Instituto Matonense Municipal de Ensino Superior

Revista Matiz Online
ISSN 21794022

CRIMES CIBERNÉTICOS

GARCIA, R. A. C[1], CARUZO, W. R.[2], ZAMQUIM JUNIOR, J.W.[3]

[1] Mestrando em Ciência, Tecnologia e Sociedade pela UFSCar - Universidade Federal de São Carlos-SP. Professor de Direito Empresarial do Instituto Matonense Municipal de Ensino Superior - IMMES - Brasil.
[2] Bacharel em Direito pelo Instituto Matonense Municipal de Ensino Superior –IMMES. Advogado.
[3]Doutorando e Mestre em Ciências Ambientais na Universidade Federal de São Carlos - UFSCar. Advogado e professor de Direito no Instituto Matonense Municipal de Ensino Superior - IMMES. Pesquisador no grupo de pesquisa Novos Direitos na UFSCar.

RESUMO
O presente trabalho tem como objetivo estudar e analisar os chamados crimes cibernéticos em suas diferentes espécies. Numa sociedade cada vez mais informatizada, a utilização cada vez maior da Internet como meio de comunicação, ferramenta de trabalho ou simplesmente de lazer criou não só uma facilidade maior para estas atividades como uma grande facilidade para a atuação de criminosos que se utilizam de inúmeras formas para a prática delitiva. Serão abordados também temas como as principais ameaças utilizadas na prática delitiva, bem como serão abordados aspectos relacionados a competência para processar e julgar estes delitos e os métodos de investigação e de produção de provas utilizados para o combate dos crimes cibernéticos, cujos quais vem crescendo de maneira exponencial. Serão apontados também, as inovações legislativas trazidas com a publicação das Leis 12.737/12 e 12.735/12.

Palavras chave: Crimes Cibernéticos, Direito Penal, Ambiente Virtual, Internet.

INTRODUÇÃO

Com a expressiva evolução e expansão da tecnologia a qual a sociedade vivencia não há equívocos em afirmar de que a distância entre as pessoas se tornou ínfima diante da variedade de recursos eletrônicos e principalmente em razão da Internet, o que possibilitou uma constante e quase infinita troca de informações entre pessoas de diferentes regiões do mundo. Esta nova realidade trouxe à tona a necessidade de uma importante adequação do Direito no intuito de garantir a segurança do ambiente virtual para que não se torne um ambiente sem regulamentação.

Essa adequação foi de grande relevância dentro do Direito Penal, em vista do aumento vertiginoso dos crimes informáticos, também conhecidos como crimes cibernéticos, culminando na criação de legislações especificas para delitos dessa natureza, bem como na criação de órgãos especializados nestes tipos de crimes, com consequente aprimoramento dos métodos de investigação e produção de provas.

Revista Matiz Online
ISSN 21794022

2. A INTERNET

A Internet trata-se de uma ferramenta de comunicação cada vez mais utilizada no cotidiano das pessoas e considerada por muitos, como algo indispensável para realização de trabalhos, além de facilitar as relações sociais sem que tenha que sair de casa (SILVA; SILVA, 2015, p.16).

Esta importante ferramenta é portadora de um vasto banco de dados, que pode ser considerado como um tesouro por indivíduos que tenham intenção a pratica criminosa, podendo em muitos casos causar graves prejuízos financeiros e pessoais aos que se utilizam da Internet.

Nas sabias palavras de Corrêa (2002, p.42): "a Internet é um paraíso de informações, e, pelo fato de estas serem riquezas, inevitavelmente atraem o crime. Onde há riqueza há crime".

Diante desta situação e na existência de previsão legal, surgem os chamados crimes cibernéticos, caracterizados pela prática de delitos no ambiente virtual ou por intermédio deste (WENDT; JORGE, 2014, p.1).

2.1. A Internet no Brasil

No ano de 1965 houve a criação do Serviço Federal de Processamento de Dados e a associação do Brasil ao consorcio internacional de telecomunicações, conhecido na época como INTELSAT. Posteriormente, em 1972, houve a criação do primeiro computador brasileiro, também chamado de "patinho feio", pela Universidade Federal de São Paulo e alguns anos depois, em 1979 foi criada a secretaria especial de informática (WENDT; JORGE, 2014, p.8).

Em 1988 houve mais um passo importante para a consolidação da Internet no Brasil com a conexão à Bitnet da Fundação de Amparo à Pesquisa de São Paulo, do Laboratório Nacional de Computação Cientifica (LNCC) e da Universidade Federal do Rio de Janeiro.

Treze anos após sua criação, em 1992, a Secretaria Especial de Informática foi extinta, dando lugar à Secretaria Política de Informática, que ficou encarregada das atribuições daquele. No mesmo ano foi implantada a primeira rede conectada à Internet, ligando as principais universidades brasileiras. Entretanto a utilização ainda era bem limitada, sendo possibilitado apenas a troca de e-mails entre os usuários. A utilização da Internet no

país de maneira comercial começou a ser disponibilizada no ano de 1995, com velocidade máxima de conexão de apenas 9,6 Kbps (WENDT; JORGE, 2014, p.9).

Neste mesmo ano houve a criação do Comitê Gestor da Internet, que tinha como função básica fomentar o desenvolvimento da Internet no Brasil. Apenas a partir deste ano que a Internet passou a ser regulamentada e ganhou força para que ocorresse sua expansão (SILVA; SILVA,2015, p.23).

