ESCOLA DA MAGISTRATURA DO ESTADO DO RIO DE JANEIRO

Crimes pela Internet

Gustavo Fuscaldo Couri

Rio de Janeiro
2009

CRIMES PELA INTERNET

Gustavo Fuscaldo Couri

Graduado pela Faculdade de Direito
Candido Mendes – Centro. Pós-Graduado
em Direito do Consumidor pela FGV.

Resumo: A criação e a popularização da internet no Brasil e no mundo fizeram surgir novos crimes, como invasão de computadores, criação de comunidades virtuais para fazer apologia ao uso de drogas e envio de vírus de computador por e-mail. Isso sem falar nos crimes tradicionais que migraram sua execução do mundo real para o virtual, e que necessitam da necessária repressão estatal. A essência do trabalho é fazer um estudo sobre os crimes que vem sendo praticados pela internet, com o objetivo de ampliar o debate democrático sobre o tema.

Palavras-chave: Crime, Internet, Computador.

Sumário: Introdução. 1- A origem da questão com o surgimento da rede de computadores e dados. 2 – A Criminalidade no seio da Informática. 3 – O Crime Informático e suas formas. 3.1 – Computador como objeto. 3.2 – Computador como instrumento. 3.3 – Computador como incidental para outro crime. 3.4 – Computador é associado à prática do crime. 4- Crime Informático Puro e Impuro. 4.1 – Crimes Informáticos Puros. 4.1.A – Crimes Informáticos Puros com previsão legal. 4.1.B – Crimes informáticos Puros sem previsão legal. 4.2- Crimes Informáticos Impuros. 5- A problemática para a apuração da autoria do delito. 6- Sujeitos ativos dos delitos. 6.1- *Hackers*. 6.2- *Cracker*. 6.3 – *Pheakers*. 6.4– *Cardes*. 6.5 – *Cyberterrorists*. 7- Do tempo do crime. 8- Do lugar do crime. 9- As provas da materialidade. 10 – O bem jurídico tutelado. 11- Competência para julgamento. Conclusão. Referências.

INTRODUÇÃO

O trabalho apresentado aborda o tema dos crimes praticados pela internet, vale dizer, modalidade de crime informático, para tal faz se a distinção entre os vários crimes praticados em que o computador aparece, bem como a difícil conceituação, definição e alcance de seu estudo enquanto novo ramo do direito moderno.

Busca-se com o presente trabalho aclarar os operadores do direito estudando minuciosamente as distinções entre os crimes já existentes e as novas condutas praticadas em decorrência do avanço tecnológico.

Bem como, evidenciar que muitos dos crimes praticados pela internet guardam perfeita subsunção com tipos penais clássicos.

Além disso, as modalidades delitivas tradicionais existentes antes da aparição do computador e agora realizadas por meio de sua utilização incrementaram as taxas de aumento da criminalidade com rapidez e impunidade.

Objetiva-se consolidar entendimento sobre o palpitante tema na difícil conceituação de termos tecnológicos sem engessar-lhes a idéia ao ponto de tornarem-se obsoletos com o avanço e o implemento de novas tecnologias.

Ao longo do artigo, serão analisados: a origem da questão com o advento da rede mundial de computadores, a relação gênero/espécie em relação aos crimes informáticos, a distinção entre as formas de execução dos crimes informáticos, a problemática da apuração da

autoria e do momento e local da consumação, os sujeitos ativos do delito, e os meios de prova e apuração do crime.

.

Essa é a proposta do presente trabalho, estimular a reflexão sobre a velocidade da evolução tecnológica, estudando as peculiaridades dessas condutas perpetradas no espaço virtual, bem como sobre o que pode ser feito, sobre o ponto de vista legal, para proteger os bens ameaçados.

1- A ORIGEM DA QUESTÃO COM O SURGIMENTO DA REDE DE COMPUTADORES E DADOS

Segundo o *site* *Wikipedia* durante a Guerra-Fria o governo norte-americano desenvolveu um sistema para que seus computadores militares pudessem trocar informações, de uma base militar para outra de forma segura. A ARPANET, projeto iniciado pelo Departamento de Defesa dos Estados Unidos, realizou essa interconexão de computadores, por meio de um sistema conhecido como comutação de pacotes; consistente em uma transmissão de dados em rede no qual as informações são divididas em pequenos pacotes, remontados quando recebidos pelo seu destinatário.

O êxito da ARPANET o popularizou e a rede se estendeu para a área de pesquisas científicas das universidades. Com o aumento do volume de informação, a ARPANET começou a ter dificuldades operacionais. Então este sistema foi dividido em dois grupos a MILNET, que servia às atividades militares, e a nova ARPANET, que servia para as atividades não militares. O desenvolvimento da rede, nesse ambiente mais livre, pôde então acontecer.

