UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

CRIMES CIBERNÉTICOS: ANÁLISE EVOLUTIVA E LEGISLAÇÃO PENAL BRASILEIRA

EDUARDO DULCETTI RAMOS

RIO DE JANEIRO

2017/2

EDUARDO DULCETTI RAMOS

CRIMES CIBERNÉTICOS: ANÁLISE EVOLUTIVA E LEGISLAÇÃO PENAL BRASILEIRA

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de Bacharel em Direito, sob a orientação do **Professor Dr. Carlos Eduardo Adriano Japiassú.**

RIO DE JANEIRO

2017/2

CIP - Catalogação na Publicação

DR175c

Dulcetti Ramos, Eduardo
CRIMES CIBERNÉTICOS: ANÁLISE EVOLUTIVA E LEGISLAÇÃO PENAL BRASILEIRA / Eduardo Dulcetti Ramos. -- Rio de Janeiro, 2017.
50 f.

Orientador: Carlos Eduardo Adriano Japiassú.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade de Direito, Bacharel em Direito, 2017.

1. Crimes cibernéticos. 2. Direito Penal. 3. Direito Processual Penal. 4. Regulamentação. 5. Competência. I. Japiassú, Carlos Eduardo Adriano, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

EDUARDO DULCETTI RAMOS

CRIMES CIBERNÉTICOS: ANÁLISE EVOLUTIVA E LEGISLAÇÃO PENAL BRASILEIRA

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de Bacharel em Direito, sob a orientação do **Professor Dr. Carlos Eduardo Adriano Japiassú.**

Data da Aprovação:_____/____/_____.

Banca Examinadora:

_____

Orientador

_____

Membro da Banca

_____

Membro da Banca

RIO DE JANEIRO

2017/2

AGRADECIMENTOS

Primeiramente, gostaria de agradecer à Deus, por ter me fortificado e ajudado a sustentar situações muitíssimo adversas no decorrer da faculdade e, principalmente, nesta reta final. Sou muito grato ao meu pai, Éverton Tenório Ramos, pois sempre que esteve presente em minha vida, com muito amor e apreço, prezou por minha formação intelectual. Muita gratidão à minha avó, Carmem da Costa Dulcetti, por ser uma segunda mãe para mim, por me dar tanto amor, aguentar meus dias ruins, ajudar na minha criação e fazer com que eu me tornasse a pessoa que sou hoje, inclusive em minha teimosia. Gratidão eterna e um sentimento enorme de saudade de minha mãe, Leila da Costa Dulcetti, a pessoa mais batalhadora e sonhadora que já conheci, a mulher que fazia tudo possível e impossível por mim, que fazia dos meus sonhos os seus, que foi minha base forte e o grande motivo para me fazer continuar sonhando e lutando por meus objetivos. Mãe, sei que o céu está em festa com esta conquista, e saiba que ela

também é sua! Eu te amo e tenho muito orgulho da mulher que sempre foi. Espero que, ao longo de minha vida, eu seja um décimo da pessoa que você foi, já estarei satisfeito. Um agradecimento especial à minha amada Daniela Caputi, que sempre soube que era o grande amor da minha vida. Retornou no momento certo, deixando tudo mais colorido e enchendo minha vida de alegria. Em meus momentos mais difíceis, mostrou-se uma mulher tão companheira que eu não poderia imaginar. Agradeço também à Rosana Amorim, ao Josafá e à todos que me apoiaram e ainda me apoiam para que eu enfrente os dilemas e desafios da vida. Agradecimentos aos meus amigos de Faculdade e da vida, os MITOS, Valmir Rodrigues (Valmito), Rodrigo Loureiro (Rodrimito), Pedro Tavares (Pedrola), Victor Lopez (Victola) e todos os demais que fizeram com que minha graduação tivesse momentos inesquecíveis de amizade, estudos e muita curtição. Agradeço ao meu professor e orientador Carlos Eduardo Adriano Japiassú, exemplo dentro e fora de sala de aula. A você, Mestre, serei eternamente grata. Por todos os ensinamentos, pela paciência e disponibilidade. Por fim, mas não menos importante, agradeço à Faculdade Nacional de Direito e à todos seus funcionários, que me proporcionaram cinco anos inesquecíveis e essenciais em minha vida, que mudaram meu jeito de ser e de encarar a vida e me tornaram um homem com pensamentos mais altruístas e me fazem, todos os dias, ter vontade de exercer o Direito e a Justiça.

RESUMO

O presente trabalho faz uma análise sobre o surgimento dos crimes cibernéticos e os atuais conceitos dessa nova forma de criminalidade, decorrente das inovações tecnológicas, da globalização e da disseminação de novos conteúdos tecnológicos. Busca também analisar a tipicidade das condutas mais comuns e mais danosas aos bens jurídicos que o Direito visa proteger. Referencialmente ao ciberespaço, serão analisadas as fraudes virtuais, crime ardiloso que está no rol de crimes que mais assolam o ambiente virtual. O estelionato, outro tipo peculiar de fraude. A invasão de privacidade, sob a ótica da Lei 12,737/2012, mais conhecida como Lei Carolina Dieckmann, que busca proteger as informações pessoais e os dados dos usuários digitais de invasores mal-intencionados. Os crimes contra a honra, levando em consideração o falso sentimento de anonimato e inalcançabilidade dos seus sujeitos ativos. A pornografia infantil, mercado obscuro que movimenta bilhões de reais e é objeto de demasiada atenção por parte das autoridades de todo o mundo. Ademais, tem também como objetivo vislumbrar a evolução do Direito brasileiro no tratamento dessas condutas delitivas, analisar a legislação estrangeira sobre o assunto e o tratamento que o Judiciário realiza nesse contexto, tanto em relação à sua competência quanto na análise de provas. Nessa meada, buscará desenvolver a dificuldade das autoridades policiais na obtenção de provas, por se tratar de um ambiente desfavorável para o rastreamento das mesmas. Além disso, versará também sobre a necessidade de perícias especializadas e o instituto da produção antecipada de provas.

Palavras-chaves: Crimes cibernéticos – Internet – Ambiente virtual – Globalização – Provas – Autoria – Investigação – Competência.

ABSTRACT

The present work analyzes the emergence of cybercrime and the current concepts of this new form of crime, resulting from technological innovations, globalization and the dissemination of new technological contents. It also seeks to analyze the typical behavior of the most common and most harmful to the legal goods that the law aims to protect. Referentially to cyberspace, will be analyzed virtual frauds, a cunning crime that is in the list of crimes that most devastate the virtual environment. Larceny, another peculiar type of fraud. The invasion of privacy, under the perspective of Law 12,737/2012, better known as the Carolina Dieckmann Act, which seeks to protect the personal information and data of digital users from malicious intruders. Crimes against honor, taking into account the false feeling of anonymity and unreachability of their active subjects. Child pornography, a dark market that moves billions of dollars and is subject to much attention by authorities around the world. In addition, it also aims to glimpse the evolution of Brazilian law in the treatment of these delinquent conduct, to analyze the foreign legislation on the subject and the treatment that the Judiciary performs in this context, both in relation to its competence and in the analysis of evidence. In this vein, it will seek to develop the difficulty of the police authorities in obtaining evidence, because it is an unfavorable environment for tracking them. In addition, it will also address the need for specialized expertise and the institute for the early production of evidences.

Keywords: Cyber crimes – Internet – Virtual environment – Globalization – Evidences – Authorship – Inquiry – Competency.

SUMÁRIO

INTRODUÇÃO

Este trabalho tem por objeto a explanação sobre o surgimento de novos delitos em decorrência do uso da internet, e a necessidade do Direito em acompanhar as mudanças trazidas pela evolução tecnológica.

Nesta baila, os crimes digitais serão tratados nesse contexto de influência da informática no Direito Penal e da necessidade de adaptação do direito à nova realidade tecnológica da sociedade atual. A promulgação da lei 12.737/12 foi o primeiro passo dado no combate a esses crimes. Contudo, além da simples tipificação dos novos delitos decorrentes da influência da evolução tecnológica na sociedade atual, outras questões, diretamente afetadas pelas particularidades características dos crimes cibernéticos, merecem especial discussão. A forma e o ponto de desenvolvimento em que estão as legislações internacionais em matéria penal cibernética. A velocidade e novidade com que esses crimes se perpetuam, bem como os bens jurídicos atingidos por esses delitos são peculiaridades que dificultam a investigação criminal e a produção de provas. A necessidade de peritos especializados, a dificuldade na identificação da autoria e a necessidade da produção antecipada de provas.

O aludido tema foi escolhido em virtude de sua contemporaneidade e, mais do que isso, da importância de despertar para um perigoso cenário de violação de direitos subjetivos e objetivos em um ambiente em que a impunidade parece reinar. Isso denota não apenas a relevância jurídica do tema, mas também a sua relevância político-social. Apesar de serem pouco difundidos e haver até certa escassez teórica sobre o tema, é certo que todos os dias milhares de pessoas em todo o mundo são vítimas de crimes cibernéticos de todas as espécies e ofensividades, chegando até mesmo a ultrapassar o número de crimes praticados no mundo real.

A sociedade contemporânea, interligada e global, passa cada vez mais rápido por grandes transformações tecnológicas. Em decorrência desse crescimento desenfreado da tecnologia da informação, houve o surgimento de diversas ferramentas para otimizar nosso tempo, ideias e conectar as pessoas a todo tempo. A mais dinâmica e importante delas, a internet, rede mundial de computadores, é capaz de interligar usuários do

mundo inteiro, inovação essa que tornou real uma maior facilidade de conexão. As vantagens e benefícios oferecidos pela internet resultaram na formação da chamada sociedade da informação, caracterizada pela importância cada vez maior da informação e pela dependência vertiginosa dos recursos tecnológicos em atividades do cotidiano.

No entanto, a internet, que a princípio surgiu como uma nova tecnologia de comunicação e deveria ser utilizada em prol da sociedade, transformou-se em um instrumento utilizado para a prática de condutas ilícitas demasiadamente perigosas, fruto da fácil adaptação das pessoas às inovações tecnológicas. A internet tornou-se um ambiente para o cometimento de novos delitos, até então não previstos na legislação, e também como um novo meio para a prática de condutas ilícitas já tipificadas.

A magnificência da tecnologia, velocidade de acesso e a disseminação da informação acrescentaram algumas peculiaridades no tratamento dos crimes cibernéticos. Estes tipos de crimes são caracterizados pela velocidade com que são cometidos e a novidade de sua apresentação ao mundo jurídico, que quando considerados juntamente com a ofensa a um bem jurídico especial, exigem conhecimentos específicos para que se possa chegar aos indícios de autoria e materialidade da infração penal.

A discussão acerca dos crimes cibernéticos se mostra muito útil, tendo em vista que, com a evolução tecnológica, a internet se mostrou o principal meio de comunicação e tráfego de informações, transformando o cotidiano da sociedade atual. Essa modernização não só atingiu as atividades cotidianas, mas também se estendeu sobre o Direito, na medida em que permitiu a prática de novos crimes pela rede mundial de computadores.

Por ocasião do Direito ser observado como um instrumento regulador e organizador da sociedade, e tendo em vista que as evoluções sociais, econômicas e políticas influenciam nos aspectos jurídicos, incumbe ao Direito verificar todas as mudanças que foram decorrentes da evolução tecnológica pela qual passa a sociedade, buscando se adaptar as mutações, a fim de promover novas soluções para as novas peculiaridades trazidas com a prática dos crimes, em especial, os cibernéticos.

Dessa forma, é importante destacar os antecedentes históricos da internet e a forma com a qual a rede mundial de computadores, a princípio um novo meio de comunicação, se transformou em um instrumento utilizado para a propagação de condutas delitivas.

Destarte, o direito está ligado à evolução da sociedade. Conforme a sociedade se desenvolve, o direito vai se adequando aos anseios da mesma. Novas normas são elaboradas para se regular a convivência, sendo assim, com o avanço da tecnologia e sua inserção no cotidiano das pessoas, é que se fez a necessidade do direito regular às relações que passaram a ser desenvolvido em ambiente virtual.

1. O SURGIMENTO DOS CRIMES CIBERNÉTICOS

1.1. HISTÓRICO

Os computadores e a rede mundial de interconexão simultânea surgiram para facilitar nosso cotidiano. As tarefas que antes eram realizadas em espaços de tempo muito longos, passaram a ser realizadas quase de forma instantânea. O computador é uma máquina que armazena e transforma informações, sob o controle de instruções predeterminadas.[1]

Desde a antiguidade até os dias atuais, o ser humano vem buscando desenvolver novos objetos e ferramentas que torne as atividades do dia-a-dia mais fáceis e, de certa forma, mais prazerosas.

Uma alteração importante que o mundo experimentou foi a Revolução Industrial, a qual alterou as feições do mundo moderno, modificou o estilo de vida da população mundial no geral e alavancou um avanço significativo na mudança do homem do campo para as cidades, iniciou primeiramente no Reino Unido, por volta do século XVIII, talvez porque a Inglaterra possuísse grandes reservas de carvão mineral em seu subsolo, a principal fonte de energia para que as máquinas daquele período[2].