2.2. As Primeiras Ameaças

As primeiras notícias que se tem com relação a programas de computador com capacidade de se auto replicar são trazidas desde o final da década de 50, contudo, foi na década seguinte que surgiram os verdadeiros códigos maliciosos, através da criação de um jogo chamado Core Wars, por um grupo de programadores. Este jogo tinha a capacidade de se reproduzir cada vez que era executado, o que sobrecarregava a memória do computador do outro usuário. Os mesmos criadores do jogo também criaram o programa capaz de destruir as cópias geradas pelo jogo. Este fato somente veio a conhecimento do público mais de duas décadas depois, com a publicação em uma revista cientifica da época (WENDT; JORGE, 2013, p. 9).

Em 1971 foi criado o Creeper Vírus, por um funcionário que trabalhava em uma empresa envolvida na construção da ARPANET, ganhando acidentalmente acesso à rede.

Anos depois, em 1982, um garoto de apenas 15 anos criou um vírus conhecido como Elk Cloner, que é considerado por alguns especialistas no assunto como o primeiro vírus desenvolvido para infectar computadores, apesar de não criar grandes danos à máquina (WENDT; JORGE, 2013, p. 10).

Em 1986 foi criado o vírus conhecido como Brain, por dois irmãos paquistaneses. Este vírus inicialmente tinha a função de monitorar o uso não autorizado de um programa de monitoramento cardíaco, contudo, sofreu alterações e com isso passava a ocupar espaço da memória dos computadores, algo que era bastante escasso na época. No mesmo ano surgiram os primeiros Cavalos de Troia de que se tem notícia.

Apenas em 1988 foi criado o primeiro programa de antivírus e era destinado para a proteção dos computadores contra o vírus Brain (WENDT; JORGE, 2013, p. 11).

Revista Matiz Online
ISSN 21794022

2.3. Principais de Ameaças Utilizadas Atualmente

As ameaças existentes irão incidir com mais facilidade em computadores considerados vulneráveis. Isso se dá em muitos casos pela deficiência no sistema de segurança da máquina que poderá ocorrer pela desatualização do antivírus, utilização de sistemas operacionais piratas, firewall desativado, falhas em softwares, entre outros. Essas vulnerabilidades dão margem a possíveis ataques e danos para computadores e dados pessoas de seus usuários (CASSANTI, 2014, p.8).

3. DIREITO E INFORMATICA

A princípio, o estudo conjunto entre duas disciplinas tão distintas como Informática e Direito parece ser uma tarefa de difícil realização, contudo, é certo que as Ciências Jurídicas devem acompanhar as evoluções tecnológicas. A confirmação dessa necessidade se dá a medida em que se observa um aumento constante nas condutas criminosas praticadas através de recursos informáticos. A busca de maior compreensão tecnológica objetiva oferecer ao usuário maior segurança, caso contrário existirá uma forte tendência ao caos, mas mesma velocidade da evolução tecnológica (LOPES, 2012, p. 20).

Com a vasta possibilidade de tarefas diárias que pode ser efetuada utilizando a informática, como pagamento de contas, realização de compras, essa tecnologia torna-se cada vez mais alvo de criminosos. Contudo, os rastros deixados não são mais os mesmos de antigamente, em que se inclui impressões digitais, documentos de papel, relatórios de toxicologia. A tecnologia ampliou esta gama de vestígios e, da mesma forma, é impreterível que sejam encontrados (LOPES, 2012, p. 21).

O avanço tecnológico na área da informática é responsável por uma revolução nas relações sociais, fato que gerou uma grande modificação na vida moderna, especialmente com a chegada da Internet (CASTRO, 2003, p. 5).

Caberá ao novo profissional do Direito o dever de garantir a proteção de inúmeros direitos como o de privacidade, a imagem, a propriedade intelectual, direitos autorais e recebimento de royalties, segurança da informação, processos contra hackers, por isso a importância de que seja o Direito Digital estudado intensamente de maneira a atender as novas necessidades advindas do ambiente virtual, cujo qual traz uma interligação que atinge pessoas, empresas, governos e instituições. Entretanto na mesma velocidade que a rede evolui, crescem os crimes em virtude de da sensação de anonimato proporcionado pelo ambiente virtual e pela massificação destes novos meios de comunicação, daí o aumento da

relevância jurídica e da necessidade de abordagem das condutas pelo Direito visando garantir a segurança jurídica e social, da mesma forma como ocorreu com outros meios de comunicação já existentes, como imprensa, rádio, televisão, telefone, cada um deles trazendo um novo desafio jurídico (PINHEIRO, 2013, p. 72).

Segundo a autora e grande estudiosa no assunto crimes digitais Patrícia Peck Pinheiro (2013, p.73) não há um Direito da Internet, assim como não há um Direito Televisivo ou radiofônico, mas sim pontos específicos a serem analisados e regulamentados.

Com isso, não há que se falar em Direito da Internet como novo ramo das Ciências Jurídicas, mas sim, o surgimento de novas peculiaridades deste veículo de comunicação que devem ser consideradas pelas várias áreas do Direito, sem necessidade de criação de um Direito especifico, cujo qual ficaria limitado num curto lapso temporal. Por ser a velocidade das transformações uma barreira no que diz respeito a atualização das normas, o que se sugere é a criação de normas mais amplas, que permitam maior resistência temporal e abrangência de condutas (PINHEIRO, 2013, p. 73).

No mesmo sentido caminha o posicionamento de Marcelo Crespo (2011, p. 39), apontando que o direito da informática não se trata de um novo e especifico ramo do Direito, mas sim uma nova interpretação jurídica relacionada a um novo momento de informação. Segundo o mesmo autor faz-se necessário que haja relação do Direito Penal com a informática visto que são debatidas questões sobre ataques a sistemas, práticas de estelionatos, engenharia social, bem como discussões sobre local onde ocorre o crime, remetendo a questões processuais deste tipo de prática delitiva.

