois, nenhuma "coisa" foi destruída no sentido material. Para este autor, conforme o Código Penal, a "coisa" é algo material, não podendo, então, sob o pretexto de uma interpretação extensiva, igualar a "coisa imaterial" a "coisa material" no que tange a adequação típica de uma conduta.

Embaraçamento ao funcionamento de sistemas: o crime foi tipificado recentemente pela Lei n.º 12.737/2012, que acrescentou ao Código Penal o Art. 266, § 1º. Porém a tipificação só se aplica ao serviço de informação de utilidade pública. Com

base neste tipo penal, comete o crime quem interrompe serviço telemático ou de informação de utilidade pública, ou impede, dificulta o restabelecimento. A criminalização da conduta tem por finalidade proteger os sistemas públicos, garantindo-lhes o funcionamento, coibindo que *crackers* realizem ataques. O alcance deste tipo penal é limitado, pois se o ataque for dirigido a um sistema informático particular, a conduta será atípica.

Interceptação ilegal de dados: Conforme o art. 10 da Lei n.º 9.296/96, 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. Como preconiza o tipo penal, no que tange os crimes digitais, constitui infração penal qualquer interceptação realizada em comunicação de informática, desde que sem autorização judicial. Contudo, há entendimentos doutrinários distintos quanto à constitucionalidade da interceptação de comunicação de dados. No tocante à inconstitucionalidade da interceptação de dados, não há até o momento nenhum julgado do Supremo Tribunal Federal no sentido de tornar esta tese doutrinária válida. Na data de 7 de agosto de 1996, foi distribuída a ADI n.º 1488 no Supremo Tribunal Federal pela Associação dos Delegados de Polícia do Brasil (ADEPOL), porém foi negado o seguimento por ilegitimidade ativa do requerente na data de 9 de março de 2001. No contexto dos crimes digitais, pode ser afirmado que a interceptação de dados com autorização judicial é válida e largamente utilizada como meio de prova.

Vírus e sua disseminação: O vírus é uma categoria de programa malicioso que tem a capacidade de prejudicar o funcionamento de sistemas de informática. Neste sentido, um vírus de computador pode causar a lentidão, o travamento ou até corromper (inutilizar) um sistema computacional. No entanto, a conduta será criminosa somente se a introdução ou disseminação de vírus ocorrer de sistema informático eleitoral, conforme o Art. 72, II, da Lei n.º 9.504/97. Restaram, assim, criminosas as condutas de 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.

Engenharia social e *phishing*: A engenharia social é um meio utilizado para obter dados ou informações de alguém, para que possam ser utilizadas para obter vantagem ilícita de alguma forma, normalmente enganando a vítima através de artifício ou ardil. Neste ínterim, a engenharia social normalmente antecede o crime de estelionato (art. 171 do Código Penal). Já o *phishing* é uma forma ou meio tecnológico de obter informações de usuários de dispositivos informáticos. Consiste em programa de computador capaz de capturar dados,

como dados pessoais, números de cartões de crédito dentre outros. Também podem ser usados para a prática de *phishing* o envio de e-mail ou a utilização de *sites* falsos, simulando pertencer a algum órgão público ou instituição bancária, com finalidade de obter dados da vítima. Conseguindo o golpista acesso às informações que lhe interessam, poderá, então, perpetrar golpes, causando prejuízos à vítima. Conforme Crespo (2011, p. 85), "caso haja o fornecimento de dados pessoais e a consequente obtenção da vantagem indevida, ter-se-ia configurado o estelionato (art. 171 do CP e Súmula 17 do STJ)".

4. DOS CRIMES DIGITAIS IMPRÓPRIOS EM ESPÉCIE

Este capítulo tem a finalidade de apresentador os crimes digitais impróprios ou impuros. Nesta categoria de crimes, os computadores ou equipamentos eletrônicos são utilizados como instrumentos ou meio para a prática de outros delitos. Por conseguinte, os sistemas informatizados ou dispositivos eletrônicos não são de forma alguma os bens jurídicos atacados, nem tutelados pelo Direito Penal.

