Estudo sobre a aplicabilidade das leis penais aos crimes informáticos no Brasil

Hélio Santiago Ramos Júnior, *UFSC*

***Resumo*—O presente estudo tem a finalidade de dissertar sobre a aplicabilidade das leis penais vigentes aos crimes informáticos no Brasil, analisando a legislação atual e fazendo comentários sobre o entendimento doutrinário e jurisprudencial acerca desta temática, destacando os limites e alcance de algumas leis penais aplicáveis e apresentando as propostas legislativas referentes aos delitos informáticos, os quais abrangem tanto aqueles cometidos contra os dados e os sistemas informáticos como também os que utilizam a informática como um meio para a prática de condutas criminosas, esclarecendo questões controvertidas sobre a matéria.**

***Palavras-chave*—Crimes Informáticos; Legislação Penal.**

I. Introdução

A origem dos crimes informáticos está relacionada com o surgimento do computador, entretanto esta temática adquire maior relevância a partir do advento da Internet em 1969, a qual foi idealizada na época da Guerra Fria, para fins militares pelo governo norte-americano, objetivando construir uma rede de comunicação que se mantivesse intacta mesmo na hipótese de ataques bélicos a uma de suas bases.

Posteriormente, esta rede se expandiu para algumas universidades com o projeto ARPANET, com fins científicos, e, em seguida, houve a sua abertura para os demais países, permitindo assim a integração de todos os computadores a esta rede, a Internet, tal qual se conhece atualmente.

É justamente com a popularidade da grande rede de computadores que começou a se praticar delitos através do ciberespaço, o qual passou a ser visto como um ambiente livre de toda e qualquer regulamentação jurídica, tornando-se necessário o exame da legislação penal vigente no tocante à possibilidade de sua aplicação aos denominados crimes cibernéticos, ou seja, tanto aos delitos praticados contra o computador quanto aos que utilizam a rede mundial como um meio para a prática de condutas criminosas.

A Internet passou a ser denominada também de 'ciberespaço' e a origem desta palavra provém da cibernética, do grego *kubernetes*, que significa 'piloto do barco' ou 'timoneiro', sendo, por isso, comum se referir à rede mundial de computadores, comparando-a a um mar digital.

O mito do ciberespaço como um ambiente virtual fora da lei começou a ser afastado a partir do momento em que os primeiros casos envolvendo crimes praticados através da Internet foram sendo punidos no país, interpretando-se as normas penais em vigor, definindo os critérios acerca da competência e verificando a possível aplicabilidade da norma penal a destes delitos.

Os crimes informáticos surgem no ordenamento jurídico a partir da entrada em vigor da legislação que os tipificou, podendo ser definidos como sendo uma "ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão". [1]

Na hipótese de não existir lei definindo uma determinada conduta como crime, a exemplo do acesso indevido a sistemas computacionais, não seria juridicamente correto dizer que se trata de um crime informático, porque esta conduta não está prevista como delito pela norma penal em vigor na atualidade, não obstante haver projeto de lei objetivando criminalizá-la.

Muito embora tais condutas ilícitas sejam reprováveis pela sociedade do ponto de vista ético, a responsabilidade penal somente ocorrerá quando existir lei que expressamente estabeleça que determinado fato constitua um crime e que determine qual a pena lhe seja aplicável, não podendo esta retroagir para punir os que a praticaram quando o comportamento ilícito não estava criminalizado, tudo isso em homenagem à segurança jurídica e à legalidade penal.

Assim, de acordo com o art. 5º, inciso XXXIX, da Constituição Federal de 1988, não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.

Isto significa que se deve observar o princípio constitucional segundo o qual ao cidadão não pode ser imputado um crime que não esteja definido em lei e que toda pena somente pode ser aplicada se estiver prevista em norma preexistente ao fato criminoso.

Por esta razão é que não se admite o uso da analogia para normas incriminadoras, uma vez que não se pode violar o princípio da reserva legal. [2]

II. Classificação dos Crimes Informáticos

Os crimes informáticos podem ser classificados, segundo o professor Luiz Flávio Gomes, em crimes contra o computador ou crimes por meio do computador. [3] Na mesma linha é a classificação adotada pela professora Ivette Senise Ferreira que os classificam em atos ilícitos dirigidos contra um sistema de informática ou cometidos por intermédio de tal sistema. [4]

Além da divisão bipartidária acima apresentada, os crimes informáticos podem ser classificados como puros, mistos ou

Manuscript received August 17, 2008.

H. S. Ramos Júnior é formado em Direito pela UFSC, advogado licenciado pela OAB/SC, assistente de Procuradoria de Justiça do MPSC e mestrando em Engenharia e Gestão do Conhecimento EGC/UFSC, com projeto de dissertação sobre delitos informáticos. Email: hsramos@mp.sc.gov.br

comuns. Neste sentido, os crimes informáticos puros são aqueles praticados com o intuito de atingir o computador, o sistema de informática ou os dados e as informações neles utilizadas; os crimes informáticos mistos, por sua vez, são aqueles nos quais o agente não visa o sistema de informática e seus componentes, mas a informática constitui instrumento indispensável para consumação da ação criminosa; e os crimes informáticos comuns, são aqueles onde o agente não visa o sistema de informática e seus componentes, mas usa a informática como instrumento (não essencial, poderia ser outro o meio) de realização da ação. [5]

Em seu parecer sobre o Projeto de Lei do Senado nº 76/00, Alexandre Atheniense já havia defendido esta classificação terciária dos crimes informáticos em puros, mistos ou comuns, classificando os crimes informáticos impuros como "aqueles que podem ser cometidos também fora do universo do computador, encontrando já definição no sistema punitivo atual" [6]; como sinônimos de 'crimes informáticos comuns'.

Entretanto, entende-se que a terminologia 'crimes informáticos impuros' seja mais apropriada do que 'crimes informáticos comuns', tendo em vista que a doutrina penal usa a expressão 'crimes comuns' para se referir aos delitos que podem ser praticados por qualquer pessoa, em contraposição aos 'crimes próprios', que exigem determinada qualidade ou condição pessoal do agente para a caracterização do delito.

Há também uma divisão quaternária a qual classifica os delitos informáticos em impróprios, próprios, mistos e mediatos ou indiretos.

De acordo com esta classificação, os delitos informáticos impróprios são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados); já os delitos informáticos próprios são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados); os delitos informáticos mistos são crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa. E, finalmente, o delito informático mediato ou indireto o qual consiste no delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação. [7]

No entanto, uma vez que o direito penal informático não é um ramo autônomo do direito penal, e pela mesma razão pela qual se ponderou não ser adequada a utilização da expressão 'crimes informáticos comuns', prefere-se utilizar a expressão 'crimes informáticos puros' para se referir aos 'crimes informáticos próprios', evitando-se, assim, a sua eventual confusão em relação aos 'crimes próprios quanto ao sujeito', praticados através da informática, já que estes possuem significado diferente daqueles.

Em relação aos delitos informáticos mistos, entende-se que estes não podem ser considerados como 'crimes complexos', eis que, salvo melhor juízo, não se vislumbra atualmente no ordenamento jurídico-penal vigente nenhum crime informático que possa ser representado a partir da fusão de mais de um tipo penal envolvendo o uso da informática.

Salienta-se, por exemplo, que o acesso indevido a sistema informatizado do processo eleitoral para alterar a apuração ou a contagem de votos constitui, por si mesmo, um único delito.

Assim, não constituem crime complexo os delitos formados por um crime acrescido de elementos que isoladamente são penalmente indiferentes. [2]

Quanto aos delitos informáticos mediatos ou indiretos, estes ainda não existem no sistema penal brasileiro em razão da ausência de tipificação do delito-meio informático que seria fundamental para viabilizar esta classificação proposta por [3], pois a simples prática de acesso indevido objetivando cometer furto, por exemplo, envolve apenas o delito-fim que é o crime de furto uma vez que a conduta de acesso indevido não é considerada um delito-meio eis que ainda não está prevista como crime pela lei penal, conforme já mencionado.