As máquinas surgiram em longuíssima escala, as *polis* começaram a se desenvolver, os trabalhadores que antes trabalhavam de forma artesanal passaram a controlar máquinas, as fábricas passaram a produzir cada vez mais, e as novas invenções, navios e locomotivas a vapor, fizeram com que a circulação das mercadorias se tornasse cada vez mais rápido, de modo que as matérias-primas chegassem mais rapidamente até as pessoas, e começaram a surgir de forma mais expressiva os inventores que viriam a mudar a maneira que vemos o mundo. Podemos citar grandes invenções, por exemplo, a Fotografia (1839), Telefone (1876), Luz Elétrica (1879), Televisão (1924), dentre outras tantas invenções que alteraram a forma como as pessoas

[1]FRAGOMENI, Ana Helena. Dicionário Enciclopédico de Informática. Vol.I. Rio de Janeiro: Campus, 1987, p.125

[2]SUAPESQUISA – Formulários e Pesquisas Online. Revolução Industrial, História da Revolução Industrial, pioneirismo inglês, invenções de máquinas, passagem da manufatura para a maquinofatura, a vida nas fábricas, origem dos sindicatos. Disponível em: <http://www.suapesquisa.com/industrial>. Acesso em: 11/10/ 2017.

viviam na época em que surgiram estes inventos, e de certa forma, o modo no qual vivemos hoje[3].

Em meados dos anos 40, foram criados os transistores, futuros microprocessadores, dando o arcabouço para que os computadores se tornassem acessíveis a qualquer pessoa[4], o que não ocorria até então. Toda essa evolução permitiu o crescente desenvolvimento tecnológico de computadores, seja para o uso pessoal, seja para o uso profissional.

Em 1957, o presidente dos EUA, em atitude de encontro ao lançamento do primeiro satélite espacial russo, Sputnik, criou a Agência de Investigação de Projetos Avançados (ARPA) com o objetivo de promover o desenvolvimento tecnológico do país e coordenar as atividades relacionadas ao espaço e aos satélites, além de criar um sistema de defesa à prova de destruição[5]. No ano seguinte, a ARPA se enfraqueceu em virtude da criação da NASA (National Aeronautics & Space Administration) e para se manter, decidiu modificar sua perspectiva de pesquisa, incluindo novos projetos, bem como a parceria com universidades, tornando sua atuação mais técnica e científica[6]. A ideia para atender a demanda da Força Aérea Americana era criar um modelo de rede independente de um único núcleo central, a fim de evitar o comprometimento de toda a rede de comunicação no caso de destruição deste. Isto é, o objetivo era a criação de uma rede de comunicações invulnerável a qualquer tentativa de destruição ou controle por parte de qualquer entidade ou potência[7].

A importância cada vez maior de se criar uma rede capaz de unir computadores distantes entre si, possibilitando o contato direto de dados entre eles, foi o fator propulsor que agilizou o crescimento contínuo da ARPANET. A rede de comunicações

---

[3]SUPERDICAS - Invenções que mudaram o mundo e sobreviveram ao tempo. Disponível em: <http://www.superdicas.com.br/almanaque/almanaque.asp?u_action=display&u_log=254>.Acesso em: 12/10/ 2017.

[4]GOUVEA, Sandra. O direito na era digital: crimes praticados por meio da informática. Rio de Janeiro: Editora Mauad, 1997, p. 31.
[5]WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos, Ameaças e Procedimentos de investigação. Rio de Janeiro: Brasport, 2013. p.5.
[6]Ibidem, p.6.
[7]TURNER, David; MUNOZ, Jesus. Para os filhos dos filhos de nossos filhos: uma visão da sociedade de internet. São Paulo: Summus, 1999.p.29.

que, à princípio, foi criada para atender um pedido da Força Aérea Americana passou a interligar universidades, órgãos militares e governo. Esse crescimento resultou na internet atual que é um dos principais meios de comunicação da sociedade contemporânea, interligando computadores do mundo todo.

A Internet é uma Rede de computadores, integrada por outras redes menores, que se comunicam entre si. Os computadores se comunicam através de um endereço lógico, chamado de endereço IP, onde uma gama de informações são trocadas, surgindo ai o problema. Existe uma quantidade enorme de informações pessoais disponíveis na rede, ficando à disposição de milhares de pessoas que possuem acesso à internet, e quando não disponíveis pelo próprio usuário, são procuradas por outros usuários que buscam na rede o cometimento de crimes[8].

Nos últimos anos, é crescente o número de pessoas conectadas à internet. O desenvolvimento tecnológico fez com que a sociedade se tornasse dependente da eficiência e segurança da tecnologia da informação. Justamente por isso, os sistemas informatizados atualmente são tão importantes na sociedade que a maioria das pessoas, seja física ou jurídica, depende de um dispositivo informatizado, para uso na esfera comercial, como a execução de ações financeiras pelo computador, ou para uso na esfera empresarial, como a utilização dos bancos de dados para o armazenamento de seus arquivos mais valiosos[9].

Apesar dos benefícios trazidos com o advento da internet e o seu crescente desenvolvimento, a evolução tecnológica permitiu também o surgimento de condutas ilícitas praticadas na rede mundial de computadores. A facilidade de acesso à internet permitiu não somente a interconexão entre pessoas do mundo todo, mas também o surgimento de aspectos negativos, novos riscos representados por práticas ilícitas.

Lévy[10], em sua obra *Cyberdémocracie: Essai de Philosophie Politique*, já havia identificado um crescente aumento por parte das pessoas que utilizavam a internet e já

[8]INELLAS, Gabriel Cesar Zaccaria. Crimes na Internet. São Paulo: Editora Juarez de Oliveira, 2004.p.3.
[9]NOGUEIRA, Sandro D'Amaro. Crimes de Informática. Leme: BH Editora, 2009, p. 36.
[10]LEMOS, André/LÉVY, Pierre. O futuro da Internet: em direção a uma ciberdemocracia. São Paulo: Paulus, 2010.p.10.

previa um aumento substancial, tendo em vista o desenvolvimento de novas tecnologias, interfaces de comunicação sem fios e o uso integrado de dispositivos portáteis.

Hoje, corroborando para a tese de Lévy, a internet está disponível em vários dispositivos portáteis, das mais diferentes formas. Milhares de pessoas permanecem por vezes mais tempo navegando na internet do que vivendo o mundo real. Mídias sociais, leitura de livros, videoconferências, enfim, a rede mundial de computadores é, acima de tudo, uma rede mundial de indivíduos, onde existem relações jurídicas fluindo. Nessa esteira, o Direito deve trazer soluções para os litígios que venham a ocorrer dentro deste ambiente virtual. O Direito é uma solução prática de planejamento e estratégia que só pode ser feita em equipe, num contato direto com as demandas e a própria evolução da sociedade. O Direito deve adaptar-se às demandas, aos anseios da sociedade, onde as transformações são cada vez mais rápidas[11].

Os primeiros crimes de informática começaram a ocorrer na década de 1970[12]. Na maioria das vezes, era praticado por especialistas em informática, em que o objetivo era driblar os sistemas de seguranças das empresas, com foco principal nas instituições financeiras. Nos dias atuais, o perfil das pessoas que praticam crimes de informática já não são mais semelhantes aos da década de 70, os usuários mudaram. Atualmente, qualquer indivíduo que possua um conhecimento não tão aprofundado, mas que obtenha acesso à internet pode praticar algum crime de informática. O usuário doméstico já tem um conhecimento bem maior sobre o uso de computadores e tecnologia voltada para internet.

1.2. CONCEITO DE CRIMES CIBERNÉTICOS

Ab initio, antes mesmo de conceituar os crimes cibernéticos, devemos fazer um esclarecimento acerca de seu sujeito ativo. Devemos, desse modo, saber qual é a diferença entre os hackers e os crackers. O hacker tem um conhecimento avançado em

[11]PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.44 e 45.
[12]CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança noBrasil. Disponível em: <http://www.cert.br>. Acesso em: 14/10/2017.

computação e usa todo esse conhecimento em favor da justiça, trabalhando junto com a polícia para combater essa rede de criminosos virtuais, enquanto os crackers são aqueles responsáveis pelos crimes praticados na rede através da internet. Geralmente, em programas televisivos ou jornais noticiam fatos errados, declarando que o hacker é o causador do dano.

Com essa rápida explicação, voltemos ao que mais nos interessa. Com a disseminação dos computadores e do acesso à Internet, surgiram crimes e criminosos especializados na linguagem da informática, proliferando-se por todo o mundo. Tais crimes são chamados de crimes virtuais, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, delitos cibernéticos, crimes transnacionais, dentre outras nomenclaturas.

Pelos ensinamentos de Sandro D'Amaro Nogueira, o rol dos crimes cometidos por meio eletrônico é extenso[13]. Dentre eles estão: os crimes contra a honra - tais como a injúria, calúnia e difamação - os furtos, estelionatos, fraudes com cartão de crédito, desvio de dinheiro de contas bancárias, dentre outros. Várias são as formas utilizadas para a prática desses delitos tais como interceptação de comunicações, modificações de dados, difusão de pornografia infantil, terrorismo[14].

Decorrentes do avanço tecnológico da sociedade, os crimes cibernéticos são condutas ilícitas praticadas com o auxílio de um computador, seja contra outros computadores e sistemas informáticos ou informações nele contidas, seja como mero instrumento para a prática de um delito. A definição mais comum para os crimes cibernéticos é:

> "(...) aquele no qual um ou mais computador (es), equipamentos telemáticos ou dispositivos eletrônicos, interligados por meio de uma rede de comunicação, são utilizados, por um ou mais indivíduos, no cometimento de uma, ou mais conduta(s) criminalizada(s), ou são alvo(s) desta(s). O homem interagindo com uma maquina – retroalimentando-a com informações por meio de mensagens – através de uma rede de computadores (cibernética) interligados (ciberespaço), agindo conforme uma conduta previamente

[13]NOGUEIRA, Sandro D'Amaro. Crimes de Informática. Leme: BH Editora, 2009, p. 36.
[14]CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. São Paulo: Editora Saraiva, 2011, p. 46.

> criminalizada (Crime informático) estereotiparia um modelo de cibercrime"[15].

O surgimento de novas condutas ilícitas praticadas através da internet, envolvendo a utilização de computadores é cada vez mais intensa e variada e acompanha o desenvolvimento das novas realidades tecnológicas e sociais. No entanto, apesar do reconhecimento da existência de tais condutas, não há um consenso quanto à denominação dos crimes cibernéticos.

Em meados da década de 1980, Tiedermann classificou os crimes de informática no âmbito dos delitos econômicos como: manipulações, espionagem, sabotagem e furto de tempo[16]. Já Ulrich Sieber elaborou um parecer especialmente para Comissão Europeia, classificando os crimes em: violações à privacidade, crimes econômicos, conteúdos ilegais e nocivos e outros ilícitos (crimes contra a vida, crime organizado, guerra eletrônica).

Mesmo que não exista uma unanimidade em relação à classificação dos crimes cibernéticos, a classificação mais comum é a de separar as condutas em que a informática é meio e as demais condutas. Para classificá-los, devem ser consideradas não só as condutas tradicionalmente tipificadas no ordenamento jurídico, agora praticadas com o auxílio da tecnologia (neste caso, o computador é utilizado como um meio para a prática do crime), mas também aquelas condutas consideradas perigosas, ainda não incriminadas no Brasil, cujos bens jurídicos atingidos são exclusivamente os sistemas informatizados[17].

Diante da diversidade de classificações dos crimes cibernéticos, a forma mais comum de se classificar os crimes cibernéticos é a que considera o bem jurídico atingido com a prática do crime: "condutas perpetradas contra um sistema informático (crimes próprios) e condutas perpetradas contra outros bens jurídicos (crimes impróprios)"[18]. Nessa meada, Ivette Senise Ferreira e Vicente Greco Filho adotam a

---

[15]COLLI, Maciel. Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos. Juruá Editora, 2010. P. 44.
[16]CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. São Paulo: Editora Saraiva, 2011. p. 60.
[17]MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012. p. 60.
[18]CRESPO, op. cit., p. 62.

classificação que divide os crimes cibernéticos em crimes próprios[19], condutas praticadas contra os bens jurídicos informáticos; e crimes impróprios, condutas praticadas contra os bens jurídicos tradicionais.

Segundo Ivette Senise Ferreira, o computador ou sistema de informática é um instrumento como tantos outros, armas de fogo, explosivos, utilizados por criminosos para facilitar o cometimento de um delito. Cabe ao Estado tutelar as novas modalidades e lesões aos diversos bens e interesses que surgiram com a crescente informatização das atividades individuais e coletivas desenvolvidas na sociedade. Essa informatização colocou novos instrumentos nas mãos dos criminosos e propiciou a formação de uma criminalidade específica da informática cujo alcance ainda não foi corretamente avaliado[20].

A criminalidade informática não trouxe apenas como consequência o surgimento de novas condutas ilícitas, além daquelas já previstas no ordenamento jurídico brasileiro, praticadas com o auxílio do computador. Outras particularidades foram trazidas com o advento da internet, já que as novas condutas atingem aos mais variados bens e interesses da sociedade tais como a violação de bens jurídicos até então não atingidos com a prática de um crime.