Nesse cenário foi estruturado um esquema técnico denominado Protocolo de Internet, que recebeu a sigla IP, e permitiu o tráfego de informações fosse caminhado de uma rede para outra de qualquer parte do planeta com acesso a informações e todo tipo de transferência de dados.

Assim, passou a ocorrer a comunicação entre um conglomerado de redes em escala mundial de milhões de computadores interligados pelo Protocolo de Internet.

O surgimento da rede mundial de computadores facilitou ao extremo o relacionamento entre pessoas, físicas e jurídicas, no uso comercial ou pessoal.

Atualmente os métodos de entrada na rede se diversificaram, sendo possível no âmbito doméstico obter acesso com conexão discada, por banda larga por cabos, ou rádio sem fio; o uso móvel por meio de satélite ou telefones celulares; e por fim, o ingresso em locais públicos como bibliotecas, *cyber-cafés,* aeroportos, etc.

2 – A CRIMINALIDADE NO SEIO DA INFORMÁTICA

A criminalidade informática, assim como o fenômeno da informatização global, apresentam as mesmas características, qual sejam, a transnacionalidade, a universalidade e a ubiquidade. Isso porque, todos os países fazem uso da informática independentemente do seu estágio econômico, social ou cultural, bem como todas as pessoas de qualquer plano econômico, social ou cultural têm acesso aos produtos informatizados; sendo certo que a informatização está presente em todos os setores públicos e privados no planeta.

Assim, a informática potencializa-se como a mais nova fonte de criminalidade, pois amplia a atuação delitiva possibilitando ilicitudes como estelionato, o racismo, a pedofilia e os crimes contra a honra; ou seja, seriam os crimes clássicos cometidos pelo uso de computador.

Ademais, além de ampliar o campo delitivo nos injustos penais clássicos, cria novos modos delitivos, como a utilização abusiva da informação armazenada, violação de segurança da informação, que seriam os crimes praticados contra os computadores e sistemas.

Todo avanço social vem acompanhado de ganhos e perdas, na sociedade da informação, não poderia ser diferente.

Outrossim, evidencia-se que os crimes praticados pela Internet são espécies de crimes informáticos, sendo certo, que a especialização se dá pelo uso da rede mundial de computadores, razão pela qual faz-se necessário a análise minuciosa dos crimes informáticos para a melhor compreensão sobre o tema.

3 – O CRIME INFORMÁTICO E SUAS FORMAS

O crime informático se distingue dos demais ante a peculiar presença do computador na prática delitiva, e segundo a doutrina capitaneada pela tese de FERREIRA (2007) pode ser classificado analisando a posição deste no delito.

3.1 – COMPUTADOR COMO OBJETO

São os crimes em que o computador é o alvo, tais como no crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação do conteúdo do banco de dados, furto de informação, furto de propriedade intelectual, vandalismo cibernético,

acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo de fora da empresa; cuja algumas condutas ainda não estão expressamente incluídas como típicas em nosso ordenamento jurídico. Vale dizer que nesta espécie se cuida de crime fim.

3.2 – COMPUTADOR COMO INSTRUMENTO

É espécie de crime no qual o computador é o instrumento para o delito, como no crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraudes de telecomunicações, divulgação ou exploração de pornografia.

Caso em que a internet também é ferramenta para a prática dos crimes, em suma, fala-se aqui dos crimes comuns em que o computador funciona apenas como meio.

3.3 – COMPUTADOR COMO INCIDENTAL PARA OUTRO CRIME

Não é propriamente um crime informático, mas o computador pode ser usado de forma secundária para a consumação de outro delito, como nos crimes contra a honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, registro de atividades do crime organizado.

3.4 – COMPUTADOR É ASSOCIADO À PRÁTICA DO CRIME

Trata-se de crime associado com o computador, como a pirataria de *software*, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas, comércio ilegal de equipamentos e programas.

4- CRIME INFORMÁTICO PURO E IMPURO

Além da classificação do crime informático quanto à forma, na lição de COSTA (2004) ainda podem-se distinguir, quanto à essência, em puros e impuros, sendo para ele os verdadeiros crimes informáticos somente os puros, pois os impuros são os crimes comuns realizados por meio do computador.

4.1 – CRIMES INFORMÁTICOS PUROS

Conforme se constata no ordenamento jurídico, os crimes informáticos puros estão divididos em os que já possuem previsão legal e os que ainda não possuem previsão legal específica.