Não obstante às diversas formas de classificar os delitos informáticos, tendo em vista o conceito de crimes informáticos utilizado neste trabalho, adota-se a seguinte classificação:

Os crimes informáticos puros são definidos como aqueles que visam atingir a incolumidade dos dados e do sistema informatizado como um todo, inclusive no que concerne ao processamento destes dados e de sua transmissão.

Por sua vez, os crimes informáticos impuros são considerados aqueles nos quais o agente não visa atingir o sistema de informática, mas esta é utilizada como um meio para a consumação de um delito o qual pode ser cometido por diversos meios, não sendo a informática elemento essencial.

Enfim, os crimes informáticos mistos são delitos praticados necessariamente por meio da informática e que, além da incolumidade dos dados e sistemas, a norma visa proteger outro bem jurídico tutelável pela lei penal.

III. Crimes contra a Vida

O uso da informática pode ser utilizado para a prática de crimes contra a vida, nestes casos, o componente informático ou a Internet se constitui no meio através do qual se comete o delito, desta forma, conforme o caso concreto, podem ser considerados delitos informáticos: o crime de homicídio e o crime de induzimento ou instigação a suicídio, conforme serão comentados a seguir.

A. Homicídio

O crime de homicídio consiste na conduta de matar alguém, nos termos do *caput* do art. 121 do Código Penal (CP), sendo a pena aplicável de reclusão, de seis a vinte anos.

A prática do crime de homicídio por meio do computador é admissível, por exemplo, quando o criminoso pratica o acesso indevido a sistemas de informações, invadindo computadores de determinada instituição e alterando dados em seu sistema informatizado, induzindo alguém ou a própria vítima em erro, fazendo com que esta se comporte de maneira a pôr em risco a sua própria vida ou a de outrem.

Embora seja de difícil ocorrência, trata-se de um delito informático possível de acontecer tendo em vista o crescente processo de informatização pelo qual passa a sociedade contemporânea, conforme exemplo ilustrado pela doutrina:

"Tício invade os computadores do CTI de um grande hospital e altera a lista de remédios a ser ministrada em Mévio. Uma enfermeira, induzida a erro pela falsa receita, acaba matando Mévio com a superdosagem de medicação". [8]

Muito embora o Código Penal seja de 1940, a lei penal é, em regra, aplicável a toda conduta criminosa na qual a Internet seja o meio para a prática do crime. No caso em questão, trata-se apenas de um novo meio de execução de conduta já tipificada, toma-se o exemplo da invenção da pólvora que não implicou na necessidade de mudança da lei para redefinir o crime de homicídio pela morte mediante arma de fogo.

B. Induzimento, instigação ou auxílio a suicídio

O artigo 122 do Código Penal tipifica como criminosa a conduta de induzir ou instigar alguém a se suicidar ou prestar-lhe auxílio para que o faça. Se o suicídio se consuma, a pena é de reclusão, de dois a seis anos; caso da tentativa de suicídio resulte lesão corporal de natureza grave, aplica-se pena de reclusão de um a três anos.

Trata-se de um delito que pode ser praticado através da rede mundial de computadores, como por meio da troca de mensagens eletrônicas ou através de comunidades virtuais de relacionamentos como o *Orkut*, onde o agente induz ou instiga a vítima a cometer o suicídio.

No caso em questão, consiste em um crime informático impuro, porque o agente não visa o sistema de informática e a Internet é apenas o meio para a prática do delito; material, porque para haja a sua consumação é necessária a ocorrência do resultado (morte ou lesão corporal de natureza grave), sendo inadmissível a tentativa; é obrigatoriamente um crime comissivo, porque somente se consuma mediante a ação do agente; e é crime doloso, pois não existe modalidade culposa.

IV. Crimes contra a Honra

Os crimes contra a honra são três: calúnia, difamação e injúria. A diferença entre eles é que na calúnia há a imputação falsa a terceiro de uma conduta criminosa; na difamação, o fato imputado é uma alegação ou afirmação ofensiva à reputação da pessoa e independe do fato ser verdadeiro ou falso; enquanto que na injúria não há a imputação de um fato, mas sim a manifestação depreciativa, com expressões vagas e imprecisas sobre qualidade negativa do ofendido.

Todos estes delitos podem ser praticados através da informática, sendo o bem jurídico ofendido a honra objetiva (no caso de calúnia e difamação, onde se atinge a reputação) ou subjetiva (na hipótese de crime de injúria, onde se ofende a dignidade e o decoro) do agente.

O grande problema envolvendo os crimes contra a honra na Internet é a dificuldade de identificar o autor das ofensas haja vista o mesmo se aproveitar do anonimato para a prática destes delitos. Assim, reporta-se ao recurso de apelação criminal nº 71001070184, julgado em 2007, pelo Tribunal de Justiça do Rio Grande do Sul (TJRS), que manteve a sentença do juízo de primeiro grau que absolveu o réu dos crimes de difamação e injúria perpetrados pela Internet por ausência de provas; ou ainda ao acórdão nº 71001329036 deste mesmo tribunal que confirmou a sentença absolutória por não haver certeza quanto à autoria das ofensas praticadas através da comunidade *Orkut*.

A Constituição garante a liberdade de expressão em seu artigo 5º, IV, porém é proibido o anonimato justamente para evitar manifestações abusivas que violem a integridade das pessoas bem como o próprio ordenamento jurídico, pois, sendo elas anônimas, não se poderá responsabilizar o agente que cometer abusos no exercício deste direito.

Além dos crimes contra a honra previstos no CP, há também os crimes de calúnia, difamação e injúria, previstos pela Lei nº 5.250, de 09 de fevereiro de 1967, a qual regula a liberdade de manifestação do pensamento e de informação, conhecida como Lei de Imprensa, cujas normas são aplicáveis em se tratando de crime praticado mediante a exploração ou utilização dos meios de informação e divulgação tipificados na referida lei.

Em geral, quando o ofensor utiliza a rede mundial de computadores para praticar um crime contra a honra (calúnia, difamação ou injúria) incide o Código Penal, como, por exemplo, nas hipóteses de cometer o delito através do envio de mensagens eletrônicas para grupos de discussão; através da postagem de recados ofensivos à honra de outra pessoa em comunidades virtuais; ou ainda por meio da publicação em páginas virtuais que não estejam vinculadas a atividades publicitárias e jornalísticas.

Por outro lado, quando o crime de calúnia, de difamação ou de injúria for praticado pela imprensa, através de jornais, periódicos ou serviços noticiosos na rede, incidem as normas penais da Lei 5.250/67, conforme decidiu o Tribunal de Alçada Criminal de São Paulo, ao julgar o recurso de *habeas corpus* nº 416.372-2, em 2002.

É importante destacar que no momento atual se discute no país a constitucionalidade da Lei de Imprensa no Supremo Tribunal Federal (STF) em virtude de uma ação de descumprimento de preceito fundamental (ADPF nº 130-DF), proposta pelo partido político PDT, argumentando que esta lei teria conteúdo autoritário, sendo recentemente suspendidos os efeitos de diversos artigos bem como os processos em tramitação no Poder Judiciário sobre este assunto até que seja julgada a referida ação.

Desta forma, se o STF julgar a Lei de Imprensa como sendo inconstitucional, o Código Penal será aplicável às hipóteses previstas na Lei de Imprensa, as quais também estão tipificadas naquele e estenderia o seu alcance para os casos em que a prática do delito contra a honra estiver vinculada a atividades de publicidade e jornalismo, sendo cometido através de jornais, revistas ou serviços noticiosos na Internet.

A. Calúnia

O crime de calúnia está previsto no art. 138 do Código Penal, com pena de detenção de seis meses a dois anos, e multa. Esta pena é aplicável não apenas a quem imputa a alguém falsamente a autoria de um crime, como também incorre neste crime o terceiro que, sabendo ser falsa a imputação, a propala e divulga. Também é punível a calúnia contra os mortos.

O crime de calúnia do art. 138 do CP admite a retratação, ou seja, se o ofensor, antes da sentença, se retratar cabalmente do delito, ficará isento de pena; ao contrário da retratação do crime de calúnia do art. 20 da Lei de Imprensa, que deve ser feita antes de iniciado o procedimento judicial para excluir a

ação penal. Acerca da retratação, o Superior Tribunal de Justiça, julgando o recurso especial nº 320958/RN, em 2007, decidiu que a retratação tem que ser completa e inequívoca, exigindo-se a publicidade desta, mormente nos casos em que a calúnia tenha sido praticada através da Internet.