Marcelo Xavier de Freitas Crespo afirma que a internet, além de permitir que a criminalidade se mostrasse de formas ainda não previstas na legislação, através de condutas ainda não tipificadas no ordenamento brasileiro, promoveu a alteração dos bens jurídicos atingidos com essa nova criminalidade. Diferentemente do que ocorria com a "criminalidade não informática", que atinge os bens jurídicos individuais, a "criminalidade informática", em face da facilidade dos meios, tem o potencial de atingir os chamados bens jurídicos difusos, valores vislumbrados a partir de uma massa não

[19]A classificação dos crimes virtuais em próprios e impróprios não se confunde com a classificação já existente no direito penal, que utiliza os termos próprio e impróprio para classificar os crimes segundo o sujeito ativo. De acordo com essa classificação, o crime próprio é definido como aquele cujo tipo penal exige uma condição especial do sujeito que praticou o crime. Neste caso, o crime só poderá ser praticado por um grupo determinado de pessoas que possuam essa condição especial. Por exemplo, para o crime de peculato só poderá ser responsabilizado o funcionário público.

[20]FERREIRA, Ivette Senise. A Criminalidade Informática. Direito & Internet – Aspetos Jurídicos Relevantes. Editora Edipro, 2011, p. 208.

definida.

Devido a existência de lacunas da lei penal e da impossibilidade de se utilizar da analogia *malam partem* no direito penal, por conta do seu princípio regente da presunção de inocência, a criminalidade informática encontrou novas formas de se fazer presente, resultando em condutas prejudiciais ainda não tipificadas como crime. Além disso, houve uma alteração nos bens jurídicos atingidos com tais condutas, uma vez que a criminalidade não informática atingia os bens jurídicos individuais. De outro lado, com a sociedade digital globalizada, outros bens jurídicos (difusos) passaram a ser afetados[21]. Nesse sentido, Crespo classifica os crimes digitais como pluriofensivos, uma vez que "há proteção dos bens jurídicos tradicionais, mas, ao mesmo tempo, proteção de novos interesses derivados da sociedade de risco e de informação[22].

Não se trata apenas do surgimento de novas condutas ilícitas não tipificadas no ordenamento brasileiro, promovidas pelo desenvolvimento da internet, mas também de uma alteração dos bens jurídicos atingidos com a nova criminalidade. A criminalidade da informática passou a atingir também os bens jurídicos difusos em contrapartida aos bens jurídicos individuais atingidos pela criminalidade não informática.

O Direito Penal, além do dever de proteger os bens jurídicos já reconhecidos pelo nosso ordenamento e lesionados com o uso da informática, deve igualmente proteger os outros valores jurídicos recentes que surgiram a partir da proliferação dos computadores[23]. Não há como ignorar a existência de novos bens jurídicos relacionados à evolução tecnológica. Assim, o Direito Penal não pode somente tratar dos crimes cibernéticos relacionados aos bens jurídicos tradicionalmente protegidos.

A prática de condutas ilícitas efetivadas por meio da internet possibilita, não só a violação a bens jurídicos já previstos no ordenamento jurídico brasileiro quais sejam a vida, o patrimônio e a integridade física, mas também a lesão a outros bens jurídicos que ainda não gozam de proteção jurídica tais como a informação e a segurança dos

[21]CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. São Paulo: Editora Saraiva, 2011. p. 36.
[22]Ibidem, p. 57.
[23]LIMA, Paulo Marco Ferreira. Crimes de Computador e Segurança Computacional. São Paulo: Editora Atlas, 2011. p. 2.

sistemas de redes de computadores[24].

Assim, conforme leciona Paulo Marco Ferreira Lima, a informação se torna um novo bem jurídico, umbem imaterial a ser tutelado pelo Direito Penal, bem como os dados, a confiabilidade e a segurança dos sistemas e redes informáticas.

Ainda sobre esse mesmo autor, podemos retirar a determinada contribuição:

> "Surge com o advento da tecnologia da informática a necessidade de preservação de um bem jurídico novo, a que chama de "a informação sobre a informação", cuida-se de algo que reveste por si só um valor (econômico ou ideológico) suficientemente interessante, como para que a conduta correspondente seja merecedora de uma qualificação jurídica e de uma sanção, atendendo exclusiva e preferentemente à importância da informação eletrônica contida nos dados eletrônicos. "[25]

No Brasil, os crimes por meio da informática estão limitados à utilização dos computadores e às condutas ilícitas já previstas no nosso ordenamento jurídico. Sendo assim, na verdade, são analisados apenas os bens jurídicos atingidos por tal conduta, já previstos no ordenamento, determinando a sua tipicidade e punibilidade[26].

Ao se considerar a integridade e a inviolabilidade dos novos bens jurídicos atingidos com a criminalidade informática quais sejam a informação e os dados, novos paradigmas devem ser discutidos de forma a acompanhar as novas perspectivas de risco da sociedade da informação.

Ademais, analisemos diversas contribuições doutrinárias acerca do conceito de crimes cibernéticos, a fim de robustecer esta discussão:

Para Ramalho Terceiro:

---

[24]CRESPO, op. cit., p. 56.
[25]LIMA, Paulo Marco Ferreira. Crimes de Computador e Segurança Computacional. São Paulo: Editora Atlas, 2011. p. 4.
[26]FELICIANO, Guilherme Guimarães. Informática e criminalidade: primeiras linhas. Ribeirão Preto/SP: Nacional de Direito, 2001.

> [...] os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas.

À luz da doutrina de Augusto Rossini, entendemos que:

> [...] o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

Podemos extrair, portanto, que estes últimos autores, assim como Guilherme Guimarães Feliciano (outro autor que versa sobre os crimes cibernéticos), apresentam um conceito um tanto quanto amplo, em relação à autores como Marcelo Xavier de Freitas Crespo e Roberto Antônio Darós Malaquias, que vão além da pura e simples conceituação para adentrar as peculiaridades e minúcias dos crimes cibernéticos.

Portanto, ante todo o exposto, observamos que a internet, rede mundial de computadores, apresenta uma maior fragilidade e possibilidade de se praticar os "cybercrimes", por se tratar de uma rede pública e de não ser regida por qualquer tipo de ordenamento. Isso permite que usuários dos mais variados níveis de conhecimento técnico sobre informática possam acessá-la sem qualquer restrição. Nas palavras de Maciel Colli: "(...) Diante deste tipo de oportunidade, o cometimento de "cybercrimes" por meio da internet pode envolver a multinacionalidade de sujeitos e bens"[27].

Outra contribuição do francês Pierre Lévy, é o entendimento de que não se pode confundir o conceito de virtualização com uma "desrealização". Para ele "virtual é aquilo que existe apenas em potência e não em ato. O campo de forças e de problemas que tende a resolver-se em uma atualização"[28].

---

[27]COLLI, Maciel. Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010. p. 45.
[28]LÉVY, Pierre. Cibercultura. São Paulo: Editora 34, 2010. p. 49

No cotidiano, enquanto a realidade pressupõe algo tangível; a palavra virtual ou cibernética costuma ser empregada no sentido de ilusão. Na verdade, a realidade se apresenta de duas formas distintas: virtualidade e atualidade. O conceito de virtual está mais associado à "desterritorialização", ou seja, ao fato da sociedade digital ter "construído" um novo território, dificilmente demarcável, que permite que pessoas no mundo inteiro, de diferentes culturas, se comuniquem e troquem informações remotamente. Nas palavras do francês Lévy "ainda que não seja possível fixar o virtual em nenhuma coordenada espaçotemporal, o virtual é real"[29]. Não é correto, entretanto, tratar o mundo cibernético como um mundo sem regras, na qual tudo é permitido, pelo simples fato de considerá-lo uma "não realidade"[30].

A ausência de um território certamente calculável não é capaz de tornar a virtualização algo irreal. Oda internet situar-se no ciberespaço (espaço virtual), caracterizado pela inexistência de espaço físico, não deve ser utilizado como argumento para afirmar a sua irrealidade. A internet não deixa de ser real em razão da ausência de espaço físico e a forma como o Direito deve lidar com essa ausência é uma das grandes questões da atualidade.

Diante desse cenário, cabe ao Direito acompanhar as diversas mudanças ocasionadas pela evolução da tecnologia, tendo em vista que as mudanças evolutivas no mundo social, econômico e político influenciam nos aspectos jurídicos, no sentido de que sejam discutidos regulamentos e leis, de forma a minimizar os conflitos entre os indivíduos que se utilizam deste meio[31].

Comumente, o Direito busca acompanhar a modernização da sociedade. Todos os veículos de comunicação (imprensa, telefone, rádio, televisão), desde o momento em que se tornaram fontes de comunicação em massa, passaram a ter uma relevância jurídica, na medida em que trouxeram ao mundo jurídico novas particularidades e desafios. Nas palavras de Patrícia Peck, "(...) a massificação do comportamento exige que a conduta passe a ser abordada pelo Direito, sob pena de criar insegurança no

[29]Ibidem, p. 50.
[30]Ibidem, p. 50.
[31]CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. São Paulo: Editora Saraiva, 2011. p. 38.

ordenamento jurídico e na sociedade”[32].

Os mecanismos inventados pelo homem, computadores e suas redes, possuem uma natureza dual, a depender da destinação que lhes é dado. Isto é, além do aspecto positivo de aproximar as pessoas e permitir a disseminação mais veloz da informação, possuem um aspecto negativo qual seja a prática de delitos à distância, caracterizados pelo anonimato, com um poder de lesividade muito maior do que aquele apresentado pela chamada criminalidade tradicional. Sendo assim, é um tipo de obrigação do Estado prever mecanismos de prevenção e repressão das condutas ilícitas.

A caráter de extrema urgência na criação de mecanismos de prevenção e repressão que suportem as peculiaridades advindas da prática de novas condutas ilícitas através da internet não impõe a criação de um novo direito. O Direito Cibernético deve ser consubstanciado como uma evolução do próprio Direito, já que, nele, são inclusos todos os princípios e regras já utilizados atualmente. Dessa forma, não há a necessidade da criação de um direito específico, qual seja o “direito da internet”, que contemple todas essas peculiaridades que advieram da internet, apenas há a necessidade de previsão dessas particularidades pelas áreas do Direito.

[32]PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Editora Saraiva, 2013, p. 76.

2. TIPOS PENAIS NO MEIO CIBERNÉTICO

Atualmente, estima-se que há, no Brasil, mais de 100 milhões de internautas, e esse número não pára de crescer, dia após dia. Segundo um estudo realizado pelo site alemão Alldas, atualmente o Brasil abriga o maior grupo de krackers do mundo, registrando-se invasões contra o Pentágono, a Microsoft e a IBM americana.

Dessa forma, é uma tarefa grandiosamente árdua e delicada verificar as condutas criminosas que se alastram pela internet, uma vez que é extremamente de difícil conhecimento em que local o agente que praticou o crime se encontra, tendo em vista que os crimes digitais não encontram barreiras na internet e se perpetuam livremente pela rede.

A maioria dos crimes que ocorrem na rede também existem no mundo real, o que ocorre é que tipos com devidas peculiaridades, o que faz com que seja necessário uma adequação quanto ao seu tipo penal.

O ambiente virtual da Internet, por proporcionar uma falsa sensação de liberdade plena, possibilitando o "anonimato" (que no Brasil é vedado pela CRFB/88, em seu art. 5º, inciso IV) e oferecendo um mundo sem fronteiras, impulsiona a prática de crimes complexos, que exigem uma solução rápida e especializada, pois o aumento desses crimes é diretamente proporcional aos avanços da tecnologia.

Destarte, avaliaremos em seguida os tipos penais de fraudes virtuais, estelionato, invasão de privacidade, crimes contra a honra, em geral, e a pornografia infantil, alguns crimes que assolam o ambiente cibernético e preocupam demais as autoridades Estatais.

2.1. FRAUDES VIRTUAIS

No tipo de crime definido como Fraude Virtual, o sujeito ativo pratica uma conduta de invasão, alteração ou modificação, pagamento ou supressão de dados eletrônicos ou programas, ou qualquer outra adulteração em um sistema de processamento de dados[33].

No entendimento de CERT-BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil)[34], a Fraude Eletrônica se define como:

> A fraude eletrônica consiste em uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, esse tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Segundo Paulo Marco Ferreira Lima[35], a definição de fraudes virtuais é a seguinte:

> É a invasão de sistemas computadorizados e posterior modificação de dados, com o intuito da obtenção de vantagem sobre bens, físicos ou não, por exemplo, a adulteração de depósitos bancários, aprovações em universidades, resultados de balanços financeiros, pesquisas eleitorais, entre outros.

As fraudes eletrônicas têm crescido assustadoramente nos últimos anos, especialmente no que diz respeito à modalidade de furto mediante fraude (art. 155 do Código Penal), a qual se caracteriza pelo envio de um e-mail falso (phishing) para um usuário, e são capturados dados de sua conta bancária, mediante a instalação de um programa em seu equipamento de acesso à internet.

---

[33]LIMA, Paulo Marco Ferreira. Crimes de computador e segurança computacional. Campinas, SP: Ed. Millennium, 2005.p.134.
[34]CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha.
[35]LIMA, Paulo Marco Ferreira. Crimes de computador e segurança computacional. Campinas, SP: Ed. Millennium, 2005.p.60.