Em sentido contrário vem a interpretação de Vladimir Aras, que defende o surgimento do Direito Penal da Informática, como um ramo do direito público, objetivando proteger bens jurídicos relacionados a computadores, ou seja, desde a máquina denominada computador e seu conteúdo interno, até bens jurídicos já tutelados, porém que possam ser atingidos por meios computacionais (ARAS apud SILVA, SILVA, 2015, p. 30).

Em suma, independentemente da nomenclatura utilizada para o estudo e aplicação do Direito aos Crimes Virtuais deve-se ter em consciência principalmente sobre a necessidade de que o Direito acompanhe e se adapte a evolução da tecnologia e as novas modalidades de fraudes e crimes que vem surgindo e crescendo de maneira exponencial, colocando em perigo número cada vez maior de bens jurídicos, influenciando dessa forma ramos do Direito público, privado e internacional (SILVA, SILVA, 2015, p. 30).

Revista Matiz Online
ISSN 21794022

4. DO CRIME

Com o passar dos dias a humanidade se depara com novas necessidades e alcança novos objetivos resultando em transformações que ocorrem em todas as áreas do conhecimento, inclusive as ciências jurídicas. Sendo assim, pode-se dizer que o direito é dinâmico e acompanha a sociedade em sua evolução e clamores. Nesta seara se encontra o Direito Penal, que de tempos em tempos deve se atualizar com a finalidade de encontrar formas de prevenção e combate à criminalidade por meio da justa aplicação de penas. Isto traz a necessidade de discorrer sobre o conceito e algumas peculiaridades inerentes ao crime, que não é apenas um fenômeno social, mas sim um episódio na vida de um indivíduo, com isso, não se deve, portanto, ser tratado de maneira isolada deste. Não deve também ser tratado apenas como um conceito, visto que cada crime tem sua história. Nem mesmo o atual código penal traz um conceito de crime, ficando esta função a cargo da doutrina o que resultou em diversas diferentes definições criadas por diferentes escolas penais (ELEUTÉRIO, 2001, p.184-185).

O crime dentro do Direito Penal deve considerar certas particularidades fundamentais para a configuração da conduta criminosa, por exemplo a prévia tipificação da conduta em lei. Conforme já foi dito, o legislador não deu uma conceituação de crime, apenas apontando como punível a conduta humana que cause lesão a bem jurídico importante. A conceituação surge da doutrina, que inclusive apresentam inúmeros critérios, apresentando-se como os mais difundidos: o formal, que corresponde a uma definição nominal, o que quer dizer criar uma relação entre um termo a aquilo que o designa; o material, que busca estabelecer o conteúdo do fato punível através de uma definição real e o analítico, cujo qual indica características, elementos constitutivos da conduta criminosa, sendo desta forma de grande importância técnica (GRECO apud SILVA, SILVA p. 38).

A conceituação jurídica do crime além de um ponto de extrema relevância é também um ponto que apresenta grandes controvérsias na atual doutrina penal, que inicialmente adotava o conceito formal, que conforme já exposto, corresponde a toda conduta humana, que infringisse a lei penal. Posteriormente a definição material passou a ser a adotada, onde se definia crime o fato oriundo da conduta humana que lesa ou é capaz de pôr em risco um bem jurídico tutelado pela norma jurídica. Por fim chega-se ao momento de utilização do conceito analítico, em que passou a ser descrito o crime como toda ação ou omissão típica, antijurídica e culpável (ELEUTÉRIO, 2001, p.184-185).

Para o ilustre doutrinador Fernando Capez (2012, p. 134), formalmente, crime resulta da adequação de uma conduta ao texto legal, ou seja, se o legislador aponta determinada conduta como criminosa, assim será, tornando-se irrelevante o conteúdo ilícito, o que de acordo com este autor a não consideração da essência ou lesividade da conduta consiste em uma afronta a dignidade da pessoa humana.

No que diz respeito ao critério material preceitua o brilhante doutrinador Guilherme de Souza Nucci (2012, p.174), conceitua o crime como algo que a sociedade entente como uma conduta que pode ou deve ser proibida por lei, já que em ofendendo a bem jurídico protegido, mereça ser penalizado.

Por fim, com relação ao aspecto analítico o posicionamento majoritário da doutrina entende como mais adequada a teoria tripartite, em que o crime consiste em fato típico, antijurídico e culpável, sendo esta oriunda da doutrina alemã, que decompõe a figura do crime em elementos constitutivos possibilitando uma análise individual de cada um deles. Contudo, deve-se ter em mente que o crime é um ato único e indivisível, onde os elementos ocorrem de maneira conjunta e não cronologicamente ordenada, como pode-se equivocadamente imaginar. Essa análise individual e desconstruída dos elementos do crime permite um melhor entendimento da conduta criminosa (ELEUTÉRIO, 2001, p.187).

Por fato típico entende-se ser a conduta na qual se identifica com a prevista no tipo penal incriminador, afetando bens relevantes tutelados pelo Direito Penal. Possui como elementos: a conduta, seja ela omissiva ou comissiva, dolosa ou culposa; resultado; nexo causal, cujo qual deve ser entendido como o liame entre a conduta e o resultado; tipicidade, que se trata da adequação da conduta com o texto de lei. (GRECO, 2013, p. 38).

Com relação a antijuridicidade ou ilicitude da conduta, esta corresponde a contrariedade entre a conduta do agente e o ordenamento jurídico, que fazendo relação com uma norma penal se tratará de um ilícito penal (GRECO, 2013, p.90).

Toda conduta típica deve ser também antijurídica, ou seja, contrária ao direito, assim considerada a conduta que não encontrar uma causa que venha a justificá-la, ou seja, uma causa que exclua sua antijuridicidade ou sua ilicitude (ELEUTÉRIO, 2001, p.187).

