Centro Universitário de Brasília - UNICEUB

Faculdade de Ciências Jurídicas e Sociais - FAJS

CAMILA BARRETO ANDRADE DIAS

CRIMES VIRTUAIS

As inovações jurídicas decorrentes da evolução tecnológica que atingem a produção de provas no processo penal

Brasília
2014

CAMILA BARRETO ANDRADE DIAS

CRIMES VIRTUAIS

As inovações jurídicas decorrentes da evolução tecnológica que atingem a produção de provas no processo penal

Monografia apresentada à Faculdade de Ciências Jurídicas e Sociais (UNICEUB / FAJS) como pré-requisito para a obtenção do grau de Bacharel em Direito.
Orientadores: Gabriel Haddad Teixeira e Larissa Maria Melo Souza

Brasília
2014

CAMILA BARRETO ANDRADE DIAS

CRIMES VIRTUAIS

As inovações jurídicas decorrentes da evolução tecnológica que atingem a produção de provas no processo penal

Monografia apresentada à Faculdade de Ciências Jurídicas e Sociais (UNICEUB / FAJS) como pré-requisito para a obtenção do grau de Bacharel em Direito.
Orientadores: Gabriel Haddad Teixeira e Larissa Maria Melo Souza

Brasília, ____ de _____ de 2014

Banca Examinadora

_____

_____

RESUMO

A popularização da internet e o desenvolvimento tecnológico possibilitaram a ocorrência de uma nova modalidade de crimes: os crimes virtuais. Considerando o surgimento desses novos delitos em decorrência do uso da internet e a necessidade do Direito em acompanhar as mudanças trazidas pela evolução tecnológica, uma vez que estas influenciam nos aspectos jurídicos, optou-se por abordar esse tema. 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 das leis 12.735/12 e 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 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 são as questões objeto de análise do presente trabalho.

Palavras-chave: Internet. Crimes virtuais. Provas. Autoria. Investigação. Perícias Especializadas.

SUMÁRIO

INTRODUÇÃO

A sociedade atual tem passado por grandes transformações em decorrência do crescimento da tecnologia da informação. Essa evolução tecnológica permitiu o surgimento da internet, rede mundial de computadores capaz de interligar computadores do mundo inteiro, proporcionando uma maior facilidade de comunicação. 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 cada vez maior dos recursos tecnológicos em atividades cotidianas.

No entanto, a internet que a princípio surgiu como uma nova tecnologia de comunicação se transformou em um instrumento utilizado para a prática de condutas ilícitas, que se tornam cada vez mais perigosas, uma vez que se adaptam facilmente 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 eficiência da tecnologia, velocidade no acesso e a disseminação da informação acrescentaram algumas peculiaridades no tratamento dos crimes virtuais. Estes tipos de crimes são caracterizados pela velocidade e novidade, que quando consideradas 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.

Por se tratar o Direito de um instrumento regulador e organizador da sociedade e considerando que as evoluções sociais, econômicas e políticas influenciam nos aspectos jurídicos, cabe ao Direito acompanhar todas as mudanças decorrentes da evolução tecnológica pela qual passa a sociedade, buscando se adaptar as transformações, a fim de promover novas soluções para as novas peculiaridades trazidas com a prática dos crimes virtuais.

A presente monografia tem por tema a análise das particularidades decorrentes da prática dos crimes digitais no que diz respeito à produção de provas. Os problemas enfrentados diante da prática desse tipo de crime não se resumem à ausência de tipificação dos crimes digitais praticados, outras questões tais como necessidade de profissionais especializados

na investigação criminal, dificuldade na identificação da autoria e a produção antecipada de provas merecem igual análise e estudo.

A discussão sobre os crimes cibernéticos se mostra relevante, visto que com a evolução tecnológica, a informática, especialmente a internet, se tornou o principal meio de comunicação e tráfego de informações, transformando o dia-a-dia da sociedade contemporânea. 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.