Os crimes digitais impróprios têm origem em tipos penais autônomos, ou seja, independem da informática ou da tecnologia para existirem, em verdade, trata-se de tipos penais abertos, os quais permitem sua prática por diversos meios (*modus operandi*).

Podem-se elencar, nesta linha, os seguintes crimes:

Crimes contra a honra: Os crimes contra a honra são perfeitamente possíveis de serem cometidos através das redes de computadores. A internet é meio hábil para a transmissão ou propagação de mensagens, fotos ou informações com conteúdo ofensivo, assim sendo compatível com as condutas definidas como calúnia, difamação e injúria. Os crimes de calúnia, injúria e difamação "são todos compatíveis com suas práticas por meio da internet, a qual, nos casos citados, funciona apenas como um novo *modus operandi* para que se possa ter a ofensa da honra, quer na sua forma objetiva, quer na forma subjetiva" (NETO, 2012, p. 47). Os crimes contra a honra estão elencados nos artigos 138 (calúnia), 139 (difamação) e 140 (injúria) do Código Penal Brasileiro, sendo nesta ordem apresentados:

Crime de calúnia: conforme o art. 138 do Código Penal, o crime de calúnia consiste na conduta de imputar a alguém falsa acusação de prática de determinado fato criminoso. A tutela do crime de calúnia "é a honra objetiva à imagem da pessoa, constituindo os objetos material e jurídico do ilícito, não exigindo a presença da vítima para a consumação, uma vez que este ocorre quando o conhecimento da imputação falsa atinge terceiras pessoas" (NETO, 2012, p. 43).

Crime de difamação: o art. 139 do Código Penal define o crime de difamação como sendo a conduta de atribuir a alguém fato ofensivo a sua reputação. "*Difamar* significa desacreditar publicamente uma pessoa, maculando-lhe a reputação" (NUCCI, p. 674). No crime de difamação, a consumação ocorre da mesma forma que no crime de calúnia, ou seja, no momento em que a imputação chega ao conhecimento de terceiros.

Crime de injúria: "Nos termos do art. 140 do Código Penal, injuriar é ofender, insultar, atingindo a dignidade, amor próprio ou o decoro (moral) de alguém, sua honra subjetiva, o conceito que cada um tem de si próprio, sendo este o objeto jurídico e material do ilícito" (NETO, 2012, p. 45). Tem como elemento subjetivo atingir a autoimagem de alguém e se consuma no momento em que a vítima tomar conhecimento da ofensa.

Crimes de ameaça: o art. 147 do Código Penal define que o crime de ameaça consiste em "intimidar, prometer castigo futuro sobre um mal injusto e grave" (NETO, 2012, p. 41). Como também nos crimes contra a honra, as redes de computadores são meios adequados para a prática do crime de ameaça. A internet oferece as mais variadas aplicações para a transmissão de mensagens, como as redes sociais, e-mail, blogs, chats, dentre outros. Estes eficientes mecanismos de comunicação proporcionam um meio eficaz para a consumação do crime de ameaça. Neste sentido, Wendt (2012, p. 104) destaca que no crime de ameaça "é corriqueiro a vítima procurar a Delegacia de Polícia para informar que recebeu e-mails, mensagens de MSN ou telefonemas com ameaças de morte".

Crimes de furto e estelionato: os crimes de furto e estelionato estão capitulados, respectivamente, nos artigos 155 e 171 do Código Penal, sendo estes alguns dos crimes contra o patrimônio possíveis de serem praticados por meio de redes de computadores.

Crime de furto: o crime de furto está capitulado no art. 155 do Código Penal. Este tipo penal tem como núcleo a conduta de *subtrair para si ou para outrem coisa alheia móvel*. No contexto dos crimes digitais, é importante discorrer sobre uma das qualificadoras do crime de furto que é a fraude (prevista no art. 155, § 4º, II). Neste sentido, cita-se:

> A fraude é uma manobra enganosa destinada a iludir alguém, configurando, também uma forma de ludibriar a confiança que se estabelece naturalmente nas relações humanas. Assim, o agente que criar uma situação especial, voltada a gerar na vítima um engano, tendo por objetivo praticar uma subtração de coisa alheia móvel, incide na figura qualificada (NUCCI, 2009b, p. 710).