B. Difamação

O crime de difamação consiste na imputação a outrem de fato ofensivo à sua reputação; estando previsto no art. 139 do CP, com pena de detenção de três meses a um ano, e multa.

Assim como na calúnia, a difamação admite a possibilidade de retratação do ofensor; entretanto, para que haja isenção da pena se faz necessário que o ofensor se retrate de forma cabal, desdizendo todos os fatos imputados ofensivos à reputação da vítima, antes de proferida a sentença.

Neste crime, somente se admite a exceção da verdade se o ofendido for funcionário público e a ofensa estiver relacionada ao exercício de suas funções. Ao contrário da calúnia, não se admite crime de difamação contra a memória dos mortos.

Uma vez praticado por meio da rede mundial de computadores, caracteriza-se como um crime informático impuro já que o bem jurídico ofendido no caso do art. 139 do CP é a reputação do sujeito e não visa o sistema de informática propriamente dito.

É crime comum quanto ao sujeito; necessariamente comissivo que exige uma ação do agente; formal, que independe do resultado; doloso, sendo imprescindível o ânimo de ofender a reputação alheia, não admitindo a forma culposa; e instantâneo, que se consuma no momento em que a imputação chega ao conhecimento de um terceiro.

C. Injúria

O crime previsto no art. 140 do CP consiste em "injuriar alguém, ofendendo-lhe a dignidade ou o decoro", com pena de detenção, de um a seis meses, ou multa.

Há situações nas quais o juiz pode deixar de aplicar a pena, quais sejam: quando o ofendido, de forma reprovável, provocou diretamente a injúria; ou no caso de retorsão imediata, que consista em outra injúria. Não há crime de injúria contra os mortos.

Na hipótese do ofensor utilizar elementos referentes à raça, cor, etnia, religião ou origem para injuriar alguém, a pena é de reclusão de um a três anos, e multa.

Em 2004, o STJ denegou o recurso de *habeas corpus* nº 37493/SP, o qual visava o trancamento da ação penal em virtude do registro de mensagens eletrônicas injuriosas na Internet, afastando a alegação de atipicidade da conduta.

Tanto na difamação quanto na injúria, há hipóteses em que não constituem crime, como, por exemplo, a opinião desfavorável da crítica literária, artística ou científica, salvo quando inequívoca a intenção de injuriar ou difamar.

Em se tratando do mesmo fato imputado, o crime de difamação absorve a injúria; ou seja, neste caso, o ofensor responde apenas pelo primeiro. Entretanto, sendo distintos os fatos, responderá por difamação e também por injúria.

V. Crimes contra a Liberdade Pessoal

Os crimes contra a liberdade pessoal que podem ser praticados através da informática são o crime de constrangimento ilegal e o crime de ameaça.

A. Constrangimento ilegal

O crime de constrangimento ilegal está inserido no art. 146 do CP e consiste na conduta de "constranger alguém, mediante violência ou grave ameaça, ou depois de lhe haver reduzido, por qualquer outro meio, a capacidade de resistência, a não fazer o que a lei permite, ou a fazer o que ela não manda", sendo a pena aplicável a este crime de detenção de três meses a um ano, ou multa.

Trata-se de um tipo penal que pode vir a ser praticado, através da tecnologia informática, apenas mediante grave ameaça, pois "claro que a partir das características da atividade tecnológica, certamente a violência como forma de constrangimento não seria passível de execução a partir da informática". [9]

O constrangimento ilegal pode ocorrer mediante envio de uma mensagem eletrônica ou qualquer outro meio através do qual o agente faz uma grave ameaça à vítima, reduzindo-lhe a sua capacidade de resistência e obrigando-a a não fazer o que a lei permite ou a fazer o que ela não manda.

B. Ameaça

Constitui crime, tipificado no art. 147 do CP, "ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto ou grave", cuja pena é de detenção de um a seis meses, ou multa.

O crime de ameaça pode acontecer através do uso da informática, como, por exemplo, por meio do envio de mensagens eletrônicas ou recados virtuais com o intuito de intimidar a vítima, ameaçando-lhe causar mal injusto ou grave.

Trata-se, neste caso, de um crime informático impuro, onde a Internet é apenas o meio utilizado para a prática da conduta delituosa: "A ameaça por escrito ou qualquer outro meio simbólico abre a possibilidade de execução do crime pela utilização de computadores, em especial de e-mails, nos quais contenham escritos ou representações gráficas que configurem a ameaça". [9]

Portanto, a ameaça, mesmo que praticada através do uso da Internet, seja através do correio eletrônico ou outro meio informático, caracteriza o crime previsto no art. 147 do CP, pois esta norma penal admite esta possibilidade ao se referir ao crime de ameaça cometido por meio de palavra, escrito ou gesto, ou qualquer outro meio simbólico.

VI. Violação de E-mail e Crime de Interceptação de Comunicação de Dados

O art. 151 do Código Penal trata do crime de violação de correspondência, definindo como típica a conduta de "devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem", atribuindo-lhe pena de detenção de um a seis meses, ou multa.

De início, surgiu uma discussão na doutrina acerca da

eventual incidência do mencionado artigo na hipótese de se tratar de violação de e-mail no tocante a sua equiparação à correspondência para fins de aplicação da lei penal.

Entretanto, predominou o entendimento de que o e-mail não pode ser considerado uma correspondência fechada, a teor do art. 151 do CP uma vez que é vedado o uso de analogia no direito penal, pois embora seja semelhante à correspondência, não pode o e-mail ser equiparado a esta para fins penais.

Em se tratando de interceptação de comunicação de dados, o art. 10 da Lei nº 9.296/96 estabelece que "constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial com objetivos não autorizados em lei", com pena de reclusão de dois a quatro anos, e multa.

O Tribunal de Justiça de Santa Catarina, ao julgar a apelação criminal nº 2007.006842-9, entendeu que configura o crime de interceptação de comunicação a conduta de quem invade provedor de Internet, apropriando-se dos *logins* e senhas de seus usuários.

Entretanto, considera-se esta uma posição jurisprudencial equivocada, porque o art. 10 da Lei nº 9.296/96 pune apenas a interceptação de comunicações de dados e não o acesso indevido ou invasão a sistemas computacionais.

Neste sentido, "só haverá o crime do art. 10 da Lei 9.296, quando, e somente quando, o autor impedir que a mensagem chegue intacta a seu destinatário". [10]

VII. Crimes contra a Inviolabilidade dos Segredos

No que se refere à inviolabilidade dos segredos, admite-se a possibilidade de se praticar os crimes de divulgação de segredo e violação de segredo profissional através da Internet.

A. Divulgação de segredo

O crime de divulgação de segredo está previsto no art. 153, *caput* do CP, e consiste em "divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem", sendo a pena de detenção de um a seis meses, ou multa.

Há também o §1º-A deste artigo que foi introduzido no Código Penal pela Lei nº 9.983/2000, estabelecendo pena mais severa no caso de divulgação, sem justa causa, de informações sigilosas ou reservadas contidas ou não nos sistemas de informações ou bancos de dados da Administração Pública; no caso, a pena será de detenção de um a quatro anos, e multa.

Quando a divulgação de segredo é praticada através da Internet, como, por exemplo, através de envio de mensagem eletrônica, caracteriza-se como um crime informático impuro; trata-se de delito formal que para sua consumação basta que o agente divulgue um segredo, sem justa causa e que este seja apto a causar dano, independente da ocorrência do resultado; é comissivo, pois exige uma ação do sujeito; e instantâneo, porque basta a sua divulgação para a caracterização do delito.

Em relação ao sujeito, somente pode praticar o crime de divulgação de segredo contido no *caput* do art. 153 do CP quem for destinatário ou detentor do documento particular ou da correspondência confidencial; já o crime de divulgação do segredo previsto no §1º-A deste artigo pode ser praticado por qualquer pessoa, mesmo que não seja funcionário publico, inclusive por *hackers* que obtenham acesso indevido a estas informações mediante a invasão de computadores alheios.