Por fim, a culpabilidade está relacionada com o juízo de reprovação pessoal que recai sobre o autor da conduta, que agiu de forma contrária ao Direito, vez que poderia ter agido de acordo com o conteúdo normativo (GRECO, 2013, p.104).

Consiste no elemento subjetivo do autor do crime, aquilo que se passa na mente do autor do delito, é a culpa em sentido amplo, que engloba o elemento subjetivo dolo, bem

como a culpa em sentido estrito e resulta da união de outros três elementos, quais sejam: imputabilidade, consciência da efetiva ilicitude da conduta e a exigibilidade da conduta conforme o Direito (ELEUTÉRIO, 2001, p.191).

5. CRIMES CIBERNETICOS

Os crimes cibernéticos podem ser tratados como sendo condutas de acesso não autorizados a sistemas de informática, resultando em ações destrutivas, afetando sistemas de comunicação, alteração de dados, violação a direitos autorais, todos tipo de ofensas, descriminações e demonstração de ódio e intolerância, exposição de pornografia infantil, terrorismo e muito mais (PINHEIRO, 2013, p.46).

Os crimes praticados em ambiente virtual apresentam denominações diversas, não havendo até o momento um consenso de qual seria a melhor para definir os delitos relacionados a tecnologia. Desta forma acredita-se que os conceitos ainda não abarcam todos os crimes ligado a tecnologia por serem inúmeras e de grande complexidade as situações envolvendo o ambiente virtual (CRESPO, 2011, p.48).

Denominam-se crimes cibernéticos os delitos realizados contra ou por meio de computadores, que segundo Emerson Wendt e Higor Vinicius Nogueira Jorge (2014, p. 19) são divididos em crimes cibernéticos abertos e crimes exclusivamente cibernéticos.

Conforme pode-se constatar, inúmeros são os conceitos e terminologias dadas ao crime cometido por intermédio de computador e seu instrumento, a Internet. Desta forma, pode-se constatar que crime de informática é toda ação típica, antijurídica e culpável contra ou pela utilização de processamento automático ou eletrônico de dados ou mesmo pela sua transmissão (LOPES, p.27).

5.1. Classificação dos Crimes Cibernéticos

De acordo com Emerson Wendt e Higor Vinicius Nogueira Jorge as condutas indevidas praticadas por computador podem ser divididas em ações prejudiciais atípicas, cujas quais correspondem a atos praticados através da Internet que embora possam trazer algum transtorno à vítima estes não podem ser punidos em âmbito criminal por falta de tipificação.

Os crimes cibernéticos, de acordo com o mesmo autor se subdividem em abertos OU impróprios, sendo aqueles que tratam dos delitos que podem ser praticados de maneira tradicional ou por meio de computadores, ou seja, este tipo de delitos pode ser praticado com ou sem a utilização de computadores.

Por outro lado, nos crimes exclusivamente cibernéticos ou próprios, como o próprio nome aponta, são os delitos que podem ser cometidos unicamente com a utilização de computadores ou outros recursos informáticos que permitam ao agente o acesso à Internet.

5.2. Exemplos de Crimes Cibernéticos Abertos ou Impróprios e Exclusivamente Cibernéticos ou Próprios

Por muitos, o ambiente virtual produz uma sensação de total liberdade, pois possibilita a prática de atos no anonimato, o que é proibido pela Carta Magna em seu artigo 5º, IV, passando a noção equivocada de um território sem fronteiras (PINHEIROS, 2014, p.17).

A seguir serão apontadas algumas condutas danosas que podem praticadas no ambiente cibernéticos em sua espécie aberta ou imprópria.

Para que se possa adentrar nesta espécie de crime torna-se imperioso que concomitantemente seja trazido à baila as novidades jurídicas advindas da lei 12.737/12, também conhecida como Lei Carolina Dickman.

A Lei nº 12.737/12 culminou em importantes alterações no Código Penal brasileiro ao acrescentar os artigos 154-A e 154-B dispondo sobre o crime de invasão de dispositivo informático, bem como realizou pequenas alterações nos artigos 266 e

298 do mesmo diploma, tipificando a interrupção ou perturbação de serviço informático, telemático ou de informação de utilidade pública e também a falsificação de cartões de crédito

Com relação ao crime tipificado ao teor do artigo 154-A do Código Penal, que dispõe sobre Invasão de Dispositivo Informático, este visa tutelar a inviolabilidade dos dados informáticos, que se relaciona ao direito de privacidade e intimidade, garantidos pela Constituição Federal, em seu artigo 5º, X. visa garantir também a integridade dos dados, proteção contra destruição e alteração (VIANNA; MACHADO, 2013, p.93). Estão abrangidos nesta proteção tanto os programas computacionais quanto os dados nele contidos.

No que tange ao sujeito ativo dos delitos previstos nesta lei pode-se dizer que trata-se de crime comum, eis que pode ser cometido por qualquer pessoa, contudo o legislador foi silente com relação ao proprietário do dispositivo informático no momento em que tipifica a conduta de invadir dispositivo informático alheio apenas o que quer dizer que será atípica a conduta do indivíduo, proprietário de uma lan house ou cyber café invadir de maneira indevida os dados do usuário que utilizou a máquina. O mesmo acontecerá com o empregador

que acessar e-mails pessoais do empregado contidos em seu computador de trabalho (VIANNA; MACHADO, 2013, p.94), fatos que poderão causar inúmeros transtornos e uma real sensação de insegurança para a utilização destas máquinas.