"Não há nenhuma restrição quanto à forma, meio ou espécie de fraude, basta que seja idônea para desviar a atenção do dono, proprietário ou simples "vigilante" da disponibilidade e segurança da *res*" (BITENCOURT, 2012, p. 50). Cita-se um

exemplo muito didático, apresentado por Neto (2012, p. 51-52), que exemplifica a conduta de furto mediante fraude por meio da internet:

> Um usuário de *net banking*[45] acessa sua conta-corrente por meio da internet e descobre pela análise do extrato que houve um saque indevido de valor considerável. Assim, verifica com o gerente da instituição bancária da qual é cliente e constata que o valor foi transferido de sua conta corrente para a conta de um terceiro, de onde foi sacado, antes que se possibilitasse o bloqueio do numerário. Toda a operação de transferência se deu com o emprego de sua senha pessoal junto ao *net banking,* subtraída com o emprego de um *Keylog*[46]. Isso permitiu que o agente se passasse pelo correntista e, sem provocar suspeita, transferisse eletronicamente um valor considerável de dinheiro para certa conta corrente junto a uma instituição bancária situada em um município distante, alugada de um terceiro, o qual, em algumas situações, desconhece a conduta ilícita que está sendo perpetrada e apenas está buscando uma maneira de obter ganho financeiro, de onde sacou o numerário.

Assim, há a perfeita adequação típica do crime de furto mediante fraude por meio da internet como instrumento para a prática do delito.

Crime de estelionato: está definido no art. 171 do Código Penal, tendo este tipo penal o núcleo de 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. No que tange a possibilidade do crime de estelionato poder ser realizado por meio da internet, cita-se:

> Por se tratar de um tipo penal aberto, o crime de estelionato pode ser praticado por qualquer meio eleito pelo sujeito ativo, inclusive pela internet, como, por exemplo, na hipótese da denominada arara virtual, em que o sujeito ativo cria um *site* de comércio eletrônico para a venda de produtos informáticos, ofertando os produtos a preços convidativos e prometendo a entrega em 15 dias úteis, mediante o pagamento em depósito no valor em conta corrente. Nesse período, contabiliza o lucro com as vendas fraudulentas, sem fazer nenhuma entrega, de forma que, após um tempo, retira o *site* do ar, deixando inúmeras vítimas em prejuízo (NETO, 2012, p. 65).

O crime de estelionato, por ser um tipo cujo, o objetivo é a trapaça, enganar e manter alguém em erro para assim obter vantagem indevida, evidente é que a internet é um ambiente muito propício a este tipo de delito.

---

45 Net banking ou home banking é um serviço oferecido por bancos ou instituições financeiras que permite que seus clientes realizem operações bancárias através da internet.

46 Keylog é um programa (código malicioso) espião, capaz de capturar dados ou senhas digitadas em um computador.

Crimes de participação em suicídio: o crime de induzimento, instigação ou auxílio ao suicídio está previsto no art. 122 do Código Penal e possui como núcleo do tipo a conduta de induzir ou instigar alguém a se suicidar ou lhe prestar auxílio para que o faça. Neto (2006, p. 39) destaca que "de início que o suicídio, em si, não é punido, constituindo uma forma de morte voluntária. Apesar disso, o suicídio é ato ilícito, embora não penalmente punido, podendo ser evitado por qualquer um". Conforme Nucci (2009, p. 631), neste crime a tentativa não é admitida, visto que o crime é condicionado à efetiva ação de o ofendido tentar o suicídio e sofrer lesões graves ou efetivamente suicidar-se. Portanto, para a sua consumação é necessário que a vítima se suicide, ou, tente e sofra lesões graves. O uso da internet é meio hábil, como instrumento de comunicação, para a execução por parte do agente dos verbos **induzir** ou **instigar** alguém a se **suicidar**, podendo este estímulo ser transmitido através de mensagens por e-mail, redes sociais, salas de bate-papo ou outros mecanismos disponíveis na rede.