O delito do *caput* do art. 153 do CP poderá ser aplicável para as hipóteses de divulgação, sem justa causa, de conteúdo de documento eletrônico, ainda que seja encaminhado por e-mail, desde que utilize mecanismo de proteção que seja hábil a garantir a confidencialidade do seu conteúdo e para que haja sua consumação, o conteúdo do documento eletrônico divulgado deve ser suscetível de ocasionar dano a alguém.

Por sua vez, o crime previsto no §1º-A do art. 153 do CP protege apenas a inviolabilidade de informações sigilosas ou reservadas, independentemente de estarem ou não contidas nos sistemas de informações ou banco de dados da Administração Pública, não sendo aplicável, por exemplo, na hipótese de um *hacker* apenas acessar indevidamente conteúdo de informações sigilosas, sendo imprescindível que ele realize a divulgação deste conteúdo sigiloso para que haja a consumação do delito.

B. Violação de segredo profissional

Além do crime de divulgação de segredo, o Código Penal também tipifica como crime a violação de segredo profissional, conforme consta em seu art. 154: "revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem", sendo a pena para este delito de detenção de três meses a um ano, ou multa.

O crime de violação de segredo profissional é um delito próprio quanto ao sujeito uma vez que somente pode praticá-lo a pessoa que tem ciência do mesmo em razão de função, de ministério, de ofício ou da profissão exercida; trata-se aqui de crime formal que não depende do resultado para a sua consumação; é um crime de menor potencial ofensivo e pode ser cometido através da rede mundial de computadores, como, por exemplo, a partir da revelação do segredo profissional mediante a sua publicação em páginas virtuais na Internet.

Em relação à jurisprudência, lembra a doutrina que já há caso na Justiça brasileira em que o conteúdo de e-mail monitorado foi utilizado como prova para demissão de um funcionário por justa causa, no caso de flagrante violação de sigilo profissional. [11]

VIII. Crimes contra o Patrimônio

Examinando os crimes contra o patrimônio, observa-se que podem ser praticados através da informática: o crime de furto, o crime de extorsão, o crime de dano e o crime de estelionato.

A. Furto

O crime de furto está tipificado no art. 155 do CP e consiste na conduta de "subtrair, para si ou para outrem, coisa alheia móvel", sendo a pena aplicada para quem incorre neste delito, de reclusão, de um a quatro anos, e multa.

No crime de furto, o agente apenas subtrai para si ou para outrem coisa alheia móvel, diferentemente do crime de roubo

no qual há o emprego de violência ou grave ameaça dirigida à pessoa além da subtração da coisa para si ou para outrem.

Trata-se de um crime que pode ser praticado em sua modalidade informática, na qual o agente utiliza o acesso indevido, invadindo computadores de instituições bancárias e desviando dinheiro para outra conta.

Para que ocorra o crime de furto é necessário que haja a efetiva subtração de coisa alheia móvel, ainda que seja energia elétrica ou qualquer outra que tenha valor econômico; tanto a doutrina quanto a jurisprudência já se manifestaram no sentido da possibilidade de aplicação desta norma penal aos furtos cometidos mediante o uso da informática.

Neste sentido, o Judiciário tem condenado *hackers* que praticam o acesso indevido a contas bancárias para transferir valores para outras contas, denegando-lhes, inclusive, ordens de *habeas corpus* que são comumente pleiteadas aos tribunais.

B. Extorsão

O crime de extorsão está previsto no art. 158 do CP e consiste na conduta de "constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa", sendo a pena de reclusão, de quatro a dez anos, e multa. A pena é aumentada se o crime for cometido por duas ou mais pessoas, por exemplo.

Trata-se de um delito que pode ser praticado, por exemplo, mediante o envio de mensagens eletrônicas na qual o indivíduo busca constranger alguém, utilizando-se de grave ameaça com o intuito de obter vantagem econômica indevida.

Neste sentido, o Tribunal de Justiça do Paraná, ao julgar a apelação criminal nº 315.642-7, manteve a condenação de um indivíduo pela prática do crime de extorsão mediante grave ameaça praticado através da veiculação de informações vexatórias em *site* da Internet com o objetivo de intimidar a vítima para obter vantagem econômica indevida.

C. Dano

O Código Penal estabelece no art. 163, como crime de dano, a conduta de destruir, inutilizar ou deteriorar coisa alheia, sendo a pena de detenção, de um a seis meses, ou multa.

Este delito passa a ser qualificado, por exemplo, quando for cometido por motivo egoístico ou com prejuízo considerável para a vítima, hipótese na qual a pena aplicável será de detenção, de seis meses a três anos, e multa.

Há uma resistência por parte da doutrina mais conservadora em admitir a possibilidade de aplicação do art. 163 do CP ao dano informático. Assim, argumenta-se que "se os dados armazenados, processados ou transmitidos por sistemas informáticos forem considerados coisas móveis, este conceito deixará de corresponder a objetos tangíveis para incluir objetos intangíveis. Ele passará da materialidade à imaterialidade, do âmbito da propriedade para o âmbito do valor. Essa tendência expande excessivamente o conceito de 'coisas móveis'. [12]

Não obstante, admite-se a incidência desta norma penal em se tratando de crime de dano praticado através da rede mundial de computadores desde que a coisa destruída, inutilizada ou deteriorada tenha valor patrimonial.

O crime de dano pode ser cometido mediante o uso da informática, como, por exemplo, através do envio de vírus por e-mail com intuito de inutilizar o computador do destinatário.

Deste modo, "caso sejam danificados as placas e circuitos internos, qualquer elemento físico externo, ou ainda, caso se introduza programas maliciosos, inclusive vírus, com o objetivo de modificar a funcionalidade do computador, em tese, poderá haver o enquadramento no crime de dano". [13]

Mesmo sendo um delito material, a consumação do crime poderá ocorrer não somente quando houver um efetivo dano físico ao computador, mas também quando forem destruídos, inutilizados ou deteriorados dados informáticos que possuam concomitantemente valor econômico e de utilidade.

Portanto, uma vez que o tipo penal está inserido nos crimes contra o patrimônio, o alcance desta norma será limitado a proteger os dados informáticos com relevância patrimonial, não abrangendo dados que possuam apenas valor de utilidade.

D. Estelionato

O estelionato é um crime que está tipificado no art. 171 do CP, consistindo na conduta 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", com pena de reclusão, de um a cinco anos, e multa.

É pacífico, tanto na doutrina quanto na jurisprudência, o entendimento no sentido da tipicidade do crime de estelionato quanto aos golpes e fraudes praticados através da informática, como, por exemplo, através do envio de mensagens eletrônicas fraudulentas ou por meio da clonagem de páginas na Internet visando induzir a vítima a erro para obter vantagem econômica indevida.

Neste sentido, o Tribunal de Justiça de Minas Gerais, ao julgar a apelação criminal nº 1.0024.02.875258-2, manteve a decisão de primeira instância que condenou um estelionatário por utilizar um *site* gratuito na Internet com o nome de fantasia de uma determinada empresa, sem a sua autorização, para induzir as pessoas em erro e obter vantagem econômica indevida mediante falsa promessa de emprego no exterior.

Assim, também comete o crime de estelionato o agente que cria página na Internet ou faz anúncios por intermédio de *sites* como o Mercado Livre, por exemplo, simulando a venda de produtos com o objetivo de induzir a vítima em erro ao efetuar o pagamento antecipado da suposta mercadoria na ilusão de que está efetuando a sua compra e que irá recebê-la posteriormente, quando, na realidade, trata-se de um golpe utilizado pelo agente para obter vantagem econômica indevida, aproveitando-se da boa-fé das pessoas para enganá-las e acarretar prejuízo ao patrimônio destas.

IX. CRIMES CONTRA A PROPRIEDADE INTELECTUAL

Dentre os crimes contra a propriedade intelectual que podem ser cometidos através da informática estão o crime de violação de direito autoral previsto no art. 184 do CP e o crime de violação de direito de autor de programa de

computador, sendo este último previsto em lei específica (art. 12 da Lei nº 9.609, de 18 de fevereiro de 1998).