A crítica feita pelos ilustres autores Túlio Viana e Felipe Machado (2013, p.95) que de maneira acertada apontam que o bem a ser tutelado deve ser a inviolabilidade dos dados, independentemente a quem pertença a máquina. A situação se agrava na medida em que não há a possibilidade de uma interpretação extensiva da conduta pois o Direito Penal pátrio veda a chamada analogia *in malam partem*, por afrontar diretamente o princípio constitucional da legalidade, com isso a correção a esta lacuna somente se dará através de nova lei.

Com relação aos sujeitos passivos, estes podem ser qualquer pessoa física ou jurídica proprietária de dados informáticos, e que não seja a proprietária do sistema computacional.

A tipificação da conduta ocorre com o ato de invadir e instalar, neste último caso está-se falando de instalação de vulnerabilidade.

Trata-se de crime previsto apenas na modalidade dolosa, ou seja, o agente deve ter consciência e vontade na prática delituosa, não sendo possível a modalidade culposa por ausência de previsão legal.

Em relação ao tempo do delito o artigo 4º do Código Penal adota a teoria da atividade como o momento do crime. Isso significa que a invasão ao dispositivo informático se tem por realizada no momento em que é emitido o comando destinado a realizar o acesso não autorizado.

Adotando também a mesma sistemática prevista no artigo 6º do Código Penal com relação ao local do crime adota-se a teoria da ubiquidade, que considera local do crime o da ação ou do resultado, isso quer dizer que o local do crime poderá ser o de onde se encontra o dispositivo informático invasor ou o de onde se encontra o dispositivo informático invadido, respectivamente (VIANNA; MACHADO, 2013, p.100).

Conforme já foi dito anteriormente, a Lei 12.737/12 trouxe algumas alterações no artigo 266 do Código Penal acrescentando-lhe os parágrafos 1º e 2º.

A mudança mais significativa decorrente desta alteração legislativa está na inclusão dos serviços telemáticos (comunicação a distância por serviços informáticos através de rede de telecomunicações) e informações de utilidade pública

ISSN 21794022

Desta forma visou o legislador proteger os serviços de Internet, alvo de número crescente de ataques que não visam a invasão do sistema, mas sim, torna-lo indisponível, conhecido como ataque de DOS (Denial of Service – Negação de Serviço).

Este ataque poderá ocorrer: forçando o sistema da vítima a se reinicializar ou causando grande sobrecarga ao sistema de comunicação resultando em mau funcionamento entre servidor afetado e usuários do sistema (SILVA E FREITAS, 2013, p.14).

Outra alteração importante ao Código Penal trazida pela Lei 12.737/12 e que também deixa claro a necessidade de adequação ao momento de expansão tecnológica pela qual a sociedade vem passando está relacionado a falsidade de cartão conforme pode-se depreender do parágrafo único do artigo 298 do referido diploma.

Buscou-se nesse caso estender aos cartões de crédito e débito a proteção oferecida aos documentos particulares e torna desta forma punível a pratica conhecida como "clonagem de cartão", não sendo necessário para sua configuração neste caso que o agente venha a se apropriar de dinheiro da vítima através de caixa eletrônico (SILVA E FREITAS, 2013, p.15).

6. COMPETÊNCIA TERRITORIAL. INVESTIGAÇÃO E MEIOS DE PRODUÇÃO DE PROVAS NOS CRIMES CIBERNÉTICOS.

A Constituição Federal apresenta dois critérios de definição de competência, sendo eles a competência em razão da matéria (ratione materiae) e a competência em razão da pessoa (ratione personae) ou por prerrogativa de função. O Código de Processo Penal por sua vez traz um terceiro critério, que se apresenta de maneira subsidiária, senda ela a competência em razão do lugar da infração (ratione loci) ou também conhecida como competência territorial. Enquanto os dois primeiros, constitucionais se configuram interesse de ordem pública e sua inobservância gera incompetência absoluta, podendo ser declarada a qualquer tempo a competência territorial constitui nulidade relativa devendo ser arguida na primeira oportunidade sob pena de prorrogação de competência (VIANNA & MACHADO, 2013, p.47).

Torna-se de extrema importância quando do cometimento de um crime que se defina qual será a autoridade competente para seu processamento e julgamento. Esta questão apresenta igual importância nos crimes cibernéticos, contudo, trata-se de uma tarefa um pouco mais difícil, visto que no meio virtual não existem fronteiras o que quer dizer, maior dificuldade em definir onde ocorreu a conduta delituosa bem como seu desenrolar, que pode ter sido tanto internamente quanto em outros países (SILVA; FREITAS, 2013, p.20).

Na Internet fica muito difícil demarcar um território, as relações jurídicas que passam a existir podem ser entre pessoas de um país e outro, diferentes culturas com a ocorrência de comunicação contínua, cujas relações criadas devem ser protegidas de modo a dirimir eventuais litígios que venham a acontecer. Para se determinar qual lei será aplicável a cada caso existem inúmeros princípios quais sejam, o do endereço eletrônico, o do local onde a conduta exerceu seus efeitos, do domicílio do consumidor, da localidade do réu, o da eficácia da execução judicial (PINHEIRO, 2010, p.80).

É necessário que o Brasil busque cooperação internacional para punir os crimes cibernéticos, visto que o modo como se realizam esses crimes, seu alcance poderá ir além dos limites territoriais nacionais, afetando também outros países, como por exemplo aderir de tratados e convenções internacionais de combate ao crime cibernético, possibilitando a aplicação da lei penal e processual penal quando o crime cometido por meio virtual tenha incidência no estrangeiro e de qualquer forma também havido relação com o território brasileiro (SILVA, 2015, p. 57).