4.1.A – CRIMES INFORMÁTICOS PUROS COM PREVISÃO LEGAL

Os crimes informáticos puros ocorrem quando o autor do fato age com o objetivo de atacar, de forma virtual ou física, sistemas, redes, programas e unidades de armazenamento de dados. Ainda é incipiente a legislação nesse sentido.

Nesse contexto temos como crime informático puro a interceptação de email, pois o art. 151 do Código Penal e o art. 10 da Lei 9296/96 prevê como ilícita a interceptação não autorizada de comunicação informática.

Igualmente ocorrendo com a interceptação de e-mail na modalidade comercial (art. 152 do CP, e art. 10º da Lei 9296/96).

Além disso, tem-se a divulgação de segredo (art. 153, §1º-A do CP), pois se constitui crime informático puro a divulgação sem justa causa, de informações sigilosas ou reservadas assim definidas em lei, contidas ou não nos sistemas de informação ou banco de dados da Administração Pública.

Do mesmo modo, a inserção de dados falsos em sistema de informações (art. 313-A do CP), no qual somente o funcionário público pode ser o sujeito ativo, sendo a administração pública o sujeito passivo. Há nesse delito quatro condutas típicas: inserir dados falsos; facilitar a inserção de dados falsos; alterar indevidamente dados corretos; excluir indevidamente dados corretos.

Em complementação ao tipo anterior tem-se a modificação ou alteração não autorizada de sistema de informação (art. 313-B do CP), no qual o sistema de informação ou o programa de informática deverá ser da Administração Pública.

Relacionado especificamente ao software há o crime de violação da proteção intelectual de programa de computador e sua comercialização (art. 12 da Lei 9.609/98), no qual a própria lei cuida do conceito de programa de computador, como sendo a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de

tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.

4.1.B – CRIMES INFORMÁTICOS PUROS SEM PREVISÃO LEGAL

Há ainda práticas ilícitas que ainda não possuem expressa tipificação penal, mas segundo COSTA (2004) o envio de vírus e o *e-mail bombing* encontram reprimenda no art. 163 do CP, pois configuram dano àqueles que o recebem. São os crimes clássicos cujo objeto é o computador. Assim como esses crimes, outros encontram dificuldade de subsunção em relação à alguns tipos penais clássicos por determinados operadores do direito.

Existem programas que registram as informações prestadas pelo usuário, bem como todos os cliques que ele faz num determinado sitio, prática essa normalmente utilizada por sítios comerciais, para que conheça, os gostos de seus clientes. O problema surge quando esses programas – chamados de *cookies* - passam a ser utilizados como espiões, ou sem controle e conhecimento do usuário, ou ainda, quando essas informações são vendidas a outras empresas sem o seu consentimento.

A diferença deste programa para o *spyware*, consiste no ato de que estes são plantados por um *website*, enquanto aqueles são introduzidos por um programa *freeware*, na verdade eles roubam as informações do computador do usuário. Normalmente o usuário instala o programa gratuito sem o conhecimento da existência do *spyware*.

Há também a prática de *spamming*, que consiste no envio de mensagens eletrônicas – em especial de natureza publicitária – não solicitadas pelo usuário, que sobrecarregam o

sistema de correio eletrônico e tempo de navegação, constitui-se como prática desleal e comércio incontrolado de informação.

O “cavalo de tróia” também é um programa espião e, uma vez instalado no computador, permite a apropriação de informações, arquivos e senhas do usuário. Normalmente o usuário recebe e-mail com um arquivo anexado e, quando abre esse arquivo, instala-se o cavalo de tróia no computador do mesmo. Na maioria das vezes, como estabelece BARROS (2007), tal programa ilícito vai possibilitar aos *cracker* o controle total de sua máquina. Poderá ver e copiar todos os arquivos do usuário, descobrir todas as senhas que ele digitar, formatar seu disco rígido, ver a sua tela e até mesmo ouvir a sua voz se o computador tiver um microfone instalado. É um verdadeiro procedimento de invasão informática.

Produzem danos semelhantes ao “cavalo de tróia” os *backdoors*, programas que podem ser abertos em razão de defeitos de fabricação ou falhas no projeto dos programas, o que pode ser acidental ou proposital.

Já os vírus, podem ser espalhados de diversas maneiras, a partir da instalação de programas de procedência duvidosa, com a utilização de disquetes ou CDs infectados, com a abertura de arquivos, entre outros. Os vírus podem destruir totalmente os programas e arquivos do computador, podendo exercer controle total sobre a máquina. Além do mais, o vírus pode permanecer encubado, reproduzindo e infectando outros computadores, até que um evento qualquer seja capaz de ativá-lo, o que normalmente ocorre em uma data específica.