Ademais, Antonio Loureiro Gil conceitua as Fraudes Virtuais como:

> Ação intencional e prejudicial a um ativo intangível causada por procedimentos e informações (software e bancos de dados), de propriedade de pessoa física, ou jurídica, com o objetivo de alcançar benefício, ou satisfação psicológica, financeira e material.

As fraudes virtuais podem possuir dois tipos de origens: a) interna: quando são praticadas por empregado ou terceiro que se encontram dentro do local a ser fraudado; e b) externa: o fraudador não possui vínculo com o local que será fraudado, mas isso não significa que o agente da fraude não possa um dia ter tido relação com a vítima[36].

Nas fraudes o usuário é induzido a fornecer seus dados pessoais e financeiros, na maioria das vezes mascarada por trás de páginas duvidosas, o qual o usuário e encaminhado para páginas fraudulentas, na maioria das vezes os fraudadores utilizam as mídias sociais, e tentam de todas as maneiras persuadir o usuário a fornecer seus dados pessoais.

Um crime que acontece diariamente é o chamado furto de dados, em que o CP conceitua como furto, em seu art. 155, como sendo "subtrair, para si ou para outrem, coisa alheia móvel", a questão que se tem discutido, é se poderia enquadrar o furto de dados como sendo o furto do art. 155 do CP, tendo em vista que poderia o mesmo não se enquadrar no tipo legal, visto que na conduta do agente o mesmo pode levar os dados da empresa e apagá-los, ou também pode levar os mesmos mediante cópia e não eliminá-los, sendo que nesta ocasião não haveria o quesito de indisponibilidade do bem, no caso para configurar a subtração[37].

2.2. ESTELIONATO

O suibconceito de Direito Penal Cibernético é relativamente novo. Alguns autores separam as condutas delituosas em razão do seu agente passivo. Sendo possível ser separado "em face dos computadores", como elemento físico e paupável, e "contra

[36]PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.311.
[37]PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.313.

os dados os quais se encontram neles".

As condutas variam conforme o uso que o agente faz dos meios eletrônicos disponíveis. Um dos crimes mais populares tanto na no "Cyberespaço" quanto fora dele é o estelionato, que vem tratado no Código Penal, em seu art. 171, caput, e reza que:

> Art. 171. 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: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Ademais, em seu § 3º, o artigo estabelece que a pena será aumentada de um terço, na situação em que o crime for cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

No caso da aplicação do estelionato no meio informático, a conduta do agente será de induzir ou manter a vítima em erro, e com isso, obtendo vantagem ilícita, para si ou para outrem. Diversas são as condutas dos estelionatários na internet, a questão é tipificá-las como estelionato, o legislador previu, como meio executório a fraude com o objetivo de obter consentimento da vítima, iludi-la para que voluntariamente entregue o bem, o agente leva a vítima a erro, enganando a mesma, mantendo-a em erro.

Uma das condutas típicas do estelionato pela Internet consiste na conduta do agente encaminhar e-mails com conteúdo falso ao usuário, induzindo o mesmo a clicar em links disponíveis no corpo do e-mail, em que muita das vezes direciona o usuário para um site falso onde o mesmo digita informações pessoais ao agente que formulou a pagina falsa, estas informações são enviadas ao agente por meio da internet, que após apropriar-se dos seus dados bancários, transfere os valores disponíveis em conta[38] para o seu domínio.

2.3. INVASÃO DE PRIVACIDADE

Chegamos ao tipo penal que foi o propulsor do crescimento dos estudos acerca

[38]INELLAS, Gabriel Cesar Zaccaria de. Editora Juarez de Oliveira. São Paulo, 2004.p.44

dos Crimes Cibernéticos no Brasil. Este crime foi alvo de diversas discussões e da elaboração de Lei específica para este delito.

Quanto à esse crime, veremos que nossa legislação elaborou a Lei 12.737/2012, justo atriz Carolina Dieckman incorreu em um incidente e teve suas fotos em momentos íntimos furtadas de seu computador pessoal. Em 2013, houve outra invasão de servidor, chamado NUVEM, em que várias celebridades dos Estados Unidos e de ouros países guardavam suas fotos pessoais. Com a invasão, muitas famosas tiveram suas fotos íntimas disponível em toda rede.

A Lei 12. 737/2012 dispõe sobre a tipificação criminal de delitos informáticos, tipificando condutas que não eram previstas, de forma específica, como infração penal. A Lei acresceu alguns artigos o 154-A e 154-B no CP, bem como alterou os artigos 266 e 298 no Código Penal - Decreto N° 2.848/1940.

As seguintes foram as inovações trazidas pela supracitada lei:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Vigência Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Vigência Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente

> do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

O art. 154-B, por sua vez, reza:

> Art. 154-B - Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionarias de serviços públicos.

Houve alterações também no art. 266, que versa:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. Parágrafo único - Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública.
>
> § 1° Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
>
> § 2° Aplicam-se as penas em dobro se o crime e cometido por ocasiao de calamidade pública.

Por sua vez, o art. 298 esclarece:

> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa. Falsificação de cartão.
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

Assim, passaram a serem punidas as condutas de uso não autorizado de dados de cartões de crédito e débito obtidos de forma indevida, invasão de dispositivos eletrônicos alheios conectados ou não à internet, produção, oferta e venda de programas de computadores que permitam a invasão com vírus de internet e obtenção de

informações sigilosas ou violação de comunicações eletrônicas privadas ou segredos comerciais.

Ademais, Patrícia Peck Pinheiro, em análise sobre os tipos penais criados com o advento da lei 12.737, dispõe que:

> "Ainda, receberá as mesmas penas da invasão aquele que instala uma vulnerabilidade em um sistema de informação para obter vantagem indevida, por exemplo, um backdoor ou uma configuração para que algumas portas de comunicação à internet fiquem sempre abertas. O usuário de gadgets e dispositivos informáticos comuns estão protegidos contra hackers e pessoas mal intencionadas que abusam de confiança ou buscam intencionalmente devassar dispositivo para se apropriar de dados do computador ou prejudicar o seu proprietário, com a exclusão ou alteração de dados, para que fiquem imprestáveis, ou ainda, informações íntimas e privadas, como fotos, documentos e vídeos. As empresas possuem maior proteção jurídica contra a espionagem digital, pois a obtenção de segredos comerciais e ou informações sigilosas definidas por lei agora também se enquadram na lei."[39]

A aprovação de dois Projetos de Leis, convertidos em Leis Ordinárias e publicados no Diário Oficial da União, em 03 de dezembro, demonstra a preocupação com a vulnerabilidade daqueles que acessam a internet, partindo-se em busca da tutela Estatal. Contudo, embora a aprovação destas leis represente um primeiro passo para discussão de tais crimes na seara do Direito Digital, punindo condutas que até então não estavam tipificadas, ainda há muito que ser discutido no que se refere à criminalidade virtual.

Para combater a criminalidade virtual, existem questões a serem discutidas, além das questões conceituais relacionadas à tipificação de delitos. Outras inovações jurídicas, como a produção de provas (investigação probatória) nos crimes digitais, por exemplo, devem ser discutidas a fim de se criar as bases legais para as próximas gerações[40].

---

[39]PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. A nova lei de crimes digitais. 2013. Disponível em: <www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1432>. Acesso em: 20/10/2017.

[40]PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Editora Saraiva, 2013, p. 308.

2.4. CRIMES CONTRA A HONRA

Os crimes contra a honra estão previstos nos arts. 138, 139 e 140 do Código Penal, sendo que os mesmos são crimes comuns na internet, tendo em vista o alto numero de usuários que navegam diariamente na rede.

Honra são as qualidades de um individuo físicas, morais e intelectuais, fazendo-a respeitada no meio social onde se convive, a qual diz respeito ainda à sua autoestima. A honra é um patrimônio que a pessoa possui, sendo que o mesmo deve ser protegido, tendo em vista que os seus atributos como pessoa em sociedade irá definir a sua aceitação ou não para conviver em um determinado grupo social[41].

Um dos crimes contra a honra e o crime de Difamação, o qual se encontra definido no art. 139 do Código Penal: "Difamar alguém, imputando-lhe fato ofensivo à sua reputação", este crime afeta a honra objetiva da pessoa, algo perpetuado por um terceiro que venha a macular a reputação da pessoa[42].

O crime de Difamação e praticado na internet nas suas mais diversas formas, seja na perpetuação de e-mails enviados a pessoas diversas da vitima, imputando à esta, algum fato que ofenda sua honra objetiva, ou publicando em redes sociais as mesmas ofensas. No crime de Difamação a pessoa Jurídica não pode ser sujeito passivo, tendo em vista que no art. 139 do CP a norma é dirigida à pessoa humana, mas, quando o crime for praticado por meio da imprensa, pode-se aplicar a Lei nº 5.250/67 – Lei de Imprensa. Na Difamação a lei não exige que a atribuição seja falsa, basta somente à perpetuação de algo que venha a ofender a reputação do agente perante a sociedade, o crime irá se consumir no momento em que o terceiro tomar conhecimento do fato, em ambiente virtual o crime irá se consumir, por exemplo, quando alguém espalhar um ato ofensivo a uma pessoa pelas redes sociais, e os usuários presentes fizeram a leitura do

[41]CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2011.p.90.
[42]INELLAS, Gabriel Cesar Zaccaria de. Crimes na Internet. São Paulo: Editora Juarez de Oliveira, 2004. p.49.

fato ofensivo[43].

O Crime de Calúnia esta descrito no art. 138 do Código Penal, o qual versa: "Caluniar alguém, imputando-lhe falsamente fato definido como crime". No crime de Calúnia a honra objetiva da vítima é abalada, ou seja, o agente atribui à vítima a prática de fato definido como crime, sabendo que a imputação é falsa, abalando assim, sua reputação perante a sociedade.

O crime de injúria, por sua vez, consiste na propagação de qualidade negativa da vítima por um terceiro, qualidade esta que diga respeito aos seus atributos morais, intelectuais ou físicos, afetando de forma significativa a honra subjetiva da vítima, o tipo penal está previsto no art. 140 do Código Penal: "Injuriar alguém, ofendendo-lhe a dignidade ou o decoro".

2.5. PORNOGRAFIA INFANTIL

Antes de adentrarmos no assunto, cabe ressaltar que o mercado mundial de Pornografia é um dos maiores mercados do mundo. Ademais, a Pornografia Infantil segue esse mesmo caminho e possui um mercado que movimenta Bilhões de Reais. Nesse sentido, é de extrema importância comentar o art. 234 do Código Penal, o qual versa:

> 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:
>
> Pena – detenção, de 6 (seis) meses a 2 (dois) anos, ou multa.
>
> Parágrafo único. Incorre na mesma pena quem:
>
> I – vende, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo;
>
> II – realiza, em lugar público ou acessível ao público, representação teatral, ou exibição cinematográfica de caráter obsceno, ou qualquer outro espetáculo, que tenha o mesmo caráter;
>
> III – realiza, em lugar público ou acessível ao público, ou pelo rádio, audição ou recitação de caráter obsceno.

[43]PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.91.

O elemento subjetivo do tipo é o dolo, o qual o agente tem a finalidade de expor ao público, ou comercializar o objeto material do crime, não é necessário que alguém venha a ter acesso ao material para que o crime venha a se consumir, basta somente a disponibilização do material e a possibilidade de que alguém venha a ter acesso ao mesmo.

Há que se fazer uma distinção entre a Pedofilia e a Pornografia Infantil, naquela, há uma perversão sexual, a qual o adulto experimenta sentimentos eróticos com crianças e adolescentes, já na Pornografia Infantil não é necessário a ocorrência da relação sexual entre adultos e crianças, mas sim, a comercialização de fotografias eróticas ou pornográficas envolvendo crianças e adolescentes[44].

O Estatuto da Criança e do Adolescente, Lei 8.069/90, estabelece algumas penalidades para o sujeito ativo e aquele que divulga ou comercializa imagens e vídeos envolvendo menores em cena de sexo, ou seja, Pornografia Infantil, conforme pode-se observar:

> Art. 240 – Produzir ou dirigir representação teatral, televisiva ou película cinematográfica, utilizando-se de criança ou adolescente em cena de sexo explícito ou pornográfica:
>
> Pena – reclusão de 1 (um) a 4 (quatro) anos, e multa.
>
> Parágrafo único. Incorre na mesma pena que, nas condições referidas neste artigo, contracena com criança ou adolescente.
>
> Art. 241 – Fotografar ou publicar cena e sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão de 1 (um) a 4 (quatro) anos.