A. *Violação de direito autoral*

O art. 184 do Código Penal tutela a proteção do direito autoral e os que lhe são conexos, sendo a pena de detenção, de três meses a um ano, ou multa.

O crime de violação de direito autoral previsto no art. 184 do CP é norma penal em branco, ou seja, a lei penal não define o que seja direito autoral tampouco o que seriam direitos conexos aos do autor, conseqüentemente ela precisa ser interpretada de acordo com a Lei nº 9.610/98, que é a lei de direitos autorais vigente no país.

Trata-se de crime comum quanto ao sujeito, podendo ser praticado por qualquer pessoa que viole direito autoral de outrem. Podem ser vítimas do crime de violação de direito autoral, o autor ou o terceiro titular do direito autoral e ainda o titular de direito conexo tais como o artista intérprete ou executante, o produtor fonográfico e empresa de radiodifusão.

A violação de direito autoral prevista no art. 184 do CP pode ser praticada através do ciberespaço, como, por exemplo, quando o agente publica obra intelectual na Internet sem citar o nome do autor e sem possuir expressa autorização para sua reprodução ou para modificar o conteúdo da obra intelectual.

B. *Violação de direito de autor de programa de computador*

Em se tratando de violação ao direito de autor de programa de computador, aplica-se o art. 12 da Lei nº 9.609/98, que tipifica como crime "violar direito de autor de programa de computador", com pena de detenção de seis meses a dois anos ou multa, não sendo aplicável o art. 184 do Código Penal, em razão da incidência do princípio da especialidade.

Neste sentido, o Tribunal de Justiça de Minas Gerais, ao julgar a apelação criminal nº 1.0145.02.005603-5/001, reconheceu a impossibilidade de aplicação do art. 184 do CP em relação à violação de direito de autor de programa de computador, entendendo ser aplicável, em virtude do princípio da especialidade, o disposto no art. 12 da Lei 9.609/98.

A violação de direito de autor de programa de computador pode ocorrer mediante o uso da informática, quando um *cracker* utiliza os seus conhecimentos técnicos e altera o programa de computador para modificar sua funcionalidade.

Também pode ocorrer através da Internet, quando um usuário disponibiliza página virtual que permite realizar o *download* de softwares proprietários, fornecendo número de série ou senha de acesso que permite ao internauta utilizar os programas sem que tenha que adquirir sua respectiva licença.

X. Crime contra o Sentimento Religioso

A doutrina admite a possibilidade de prática de crime contra o sentimento religioso através da informática no tocante ao disposto no art. 208 do CP, o qual prevê o crime de escárnio por motivo de religião: "escarnecer de alguém publicamente, por motivo de crença ou função religiosa; impedir ou perturbar cerimônia ou prática de culto religioso; vilipendiar publicamente ato ou objeto de culto religioso", sendo a pena de detenção, de um mês a um ano, ou multa.

Trata-se de delito de ação múltipla que pode ser cometido tanto pelo escárnio por motivo de religião, pelo impedimento ou perturbação da cerimônia ou prática de culto religioso ou pelo vilipêndio público de ato ou objeto de culto religioso.

Dentre estas modalidades, é admissível a prática do crime de escárnio por motivo de religião pela Internet, desde que cometida em ambiente virtual dotado de certa publicidade, como, por exemplo, em listas de grupos de discussão por e-mail ou em comunidades virtuais como o *Orkut*, onde o agente escarnece de alguém em razão de sua crença religiosa.

XI. Crimes contra os Costumes

Em relação aos crimes contra os costumes previstos no Código Penal, há três tipos penais que, *a priori*, poderiam ser cometidos através da Internet: o favorecimento da prostituição que atenta contra a moralidade pública sexual; o ato obsceno e o escrito ou objeto obsceno os quais tutelam o pudor público.

A. *Favorecimento da prostituição*

O crime de favorecimento da prostituição está previsto no art. 228 do CP e consiste na conduta de induzir ou atrair alguém à prostituição, facilitá-la ou impedir que alguém a abandone, com pena de reclusão, de dois a cinco anos.

Trata-se de um crime de ação múltipla que contempla as condutas de induzir ou atrair à prostituição, facilitar a sua prática ou impedir que alguém a abandone. Somente as duas primeiras condutas podem ser praticadas pela Internet.

Em relação à conduta de induzir, o crime pode ocorrer, por exemplo, quando o agente mantém conversa com a vítima através da Internet, convencendo-a a se prostituir.

Quanto à modalidade de facilitar, o delito pode acontecer quando o indivíduo publica página virtual na Internet, intermediando e facilitando a prática da prostituição, pois "inúmeras são as home pages que oferecem serviços de acompanhantes sexuais em troca de pagamento, facilitando, a partir do oferecimento de material fotográfico e de telefones de contato, a prática da prostituição". [9]

B. *Ato obsceno*

O crime de ato obsceno está tipificado no art. 233 do CP e consiste na conduta de praticar ato obsceno em lugar público, ou aberto ou exposto ao público, com pena de detenção, de três meses a um ano, ou multa.

O ato obsceno pode ser praticado através da Internet, considerando-se a rede mundial de computadores como espaço virtual aberto ao público. Neste sentido, "algumas pessoas chegam a instalar câmeras dentro de suas casas e transmitem, em tempo real, cenas de sexo. (...). Tal conduta constitui ato obsceno, uma vez que qualquer pessoa pode acessar a página e ver as cenas". [14]

C. *Escrito ou objeto obsceno*

O crime de escrito ou objeto obsceno está tipificado no art. 234 do CP e consiste em "fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou

de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno", sendo a pena aplicável de seis meses a dois anos, ou multa.

O crime de objeto obsceno, embora esteja previsto em lei com cominação de pena, não deverá ser aplicável a estas condutas que forem praticadas na Internet, pois consiste em um delito que é tolerado pelo poder público por não mais ofender o pudor público como na época em que foi tipificado.

Assim, "trata-se de um tipo penal alheio à realidade mundial, cego diante do panorama que se apresenta. Caso fosse aplicado, 90% dos proprietários de bancas de revistas estariam atrás das grades. É reflexo da moralidade exigida na década de 40, desprovido de qualquer interesse jurídico-penal". [9]

XII. Crimes contra a Paz Pública

Os crimes contra a paz pública que podem ser cometidos através da Internet são: a incitação ao crime, a apologia de crime ou criminoso e a formação de quadrilha.

A. *Incitação ao crime*

A incitação ao crime está prevista como delito no art. 286 do CP e consiste na conduta de "incitar, publicamente, a prática de crime", sendo a pena de detenção, de três a seis meses, ou multa. Assim, trata-se de crime de menor potencial ofensivo, que pode ser praticado por qualquer pessoa e que tem como sujeito passivo a coletividade.

É um delito formal que se consuma com a incitação pública da prática de um crime determinado, sendo desnecessário que alguém cometa o crime objeto da incitação para que haja a sua perfeita caracterização, é crime doloso que não admite a modalidade culposa e pode ser cometido através da rede mundial de computadores, sendo comum sua prática no *Orkut*, onde o agente cria comunidade virtual para induzir e estimular as pessoas a praticarem uma conduta definida como crime.

O Superior Tribunal de Justiça, ao decidir o conflito de competência nº 62949/PR, concluiu que em se tratando de divulgação na Internet de técnica de cultivo de planta destinada à preparação de substância entorpecente por hospedeiro estrangeiro e tendo a ação de incitar sido desenvolvida dentro do território nacional, é competente a justiça estadual, e não a federal, para julgar o feito.

B. *Apologia de crime ou criminoso*

A apologia de crime ou criminoso está prevista no art. 287 do CP e consiste em fazer, publicamente, apologia de fato criminoso ou de autor de crime, sendo a pena aplicável para este delito de detenção, de três a seis meses, ou multa.

É um delito formal, de menor potencial ofensivo, comum quanto ao sujeito, sendo vítima a coletividade, doloso e não há tipo culposo, podendo ser praticado por meio da internet.