Todas essas praticas e programas, por certo traduzem em dano àquele a que se destinem, mas a ausência de definição de legal, de seus conceitos e implicações, bem como a expressa sanção penal, geram dúvidas aos operadores do direito.

4.2- CRIMES INFORMÁTICOS IMPUROS

Enquanto os delitos impuros são aqueles em que o computador é utilizado como mero instrumento para se produzir a ofensa a outros bens juridicamente tutelados que não sejam exclusivamente do universo informático, tais como: os crimes contra a honra (arts. 138, 139 e 140 do CP); crime de ameaça (art. 147 do CP); furto (art. 155 do CP); apropriação indébita (art. 168 do CP); violação de direito autoral (art. 184 do CP); escárnio por motivo de religião (art. 208 do CP); favorecimento da prostituição (art. 228 do CP); ato obsceno (art. 233 do CP); escrito ou objeto obsceno (art. 234 do CP); incitação ao crime (art. 286 do CP); apologia de crime ou criminoso (art. 287 do CP); jogos de azar (art. 50 da LCP e art. 75 da Lei 9.615/98); entre outros.

Há ainda os crimes informáticos impuros com previsão legal em que se admite a sua prática por meio da internet, são eles: estelionato (art. 171 do CP); pedofilia (art. 241 da Lei 8.069/90); crime de divulgação do nazismo (art. 20º §2º. da Lei 7.716/89); entre outros.

5- A PROBLEMÁTICA PARA A APURAÇÃO DA AUTORIA DO DELITO

A garantia à liberdade de expressão e de comunicação pode-se dizer que é como uma expressão da própria liberdade do homem e direito fundamental seu.

Por outro lado, o anonimato é o ato de não ser identificado ou de expor idéias sem ser identificado. O anonimato, em princípio, é vedado pelo art. 5º, IV da Constituição da República, pois é fundamental a identificação da autoria de determinado pensamento, para sua eventual responsabilização perante terceiros, no caso de excesso ou abuso desse direito.

A internet propicia para que o anonimato seja garantido, inclusive, está é uma das características mais populares da rede, mas que pode ter reflexos negativos no mundo real. Não se pode admitir que essa liberdade extremada seja utilizada para fins ilícitos.

Assim como a liberdade de expressão, o direito à privacidade é um bem maior dos cidadãos. O Código Penal trata dos crimes contra a liberdade individual relacionados com violação de privacidade, seja por invasão de domicilio (art. 150 do CP), seja por violação, sonegação ou destruição de correspondência (art. 151 do CP). Por seu turno o Código Civil dispõe em seu art. 21 que a vida privada da pessoa natural é inviolável, e também em seu art. 187, dispõe que comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes. Portanto há proteção legal para a privacidade.

São muitas as questões sobre a privacidade na *web*, mas a resposta legal e jurisprudencial no Brasil ainda deixam a desejar. Ante a esse vazio a própria rede tem criado regras e políticas de privacidade.

Registre-se, por oportuno, que o já citado IP constitui uma forma de identificação virtual, como assenta COSTA (2008), o que importa dizer que o anonimato na rede é relativo. Assim, nos provedores pagos, é mais fácil identificar os usuários e restringir práticas delituosas, no entanto, as contas gratuitas não possibilitam um controle tão constante.

Por seu turno, é de responsabilidade do usuário criar senhas de difícil decifração, assim como cabe ao provedor conferir-lhe a necessária segurança no processamento de informações. Usar datas de nascimentos ou nomes comuns, por exemplo, torna muitas operações bancárias do mundo real inseguras, em ambiente virtual, a insegurança é ainda maior. Como as senhas equivalem à assinatura eletrônica dos indivíduos na rede, decifrá-las significa aprender a falsificar uma assinatura.

De uma forma geral, o maior problema jurídico dos crimes virtuais é a raridade de denúncias e, pior, o despreparo do aparato policial para apurá-los. Embora já seja possível fazer boletins de ocorrência pela internet, são poucas as equipes e profissionais preparados para a investigação de um crime pela internet.

6- SUJEITOS ATIVOS DOS DELITOS

Os infratores são pessoas que detém conhecimentos avançados em computação, geralmente novos, e seu perfil acusa pouco temor em relação à norma, indiferença à sanção penal, motivado por dinheiro, auto-promoção ou vingança.