A norma que tipifica o crime previsto no art. 241 é entendida como norma aberta, e o Supremo Federal já entende que sua aplicação se dá também para os crimes que são perpetrados pela Internet, tendo em vista que o crime caracteriza-se pela simples publicação, a qual independe do meio que foi utilizado, basta a divulgação e o delito está consumado, vejamos o entendimento da Colenda Primeira Turma do STF[45]:

---

[44]INELLAS, Gabriel Cesar Zaccaria de. Crimes na Internet. São Paulo: Editora Juarez de Oliveira, 2004. p.46

[45]BRASIL. Supremo Tribunal Federal – RHC n. 76.689-0 – Pernambuco – Primeira Turma –

> ESTATUTO DA CRIANÇA E DO ADOLESCENTE – Art. 241 – Inserção de cenas de sexo explícito em rede de computadores (Internet) – Crime caracterizado – Prova pericial necessária para apuração da autoria. "Crime de computador"; publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores atribuída a menores – Tipicidade – Prova pericial necessária à demonstração da autoria – Habeas Corpus deferido em parte.
>
> 1. O tipo cogitado – na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma normal aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.
>
> 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta incriminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da Lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.
>
> 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada do conhecimento do homem comum, impõe-se a realização de prova pericial.

Para que se encontre o agente que praticou uma das condutas previstas nos citados artigos, muitas das vezes é necessária a quebra de sigilo, tendo em vista que será preciso rastrear aquele que praticou o ilícito. Após conseguir localizar o culpado é necessário, muitas das vezes, que sejam as provas eletrônicas analisadas por uma perícia técnica rigorosa, para que sejam aceitas em processos[46].

Além das dificuldades de investigação inerentes à Internet, a polícia também esbarra na questão da territorialidade, pois se o site está hospedado em um provedor estrangeiro, de um país como os Estados Unidos da América, onde é totalmente livre qualquer tipo de manifestação de opinião, então não é possível exigir a retirada do site

---

Relator: Ministro Sepúlveda Pertence, DJU de 6.11.1998, p.03.

[46]PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.300 e 301.

ou das mensagens, nem mesmo processar o autor do crime.

3. LEGISLAÇÃO ATUAL E COMPETÊNCIA

3.1. LEGISLAÇÃO ESTRANGEIRA EM RELAÇÃO AOS CRIMES CIBERNÉTICOS

Com a explosão da globalização através do meio cibernético e o crescimento dos crimes virtuais ou crimes cibernéticos, esses fatos abriram os olhos do mundo, e a Europa se uniu para criar a Convenção de Budapeste ou Convenção sobre o Cibercrime. Sendo criada em 2001, na Hungria, pelo Conselho da Europa, a Convenção de Budapeste, que está em vigor desde 2004, após a ratificação de cinco países, que engloba mais de 20 países e tipifica os principais crimes cometidos na Internet.

Traz em seu preâmbulo priorizando uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional e reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada. Ainda em seu escopo inicial, ressalta o obrigatório respeito: I - à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa em 1950; II - ao Pacto Internacional sobre os Direitos Civis e Políticos da ONU em 1966; à III - Convenção das Nações Unidas sobre os Direitos da Criança em 1989; e IV - à Convenção da Organização Internacional do Trabalho sobre as piores formas do trabalho infantil em 1999. Bem com o Tratado de 2001 que possui quatro capítulos são eles: Terminologia, Medidas a tomar a nível nacional, Cooperação internacional e Disposições finais, assim como 48 artigos encorpados num texto de fácil compreensão, sobretudo porque não traz informações técnicas. O que chama a atenção na Convenção é que ela se alto define: Capítulo-I, diz respeito aos cibercrimes, tipificando-os como infrações contra sistemas e dados informáticos; Capítulo-II, Título 1, fala de infrações relacionadas com computadores; Capítulo-II, Título 2, faz referência as infrações

relacionadas com o conteúdo, pornografia infantil; Capítulo-II, Título 3, diz respeito a infrações relacionadas com a violação de direitos autorais e por fim o Capítulo-II, Título 4, todos dentro do Direito Penal Material. Quanto às matérias do Direito Processual são as que seguem no âmbito das disposições processuais, condições e salvaguardas, injunção, busca e apreensão de dados informáticos armazenados, enfim um rol de conteúdo. Quanto a Competência e Cooperação internacional é vista no artigo 22º, o qual aponta quando e como uma infração é cometida, além de deixar a critério das partes a "jurisdição mais apropriada ao procedimento legal."

É oportuno transcrever o artigo 22, da Convenção sobre o Cibercrime, uma vez que não dita às regras, mas sim orienta sobre o tema, deixando a critério de cada País, criar sua própria legislação específica sobre o assunto.

> Art. 22 – Competência: 1. Cada parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer à competência relativamente a qualquer infração penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infração seja cometida: a) no seu território; b) a bordo de um navio; c) a bordo de aeronave matriculada nessa parte e segundo as suas leis; ou d) por um dos seus cidadãos nacionais, se a infração for punível criminalmente onde foi cometida ou se a infração não for de competência territorial de nenhum Estado. 2. Cada parte pode reservar-se o direito de não aplicar ou de apenas aplicar em casos ou condições específicas as regras de competência definidas no nº 1, alínea b à d do presente artigo ou em qualquer parte dessas alienas; 3. Cada parte adotará medidas que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infração referida no artigo 24, nº1 da presente convenção, quando o presumível autor da infração se encontre no seu território e não puder ser extraditado para outra Parte, apenas com base na sua nacionalidade, após um pedido de extradição. 4. A presente convenção não exclui qualquer competência penal exercida por uma Parte sem conformidade com seu direito interno. 5. Quando mais que uma Parte reivindique a competência em relação à uma presumível infração prevista na presente Convenção, as Partes em causa, se for oportuno, consultar-se-ão a fim de determinarem qual é a jurisdição mais apropriada para o procedimento penal.

Esse acordo parte, portanto, do entendimento que o combate ao cibercrime deve

ser realizado através de um Regime Internacional de mutuo acordo. Desse princípio, pode se partir para outro, que suporta a seguinte ideia: a prática do crime é tão antiga quanto à própria humanidade. Mas o crime global, a formação de redes entre poderosas organizações criminosas e seus associados, com atividades compartilhadas em todo o planeta, constitui um novo fenômeno que afeta profundamente a economia no âmbito internacional e nacional, a política, a segurança e, em última análise, as sociedades em geral.

É visível que com a globalização e com o acesso fácil a Internet, as fronteiras dos ciberespaços abrigaram não apenas criações em prol da cidadania e da participação universal, mas também facilitaram a inserção de pessoas somente com a intenção de cometer crimes, comumente praticados no mundo real, e estes, se moldaram ao ciberespaço.

Ademais, cabe-se ressaltar, especificamente, como é tratada esta questão por determinados países, quais sejam:

Espanha – No Código Penal espanhol, em seu art. 197, 1, há incriminação daquele que se apodera, sem autorização, de papeis, cartas, mensagens de correio eletrônico ou qualquer outro documento, com o intuito de descobrir segredo ou violar a intimidade de outrem, no inciso 2° do referido artigo há incriminação de interceptação de telecomunicações.

O art. 256 do Código Penal espanhol incrimina a utilização não autorizada de terminal de telecomunicação, e o art. 248, 2, incrimina a fraude informática e o estelionato tendo como meio o uso de tecnologia.

Portugal – Os crimes informáticos passaram a ser criminalizados com o advento da Lei n. 109/91, a qual repreende as seguintes condutas:

a) Art. 4° - Falsidade Informática – introdução, modificação ou supressão de dados ou programas informáticos, com o intuito de falsear a obtenção de dados eletrônicos;

b) Art. 5° - Dano a dados ou programas informáticos – destruição de dados

eletrônicos ou de programas de computador, com o objetivo de dado ou, vantagem ilícita.

c) Art. 6° - Sabotagem Informática – apagar, alterar, introduzir ou suprimir dados ou programas informáticos, com o objetivo de perturbar o funcionamento informático ou de comunicação de dados à distância.

d) Art. 7° - Acesso Ilegítimo – invadir sistemas informáticos.

e) Art. 8° - Interceptação ilegítima – interceptações irregulares em ambiente computacional.

f) Art. 9° - Reprodução ilegítima de programa protegido – reprodução, divulgação ou a comunicação de software ao público sem autorização.

França – Em 1988 houve uma alteração no Código Penal Francês, o qual a Lei n. 88-19, introduziu capítulo especial o qual passou a reprimir atentados contra sistemas informáticos, foram feitas as alterações:

a) Acesso fraudulento a sistema de elaboração de dados, sendo considerados delitos tanto o acesso ao sistema, como nele manter-se ilegalmente.

b) Sabotagem informática, punindo quem apaga ou falseia o funcionamento de sistema eletrônico.

c) Destruição de dados, pune aquele que dolosamente introduz dados em sistema ou, suprime ou modifica dados.

d) Falsificação de sistemas informatizados, pune quem falsifica documentos informatizados, com intenção de prejuízo a terceiros.

e) Uso de documentos informatizados falsos, falsos retromencionados.

Itália – O Código Penal italiano desde 1993 trata de alguma forma dos delitos relacionados com a informática, vejamos:

a) Art. 615 – pune o acesso abusivo a sistema informático ou telemático.

b) Art. 617 – pune a instalação, interceptação, impedimento ou interrupção ilícita de comunicação informática ou telemática, e, ainda aquele que falsifica ou suprime conteúdo de comunicação informática ou telemática, quando o intuito é de lucrar ou causar prejuízo.

c) Art. 635 – pune aquele que causou destruição, deterioração ou inutilização a qualquer sistema informático.

Além de países europeus, também possuímos exemplos de países da América Latina que armaram-se desde muito cedo contra os Crimes cibernéticos:

Chile – o primeiro país da America Latina a incorporar a sua legislação alguns crimes digitais, a Lei n. 19.223/93, a qual em seu art. 1° pune aquele que destrua ou inutilize um sistema ou seus componentes; no art. 2° incimina-se a interceptação indevida em sistema; o art. 3° pune aquele que altera, danifica ou destrua os dados contidos em determinados sistemas.

Argentina – A Lei n. 26.388/08 alterou o Código Penal argentino, o qual passou a versar:

a) Art. 128 – incrimina aquele que armazena mensagens contendo pornografia de menores de 18 (dezoito) anos.

b) Art. 153 – pune aquele que abre ou se apropria sem autorização, de correspondência aberta ou fechada, ou comunicação eletrônica ou telegráfica.

c) Incrimina o acesso não autorizado a sistema informático.

d) Incrimina aquele que dá publicidade a informações, inclusive aquelas obtidas em mensagens eletrônicas, desde que possam causar prejuízo a outrem.

Já no Oriente, a Lei japonesa atualizou-se de tal forma que:

Em 1987 houve uma reforma na legislação penal que trouxe novas formas de tipificação quanto a manipulação e sabotagem informática, onde foi acrescentado a fraude com o uso de computador, e, a interferência em sistemas.

Nos Estados Unidos da América, cabe lembrar que cada Estado pode criar seus estatutos penais, sendo que a intervenção Legislativa Federal tem um papel secundário.

A Principal Lei Federal que criminaliza ilícitos informáticos é a Computer Fraud and Abuse Act – Lei de Fraude e Abuso Computacional, a qual é datada de 1986, sendo que a mesma incrimina o acesso não autorizado a sistemas para obtenção de segredos nacionais ou para auferir vantagens financeiras.

3.2. LEGISLAÇÃO NACIONAL EM RELAÇÃO AOS CRIMES CIBERNÉTICOS

São princípios constitucionais, previstos no art. 5º, XXXIX da Constituição Federal Brasileira de 1988, o princípio da reserva legal e da legalidade. Assim, as condutas que não estejam previstas em lei e aquelas formuladas sem a observância ao devido processo legislativo, não podem ser considerados crimes[47].

Para Marco Antônio Marques da Silva, o princípio da legalidade ou reserva legal se caracteriza por ser um limite ao poder punitivo do Estado, bem como um limite ao poder normativo do Estado, uma vez que impede a criação de tipos penais, com exceção do processo legislativo regular. Segundo o autor, tal princípio é uma "consequência direta do fundamento da dignidade da pessoa humana, pois remonta à ideia de proteção e desenvolvimento da pessoa que o tem como referencial"[48]. O Código Penal Brasileiro confirma essa previsão, no seu artigo 1º, ao afirmar que "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal" [49].

Considerando a obrigatoriedade de previsão legal para punição de uma conduta proibida, no caso dos crimes virtuais, até o ano 2012, não havia qualquer legislação para punir os crimes virtuais próprios, aqueles voltados contra os dispositivos e sistemas de informação. A legislação penal existente permitia que os crimes virtuais impróprios pudessem ser punidos, uma vez que consistiam em crimes já tipificados no ordenamento brasileiro, com a particularidade do computador ser utilizado como meio para a prática do crime.

Há algum tempo, diante da evolução tecnológica e da ausência de normas punitivas específicas que protegessem o usuário, vítima dos crimes digitais, já

---

[47]CF/88, art. 5º, XXXIX: "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".
[48]SILVA, Marco Antônio Marques da Silva. Acesso à Justiça Penal e Estado Democrático de Direito. São Paulo: Ed. J. de Oliveira, 2001, p. 07.
[49]BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 24/10/2017.

tramitavam no Congresso Nacional alguns projetos de lei visando à regulamentação de tais crimes, dentre eles o projeto de lei nº 2126/11, que institui o marco civil na internet; projeto de lei nº 2793/11, de autoria do Deputado Paulo Teixeira; e o projeto de lei nº 84/99, de autoria do Deputado Eduardo Azeredo[50].