Neste sentido, "como na incitação ao crime, aqui também é necessária a publicidade. Desta forma, este crime pode ser praticado através de sites, homepages ou nas salas de conversas. A utilização de e-mail não é possível, pois falta a publicidade exigida no tipo penal." [14]

C. *Formação de quadrilha*

O art. 288 do CP tipifica o crime de formação de quadrilha que consiste em "associarem-se mais de três pessoas, em quadrilha ou bando, para o fim de cometer crimes", sendo a pena de reclusão, de um a três anos. Trata-se de crime que não é contemplado pelos benefícios da lei dos juizados especiais eis que a pena cominada é superior a dois anos; sendo a pena duplicada se a quadrilha ou bando é armado.

O crime de formação de quadrilha pode ser cometido através da Internet, pois a associação de mais de três pessoas para a prática de crimes informáticos pode ser realizada através do próprio ambiente virtual, sendo desnecessária a presença física, basta que estejam reunidos com o intuito de se associarem para cometer delitos de forma reiterada.

Em 2007, o Tribunal de Justiça de Santa Catarina denegou o pedido de *habeas corpus* nº 2006.046877-4, mantendo a prisão preventiva de um dos pacientes acusados por formação de quadrilha e pela prática de crimes na Internet, envolvendo onze denunciados, baseando-se a sentença na necessária prisão do acusado para a garantia da ordem pública já que este havia reiterado a prática dos mesmos delitos inclusive após a obtenção de outro *habeas corpus* que foi concedido e que o tinha posto em liberdade.

XIII. Crime contra a Fé Pública

Dentre os crimes contra a fé pública, tem-se o delito de falsa identidade o qual pode ser cometido através da informática.

Este crime está previsto no art. 307 do CP e consiste em "atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem", com pena de detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

Trata-se de delito formal, o termo "para" contido no tipo penal foi utilizado para determinar o dolo do agente, ou seja, para que a conduta de atribuir a si ou a terceiro uma falsa identidade seja punida é necessário que o agente tenha a intenção de obter vantagem para si ou para outrem ou que tenha a intenção de causar danos a terceiros.

É um crime de menor potencial ofensivo, sendo cabíveis os benefícios da transação penal e da suspensão condicional do processo, desde que o fato não constitua elemento de crime mais grave com pena máxima superior a dois anos.

A falsa identidade pode ser cometida através da Internet, quando, por exemplo, o agente registra uma conta gratuita de e-mail com dados pessoais de outra pessoa como se fossem suas informações e, a seguir, manda mensagem eletrônica para outra pessoa se identificando com a falsa identidade, ou ainda quando o agente se cadastra em comunidades virtuais como o *Orkut* utilizando o nome e a foto de determinada pessoa com o objetivo de, em ambos os casos, obter vantagem indevida para si ou para outrem ou para causar dano.

XIV. Crimes contra a Administração Pública

Dentre os crimes contra a Administração Pública que podem ser cometidos mediante o uso da informática, destacam-se a

inserção de dados falsos em sistemas de informações, a modificação não autorizada de sistemas de informação ou programa de informática e o crime de concussão.

A. *Inserção de dados falsos em sistemas de informações*

De acordo com o art. 313-A do Código Penal, considera-se crime de inserção de dados falsos em sistemas de informações 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", sendo aplicável pena de reclusão, de dois a doze anos, e multa.

Quando o funcionário autorizado insere dados falsos no sistema de informações da Administração Pública com a consciência de que tais dados são falsos e com a vontade de realizar esta ação para obter vantagem para si ou para outrem ou para causar dano, o crime se consuma a partir do momento em que os dados falsos foram inseridos no sistema de informações, independentemente da obtenção de vantagem ou do dano causado em decorrência da prática do crime. [15]

B. *Modificação ou alteração não autorizada de sistema de informações*

O crime de modificação ou alteração não autorizada de sistemas de informações está tipificado no art. 313-B do CP e consiste na conduta de "modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação da autoridade competente", com pena de detenção de três meses a dois anos, e multa.

O art. 327, *caput*, do Código Penal estabelece que, para efeitos penais, considera-se funcionário público quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública; sendo que o §1º deste artigo determina que se equipara a funcionário público quem exerce cargo, emprego ou função pública, em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública.

Diferentemente do artigo anterior (art. 313-A) que exige que o funcionário público seja autorizado pela Administração Pública para operar o sistema, o crime do art. 313-B pode ser praticado por qualquer funcionário desde que a modificação ou alteração do sistema de informações ou do programa de computador não tenha sido autorizada nem solicitada pela autoridade competente. [15]

C. *Concussão*

O crime de concussão está previsto no art. 316 do CP, e consiste na conduta de "exigir, para si ou para outrem, direta ou indiretamente, ainda que fora da função ou antes de assumi-la, mas em razão dela, vantagem indevida", com pena de reclusão de dois a oito anos, e multa.

Em 2007, o STJ denegou o pedido de *habeas corpus* nº 83188/PA de um investigador da política militar acusado de concussão e por fazer parte de um grupo criminoso voltado para a prática de ilícitos contra a Caixa Econômica Federal e outras instituições bancárias, que realizava transferências de valores de correntistas por meio da Internet.

XV. Crimes contra a Criança e o Adolescente

A Lei nº 8.069, de 13 de julho de 1990, dispõe sobre o Estatuto da Criança e do Adolescente (ECA) e tipifica em seu art. 241 o crime de pedofilia ou pornografia infantil.

Em sua redação original, o art. 241 do ECA dispunha que constitui crime: "fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente", com pena de reclusão de um a quatro anos.

Este artigo foi alterado pela Lei nº 10.764/2003 que lhe deu nova redação, ampliando a aplicação da referida norma penal: "apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente", sendo a pena de dois a seis anos, e multa.

Na mesma pena incorre quem: I - agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo; II - assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo; III - assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo.

Não há a menor dúvida quanto à aplicação do art. 241 do ECA ao crime de pornografia infantil cometido através da Internet, haja vista a previsão expressa no tipo penal quanto ao seu alcance. Além disso, mesmo antes da entrada em vigor da Lei nº 10.764/2003 que deu nova redação ao art. 241 do ECA, o STF já havia se pronunciado sobre a tipicidade desta conduta criminosa, ainda que praticada através da Internet, ao julgar o *habeas corpus* nº 76689/PB, ante a publicação de cena de sexo infanto-juvenil na rede mundial de computadores.

XVI. Crimes contra a Segurança nacional

A Lei nº 7.170, de 14 de dezembro de 1983 define os crimes contra a segurança nacional e a ordem política e social, dentre os quais, podem ser praticados através da Internet, por exemplo, os delitos previstos nos artigos 22 e 23 desta lei.

A. *Propaganda ofensiva à segurança nacional e à ordem política e social*

Constitui crime previsto no art. 22 da Lei nº 7.170/83, a conduta de fazer, em público, propaganda: "I - de processos violentos ou ilegais para alteração da ordem política ou social; II - de discriminação racial, de luta pela violência entre as classes sociais, de perseguição religiosa; III - de guerra; IV - de qualquer dos crimes previstos nesta lei", sendo a pena de detenção de um a quatro anos.

A pena deste crime é aumentada de um terço quando a propaganda for feita em local de trabalho ou por meio de rádio ou televisão. Tal penalidade também é aplicada a quem distribui ou redistribui: a) fundos destinados a realizar a propaganda de que trata este artigo; b) ostensiva ou clandestinamente boletins ou panfletos contendo a mesma

propaganda. Por sua vez, estabelece a Lei nº 7.170/83 que não constitui propaganda criminosa a exposição, a crítica ou o debate de quaisquer doutrinas.

Trata-se de um crime que pode ser praticado através da Internet, devendo a propaganda ser realizada em espaço público para que haja a consumação do delito, não se admitindo a sua prática pelo envio de correspondência eletrônica individualizada.

Salienta a doutrina que "em relação à discriminação racial não se aplica esta lei e, sim a Lei nº 7.716/89, pois além de ser especial é posterior. Assim, diante de uma propaganda na Internet sobre racismo deve ser aplicada a lei contra o preconceito de raça e cor". [14]

B. Incitação à subversão da ordem política ou social

Outro crime previsto na lei que define os crimes contra a segurança nacional, é o delito de incitação contido no art. 23 que pune as condutas de incitar: "I - à subversão da ordem política ou social; II - à animosidade entre as Forças Armadas ou entre estas e as classes sociais ou as instituições civis; III - à luta com violência entre as classes sociais; IV - à prática de qualquer dos crimes previstos nesta lei", sendo cominada também pena de reclusão de um a quatro anos.