Em sua obra BARROS (2007) destaca alguns dos principais sujeitos ativos o *hacker*, o *cracker*, o *pheakers*, o *cardes* e o *cyberterrorist.*

6.1- *HACKERS*

O *hackers* é pessoa que consegue invadir sistemas de empresas e outros sistemas conectados à rede, seu intuito é a invasão de máquinas de terceiros para satisfazer o próprio ego, buscando reconhecimento e notoriedade. Segundo BARROS (2007) o *hacker* invade sistemas para provar que é capaz de tal proeza, equiparando-se à uma espécie de invasão de domicilio, e tipificável como crime de mera conduta.

6.2- *CRACKER*

O *cracker* é um profissional, cuja origem remonta às grandes corporações privadas e aos órgãos de espionagem governamental. Seu aprimoramento é financiado pela espionagem entre países e pela espionagem industrial, como um meio para o roubo de informações secretas. Para BARROS (2007) são responsáveis também pelos grandes investimentos feitos pelas corporações em sua própria segurança, o item mais caro dentro da categoria de tecnologia nas empresas, e pelos custos gerados por sua constante necessidade de atualização.

Ressalte-se que o crime se configura na invasão não autorizada, no furto de informações confidenciais, no acesso não permitido, independentemente do uso de senha autorizada. O *cracker*, ou pirata digital, em suma, é a pessoa especialista em sistemas informatizados, que invade sistemas alheios, sem autorização.

6.3 – *PHEAKERS*

Pheakers são, como definido por BARROS (2007), agentes especialistas em telefonia, que atacam visando a fraudar sistemas de telecomunicação, em linhas telefônicas convencionais ou celulares, de forma gratuita ou remunerada. Além disso, facilitam o ataque aos sistemas a partir de acesso externo, prejudicando o rastreamento de ataques informáticos. São aqueles indivíduos especialistas em realizar ligações clandestinas de telefone ou mesmo clonar linhas telefônicas, fixas ou móveis.

6.4 – *CARDES*

O *cardes* é a denominação atribuída aos “criminosos que se apropriam do número de cartões de crédito, obtidos através de invasão de listas eletrônicas constantes nos sites de compras efetivadas pela internet, ou de outros meios ilícitos para realizar toda a espécie de compras” na exata definição de LIMA (2006).

6.5 – *CYBERTERRORISTS*

O *cyberterrorist*, na exata explanação de BARROS (2007), é o termo que por si já define a atividade ilícita do agente, consistente em desenvolver programas ou rotinas capazes de sabotar e/ou provocar danos em computadores e sistemas, com o intuito de gerar terror.

7- DO TEMPO DO CRIME

Para a correta aplicação da norma penal é necessária a apuração do momento exato da ocorrência do fato típico. A relevância disto não se restringe à análise das próprias

circunstâncias do crime, todavia serve de parâmetro para solucionar antinomias, aferir a imputabilidade do agente, bem como aplicar institutos como a anistia e a prescrição.

Ocorre que os meios informáticos proporcionam uma dissociação temporal, visto que possibilitam programar a execução de um delito informático no tempo. Isto é, os computadores possuem um relógio interno, que torna possível a sua programação para ativar um programa qualquer ou executar determinada instrução em data predeterminada, o que pode acontecer quando invadidas e tiveram dados manipulados pelos invasores da internet.

Assim, a ação poderia acontecer em tempo real ou ficto, a depender da vontade do agente.

Registre-se que em relação ao momento de consumação do delito o Código Penal em seu art. 4º, das várias teorias que disputam o tratamento da matéria, o mesmo adotou como regra a teoria da atividade, ou seja, o momento da ação ou da omissão será o marco inicial para o raciocínio sobre a aplicação da lei penal.

Desse modo, para efeito penal, valerá como referência a ação inicial que programou a execução, ainda que a mesma ocorra em momento posterior.

8- DO LUGAR DO CRIME

No que tange ao lugar, o Código Penal adotou, em seu art. 5º., o princípio da territorialidade, como regra, e como exceções, os princípios da defesa previsto no art. 7º., I e § 3º., da justiça universal expresso no art. 7º., alínea “a”, da nacionalidade contemplado no art.

7º., inciso II, alínea “b”, e da representação constante do art. 7º., II alínea “c”. Na precisa exposição de GRECCO (2008).

Além disso, o CP adotou a teoria da ubiqüidade para delimitar o local do crime. É comum o crime à distância, aquele em que a conduta é praticada fora do país e o resultado aqui ocorre, ou vise e versa. Na prática, é necessário identificar-se o local da ação e do resultado.