Em decorrência de alguns episódios, em que em meados de 2011, ocorreram vários ataques de negação de serviço a sites do governo brasileiro que ficaram instáveis até sair do ar, ocasionando à atriz Carolina Dieckmann 36 fotos roubadas por hackers de seus arquivos pessoais e divulgadas na internet, que contribuíram para que as leis específicas sobre o tema fossem aprovadas em regime de urgência e com o objetivo de preencher as lacunas existentes no ordenamento, no que se refere aos crimes digitais, em 30/11/2012, foram sancionadas e promulgadas as leis 12.735, que trata da necessidade de instalação de órgãos investigativos especializados, e a lei 12.737, pela qual foram incluídos no Código Penal Brasileiro o tipo penal invasão de dispositivo informático (Art. 154-A) e a regra da ação penal para esse crime (Art. 154-B), conforme se extrai do Código Penal Brasileiro. Além da inclusão desses dois dispositivos, a lei alterou a redação de dois delitos já existentes, previstos no Art. 266 do Código Penal, interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública; e no Art. 298 do Código Penal, que prevê a falsificação de documento particular, equiparando agora o cartão de crédito e débito ao documento particular a que se refere o artigo.

Assim, passaram a serem punidas as condutas de uso não autorizado de dados de cartões de crédito e débito obtidos de forma indevida, invasão de dispositivos eletrônicos alheios conectados ou não à internet, produção, oferta e venda de programas de computadores que permitam a invasão com vírus de internet e obtenção de informações sigilosas ou violação de comunicações eletrônicas privadas ou segredos comerciais.

Em uma breve análise sobre os novos tipos penais criados com o advento da lei 12.737, Patrícia Peck Pinheiro afirma que:

[50]PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Editora Saraiva, 2013, p. 314.

> "Ainda, receberá as mesmas penas da invasão aquele que instala uma vulnerabilidade em um sistema de informação para obter vantagem indevida, por exemplo, um backdoor ou uma configuração para que algumas portas de comunicação à internet fiquem sempre abertas. O usuário de gadgets e dispositivos informáticos comuns estão protegidos contra hackers e pessoas mal intencionadas que abusam de confiança ou buscam intencionalmente devassar dispositivo para se apropriar de dados do computador ou prejudicar o seu proprietário, com a exclusão ou alteração de dados, para que fiquem imprestáveis, ou ainda, informações íntimas e privadas, como fotos, documentos e vídeos. As empresas possuem maior proteção jurídica contra a espionagem digital, pois a obtenção de segredos comerciais e ou informações sigilosas definidas por lei agora também se enquadram na lei."[51]

A aprovação de dois Projetos de Leis, convertidos em Leis Ordinárias e publicados no Diário Oficial da União, em 03 de dezembro, demonstra a preocupação com a vulnerabilidade daqueles que acessam a internet, partindo-se em busca da tutela Estatal. Contudo, embora a aprovação destas leis represente um primeiro passo para discussão de tais crimes na seara do Direito Digital, punindo condutas que até então não estavam tipificadas, ainda há muito que ser discutido no que se refere à criminalidade virtual. Para combater a criminalidade virtual, existem questões a serem discutidas, além das questões conceituais relacionadas à tipificação de delitos. Outras inovações jurídicas, como a produção de provas (investigação probatória) nos crimes digitais, por exemplo, devem ser discutidas a fim de se criar as bases legais suficientes para engrandecer o Direito Penal frente às novidades delituosas[52].

3.3. ANÁLISE DAS PROVAS NOS CRIMES CIBERNÉTICOS

Os avanços tecnológicos e as novas descobertas científicas propiciaram o surgimento de uma nova realidade para o ser humano. O espaço cibernético, novo ambiente social onde a prática de atos e fatos jurídicos independem da existência de um espaço e presença física, foi o propulsor que permitiu o surgimento dessa nova realidade[53].

---

[51]PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. A nova lei de crimes digitais. 2013. Disponível em: <www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1432>. Acesso em: 26/10/2017.
[52]PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Editora Saraiva, 2013, p. 308.
[53]MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova – A investigação criminal

O desenvolvimento tecnológico, além de permitir o tratamento e processamento automatizado de informações e telecomunicações em vários setores da vida, possibilitou também uma maior diversidade e periculosidade em relação à prática de ilícitos informáticos. Nas palavras de Crespo: "a evolução tecnológica da sociedade supõe uma evolução tecnológica dos ilícitos, tanto nos meios quanto nos objetos"[54].

Os crimes cibernéticos, caracterizados cada vez mais pela diversidade e a periculosidade com que se apresentam, geram uma maior dificuldade para sua averiguação e comprovação, bem como outras questões como a efetivação de perícias e identificação da autoria.

No presente capítulo serão apresentadas as questões relacionadas à prova a ao processo penal quando estudados sob a ótica dos crimes virtuais, identificando os principais aspectos que devem ser repensados no atual modelo de investigação brasileiro. Primeiramente, será tratada a necessidade da presença de profissionais especializados, de qualificação técnica específica em todas as localidades em que os crimes se consumam. Em seguida, será discutida a dificuldade na identificação de autoria, apesar da maior facilidade de rastreamento proporcionada pelos meios eletrônicos. Na sequência, será abordada a necessidade da produção antecipada de prova, considerando o dinamismo, celeridade e velocidade características dos crimes digitais.

3.3.1. DA DIFICULDADE DE OBTENÇÃO DE PROVAS

No ordenamento jurídico pátrio, não há qualquer empecilho para a utilização de provas eletrônicas, conforme versa o art. 225 do Código Civil:

> As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão.

em busca da verdade. Curitiba: Juruá Editora, 2012. p. 59.

[54]CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. São Paulo: Editora Saraiva, 2011, p. 159.

Pedro Batista Martins conceitua prova como sendo “o conjunto de elementos de que se serve o juiz para formar a convicção sobre os fatos que se funda a demanda”[55].

O Código de processo penal também aceita as provas eletrônicas, conforme versa o art. 231, “salvo os casos expressos em lei, as partes poderão apresentar documentos em qualquer fase do processo”, e, ademais, o art. 232 também versa que “consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares”.

Cabe citar também da Medida Provisória n° 2.200-1/2001, sendo que a mesma institui a Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, a qual já em seu art. 1º versa sobre sua finalidade[56].

Caso se verifique que o documento eletrônico não tenha sido assinado, ou o certificado não esteja vinculado ao ICP-Brasil, pode-se realizaruma perícia no computador para que se verifique a autenticidade da documentação[57], o credenciamento serve como um selo de qualidade técnica, e não é preponderante na apreciação da prova, uma vez que o Juiz dispõe do Livre Convencimento Motivado, sendo que o mesmo apreciará livremente as provas.

Nos dias atuais as pessoas podem utilizar da assinatura digital e certificação digital, a certificação digital é um tipo de tecnologia de criptografia a qual se usa uma ferramenta de codificação usada para envio de mensagens seguras em redes eletrônicas.

A assinatura eletrônica é uma chave privada, um código pessoal que não pode ser reproduzido, a qual evita que o que se esta transmitindo seja lido somente por aquele receptor que possua a mesma chave e é reconhecida com a mesma validade da assinatura tradicional[58].

---

[55]MARTINS, Pedro Batista. Comentários ao Código de Processo Civil. Forense, v.2, p. 383.
[56]BRASIL. PRESIDÊNCIA DA REPÚBLICA – Casa Civil – Subchefia para Assuntos Jurídicos – Medida Provisória n° 2.200-1, de 27 de Julho de 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-1.htm>. Acesso em: 30/10/2017.
[57]PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.214
[58]PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.216

Os certificados digitais são excelentes instrumentos do mundo atual, pois propiciam autenticidade aos documentos virtuais, não deixando pairar duvidas sobre a origem dos mesmos.

Quando um usuário navega na internet, lhe é atribuído um numero de IP – Internet Protocol é esse numero que propicia a identificação do usuário na rede, ou a investigação de algum crime que tenha ocorrido, a questão é que este numero só é atribuído ao usuário no momento em que ele esta conectado, após este período, quando o mesmo desligar o modem, o endereço de IP será atribuído a outro usuário, caso o mesmo não tenha optado por um IP Fixo. O IP quando solicitado ao provedor de acesso à internet, deve vir acompanhado de data, hora da conexão, e o fuso horário do sistema, sendo que esses dados são imprescindíveis, tendo em vista que sem os mesmos fica impossível fazer a quebra de sigilo dos dados.

Após a localização do provedor, deve-se requerer ao juiz o pedido de quebra do sigilo de dados telemáticos, para que o provedor de acesso informe quem estava vinculado ao endereço de IP naquele momento em que ocorreu o crime, ou seja, seu endereço físico.

3.3.2. NECESSIDADE DE PERÍCIAS ESPECIALIZADAS

O crescente aumento da utilização de computadores e da internet para a prática de crimes, ensejou a necessidade de apuração dos crimes praticados através rede mundial decomputadores. Foi assim que surgiu a computação forense, cujo objetivo é a investigação e a coleta de evidências das condutas ilícitas praticadas por meio de computadores[59].

Toda investigação tem início com base nas evidências e informações coletadas e o meio virtual não difere do físico. No caso dos crimes virtuais, as evidências poderão ser retiradas de qualquer dispositivo eletrônico (celulares, discos rígidos). Isto é, a evidência digital pode ser definida como toda informação retirada de um compilado ou

[59]RODRIGUES, Thalita Scharr; FOLTRAN JUNIOR, Dierone César. Análise de ferramentas forenses na investigação digital. 2010. Disponível em: <http://www.revistaret.com.br/ojs-2.2.3/index.php/ret/article/viewFile/64/93>. Acesso em: 30/10/2017.

depositário eletrônico, através da intervenção humana ou não, em um formato inteligível ao ser humano[60].

Nas investigações sobre crimes digitais, em decorrência da volatilidade dos dados e facilidade de adulteração, as provas eletrônicas deverão passar por perícias técnicas rigorosas para serem aceitas em processos, de forma a garantir a validade e integridade dos resultados. Esse é o objetivo da computação forense: provar os fatos ocorridos da forma mais clara possível.

A computação forense é a ciência responsável por elucidar os fatos, através da utilização de métodos científicos na coleta, validação, identificação das evidências digitais, para que se possa punir os infratores. O objetivo da computação forense é extrair o máximo de informações quando da análise dos vestígios relacionados ao delito praticado que permitam a formulação de conclusões[61].

Isto é, a computação forense é um tipo de perícia caracterizada pela inspeção científica e sistemática em computadores que, através da coleta de evidências digitais, busca chegar a conclusões sobre o caso investigado. É feita uma reconstituição dos eventos encontrados que possibilita determinar se o computador em análise foi utilizado para a realização ou não de condutas ilícitas ou não autorizadas.

São exemplos de indícios que podem auxiliar na investigação dos crimes digitais: arquivos de imagem de pornografia infantil, mensagens eletrônicas com ameaças e chantagens, arquivos com informações incriminatórias ou dados roubados[62].

Pelo fato de se desenvolverem e de se consumarem em ambiente virtual, caracterizado pela inexistência física do sujeito ativo, uma vez que o criminoso está presente exclusivamente no espaço cibernético, os crimes virtuais geralmente são considerados crimes bastante complexos[63]. Ademais, contribui para essa complexidade

[60]PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Editora Saraiva, 2013, p. 216.
[61]PINHEIRO, op. cit., p. 233.
[62]PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Editora Saraiva, 2013, p. 232.
[63]Não se pode confundir essa característica dos crimes virtuais com a definição de crime complexo já existente no direito penal em que a configuração típica do crime é caracterizada pela fusão de dois ou mais tipos penais.

a facilidade de perecimento das provas apresentadas para esse tipo de crime (fotografias, vídeos, arquivos digitais, dados). Isto é, a facilidade com que tais provas podem ser modificadas, perdidas ou até apagadas[64].

Os crimes digitais apresentam grandes dificuldades para a sua comprovação. Se por um lado há uma grande facilidade na prática do delito por meio dos computadores; por outro lado a verificação dos vestígios exige qualificação técnica específica nem sempre disponível em todos os lugares de consumação dos crimes.

A vulnerabilidade de modificação característica dos documentos digitais exige a nomeação de perito tecnicamente qualificado para afirmar a autenticidade do documento. Apesar da precisão da computação forense, a coleta de evidências se torna frágil. Quando feita erroneamente, violando disposições de direito material ou princípios constitucionais, pode tornar a prova ilícita ou invalidá-la[65].

A produção de prova ilícita pode ser extremamente prejudicial ao processo, na medida em que esse tipo de prova contamina todas as provas dela decorrentes. Considerando a teoria dos frutos da árvore envenenada, "os efeitos da ilicitude podem transcender a prova viciada, contaminando todo o material dela decorrente"[66]. Sendo assim, todas as provas originárias de uma prova ilícita devem ser retiradas do processo, conforme previsão do Código de processo penal no seu artigo 157 pela qual "são inadmissíveis, devendo ser desentranhadas doprocesso, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais".