Assim como a incitação ao crime, prevista no art. 286 do CP, pode ser praticada através da Internet, da mesma forma, tem-se que a incitação aos crimes previstos na Lei nº 7.170/83 pode ser cometida por meio da rede mundial de computadores.

Caso a incitação esteja relacionada a atos de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, será aplicável o art. 20 da Lei nº 7.716/89 o qual prescreve pena de reclusão, de um a três anos e multa.

XVII. Crimes contra a Propriedade Industrial

A Lei nº 9.279, de 14 de maio de 1996 dispõe sobre os crimes contra a propriedade industrial, dentre eles, os crimes de concorrência desleal, tipificados no art. 195 desta lei, dentre os quais, por exemplo, a conduta criminosa descrita no inciso primeiro, cometendo o delito quem "publica, por qualquer meio, falsa afirmação, em detrimento de concorrente, com o fim de obter vantagem", sendo a pena de detenção, de três meses a um ano, ou multa.

Desta forma, uma vez que o tipo penal permite a publicação por qualquer meio de informação falsa em detrimento do concorrente, o crime de concorrência desleal pode ser praticado, por exemplo, através da publicação de uma falsa afirmação em *sites* da Internet que tenham a finalidade de obter vantagem em detrimento do concorrente.

O mesmo se pode dizer, por exemplo, quanto ao inciso II no que concerne à conduta de quem "presta ou divulga, acerca de concorrente, falsa informação, com o fim de obter vantagem", tal divulgação pode ocorrer pela Internet, através do e-mail.

XVIII. Crimes contra a Saúde Pública

A Lei nº 11.343, de 23 de agosto de 2006, instituiu o Sistema Nacional de Políticas Públicas sobre Drogas – SISNAD, e, dentre outras coisas, tipificou como crime, em seu art. 33, a conduta de "importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor à venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar", sendo a pena de reclusão de cinco a quinze anos e pagamento de quinhentos a mil e quinhentos dias-multa.

Trata-se de um crime que pode ser cometido por meio da rede mundial de computadores, por exemplo, principalmente no que concerne à conduta de oferecer, na hipótese do traficante enviar mensagens eletrônicas oferecendo drogas a terceiros, ou ainda, através de sua oferta ou comercialização através de páginas da Internet.

Há ainda o parágrafo segundo deste artigo o qual prevê como crime a conduta de "induzir, instigar ou auxiliar alguém ao uso indevido de droga", com pena de detenção, de um a três anos, e multa de cem a trezentos dias-multa.

De igual modo, quanto a esta norma penal específica, admite-se a possibilidade de sua consumação através da Internet, caracterizando-se como crime informático impuro.

XIX. Crime de Lavagem de Dinheiro

A Lei nº 9.613, de 03 de março de 1998, dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores, os quais estão previstos no art. 1º desta lei.

Constitui crime de lavagem de dinheiro a conduta de ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de crime de tráfico ilícito de substâncias entorpecentes; de terrorismo; de contrabando; de extorsão mediante seqüestro; contra a Administração Pública; contra o sistema financeiro nacional; praticado por organização criminosa ou praticado por particular contra a administração pública estrangeira; sendo a pena de reclusão de três a dez anos e multa.

Os crimes de lavagem de dinheiro podem ser praticados por qualquer pessoa, independente de ser ou não o mesmo autor dos crimes anteriores previstos no artigo primeiro. Além disso, são crimes de mera conduta, sendo suficiente que o indivíduo pratique a conduta descrita na norma penal para que haja a sua consumação; podendo ser cometidos através da Internet. Assim, "a informática pode ser utilizada para ocultar a procedência e a localização do dinheiro através de sucessivas transferências feitas em Home Bank, ou seja, na Internet" [14]

XX. Crimes Eleitorais

Há diversas leis vigentes que definem crimes eleitorais. Dentre elas, destacam-se, por exemplo, o Código Eleitoral (Lei nº 4.737/65), a Lei nº 6.996/82 e a Lei nº 9.504/97.

O art. 299 do Código Eleitoral tipifica como crime: "dar, oferecer, prometer, solicitar ou receber, para si ou para outrem, dinheiro, dádiva, ou qualquer outra vantagem, para obter ou dar voto e para conseguir ou prometer abstenção, ainda que a oferta não seja aceita", com pena de reclusão até

quatro anos e pagamento de cinco a quinze dias-multa.

Trata-se de um delito que pode ser cometido através da rede mundial de computadores, como, por exemplo, mediante a oferta encaminhada por mensagem eletrônica ao eleitor, oferecendo a este dinheiro pelo voto em um determinado candidato. Além do sujeito que faz a oferta, também responde pelo crime o eleitor que solicita qualquer vantagem em troca de seu voto, ainda que esta não seja aceita.

Quanto à conduta de alterar resultados no processamento eletrônico das cédulas eleitorais, a Lei nº 6.996/82 dispõe sobre a utilização de processamento eletrônico de dados nos serviços eleitorais, e prevê em seu art. 15 que "incorrerá nas penas do art. 315 do Código Eleitoral quem, no processamento eletrônico das cédulas, alterar resultados, qualquer que seja o método utilizado", ou seja, comina pena de reclusão até cinco anos e pagamento de 5 a 15 dias-multa.

A Lei nº 9.100/95, em seu art. 67, VII, passou a dispor sobre o crime de acesso indevido ao sistema informático eleitoral para alterar o resultado das eleições, nos seguintes termos: "obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos", a pena cominada era de reclusão, de um a dois anos, e multa.

Entretanto, a Lei nº 9.504/97 revogou tacitamente este artigo, em parte, em seu art. 72, inciso primeiro, ao tipificar a conduta de "obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos", com pena de reclusão de cinco a dez anos, sendo o art. 67, inc. VII da Lei nº 9.100/95 aplicável somente aos casos de tentativa previstos nesta lei. [7]

Também constitui crime eleitoral, segundo o art. 72, inciso segundo, da Lei nº 9.504/97, a conduta 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", sendo aplicável a este a mesma pena do inciso primeiro.

XXI. Crimes contra a Relação de Consumo

A Lei nº 8.078, de 11 de setembro de 1990, conhecida como Código de Defesa do Consumidor (CDC), tipifica alguns crimes contra as relações de consumo os quais podem ser cometidos através da Internet, conforme serão examinados.

O art. 63 do CDC define como crime a conduta de "omitir dizeres ou sinais ostensivos sobre a nocividade ou periculosidade de produtos, nas embalagens, nos invólucros, recipientes ou publicidade", sendo a pena de detenção de seis meses a dois anos e multa. Assim, trata-se de um delito que pode ser cometido pela Internet, por exemplo, através da promoção de publicidade de um produto em página virtual, omitindo informação sobre a sua nocividade.

Além da omissão de informação sobre a nocividade do produto, o art. 66 do CDC também pode ser aplicável para responsabilizar penalmente o fornecedor que, em página virtual de sua empresa, faz afirmação falsa ou enganosa ou omite informação relevante sobre a natureza, característica, qualidade, quantidade, segurança, desempenho, durabilidade, preço ou garantia de produtos ou serviços, sendo a pena de detenção de três meses a um ano e multa. Também incorre nesta mesma pena quem patrocinar a oferta.

Em relação à promoção de publicidade enganosa ou abusiva na Internet, o sujeito poderá incorrer no crime do art. 67 do CDC, com pena de detenção de três meses a um ano e multa; no caso da publicidade ser suscetível de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança, poderá incidir o art. 68 do CDC que prescreve pena de detenção de seis meses a dois anos e multa.

Nada impede que a Internet seja também utilizada como um meio para praticar o crime do art. 71 do CDC o qual consiste em "utilizar, na cobrança de dívidas, de ameaça, coação, constrangimento físico ou moral, afirmações falsas, incorretas ou enganosas ou de qualquer outro procedimento que exponha o consumidor, injustificadamente, a ridículo ou interfira com seu trabalho, descanso e lazer", com pena de detenção de três meses a um ano e multa.