O controle da criminalidade é altamente seletivo. Malgrado, nos tempos atuais a impunidade o caracteriza, visto que não se trata de crime ostensivo, havendo complexidade técnica dos sistemas informáticos, o domínio da tecnologia, a confiança no computador, a falta de documentos escritos das operações, a insuficiência de medidas de segurança e controle, a característica dos crimes plurilocais, a difícil prova da autoria, o medo da vítima de que durante o processo seja descoberto segredo empresarial.

São características do atuar desvalorado: a alta lesividade econômica, a conduta realizada em local distante do resultado, e a reiteração freqüente.

Revele-se que, quanto ao lugar do crime, a soberania dos Estados impõe a aplicação da lei penal incidente ao caso, em todo o seu território, ocorrendo situações que ultrapassam a sua fronteira, o que usualmente ocorre nos crimes pela internet, enquanto crimes praticados pelo computador.

Nada obstante, quando se trata de crime praticado em ambiente virtual, pode-se deparar com a problemática definição do momento em que ocorreu a conduta, sobretudo se a ação tiver sido programada com meses de antecedência, como já visto.

É notório, que o meio virtual também não possui um espaço físico predeterminado. Dessa forma, considera-se que o espaço na está delimitado geograficamente e seu acesso é muito dinâmico. Assim, a concepção clássica de território, como espaço físico, ganha outra

conotação, qual seja: de espaço virtual, posicionado em ambiente global, no qual há uma transcendência dos limites territoriais.

Ressalve-se que o ciberespaço não é propriamente um território, mas se caracteriza por um fluxo constante de informações, composto de redes de comunicação, de forma que a localização da informação passa a ter relevância, uma vez que é ela quem dá idéia de território, desvinculado da idéia de espaço físico.

Grande parte dos delitos informáticos suplanta fronteiras territoriais, logo as infrações desta natureza fazem parte da camada ilícita transnacional que se espalhou pelo mundo. Ante a falta de legislação processual pronta e de imediata aplicação, que responda adequadamente tais indagações, resta a aplicação de alguns princípios da territorialidade, extraterritorialidade, nacionalidade, defesa, justiça penal universal e representação, contidos no Código Penal. Tais princípios regulam a aplicação da lei penal no espaço, tendo o legislador adotado a teoria da territorialidade temperada. Pelo princípio da territorialidade, aplica-se a lei penal brasileira aos crimes cometidos em território nacional, sem prejuízo das convenções, tratados e regras de Direito Internacional.

Os demais princípios orientam a extraterritorialidade da lei penal brasileira, ou seja, quando se aplica nossa legislação para punir condutas criminosas praticadas fora do território nacional.

9- AS PROVAS DA MATERIALIDADE

O crime informático é, em regra, um ilícito material, ou seja, crime que deixa vestígios, impondo-se a realização da perícia nos termos do art. 158 do Código de Processo

Penal. Cabe ao perito informar ao juiz os detalhes e as circunstâncias que envolvam o equipamento, os programas, os arquivos, enfim, tudo aquilo que se mostrar necessário para demonstrar a ocorrência do crime, bem como para comprovar a sua autoria. Pendendo de autorização judicial para se efetuar a busca e apreensão do computador utilizado como instrumento do crime.

A perícia deverá ser realizada preferencialmente por profissional habilitado, com conhecimentos em informática e em sistemas de comunicação, portador de diploma de curso superior.

Para melhor viabilidade da instrução probatória, algumas investigações sobre crimes virtuais exigirão a quebra de sigilo.

Os registros dos usuários conectados à rede, mantidos por seus provedores, gozam de proteção e só podem ser requeridos pela autoridade judicial competente.

O STJ já se posicionou sobre o tema, quando do julgamento do HC 83.338-DF, afirmando que a obtenção de dados do usuário de determinado IP consistente tão só na identificação da propriedade e do endereço em que instalado o computador do qual partiu o escrito criminoso não está resguardada pelo sigilo de que cuida o art. 5º, XII, da CF/1988, nem pelo direito à intimidade, que não é absoluto, prescrito no inciso X daquele mesmo artigo.

Isso porque, a testemunha do crime é aquele que detém os protocolos de IP, aquele que armazena os dados sobre as transações ocorridas eletronicamente. Da mesma forma, as provas eletrônicas – que muitos hesitam em aceitar juridicamente, alegando que são altamente adulteráveis – podem passar por perícia técnica rigorosa para serem aceitas em processos, sendo até mesmo possível, com profundo conhecimento da tecnologia, a produção de provas virtuais muito mais confiáveis que as do mundo real.

O Direito Digital traz a obrigação de atualização tecnológica para todos aqueles que atuam no processo como: advogados, juízes, delegados, procuradores, investigadores, peritos, etc.