Crimes contra a paz pública: os delitos de incitação ao crime (artigo 286 do Código Penal) e apologia de crime ou criminoso (artigo 287 do mesmo instituto) são os crimes contra a paz pública com condutas compatíveis aos crimes digitais, os quais podem ser praticados por meio de comunicações informatizadas. Apresentam-se os crimes:

Incitação ao crime: o crime de incitação ao crime está previsto no art. 286 do Código Penal, tendo como núcleo central a conduta de **incitar**, publicamente, a prática de crime. No sentido de melhor compreender o tipo penal, Delmanto (2010, p. 818) ensina:

> O verbo *incitar* tem a significação de açular, excitar, provocar. Pune-se o comportamento de quem incita a *prática de crime*. Portanto, deve tratar-se de fato expressamente previsto em lei como *crime*, não se enquadrando na figura o incitamento para praticar contravenção penal ou ato imoral. É imprescindível que se trate de fato criminoso determinado. Registra a lei que a ação deve ser realizada *publicamente*. A publicidade é, assim, requisito do tipo.

No contexto dos crimes digitais impuros, é perfeitamente viável a execução do delito de incitação por meio eletrônico, podendo ser a prática realizada através de blogs, redes sociais, dentre outros meios, pois nestes casos as publicações ou as mensagens poderão atingir um número indeterminado de pessoas.

Apologia ao crime: o delito de apologia ao crime está tipificado no art. 287 do Código Penal e tem como núcleo central a conduta de **fazer**, publicamente, apologia de fato criminoso ou de autor de crime. Conforme Delmanto (2010, p. 819), a

conduta delituosa de *apologia de crime ou criminoso* "deve ser realizada de maneira a ser percebida ou perceptível por indeterminado número de pessoas. É indiferente o meio de que se vale o agente para a prática deste crime: palavras, gestos, escritos ou outro meio de comunicação, inclusive pela internet".

Crimes de falsa identidade: trata-se de um crime contra a fé pública e está descrito no art. 307 do Código Penal. Este dispositivo penal criminaliza a conduta de **atribuir-se** ou **atribuir** a terceiro **falsa identidade** para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem. Com o objetivo de melhor descrever o tipo penal de falsa identidade no contexto dos crimes digitais, infere-se:

Falsa identidade: ação de se atribuir ou atribuir a outra pessoa falsa identidade para obter vantagem em proveito próprio ou de outro indivíduo ou para proporcionar algum dano. Tem sido frequente a utilização de *fakes* em sites de relacionamento, como no caso de uma mulher casada que criou um *fake* para poder se passar por pessoa solteira e conhecer outros homens. Também recentemente uma pessoa utilizou a foto de um desafeto para criar um perfil falso no Orkut, se passou por ele e começou a proferir ofensas contra diversas pessoas, visando colocar a vítima em uma situação embaraçosa (WENDT, 2012, p. 104).

O crime de falsa identidade, no contexto dos crimes digitais, pode ser identificado nos casos em que usuários da internet criam usuários, perfis com nomes ou caracteres pessoais falsos, em *sites* de relacionamentos ou redes sociais, com a finalidade de obter qualquer tipo de vantagem.

Crimes Violação de direitos autorais: o art. 184 do Código Penal define o delito, sendo que o tipo penal incrimina a conduta de violar os direitos de autor e os que lhe são conexos. As condutas criminosas no que tange o delito de violação de direito autoral através das redes de computadores são diversas, das quais se destaca a disponibilização sem autorização para *download* de livros, filmes, programas de computador (neste caso aplica-se o art. 12 da Lei nº 9.609/98), músicas ou outras obras protegidas, com ânimo de lucro.

Crimes de Pornografia Infantil: os crimes de pornografia infantil, que podem ser cometidos através de sistemas informatizados, estão previstos nos artigos 240, 241, 241-A, 241-B, 241-C, 241-D e 244-B da Lei n.º 8.069/1990 (ECA – Estatuto da Criança e Adolescente). Os referenciados tipos penais serão aqui apresentados. Com a finalidade de melhor compreensão a respeito dos crimes de pornografia infantil, está presente no ECA o artigo 241-E, que preconiza o seguinte: a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.