Em decorrência da minuciosidade exigida por esse tipo de perícia, o maior problema jurídico em relação à produção de provas nos crimes virtuais é o despreparo da polícia investigativa e da perícia. São poucos os profissionais preparados para esse tipo de investigação, por esse motivo, estes deverão ser extremamente capacitados e especializados para lidar com a perícia voltada para investigação dos crimes digitais, de forma a atender exigências técnicas de coleta e guarda a fim de evitar os

[64]MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012. p. 65.
[65]PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Editora Saraiva, 2013, p. 234.
[66]TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. Curso de Direito Processual Penal. Salvador: Jus Podivm, 2012. p. 383.

questionamentos que venham a surgir sobre a identidade da prova e a licitude de sua obtenção[67].

A respeito da investigação policial e elaboração do laudo pericial, a capacitação do investigador ou perito está diretamente associada ao sucesso ou não das provas produzidas. Estes profissionais devem estar aptos e treinados para, através da utilização das mais modernas tecnologias, buscar os indícios que possibilitarão a coleta de provas, a preservação do local e das ferramentas e objetos utilizados na prática da conduta ilícita[68].

Com o intuito de dar legitimidade às provas produzidas nos crimes virtuais, a investigação criminal e a instrução processual demandam procedimentos técnicos. Os profissionais especializados em hardware, software, tráfego e segurança de rede, através da realização de exames periciais, buscarão apontar a veracidade dos fatos. A eficiência da investigação criminal será resultado da atuação desses peritos na análise do ambiente aonde o crime foi praticado e na constatação da veracidade.

Analisando o ambiente em que o delito foi cometido, os profissionais poderão constatar a existência de vestígios das atividades criminosas praticadas. Roberto Antônio Malaquias, considerando o envio de um e-mail não autorizado, exemplifica vestígios que podem indicar a prática da conduta infracional quais sejam a indicação da origem de um e-mail, sua autoria, destinatário, adulteração, o itinerário utilizado para se chegar ao destinado final, os endereços virtuais e protocolos de comunicação envolvidos que identificarão o caminho feitopela mensagem na rede de computadores[69]. Neste exemplo, a identificação do e-mail, objeto da investigação criminal e produção de provas, e de todos os seus componentes funcionará como um rastreador para identificar a máquina que originou tal mensagem que servirá como prova documental.

[67]COLLI, Maciel. Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010. P. 160.
[68]MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012. p. 65.
[69]MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012. p. 80.

Diante da necessidade de especialização dos profissionais responsáveis pela investigação dos crimes digitais, Maciel Colli afirma que a criação de divisões especializadas em computadores, mídias e meios de comunicação poderia ser um dos caminhos a serem seguidos para a resolução de algumas questões ligadas aos cibercrimes. Já que a velocidade e novidade com que ocorrem somadas a ofensa a um bem jurídico especial (a informação) ensejam um conhecimento especifico para que se possa chegar aos indícios de autoria e materialidade da infração penal[70].

No Brasil, no âmbito da polícia civil, existem sete Estados que possuem delegacias especializadas na investigação de cibercrimes. No âmbito da polícia federal, atualmente, o combate aos crimes virtuais é responsabilidade da Unidade de Repressão a crimes cibernéticos da Polícia Federal (URCC).

Embora o país esteja se preparando para o combate aos crimes virtuais, através da criação de delegacias especializadas e do treinamento de profissionais responsáveis por investigar tais crimes, a quantidade de profissionais dessa área não é suficiente para apurar as condutas ilícitas praticadas diariamente na rede mundial de computadores. Na sociedade atual a qual a tecnologia se faz presente no cotidiano das pessoas, inclusive em momentos de práticas criminosas, o papel do perito computacional, responsável por desvendar e solucionar crimes que necessitam de um conhecimento específico, é de extrema importância.

Diante da escassez de técnica e recursos humanos preparados no que diz respeito à investigação e punição do criminoso cibernético, os exames periciais transformam-se em um instrumento eficiente na produção de prova no crime cibernético[71].

Além dos problemas relacionados a falta de especialização dos profissionais da área do direito, no que se refere ao crimes virtuais, outras particularidades devem ser considerada na análise das provas produzidas em tais crimes quais sejam a questão do anonimato on-line e a necessidade da produção antecipada de provas.

---

[70]COLLI, Maciel. Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010. P. 167.
[71]MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012. p. 83.

3.3.3. IDENTIFICAÇÃO DA AUTORIA

O principal objetivo da prova judiciária é a reconstrução da verdade. É a busca pela ligação existente entre os fatos investigados no processo e a realidade histórica, ou seja, a verdade dos fatos tal como realmente ocorreram no tempo e espaço[72].

O material probatório colhido durante o processo é de suma importância para o convencimento do magistrado acerca da ocorrência dos fatos objetos da lide. A condenação só poderá ocorrer diante da certeza de culpabilidade, e esta não poderá ser obtida através de suposições, e sim por meio de um conjunto probatório sólido[73].

Para que a sanção penal seja aplicada ao indivíduo que figura como imputado, é necessária a comprovação de que este indivíduo tenha praticado a conduta caracterizada como crime cibernético. Não basta a simples dedução, inferência ou conhecimento superficial sobre a autoria do delito[74].

Principalmente em relação aos crimes virtuais, a correta identificação do acusado é uma grande preocupação, para que a pretensão punitiva seja justa e direcionada àquele que realmente cometeu o crime cibernético. Essa preocupação é ainda maior, em relação a identificação do autor, quando se considera, por exemplo, a facilidade que os criminosos têm emse apropriar de senhas e códigos de acesso alheios e utilizá-los para aplicar golpes financeiros ou invadir sistemas por meio dessa identidade[75].

Quando a imputação do crime virtual é determinada somente através da simples indicação do possível autor que cometeu o ilícito penal, não poderá ser instaurado um juízo. A individualização do autor da infração penal, sua correta identificação e

---

[72]OLIVEIRA, Eugênio Pacelli. Curso de Processo Penal. Rio de Janeiro: Lúmen Júris, 2011. p. 327.
[73]TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. Curso de Direito Processual Penal. Salvador: Jus Podivm, 2012. p. 376.
[74]MALAQUIAS, op. cit., p. 65.
[75]MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012. p. 66.

qualificação, é pressuposto essencial para a instauração da instrução processual penal[76].

Nas palavras de Roberto Malaquias, "O Estado não pode estigmatizar o indivíduo e tampouco alcançar pessoas abstratas com meras inferências". A perfeita identificação do autor e a correta delimitação da infração cometida são essenciais para se punir o criminoso virtual principalmente, quando se considera o ambiente virtual em que o crime foi praticado, caracterizado pela ausência da presença física do infrator.

Ao se considerar a possibilidade de identificação do computador, esse anonimato on-line torna-se relativo. A princípio, o anonimato on-line é apenas aparente, porque o mais anônimo dos sujeitos poderá ter o seu computador identificado ao se conectar a rede mundial de computadores, através do endereço IP atribuído ao computador quando da conexão.

No direito digital, a identificação de um computador é feita por meio do endereço IP (*internet protocol*). O número IP é atribuído a cada usuário ou internauta, toda vez que uma conexão é estabelecida com a rede mundial de computadores. Além de permitir a identificação virtual, o IP descreve todo o tráfego de rede e acessos feito pelo usuário em determinado período[77].

A identificação de um indivíduo no "mundo real" e no "mundo virtual" é feita de modo semelhante. No "mundo real", a identificação de uma pessoa na sociedade mescla uma espécie de concretização qualitativa, que corresponde à uma identificação visual, através do reconhecimento das principais características do indivíduo tais como feições, altura, voz; com uma espécie de concretização numérica, que corresponde a um reconhecimento e identificação legal, através do número de um documento como o passaporte ou registro geral. No mundo virtual, a identificação do endereço IP corresponde à concretização numérica, contudo, a grande diferença é que esse número identifica o computador e não uma pessoa.

Toda investigação criminal deve considerar as evidências deixadas pelo

[76]Ibidem, p. 64.
[77]PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Editora Saraiva, 2013, p. 308.

criminoso cibernético por intermédio do endereço IP. Outra forma de se obter informações de acesso à rede é através do servidor proxy, responsável por armazenar os logs de registro de navegação que identificam os locais acessados pelo usuário, bem como os serviços utilizados, quando a conexão com a rede mundial de computadores é direta. Apesar dessas duas hipóteses investigativas, não há como fazer esse rastreamento, quando o usuário se conecta à rede através de uma conexão indireta, pela qual o internauta fica protegido e usufrui do anonimato on-line para acessar vários conteúdos, utilizando apenas o IP do servidor hospedeiro[78].

Quando se compara o mundo real e o mundo virtual, no que diz respeito à averiguação das provas, a prova obtida em meios eletrônicos é mais facilmente averiguada do que as provas do mundo real. Os peritos especializados, através de uma análise da memória do computador, equipamentos e softwares, podem localizar um criminoso em qualquer parte do mundo por um endereço IP.

O primeiro passo na investigação dos crimes cibernéticos é identificar a origem da comunicação. Por meio de uma análise do tráfego de dados, se chegará ao endereço IP de origem e ao usuário que está vinculado a esse IP. Uma vez identificado o endereço IP, serãoanalisados possíveis provas da prática do delito. Essa análise, feita por peritos especializados, é uma atividade extremamente complexa, considerando a presença de programas de computador cujo objetivo é o mascaramento da verdadeira identidade do autor, principalmente quando os computadores estão localizados em locais públicos tais como universidades, bibliotecas e cybercafés. Assim, a localização de uma pessoa no mundo virtual ocorre através da atribuição de um endereço IP no momento da conexão com a rede mundial de computadores. O problema em relação à autoria, é que essa identificação é sempre do computador, e nunca do sujeito.

Apesar da facilidade de rastreamento, permitindo que o computador utilizado para a prática da conduta criminosa seja facilmente localizado e identificado, a grande dificuldade em identificar o autor decorre da associação feita entre o proprietário do computador e o sujeito que cometeu o crime.

---

[78]MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012. p. 65.

A identificação do criminoso cibernético não é tão fácil quando parece, quando se considera que a localização através do endereço IP permite a identificação de um computador e não, efetivamente, do autor do delito. Na verdade, a grande dificuldade decorrente da identificação da autoria está em correlacionar o computador e o sujeito que o opera em determinado espaço de tempo. Maciel Colli traz como exemplo para demonstrar essa dificuldade na identificação da autoria quando o crime é praticado em um computador de uso público ou um computador compartilhado por uma família de 12 pessoas, dentre maiores e menores de idade, a qual estes não seriam punidos.

Os problemas de identificação de autoria não dizem respeito à identificação do computador de onde se originou o fato ilícito ou do responsável por tal computador; dizem respeito à identificação da pessoa que agiu com a intenção de praticar o ato ilícito ou que contribui para prática de tal conduta.

Patrícia Peck afirma que a questão da prova de autoria é um dos grandes desafios do direto na era digital. A identificação do criminoso cibernético, de maneira mais inequívoca, só é possível através do uso da biometria que corresponde à utilização de características fisiológicas mensuráveis para autenticar um usuário tais como a impressão digital ou o reconhecimento facial[79].

O tema da identidade digital obrigatória pode ser considerado como um dos assuntos mais importantes do direito atual. A ausência de uma lei para gerar prova de autoria e de um entendimento consolidado e unificado incorre em várias possibilidades de entendimento por parte do juiz quando se depara com um crime cibernético. Há juiz que entende que a senha é suficiente para comprovação da identidade do autor, outros aplicam isso apenas quando há o certificado digital da ICP-Brasil, e há ainda os que dizem que só com a assinatura do papel[80]. Assim, a única forma realmente segura de identificação de autoria em crimes virtuais é aquela que tem como fundamento a análise do infrator penal, quando este se utiliza de elementos corporais para ter acesso à rede e aos computadores.

[79]PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Editora Saraiva, 2013, p. 93.
[80]Ibidem, p. 93.

Em suma, apesar da aparente facilidade na identificação de um usuário, por meio de seu endereço IP, qualquer órgão policial envolvido na investigação de um crime cibernético terá que enfrentar dois problemas: de que maneira correlacionar o endereço IP identificado com a máquina utilizada para a prática do delito; e de que maneira correlacionar a máquina com o sujeito que a opera.

A instauração de uma investigação baseada somente na mera presunção de suspeição decorrente da titularidade de um contrato de acesso à internet, por exemplo, estaria orientada pela responsabilização objetiva do direito penal que, de acordo com Maciel Colli, deve ser repudiada a todo o custo.

A fim de solucionar o problema de identificação de autoria, Maciel Colli propõe que o sujeito que praticou o cibercrime a partir de um computador somente poderá serindiciado e responsabilizado se houver prisão em flagrante com esse computador operante (ligado). Para ele, essa solução pode ser utilizada tanto "na investigação preliminar que busca vestígios de materialidade e autoria, quanto na ação penal dela decorrente." [81]

3.3.4. PRODUÇÃO ANTECIPADA DE PROVAS

A investigação criminal, realizada pela polícia judiciária, tem como objetivo reunir elementos comprobatórios do crime praticado a fim de determinar o fato típico e quem foi seu suposto autor, ou seja, a finalidade da investigação é apurar o delito e sua autoria. A investigação é materializada nos autos chamados de inquérito policial.