O maior estímulo aos crimes virtuais é dado pela crença de que o meio digital é um ambiente a margem do mundo real. Essa postura existe porque a sociedade não crê na vigilância e na adequada punição aos ilícitos praticados no mundo virtual.

A mais, o conjunto norma-sanção é tão necessário no mundo digital quanto no real. Se houver essa falta de crédito na capacidade punitiva da sociedade digital, os crimes aumentarão e os negócios virtuais serão desestimulados; e muitas pessoas que não cometem crimes no mundo real por medo, acabarão, de algum modo, interessando-se pela prática delituosa virtual.

Em contraponto, a cooperação internacional entre as policias, e demais órgãos de fiscalização e controle de sistemas de dados, com agilidade e eficiência, traduziriam em um salutar intercâmbio, para a apuração e solução dos crimes cometidos pela internet dada a sua natureza, em muitas das vezes, transnacional.

10 – O BEM JURÍDICO TUTELADO

No que concerne ao bem jurídico COSTA (2004), à luz do Direito Penal Internacional, sugere: i) crimes que violam direitos à privacidade e outros direitos humanos; ii) crimes que importam em novas formas de criminalidade econômica; iii) crimes que representam perigos à segurança nacional.

E não menos importante neste novo campo do direito sob um aspecto multifacetado: i) tutela legal dos instrumentos informáticos; ii) proteção da intimidade e de dados reservados; iii) contratos informáticos; iv) responsabilidade civil por danos emergentes da informática; v) delitos instrumentados mediante o uso do computador.

Assim, o delito informático é qualquer conduta ilegal, não ética e não autorizada que viole o processamento automático de dados e/ou a transmissão de dados; a outra, de que a criminalidade mediante computadores alude a todos os atos antijurídicos realizados com emprego de um equipamento automático de processamento de dados.

Revele-se que o uso da internet acompanha diferentes condutas passíveis de causar lesão a diversos bens jurídicos; pois os benefícios da modernidade e celeridade trazidos com a rede mundial, como já analisado, são proporcionais aos problemas dela decorrentes.

Razão pela qual, suscita-se a possibilidade de se amoldar condutas praticadas no meio virtual aos tipos penais já existentes. Em que pesem inúmeras ocorrências envolvendo atividades ilícitas cometidas na internet, ainda não se formou um consenso sobre o conceito de crime informático.

Casuisticamente, quando essas condutas podem ser subsumidas a um tipo penal existente na legislação brasileira, não há maiores problemas. Geralmente não há óbice para moldar-se a ação do agente a um crime previsto no Código Penal ou em leis extravagantes, especificamente quando a internet é utilizada apenas como seu meio de execução.

Como meio de execução de crimes praticados com o emprego da rede, o sistema pode ser útil, como já visto, nas hipóteses de crime contra a honra, crime de ameaça, etc.. Casos em que o agente envia mensagens eletrônicas para a vítima ameaçando-a ou injuriando-a, ou para terceiros, caluniando ou difamando o ofendido. Em outras palavras, quando o meio executório para a prática do delito é escrito ou alguma forma de divulgação, é possível a utilização da internet para a sua prática.

Por outro lado, o problema a ser solucionado surge quando a conduta praticada não encontra tipificação legal, como na hipótese em que o lesado é a informação, ou a rede, cuja proteção jurídico-penal é reclamada pela sociedade atual. Nesse passo, se está diante doss chamados crimes informáticos puros, os quais ainda não encontram total correspondência na legislação, e necessitam em sua maioria de produção legislativa específica.

11- COMPETÊNCIA PARA JULGAMENTO

Jurisdição é o poder atribuído ao juiz de dizer o direito, isto é, o poder conferido ao juiz de julga. A jurisdição é própria do Poder Judiciário, ou seja, todo juiz a possui mas, por óbvio, sofre algumas limitações.

Ademais, os crimes praticados pela internet carecem de legislação específica sobre a forma de seu processamento, razão pela qual seguir-se-á a regra geral.

Segundo o art. 69 do CPP a competência será determinada: i) pelo lugar da infração; ii) pelo domicílio ou residência do réu; iii) pela natureza da infração; iv) por distribuição; v) pela conexão ou continência; vi) pela prevenção; vii) pela prerrogativa de função.

Assim, seguindo a regra do CPP, sendo possível a constatação do lugar do resultado do crime praticado pela internet, o mesmo será processado no foro do resultado. No caso dos efeitos terem se protraído para além do território brasileiro, será competente o foro no Brasil do lugar onde se operou o último ato de execução.

Não sendo possível a constatação do lugar, para efeito de fixação da competência territorial terá curso a regra do arts. 72 e 73 do CPP, ou seja, pelo domicílio ou residência do réu.