São Crimes de pornografia:

Pornografia envolvendo criança ou adolescente: o art. 240 do ECA elenca as condutas de **produzir, reproduzir, dirigir, fotografar, filmar** ou **registrar**, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente e, também, em seu § 1º, incrimina, no mesmo tipo penal, quem **agencia, facilita, recruta, coage**, ou de qualquer modo **intermedeia** a participação de criança ou adolescente nas cenas referidas ou ainda quem com esses **contracena**. No que se refere aos crimes digitais, é possível a realização dos verbos descritos neste tipo penal, através do uso da internet ou qualquer meio de comunicações eletrônicas para a consumação do delito.

Vender ou expor à venda fotografia pornografia infantil: o artigo 241 do ECA define como condutas típicas os atos de **vender** ou **expor à venda** fotografia, vídeo ou outro registro, desde que envolvendo criança ou adolescentes em cenas de sexo explícito ou pornográfico. Neste ínterim, incide na figura delitiva quem realizar a venda ou expor na internet (sites, redes sociais, blogs, salas de bate papo, dentre outros), fotos ou vídeos com conteúdo pornográfico de menor de idade.

Disponibilizar, transmitir ou publicar pornografia infantil: o crime previsto no art. 241-A do ECA criminaliza a conduta de **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. Destarte, quem realiza qualquer um dos verbos elencados no referido tipo penal comete o delito, inclusive através da internet. O tipo penal contempla a publicação em *sites,* blogs, redes sociais, bate-papos, e-mail ou qualquer outra aplicação disponível na rede mundial de computadores. Conforme o §1º, incisos I e II, do artigo 241-A, também incorrem neste tipo penal os provedores de acesso, por deterem conforme o texto legal a responsabilidade por: assegurar o serviço de armazenamento das fotografias, cenas ou imagens pornográficas; ou garantir o acesso por rede de computadores às fotografias, cenas ou imagens pornográficas. Entretanto, conforme o §2º do art. 241-A, as condutas tipificadas são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado deixa de desabilitar o acesso ao conteúdo ilícito.

Posse de vídeo ou foto contendo pornografia infantil: o artigo 241-B define como criminosa a conduta de adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. O tipo penal incrimina quem, por qualquer meio, possuir fotos ou vídeos com conteúdo pornográfico de criança ou adolescente. Assim, quem tiver este conteúdo armazenado em qualquer tipo de dis-

positivo (tablets, pen drive, telefone celular, CDs, DVDs, etc.) estará cometendo o crime. Porém, o tipo penal admite algumas exceções: **agente público** no exercício de suas funções; **membro de entidade**, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes; **representante legal** e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.

Simular a participação de criança ou adolescente em pornografia: a conduta criminosa tipificada no artigo 241-C do ECA consiste em simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual. No que se refere aos crimes digitais, o importante neste tipo penal é o conteúdo do parágrafo único do supracitado dispositivo legal, tendo sua literalidade como: incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo.

Aliciamento de criança, para a prática de ato libidinoso: a conduta criminosa, conforme o Art. 241-D do ECA, consiste em **aliciar, assediar, instigar** ou **constranger**, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso. No aspecto jurídico, tem-se definido como criança a pessoa com idade de até 12 anos, assim evidentemente, não comete o delito se a conduta for praticada contra adolescente (idade maior que 12 anos). O delito consiste na conduta do agente ativo de alguma forma tentar seduzir, por qualquer meio de comunicação (no contexto dos crimes digitais, pela internet), que criança venha a ter com ele a prática de qualquer ato libidinoso. O delito pode ser cometido por qualquer ferramenta da internet como: Skype, Facebook, Orkut, Twitter, sala de bate-papo, e-mail, dentre outros.

Corrupção de menor: o art. 244-B do ECA incrimina a conduta de **corromper** ou **facilitar** a corrupção de menor de 18 (dezoito) anos, com ele **praticando** infração penal ou **induzindo-o** a praticá-la. Assim, incorre no mesmo crime quem pratica as condutas ali tipificadas, utilizando-se de quaisquer meios eletrônicos, inclusive salas de bate-papo da internet. O tipo penal também tem alcance aos fatos praticados por quaisquer meio eletrônicos, ou seja, o uso de qualquer ferramenta da internet, com a finalidade de aliciar crianças ou adolescentes à prática de crimes, também constitui ilícito penal.