A monografia buscou responder a seguinte problemática: diante do surgimento dessa nova modalidade criminal, quais as medidas tomadas para combate-la? A tipificação de novas condutas é suficiente para a solução dos novos delitos? Quais são as particularidades decorrentes da prática de um crime virtual que podem influenciar a investigação de tais crimes? E de que forma essas peculiaridades dificultam a investigação? Apesar dos esforços empenhados no combate aos crimes virtuais, a criminalidade informática, usufruindo das novas tecnologias que surgem a cada momento, desafia os profissionais da área, no sentido de que os operadores ainda não estão totalmente preparados para enfrentar esse tipo de crime em decorrência de suas características que acabam por dificultar a investigação criminal.

No primeiro capítulo, serão abordados os antecedentes históricos da internet e a forma com a qual a rede mundial de computadores, a princípio um novo meio de comunicação consequência da evolução tecnológica, se transformou em um instrumento utilizado para a propagação de condutas delitivas. Serão apresentadas a definição e a classificação dos crimes virtuais, bem como analisados os bens jurídicos atingidos com a prática desses crimes.

Outro aspecto desse capítulo é a análise do significado de virtual e real, uma vez que os crimes virtuais são praticados em um ambiente desprovido de barreiras físicas, ou seja, um ambiente caracterizado pela ausência de um espaço demarcável, mas que nem por isso pode ser considerado um “terreno sem lei”, algo irreal. Por último será tratado o que há de legislação existente para combater essas novas condutas.

No segundo capítulo, serão apresentadas as questões da Teoria Geral da Prova relacionadas às particularidades dos crimes virtuais. Neste capítulo, o objetivo não é esgotar o tema Teoria Geral da Prova, mas apenas discutir os assuntos que possuem uma relação com os

crimes virtuais quais sejam a necessidade da coleta de provas para se chegar à autoria do delito, os fatos que podem ser considerados objeto de prova, sistema de valoração das provas e os meios de prova que podem ser admitidos para a comprovação dos fatos levantados no processo.

No terceiro capítulo serão apresentadas as particularidades dos crimes virtuais no que diz respeito à investigação criminal. A celeridade, velocidade e dinamismo com que eles se propagam trazem algumas dificuldades para a sua investigação quais sejam a necessidade de perícia especializada, a dificuldade na identificação da autoria, uma vez que o ambiente no qual são praticados facilita o anonimato do sujeito ativo e a necessidade de produção antecipada de provas, quando se considera a volatilidade e efemeridade dos dados que servirão como provas do delito praticado.

Por fim, cabe ressaltar que a presente monografia não pretende exaurir a matéria dos crimes virtuais que é um assunto relativamente novo, que abrange questões diversas além das questões probatórias discutidas no trabalho.

1. CRIMES VIRTUAIS

Os crimes virtuais são uma espécie de crime originária da evolução tecnológica por qual passa a sociedade contemporânea. Os avanços tecnológicos e as novas descobertas científicas trouxeram uma nova realidade para o ser humano, onde o espaço e a presença física não são fundamentais para a realização de condutas ilícitas[1].

Neste capítulo será abordada a evolução do direito digital, será analisado de que forma o desenvolvimento da internet e sua influência na sociedade contribuíram para o surgimento dos chamados crimes virtuais. Se por um lado a internet trouxe vários benefícios para a sociedade; por outro lado permitiu o surgimento de condutas ilícitas até então desconhecidas. Após um breve relato sobre o histórico dos crimes digitais, será apresentada a sua definição, classificação e as particularidades trazidas com esses crimes no que diz respeito aos bens jurídicos atingidos com a prática das condutas ilícitas na rede mundial de computadores. Ademais, apesar da ausência de um ambiente físico para a perpetuação desses crimes, uma vez que eles ocorrem em um "mundo virtual", não se pode confundir o virtual com o irreal, esses dois termos não se confundem. Por último será tratado como o Brasil tem se preparado para combater essa nova espécie de crime e o que há de legislação existente tipificando essas novas condutas.

1.1 Histórico, definição e classificação dos crimes virtuais

Desde sua origem até os dias atuais o homem tem a constante necessidade em desenvolver ferramentas úteis para auxiliá-lo no seu dia-a-dia. Esta evolução pode ser observada desde a criação do ábaco, instrumento utilizado para fazer cálculos, passando pela criação do primeiro computador digital automático e do primeiro computador eletrônico (ENIAC – *Eletronic Numerical Integrator and Calculator*) projetado e construído a pedido do exército norte-americano para automatizar o cálculo de tabelas balísticas.