No que tange, a competência material, se houver crime federal conexo o processamento e julgamento correrão perante a justiça federal.

CONCLUSÃO

O acesso a um grande número de informações disponível às pessoas, com idéias e culturas diferentes, pode influenciar o desenvolvimento moral e social das pessoas. A criação dessa rede beneficia em muito a globalização, mas também cria a interferência de informações entre culturas distintas, mudando assim a forma de pensar das pessoas. Isso pode acarretar tanto uma melhora quanto um declínio dos conceitos da sociedade.

Essa praticidade em disseminar informações na Internet contribui para que as pessoas tenham o acesso a elas, sobre diversos assuntos e diferentes pontos de vista. Mas nem todas as informações encontradas na Internet podem ser verídicas. Existe uma grande força no termo "liberdade de expressão" quando se fala de Internet, e isso possibilita a qualquer indivíduo um pouco mal-intencionado publicar informações ilusórias sobre algum assunto, prejudicando, assim, a consistência dos dados disponíveis na rede.

Há condutas ofensivas aos sistemas informáticos ou telemáticos ou mesmo pertinentes ao uso do computador que não se amoldam às figuras penais descritas em nossa legislação, que estão a exigir a imediata criminalização.

É importante lembrar que os criminosos da internet já não são criminosos incomuns – a imagem de um sujeito extremamente inteligente e com vasto conhecimento técnico já não corresponde à realidade, pois atualmente é muito fácil encontrar na internet o código-fonte aberto de um vírus ou “cavalo de troia”. Alguns criminosos praticam até mesmo a clonagem

de *site*, que nesse caso, exige *expertise* tecnológica acima da média, utilizando-os para roubar informações dos usuários – informações utilizadas posteriormente para que o criminoso assuma outras identidades em operações comerciais com uso de cartão de crédito clonado. O combate a esses crimes torna-se extremamente difícil por dois motivos: a) falta de conhecimento do usuário, que dessa forma, não passa às autoridades informações relevantes e precisas; e b) a falta de recursos em geral das autoridades policiais.

É natural que as condutas humanas evoluam e se aprimorem, o que também se espera da legislação criminal.

Logo, podemos observar que a questão ganhou destaque e profundidade, na proporção em que a ordem econômica e o respeito à dignidade da pessoa transnacionalizada causam prejuízos vultosos ao mundo globalizado.

REFERÊNCIAS BIBLIOGRÁFICAS.

BARROS, Marco Antonio, GARBOSSA, Daniella D´Arco, CONTE, Christiany Pegorari. Crimes Informáticos e a proposição legislativa: considerações para uma reflexão preliminar, Revista dos Tribunais, novembro 2007.
BRASIL. Constituição da República Federativa do Brasil de 5 de outubro de 1988.
BRASIL. Código Penal Brasileiro. Decreto-Lei 2.848 de 7 de dezembro de 1940.
BRASIL. Código de Processo Penal. Decreto-Lei 3.931 de 31 de dezembro de 1941.
BRASIL. Lei nº. 7.170 de 14 de dezembro de 1983.
BRASIL. Lei nº. 7.716 de 5 de janeiro de 1989.
BRASIL. Lei nº. 8.069 de 13 de julho de 1990.
BRASIL. Lei nº. 9.296 de 24 de julho de 1996.
BRASIL. Lei 9.609 de 19 de fevereiro de 1998.
BRASIL. Superior Tribunal de Justiça. HC 83.338-DF. Publicado no DJEde 26.10.2009.
COSTA, Alvaro Mayrink, CRIME INFORMÁTICO: REVISTA DA EMERJ, V.7, N.28, 2004, P. 24/40.
COSTA, Ligia Maura Costa, Direito Internacional Eletrônico: Ed. Quartier Latin do Brasil, 2008.
FARIAS, Cristiano Chaves, Direito Civil – Teoria Geral: Ed. Lumen Juris, 2007.
FERREIRA, Robson, *apud* PINHEIRO, Patrícia Peck. Direito Digital. 2 ed. São Paulo: Saraiva, 2007. p. 250-251.
GRECO, Rogério, Curso de Direito Penal: Ed. Impetus, 2007..
INELLAS, Gabriel Cesar Zaccaria, Crimes na internet: Ed. Juarez de Oliveira, 2009.
LIMA, Paulo Marco Ferreira. Crimes de computador e segurança computacional. Campinas: Millennium, 2006.

INTERNET. Disponível em <http://pt.wikipedia.org/wiki/Internet> Acesso em 10 dez. 2009.