Quanto às informações do consumidor que constem em bancos de dados informáticos, admite-se a incidência do art. 72 do CDC que define como crime a conduta de "impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, bancos de dados, fichas e registros", com pena de detenção de seis meses a um ano ou multa.

XXII. Considerações sobre o Projeto de Lei Substitutivo referente aos Delitos Informáticos

O Senador Eduardo Azeredo propôs um projeto de lei (PL) substitutivo ao PL nº 89/2003, de iniciativa do Deputado Luiz Piauhylino, ao projeto de Lei nº 137/2000, de autoria do Senador Leomar Quintanilha, e ao PL nº 76/2000, de autoria do Senador Renan Calheiros, todos sobre crimes informáticos.

Considera-se importante examinar, ainda que sucintamente, algumas das propostas legislativas relacionadas com os crimes cibernéticos, pois, conforme foi possível observar ao longo deste estudo, as normas penais em vigor nem sempre conseguem tutelar de forma adequada os bens jurídicos que se dispôs a proteger, bem como novos bem jurídicos passam a necessitar de proteção especial nesta era da informação.

Em relação aos crimes contra a honra, o projeto agrega o art. 141-A no capítulo V, do título I, da parte especial do Código Penal, estabelecendo que "as penas neste Capítulo aumentam-se de dois terços caso os crimes sejam cometidos por intermédio de rede de computadores, dispositivo de comunicação ou sistema informatizado".

Já em relação aos crimes contra o patrimônio, será inserido o inciso V no §4º do art. 155 do CP, para definir como furto qualificado o crime cometido "mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares". Por sua vez, também há a pretensão de tipificar como crime a difusão de código malicioso, que será típico, salvo quando for cometido para fins de defesa digital. Além

disso, o projeto irá garantir de vez a tutela penal do dano informático ao equipará-lo a 'coisa' para fins penais.

No que concerne à defesa digital, para efeitos penais, ela é definida como a "manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação".

O projeto pretende ampliar o âmbito da incidência dos artigos 265 e 266 do CP, tipificando o atentado contra a segurança de serviços de informação e a interrupção ou perturbação destes serviços e dos já definidos no tipo penal.

A falsificação de cartão de crédito ou dispositivo eletrônico similar será acrescida no parágrafo único do art. 298 do CP, equiparando o cartão de crédito a documento particular. Será tipificado no art. 298-A do CP o crime de falsificação de telefone celular ou meio de acesso à rede de computadores, com pena de reclusão de um a cinco anos e multa.

Especificamente no que concerne aos crimes contra a rede de computadores, dispositivo de comunicação ou sistema informático, o projeto insere novos tipos penais no capítulo VI-A no título I, parte especial do Código Penal, que passa a considerar como crime: a) o acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado; b) a obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica, digital ou similar; e c) a divulgação ou utilização indevida de informações contidas em bancos de dados.

O crime de acesso não autorizado à rede de computadores será acrescido no art. 154-A, com pena de reclusão de dois a quatro anos e multa. Caracteriza-se como um crime de mera conduta, sendo suficiente que o sujeito pratique o acesso ao computador sem autorização para que haja a consumação do delito. Entretanto há previsão no §4º deste artigo de que não haverá crime quando o agente acessa a título de defesa digital, excetuando o desvio de finalidade ou o excesso.

Já o art. 154-B a ser inserido no CP, define como crime a conduta de "obter dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida", com pena de detenção de dois a quatro anos e multa.

Por fim, o crime do art. 154-D do CP consistirá na divulgação ou utilização de informações contidas em banco de dados com finalidade distinta da que motivou o seu registro, incluindo informações referentes a dados pessoais. A pena prevista para este delito será de detenção de um a dois anos e multa.

XXIII. Conclusão

Através do presente estudo se constatou a possibilidade de aplicação da lei penal vigente aos crimes informáticos, principalmente quando a conduta praticada está descrita na norma penal, ainda que o meio utilizado seja a Internet.

Por outro lado, verificou-se que o velho Código Penal de 1940 vigente não é suficiente para resolver todas as questões, mormente em se tratando de condutas ilícitas que atentem contra os dados informáticos e sistemas informatizados.

Constata-se que o direito penal ainda não está totalmente preparado para lidar com os crimes cibernéticos, porém se percebe um esforço tanto por parte da doutrina quanto da jurisprudência em consolidar entendimento jurídico acerca das questões controvertidas que foram apresentadas e suscitadas.

A relevância deste estudo consiste justamente em ajudar a esclarecer os limites e o alcance de diversas leis penais aplicáveis aos delitos informáticos, bem como conhecer as propostas legislativas referentes à matéria, para que a sociedade saiba com maior exatidão quais são as condutas criminosas que devem ser coibidas, bem como as penas cominadas em relação a um determinado delito cometido mediante o uso da informática ou contra tais sistemas.

Referências

[1] TRUZZI, G.; DAOUN, A. "Crimes informáticos: o direito penal na era da informação". In: *Proceedings of the Second International Conference of Forensic Computer Science*. Guarujá (SP), ABEAT, 2007. pp. 115-120.

[2] CAPEZ, F. *Curso de Direito Penal*: parte geral. v.1. 7.ed. São Paulo: Saraiva, 2004. 563 p.

[3] GOMES, L. F. "Atualidades criminais". In: *Instituto Brasileiro de Ciências Criminais*. Disponível em: <http://www.direitocriminal.com.br>. Acesso em: 12 jan. 2008.

[4] FERREIRA, I. S. "A criminalidade informática". In: LUCCA, N. de; SIMÃO FILHO, A. (Org.). *Direito e Internet*: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

[5] CASTRO, A. A. "A internet e os tipos penais que reclamam ação criminosa em público". In: *Revista de Direito Eletrônico*. Petrópolis: IBDE, v. 1, n. 3, 2003. pp. 41-51. ISSN – 1679-1045. Disponível em: <http://www.ibde.org.br/index_arquivos/rede3.pdf>. Acesso em: 29 jan. 2008.

[6] ATHENIENSE, A. *Parecer sobre o Projeto de Lei do Senado nº 76/2000*. Disponível em: <http://www.oab.org.br>. Acesso em: 25 jan. 2008.

[7] VIANNA, T. L. *Fundamentos do Direito Penal Informático*: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003. 170 p.

[8] VIANNA, T. L. "Dos crimes por computador". In: *Revista dos Tribunais*. Ano. 91. v. 801. jul. 2002. São Paulo: RT, 2002. pp. 405-421.

[9] OLIVEIRA, F. C. M. de. *Criminalidade Informática*. Dissertação. Mestrado em Ciências Criminais. Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre: PUC/RS, 2002. 160 p.

[10] VIANNA, T. L. "Dos crimes pela internet". In: Reinaldo Filho, D. (Org.). *Direito da Informática*: temas polêmicos. Bauru: Edipro, 2002, p. 211-224.

[11] PINHEIRO, P. P. *Direito Digital*. 2.ed. Sâo Paulo: Saraiva, 2007. 407p.

[12] ALBUQUERQUE, R. C. de. *A criminalidade informática*. São Paulo: Juarez de Oliveira, 2006. 241 p.

[13] RODRIGUES, J. da S. "Aspectos Práticos dos Crimes Informáticos". In: BLUM, R. M. S. O.; BRUNO, M. G. da S.; ABRUSIO, J. C. (Org.). *Manual de Direito Eletrônico e Internet*. São Paulo: Lex Editora, 2006. pp. 85-98.

[14] CASTRO, C. R. A. de. *Crimes de Informática e seus Aspectos Processuais*. 2.ed. rev., ampl. e atual. Rio de Janeiro: Lumen Juris, 2003. 230 p.

[15] RAMOS JÚNIOR, H. S. "Crimes contra a Segurança dos Sistemas de Informações da Administração Pública". In: *Proceedings of the Second International Conference of Forensic Computer Science*. Guarujá (SP), ABEAT, 2007. pp. 64-69.