No que tange a competência, a legislação penal brasileira adota a teoria da ubiquidade, conforme disposto em seus artigos 5º, 6º, 7º, aplicando a legislação pátria, para os crimes praticados no Brasil ou realizado por brasileiro ainda que tenha caráter transnacional, mesmo em caso de prática criminal no estrangeiro (CRESPO, 2011, p.118).

A legislação processual penal por outro lado segue a teoria do resultado, e dispõe sua aplicação quando o lugar onde os crimes cujo resultado ou último ato executório tenha ocorrido em território nacional, nos termos do artigo 70 do Código de Processo Penal. Poderão ocorrer também as hipóteses de prevenção de competência nos casos em que for incerto os limites entre duas comarcas, sendo a infração praticada em sua divisa, ou nos casos de crime continuado ou permanente praticado em território de duas ou mais jurisdições (SILVA, 2015, p. 57).

6.1. Competência nos Crimes Cibernéticos Próprios

Os crimes informáticos próprios obedecem às regras gerais de competência, tanto as existentes na Constituição Federal qual as existentes no Código de Processo Penal, contudo, apresentam algumas particularidades. No que tange a competência por prerrogativa de função, não há nenhuma ressalva. Contudo, com relação a competência em razão da matéria em se tratando do crime previsto no artigo 154-A do Código Penal entende-se que o bem jurídico tutelado no crime informático próprio é a inviolabilidade das informações

informatizadas, podendo ser seu titular tanto o particular quanto agente de órgão público, o que quer dizer que para que se defina a competência em razão da matéria (Federal ou Estadual) faz-se necessário que se defina a titularidade do bem violado sendo considerado a Internet apenas como mero instrumento para a prática delitiva (VIANNA & MACHADO, 2013, p.49).

Em se tratando de competência territorial aponta o artigo 70 do Código de Processo Penal que a competência será definida "pelo lugar em que se consumar a infração, ou em caso de tentativa, pelo lugar onde se deu o último ato executório".

Esta interpretação encontra respaldo na ideia de haver maior facilidade na coleta de provas, entretanto, há críticas no que diz respeito ao termo "momento da consumação", pois este poderá se dar em local completamente diverso da prática delitiva, o que dificultaria a produção do conjunto probatório. Sendo assim, se forem diversos os locais de realização dos atos executórios e da consumação, acredita-se ser adequado a utilização da prevenção, ou seja, competente seria aquele que primeiro realizasse algum ato valido no processo (VIANNA & MACHADO, 2013, p.49).

Segundo Vianna e Machado (2013, p.50) a competência para processar e julgar os crimes cibernéticos próprios caso seja seguido estritamente o Código de Processo Penal será o do juízo onde ocorrer o resultado do delito, ou seja, se alguém do estado A violar computador que se encontre em estado B, o juízo competente para processamento e julgamento do feito será o do estado B. Ademais estes mesmos autores consideram ainda mais adequado que o Código de Processo Penal siga as diretrizes do Código Penal no que diz respeito ao seu artigo 6º que tornaria competente tanto o juízo local da conduta quanto o juízo do local do resultado.

Nos casos de crimes cibernéticos com caráter de transnacionalidade, os critérios adotados devem ser dos descritos no artigo 70, §§ 1º e 2º do Código de Processo Penal.

Nestes dois casos, se o crime estiver previsto em tratado ou convenção internacional a competência será da justiça federal. Quando incerto o limite territorial da consumação do crime informático ou no caso de crime continuado a competência será fixada pela prevenção, nos termos do artigo 70, § 3º do Código de Processo Penal (VIANNA & MACHADO, 2013, p.49).

Revista Matiz Online
ISSN 21794022

6.2. Competência nos Crimes Cibernéticos Impróprios.

Inicialmente cumpre destacar que muitos podem ser os crimes praticados por meio de dispositivos informáticos, contudo a legislação processual penal não traz de maneira expressa disposições relativas à competência para julgar estes crimes (SILVA, 2015, p. 66)

Nesta espécie de prática delitiva é respeitada ordem de competência normalmente aplicada na Constituição Federal e no Código de Processo Penal, pois neste caso o computador nada mais é do que um instrumento para a prática criminosa, não havendo neste caso ofensa do direito à inviolabilidade da informação de dados informáticos (VIANNA & MACHADO, 2013, p.50).

Conforme dispõe o artigo 70 do Código de Processo Penal, a competência em regra é determinada em razão do lugar onde a conduta criminosa se consumou ou no caso de crime tentado, no local da prática do último ato de execução. Contudo, levando-se em conta que o crime cibernético não apresentará apenas um alcance local, mas em muitos casos de ordem internacional, surge a necessidade de que tais crimes sejam estudados observando-se se os efeitos por eles produzidos incidem apenas em território nacional, mesmo que em diferentes localidades, ou se ultrapassam os limites territoriais brasileiros, o que caracterizará o chamado crime a distância (SILVA, 2015, p. 67).

Neste caso, vale tratar de algumas modalidades de crimes cometidos utilizando-se de dispositivos eletrônicos.

No crime de estelionato, em que a consumação ocorre no momento e lugar onde o criminoso obtém a vantagem indevida, por exemplo no caso de loja virtual fraudulenta onde a consumação ocorre onde o agente toma posse do dinheiro da vítima, seguindo a regra do artigo 70 do CPP a competência será a do local onde o agente delituoso se apropria da vantagem ilícita (VIANNA & MACHADO, 2013, p.50).

Grande dúvida prevalece com relação a competência dos crimes previstos nos artigos 241-A, e 241-B, da Lei 8.069/90 (Estatuto da Criança e do Adolescente) quando praticados pela Internet. Em se tratando do artigo 241-A, cuja consumação ocorre com a proliferação do conteúdo pornográfico infantil a consumação será a do local onde foi realizado o lançamento na Internet do referido material. Já, com relação a conduta descrita no 241-B, que consiste em armazenar material pornográfico infantil, a competência será a do local onde o material armazenado foi encontrado (VIANNA & MACHADO, 2013, p.51).