Outros crimes digitais impróprios: é importante salientar que o rol de crimes digitais apresentados não é taxativo, ou seja, existem outras possibilitadas de cometimentos

de outros tipos penais não explorados neste trabalho, tendo em vista que com a aceleração do desenvolvimento tecnológico, mais ferramentas são criadas e perfectibilizadas e, lamentavelmente, acabam sendo utilizadas como meio, instrumento para prática de crimes.

5. CONSIDERAÇÕES FINAIS

Neste trabalho foi realizada a verificação dos principais crimes (infrações penais), cujas condutas criminosas são verificáveis no contexto do meio eletrônico. Nesta acepção, o resultado foi muito profícuo, visto que foi possível identificar uma gama considerável de delitos que se submetem a égide dos crimes digitais.

Nota-se que os crimes digitais podem dividir-se em duas categorias, sendo: os crimes digitais próprios (puros) e os crimes digitais impróprios (impuros). Nesta senda, os crimes digitais próprios são os crimes praticados contra os sistemas de informática, enquanto os crimes digitais impróprios são os que têm a finalidade de atingirem outros bens jurídicos diversos aos sistemas informáticos. No entanto, a informática é o meio ou instrumento para a realização do delito.

Diante do contexto dos crimes digitais, salienta-se que qualquer que seja a utilização da internet, sem a implementação de mecanismos de segurança estará a comunicação de dados à mercê de ser interceptada ou violada facilmente por usuários mal intencionados, normalmente denominados *crackers*.

Destaca-se que a internet, apesar de ser extremamente funcional, por possuir grande eficiência na difusão de dados e proporcionar conectividade entre os mais variados tipos de dispositivos eletrônicos, traduz-se em um ambiente inseguro, o qual necessita de inúmeras regulamentações. Diante desta realidade, a grande rede mundial de computadores é um cenário tentador a pessoas inescrupulosas, que buscam uma forma de obter algum tipo de vantagem ilícita através de atos tipificados pela lei penal brasileira como crimes.

6. REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. A Criminalidade Informática. 1. Ed. São Paulo: Editora Juarez de Oliveira. 2006.

CORREA, Gustavo Testa. Aspectos Jurídicos da Internet. 2ª edição. São Paulo: Saraiva. 2002.

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. 1. Ed. São Paulo: Saraiva. 2011.

DELMANTO, Celso; Delmanto, Roberto; Junior, Roberto Delmanto; Delmanto, Fabio Machado de Almeida. Código Penal comentado. 8. Ed. São Paulo: Saraiva. 2010.

FERREIRA, Ivette Senise; LUCCA, Newton de; SIMÃO FILHO, Adalberto. Direito e Internet: Aspectos Jurídicos Relevantes. Bauru: Edipro. 2000.

FONSECA FILHO, Cléuzio. História da computação: O Caminho do Pensamento e da Tecnologia. Porto Alegre: EDIPUCRS. 2007.

LOPES JR., Aury. Direito Processual Penal e sua Conformidade Constitucional. 7. Ed. volume 1. Rio de Janeiro: Lumen Juris. 2011.

MIRABETE, Julio Fabbrini. Código Penal interpretado. 2. Ed. São Paulo: Atlas. 2001.

NETO, Mário Furlaneto; Dos Santos, José Eduardo Lourenço; Gimenes, Eron Veríssimo. Crimes na Internet e Inquérito Policial Eletrônico. 1. Ed. São Paulo: Edipro. 2012.

NUCCI, Guilherme de Souza. Código de Processo Penal Comentado. 9. Ed. São Paulo: Revista dos Tribunais. 2009.

NUCCI, Guilherme de Souza. Manual de direito penal: parte geral: parte especial. 6. Ed. São Paulo: Revista dos Tribunais. 2009.

SILVA, Rita de Cássia Lopes da. Direito penal e sistema informático. Volume 4 da Série Ciência do direito penal contemporâneo. São Paulo: Revista dos Tribunais. 2003.

WENDT, Emerson; Jorge, Higor Vinicius Nogueira. Crimes cibernéticos: ameaças e procedimentos de investigação. 1. Ed. Rio de Janeiro: Brasport. 2012.