Quando um delito é praticado, surge para o Estado o poder-dever de punir o suposto autor do delito. A existência de elementos de informação da autoria e materialidade da infração são pressupostos indispensáveis para que o Estado possa dar início à persecução criminal em juízo. Isto é, para que se possa deflagrar um processo criminal contra alguém é necessário um conjunto probatório mínimo que aponte a

[81]COLLI, Maciel. Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010. p. 92.

prática da conduta delituosa, bem como a probabilidade do acusado ser o autor do crime.

O inquérito policial é um procedimento administrativo cautelar. Conforme previsto no Art. 6, III, do Código de Processo Penal, é, em regra, uma instrução provisória decorrente da necessidade das autoridades policiais em "colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias", com o objetivo de instrução de uma futura ação penal. No entanto, além da coleta de provas testemunhais, documentais ou periciais, o inquérito poderá trazer atos de instrução não provisórias quais sejam buscas, apreensões, exames de corpo delito.

Assim, o inquérito policial pode ser definido como um procedimento administrativo inquisitório e preparatório que corresponde à realização de um conjunto de medidas realizadas pela autoridade policial a fim de coletar informações a respeito da autoria e materialidade do fato. Isto é, o inquérito policial corresponde à uma investigação e averiguaçãofeita pela polícia judiciária quando da ocorrência de uma infração penal e na tentativa de determinar quem foram seus autores.

Considerando o caráter instrumental do inquérito policial, no que se destina a esclarecer os delitos praticados a fim de fornecer subsídios para o seguimento da persecução penal, Renato Brasileiro de Lima atribui duas funções ao inquérito policial: uma função preservadora e uma função preparatória. Enquanto a primeira evita a instauração de um processo infundado; a segunda fornece elementos ao titular da ação penal, para que este ingresse em juízo, além de resguardar meios de prova que poderiam se perder no decorrer do processo.

A principal finalidade do inquérito policial é a coleta de elementos de informação quanto à autoria e à materialidade do delito. No entanto, não se pode confundir os elementos de informação com a prova.

Um dos princípios norteadores do processo penal é o principio do contraditório pela qual quando uma parte produz determinada prova, é direito da parte adversa não somente se manifestar a respeito da prova como também produzir prova em contrário. Segundo Mossim, "toda prova admite contraprova, não sendo admissível a produção

de uma delas sem o conhecimento da outra parte". O contraditório é uma condição de existência e validade das provas; sem ele, não caberá a designação de prova.

Com as alterações trazidas pela lei 11.690/2008, o Código de Processo Penal passou a prever a distinção entre prova e elementos informativos. Enquanto a prova admite o contraditório e a ampla defesa, os elementos informativos não comportam tais institutos. Isto é, a prova só pode ser utilizada para se referir a elementos de convicção produzidos no curso do processo judicial, observando o contraditório e a ampla defesa; já os elementos informativos são colhidos durante a fase de investigação, sem a obrigatoriedade de observância do contraditório e da ampla defesa.

Diante da inexistência de contraditório na produção dos elementos de informação de autoria e materialidade do delito na fase de inquérito policial, considera-se que o valor probatório do inquérito é relativo. Para Aury Lopes Jr., o inquérito policial possui eficácia probatória limitada, uma vez que somente gera atos de investigação[82].

Considerando a relatividade do valor probatório do inquérito policial, já que este necessita de confirmação de outros elementos colhidos durante a instrução processual, o Código de Processo Penal, no seu artigo 155, prevê que o magistrado, salvo algumas exceções previstas em lei, não poderá considerar somente os elementos informativos como meio para condenação do réu.

O magistrado não poderá considerar somente os dados colhidos durante a fase de inquérito para decidir a respeito da condenação do réu. Nas palavras de Nestor Távora e Rosmar Alencar, "é essencial que a instrução probatória em juízo, regida pelo contraditório e ampla defesa, oportunize colher elementos convincentes e robustos a fundamentar um decreto condenatório".

Atento à existência desse tipo de prova, o legislador admite, conforme artigo 155 do Código de Processo Penal, que o juiz, na valoração das provas, poderá formar sua convicção baseado nas provas cautelares, não repetíveis e antecipadas, mesmo que estas

[82]LOPES Jr., Aury. Sistemas de investigação preliminar no processo penal. Rio de Janeiro: Lumen Juris, 2001. p. 190.

tenham sido produzidas na fase investigatória.

As provas cautelares são aquelas sujeitas a um risco de perecimento em razão do decurso do tempo. A prova não repetível é aquela que não pode ser produzida novamente devido ao desaparecimento, destruição ou perecimento da fonte probatória. Diante do perigo de dispersão da fonte probatória, assim que a autoridade policial tomar conhecimento da prática do delito poderá determinar sua realização, independentemente de prévia autorização judicial. Já provas antecipadas, em razão de uma situação de urgência ou relevância, são aquelas produzidas

Nesse mesmo sentido, Lucrecio Rebollo Delgado afirma que as condutas ilícitas praticadas através da informática são caracterizadas pela facilidade de encobrimento e dificuldade probatória. O encobrimento dos fatos é característica praticamente inseparável do crime virtual e se traduz na facilidade de se modificar um programa de forma que este traga benefícios para o autor e imediatamente depois o modificar novamente para a versão original, a fim de encobrir os rastros deixados pela prática do delito. Dessa forma, se posteriormente fosse realizada uma investigação policial tendo como objeto esse programa seria impossível detectar a maneira como o fato ilícito foi praticado.

Mesmo diante da previsão da produção antecipada de provas para os crimes virtuais, esse procedimento só será válido quando a prova em questão for indispensável para a prolação de uma sentença futura e houver indícios suficientes que demonstrem estar a prova sob o risco de perecimento. Ainda, o procedimento deve ser realizado sob o crivo do contraditório e da ampla defesa para que tenha validade.

3.4. COMPETÊNCIA PARA PROCESSAR E JULGAR

No momento em que ocorre um determinado crime na internet, o que se deve observar primeiramente, é onde se desenrolou o mesmo, em qual território a ação se deu.

O problema é que na internet fica muito difícil estabelecer uma demarcação de território, as relações jurídicas que existem podem ser entre pessoas de um país e outro,

e entre diferentes culturas, as quais se comunicam o tempo todo, e o direito deve intervir para proteger os litígios que eventualmente vierem a acontecer[83].

Vários usuários registram sites na internet em outros países diferentes daquele em que estão sendo praticadas suas atividades, mas o que ocorre é que a internet não tem barreiras, e pessoas de vários outros países podem acessar um site registrado nos Estados Unidos, mas que as atividades estão sendo elaboradas no Brasil.

Na atualidade existem diversos princípios para se determinar qual será a lei aplicável a cada caso, há o principio do endereço eletrônico, o do local em que a conduta se realizou ou exerceu seus efeitos, o do domicílio do consumidor, da localidade do réu, o da eficácia na execução judicial[84].

No ordenamento jurídico Brasileiro, aplicam-se os artigos 5° e 6° do Código Penal Brasileiro, no que tange a competência para processar e julgar os crimes praticados na internet, sejam eles:

> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
>
> Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.

Como se pode verificar, o ordenamento jurídico pátrio adotou a teoria da ubiquidade, conforme versa o art. 6° do CP, sendo que os delitos quesão praticados por brasileiro, tanto no país quanto fora, ainda que transnacionais, será aplicado à lei brasileira, tendo em vista ainda o que dispõe o art. 7° do Código Penal, o qual sujeita a lei brasileira a alguns crimes praticados no estrangeiro[85].

---

[83]PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.80
[84]PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.82
[85]CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2011.p.118.

CONCLUSÃO

O presente trabalho teve como seu principal objetivo averiguar os crimes cibernéticos à luz do Direito Penal e Processual brasileiro e também sob a ótica da legislação estrangeira, analisando as peculiaridades decorrentes desse novo ambiente de incidência de crimes que influenciam e dificultam a investigação criminal.

Dessa forma, as recentes tipificações de algumas condutas delitivas não são suficientes para solucionar as dificuldades encontradas na resolução de tais crimes. Concluiu-se que a criminalidade cibernética não foi somente responsável pelo surgimento de novas práticas ilícitas, com o sustento do computador, mas também, consequentemente, possibilitou a violação de bens jurídicos até então não atingidos com a prática dos delitos já previstos no ordenamento jurídico brasileiro tais como a informação, dos dados e os sistemas de computadores.

As particularidades obtidas com a incidência dos crimes cibernéticos, tais como o dinamismo com que estes crimes se concretizam, estão intimamente ligadas à investigação probatória. Ao se considerar a importância da prova no processo, bem como os seus elementos. Conclui-se que, ao se considerar os crimes cibernéticos e suas particularidades, certas questões em relação à dilação probatória merecem discussão: a necessidade de peritos especializados, a dificuldade na identificação da autoria e a importância da produção antecipada de provas para esse tipo de crime. Os exames periciais são de extrema importância, no sentido de que as investigações dos crimes cibernéticos necessitam dessas perícias. Dessa forma, diante da falta de técnica e arcabouços humanos preparados, nasce a importância da especialização dos profissionais que atuarão neste tipo de investigação.

Ademais, quanto à identificação de autoria, apesar de certa facilidade ao se rastrear um computador em que houve a prática de um crime, há uma dificuldade em associar o computador ao sujeito ativo do crime. A utilização da biometria e a prisão em flagrante com o computador ativo seriam algumas soluções propostas a fim de sanar tal problema. Portanto, considerando a grande capacidade de volatilidade dos meios que servirão como prova do crime cibernético praticado, o instituto da produção antecipada de provas ganha

importância, diante da possibilidade de perecimento das provas.

REFERÊNCIAS BIBLIOGRÁFICAS

SUAPESQUISA – Formulários e Pesquisas Online. Revolução Industrial, História da Revolução Industrial, pioneirismo inglês, invenções de máquinas, passagem da manufatura para a maquinofatura, a vida nas fábricas, origem dos sindicatos. Disponível em: <http://www.suapesquisa.com/industrial>. Acesso em: 11/10/ 2017.

FRAGOMENI, Ana Helena. Dicionário Enciclopédico de Informática. Vol.I. Rio de Janeiro: Campus, 1987.

SUPERDICAS - Invenções que mudaram o mundo e sobreviveram ao tempo. Disponível:<http://www.superdicas.com.br/almanaque/almanaque.asp?u_action=display&u_log=254>.Acesso em: 12/10/ 2017.

GOUVEA, Sandra. O direito na era digital: crimes praticados por meio da informática. Rio de Janeiro: Editora Mauad, 1997.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos, Ameaças e Procedimentos de investigação. Rio de Janeiro: Brasport, 2013.

TURNER, David; MUNOZ, Jesus. Para os filhos dos filhos de nossos filhos: uma visão da sociedade de internet. São Paulo: Summus, 1999.

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

NOGUEIRA, Sandro D'Amaro. Crimes de Informática. Leme: BH Editora, 2009.

LEMOS, André/LÉVY, Pierre. O futuro da Internet: em direção a uma ciberdemocracia. São Paulo: Paulus, 2010.

PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.

CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <http://www.cert.br>. Acesso em: 14/10/2017.

NOGUEIRA, Sandro D'Amaro. Crimes de Informática. Leme: BH Editora, 2009.

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

LIMA, Paulo Marco Ferreira. Crimes de Computador e Segurança Computacional. São Paulo: Editora Atlas, 2011.

FERREIRA, Ivette Senise. A Criminalidade Informática. Direito & Internet – Aspetos Jurídicos Relevantes. Editora Edipro, 2011.

FELICIANO, Guilherme Guimarães. Informática e criminalidade: primeiras linhas. Ribeirão Preto/SP: Nacional de Direito, 2001.

LÉVY, Pierre. Cibercultura. São Paulo: Editora 34, 2010.

CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha.

PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. A nova lei de crimes digitais.2013.Disponível:www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1432>. Acesso em: 20/10/2017.

BRASIL. Supremo Tribunal Federal – RHC n. 76.689-0 – Pernambuco – Primeira Turma – Relator: Ministro Sepúlveda Pertence, DJU de 6.11.1998, p.03.

CF/88, art. 5º, XXXIX: "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".

SILVA, Marco Antônio Marques da Silva. Acesso à Justiça Penal e Estado Democrático de Direito. São Paulo: Ed. J. de Oliveira, 2001.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 24/10/2017.

MARTINS, Pedro Batista. Comentários ao Código de Processo Civil. Forense, v.2.

BRASIL. PRESIDÊNCIA DA REPÚBLICA – Casa Civil – Subchefia para Assuntos Jurídicos – Medida Provisória n° 2.200-1, de 27 de Julho de 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-1.htm>. Acesso em: 30/10/2017.

RODRIGUES, Thalita Scharr; FOLTRAN JUNIOR, Dierone César. Análise de ferramentas forenses na investigação digital. 2010. Disponível em: <http://www.revistaret.com.br/ojs-2.2.3/index.php/ret/article/viewFile/64/93>. Acesso em: 30/10/2017.

TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. Curso de Direito Processual Penal. Salvador: Jus Podivm, 2012.

OLIVEIRA, Eugênio Pacelli. Curso de Processo Penal. Rio de Janeiro: Lúmen Júris, 2011.

LOPES Jr., Aury. Sistemas de investigação preliminar no processo penal. Rio de Janeiro: Lumen Juris, 2001.