Com relação aos crimes contra a honra, estes seguirão o mesmo raciocínio dos crimes dispostos no ECA, acima citados, devendo ser a competência definida a partir do local

onde foi concluída a conduta delituosa, ou seja, o local onde o criminoso veiculou a mensagem, e não o do provedor onde está locada a mensagem ofensiva (VIANNA & MACHADO, 2013, p.51).

6.3. Investigação e Meios de Produção de Provas nos Crimes Cibernéticos.

A crescente evolução tecnológica e consequente aumento do número de dispositivos que acessam a rede mundial vem acompanhado de um aumento exponencial na pratica de delitos de natureza informática, o que representa um enorme desafio para os órgãos de investigação, em especial no Brasil que deverá traçar um planejamento e preparação para os problemas penais existentes e os que ainda surgirão (WENDT & JORGE, 2013, p. 230).

A investigação tem a finalidade de fornecer ferramentas para que o titular da ação penal possa ingressar em juízo, ficando a cargo da autoridade policial a tarefa de identificar a autoria e a materialidade do delito (CASTRO apud LOPES, 2014, p. 50).

Devido as inúmeras formas de prática de ilícitos por meios cibernéticos, torna-se imprescindível para o sucesso da investigação ao se tomar conhecimento da prática delitiva, identificar qual foi a ferramenta utilizada para sua prática, podendo ser citado a título de exemplo a utilização de programas maliciosos, e-mail, websites, programas de transferência de informações, grupos de debates, redes sociais, sites de comercio eletrônico dentre outros (CAVALCANTE, ano p. 6).

Estes delitos são marcados por algumas particularidades que resultam em maior dificuldade para a pratica investigativa, quais sejam, facilidade em ser apagados, alterados e perdidos seus vestígios, que apresentam complexo meio de apuração, muito acima das outras espécies de crimes.

Relevante também que se ressalte outras dificuldades comuns impostas a investigação dos delitos informáticos relacionadas a criação de dados criptografados, existência de senhas (ALMEIDA, 2011 p. 32).

Outra característica importante está relacionada a sua transnacionalidade, bem como a própria Internet, visto que a prática de delitos pode ocorrer de qualquer lugar do mundo.

Em que pese a complexidade dos crimes cibernéticos, seu procedimento é dividido de maneira relativamente simples em que se compreendem duas fases: a fase técnica, que é tida como a fase inicial da investigação e a fase de investigação policial propriamente dita. Durante a fase técnica são executadas tarefas cuja finalidade está relacionada a

localização do computador utilizado para a prática delitiva e entre essas tarefas estão a análise dos fatos narrados pela vítima e do fato ocorrido; orientações, com o fim de preservar material probatório; coleta inicial de provas, formalização do boletim de ocorrência; investigação dos dados na Internet sobre possíveis autores, registro de hospedagem e domínio; formalização das provas coletadas e apuração inicial; representação perante o Poder Judiciário para a quebra de dados, conexão e acesso; análise das informações enviadas pelos provedores (WENDT, JORGE, 2014, p.52-53).

As informações fornecidas pelos provedores são de suma importância, visto que quando ocorre a conexão de um computador ou aparelho similar a Internet lhe é atribuído um número de IP (Internet Protocol) cujo qual é exclusivo para aquele usuário e permite sua identificação e localização. Desta forma torna-se possível da realização da fase de campo, em que ocorrerão diligencias que permitirão o reconhecimento do local dos fatos sempre de maneira discreta devido a possibilidade de que se necessite da concessão de mandado de busca e apreensão, que ocorrerá de imediato caso seja identificado local que corresponda a residência (WENDT, JORGE, 2014, p.54).

Em regra, a autoridade policial ao proceder com as investigações irá se utilizar do procedimento previsto ao teor do artigo 6º do Código de Processo Penal, entretanto, para cada ferramenta utilizada na pratica de delitos virtuais haverá um procedimento especifico utilizado em sua investigação, a exemplo dos crimes praticados via e-mail em que deverá ser intimado o provedor para que este informe a autoria do delito. Neste caso a vítima do delito sabe o endereço eletrônico do agente e provedor utilizado e de maneira simples seria necessário somente que o provedor disponibilizasse o nome, qualificação e endereço do autor do crime. No caso de crime praticado através de sites deve-se identificar quem seria o responsável por este, o que na prática não é tão simples assim. Muitas vezes os administradores de sites, estrangeiros, se recusam a quebrar o sigilo de seus usuários e como não estão submetidas as leis nacionais, resulta em grande obstáculo para as autoridades brasileiras. As dificuldades não se limitam a questão supracitada, pois há também a questão da utilização de dados falsos pelo agente, computadores públicos ou acessados por mais pessoas além do autor do delito. Nestes casos o mais indicado é a realização da busca e apreensão dos computadores e a realização de uma análise profunda e minuciosa dos dados no intuito de buscar maiores informações (LOPES, 2012, p. 55).

Atinente aos meios de produção de provas deve-se deixar claro que os crimes cibernéticos admitem que estas sejam produzidas por todos meios lícitos, o que importa dizer

que podem ser utilizadas provas documentais, prova testemunhal, prova pericial. Todas estas hipóteses podem ser admitidas e utilizadas para a caracterização da materialidade e autoria dos crimes cibernéticos, contudo, em se tratando desta modalidade de crime merece especial atenção a prova pericial (VIANNA & MACHADO, 2013, p.74).

Em que pese não haja hierarquia entre os tipos de provas existentes, há de se concordar que a prova pericial é a mais significativa na apuração da materialidade e autoria do delito, visto a especificidade de sua prática e poderá ocorrer nos mais diversos tipos de equipamentos, como: maquinas caça-níqueis, placas de rede, roteadores, entre outros. Diversos também podem ser os tipos de procedimentos realizados no trabalho de perícia.

Diante disso deve-se ressaltar a importância da Lei 12.735/12, também publicada em 03 de dezembro de 2012 e dispõe em seu artigo 4º sobre a estruturação pelos órgãos da polícia judiciária de setores e equipes especializadas no combate aos delitos informáticos, apesar de já existirem em algumas cidades antes mesmo da publicação da referida lei, a exemplo da Delegacia Especializada de Investigação de Crimes Cibernéticos, ou DEICC (VIANNA & MACHADO, 2013, p.62).

7. **CONCLUSÃO**

O presente trabalho procurou abordar a evolução da Internet apresentando seu momento de criação e passando por momentos históricos de grande relevância para a compreensão da referida evolução.

Buscou-se no presente trabalho realizar uma abordagem acerca das principais ameaças, cada vez mais utilizadas a medidas que aumentam o número de pessoas que se utilizam desta ferramenta, seja para trabalho ou simplesmente para o lazer, o que deixa clara a necessidade de cautela por parte do usuário de dispositivos informáticos a fim de evitar a contaminação com tais ameaças.

Foi realizado também uma análise dos crimes mais praticados pelos meios informáticos ou contra dispositivos informáticos, abordando suas formas de tipificação bem como as classificações dadas pela doutrina para as diferentes espécies de crimes cibernéticos.

A análise dos crimes levou a uma abordagem sobre os métodos de investigação e principais meios de produção de provas tratando de maneira mais enfática a perícia, que apresenta especial relevância neste contexto visto ser realizado por especialista técnico capaz de exteriorizar através de laudo o conteúdo fático de um crime informático.

Revista Matiz Online
ISSN 21794022

Diante desta analises foi possível constatar que o Brasil evoluiu significativamente no trabalho de combate aos crimes cibernéticos, principalmente com o advento da Lei 12.737/12, que passou a tipificar condutas especificas para crimes desta natureza, bem como com a publicação da Lei 12.735/12 que trata da criação de setores especializados de investigação e repressão aos crimes cibernéticos dentro da polícia judiciária embora estes já existissem em determinadas localidades antes mesmo da criação da referida lei.

Com relação aos métodos de investigação e produção de provas percebe- se a necessidade de cooperação de empresas provedoras de Internet para o sucesso dos trabalhos, contudo observa-se a dificuldade diante do fato de muitas dessas empresas se encontrarem em outros países, muitas com políticas e legislações muito diversas da legislação brasileira.

Por se tratar de um ramo do direito ainda novo, o direito digital ainda carece muito de maiores estudos que visem trazer maiores informações sobre a relação do Direito, em especial do Direito Penal com o ambiente virtual.

Acima de tudo, ainda faz-se necessário o surgimento de novas de legislações, que busquem abranger o maior número possível de condutas delituosas dentro do ambiente virtual, visto ser este um ambiente dinâmico e que permite a criação incessante de novos meios para a prática delitiva.

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, Rafael Nader. **Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais**. 2011. Trabalho de Conclusão de Curso (Graduação) - Faculdade de Tecnologia de São Paulo, São Paulo, 2011.

CASSANTI, Moises de Oliveira. **Crimes Virtuais, Vítimas Reais**. 1ª Ed. Rio de Janeiro: Brasport, 2014.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. 2ª Ed. Rio de Janeiro: Lumen Juris, 2003.

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

CRESPO, Marcelo Xavier de Freitas. **Os crimes digitais e as Leis 12.735/2012 e 12.737/2012.** Boletim IBCCRIM, ano 21, n. 244, 2013.

ELEUTÉRIO, Fernando . **Análise do conceito de crime**. Revista Jurídica Mater Dei , Pato Branco - PR, v. 1, 2001.

FARIAS, Karen Steffani Coelho. C**rimes Sexuais Praticados No Meio Virtual No Século XXI**. 2013 Trabalho de Conclusão de Curso (Graduação) - Universidade Católica de Brasília, Brasília, 2013.

FRAGOSO, Heleno Cláudio. **Lições de direito penal: parte especial**: arts. 121 a 212 do CP. Rio de Janeiro: Forense, 1983.

GRECO, Rogério. **Curso de Direito Penal, Parte Geral**. 15ª Ed. Rio de Janeiro: Impetus, 2013. Vol. I.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet.** São Paulo: Editora Juarez de Oliveira, 2004.

KERR, Vera Kaiser Sanches. **A disciplina, Pela Legislação brasileira penal processual, da prova pericial relacionada ao crime informático praticado por meio da Internet**. Dissertação (Mestrado) – Faculdade de Engenharia, USP, São Paulo, 2011.

LOPES, Alan Moreira. **Crimes praticados por meio eletrônico**. 1ª Ed. Curitiba: Ag Book, 2012.

OLIVEIRA, Felipe Cardoso Moreira de. **Criminalidade informática**. 2002. Dissertação (Mestrado em Ciências Criminais) – Faculdade de Direito, PUC RS, Porto Alegre, 2002.

PINHEIRO, Patrícia Peck. **Direito Digital**. 5. Ed. São Paulo: Saraiva, 2013.

SILVA, Patrícia Santos. Direito e Crime Cibernético: Análise da competência em razão do lugar no julgamento das ações penais. 1ª Ed. Brasília: Vestnik,. 2015.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. 2ª Ed. Rio de Janeiro: Brasport, 2013.