Em 1946, foram criados os transistores, futuros microprocessadores, possibilitando que os computadores se tornassem acessíveis a qualquer pessoa[2], o que não ocorria

---

[1] MALAQUIAS, Roberto Antônio Darós. *Crime Cibernético e Prova – A investigação criminal em busca da verdade.* Curitiba: Juruá Editora, 2012. p. 52.

[2] GOUVEA, Sandra. *O direito na era digital: crimes praticados por meio da informática*. Rio de Janeiro: Editora Mauad, 1997, p. 31.

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 resposta 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[3].

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[4].

Diante dessa mudança de perspectiva, foi criada na década de 60, a ARPANET, uma rede de comunicação militar descentralizada, encomendada pela Força Aérea Estadunidense, cuja preocupação era se proteger no caso de eventual guerra ou ataque nuclear. O objetivo era a construção de um modelo de comunicação que garantisse a continuidade das operações de comunicações governamentais. Assim, mesmo diante de um ataque, as informações sigilosas não se perderiam, uma vez que poderiam ser distribuídas de forma descentralizada a outras localidades[5].

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[6].

A importância cada vez maior de se criar uma rede capaz de interligar computadores distantes entre si, permitindo a comunicação de dados entre eles, foi o fator propulsor que promoveu o crescimento contínuo da ARPANET. A rede de comunicações que a princípio foi criada para atender um pedido da Força Aérea Americana passou a interligar

---

[3] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. *Crimes Cibernéticos, Ameaças e Procedimentos de investigação.* Rio de Janeiro: Brasport, 2013. p.5.
[4] Ibidem, p.6.
[5] CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais.* São Paulo: Editora Saraiva, 2011, p. 30.
[6] TURNER, David; MUNOZ, Jesus. *Para os filhos dos filhos de nossos filhos: uma visão da sociedade de internet.* São Paulo: Summus, 1999.p.29.

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.

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. Isto é, os sistemas informatizados atualmente são tão importantes na sociedade que a maioria das pessoas, seja física ou jurídica, depende de um dispositivo informatizado, seja para uso na esfera comercial, como a execução de ações financeiras pelo computador, seja na esfera empresarial, como a utilização dos bancos de dados para o armazenamento de seus arquivos mais valiosos[7].

Várias pesquisas já foram realizadas com o objetivo de demonstrar o crescente uso da internet no Brasil. Uma pesquisa do Ibope Media revelou que o Brasil é atualmente um dos principais países no acesso a internet, o quinto país mais conectado à rede. De acordo com o Fecomércio-Rj/Ipsos, houve um aumento de 27% para 48%, entre 2007 e 2011, de brasileiros conectados à internet. A pesquisa especifica também os principais locais de acesso à rede quais sejam a *lan house* (31%), residência (27%) e a casa de parentes e amigos (25%)[8].

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.

Pelos ensinamentos de Sandro D'Amaro Nogueira, o rol dos crimes cometidos por meio eletrônico é extenso[9]. 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

[7] CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais*. São Paulo: Editora Saraiva, 2011, p. 31.
[8] ANTONIOLI, Leonardo. *Estatísticas, dados e projeções atuais sobre a internet no Brasil.* 2014. Disponível em: <http://tobeguarany.com/internet_no_brasil.php>. Acesso em: 05 mar. 2014.
[9] NOGUEIRA, Sandro D'Amaro. *Crimes de Informática*. Leme: BH Editora, 2009, p. 36.

como interceptação de comunicações, modificações de dados, difusão de pornografia infantil, terrorismo[10].

Decorrentes do avanço tecnológico da sociedade, os crimes virtuais 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 virtuais 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 criminalizada (Crime informático) estereotiparia um modelo de cibercrime"[11].

O surgimento de novas condutas ilícitas praticadas através da internet, envolvendo a utilização de computadores é cada vez mais intensa e variada, acompanhando 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 de computador. Os chamados crimes virtuais recebem várias denominações em diversos países do mundo; são também chamados de "crimes de informática" ou "*cybercrimes*", "delitos computacionais", "crimes eletrônicos", "crimes telemáticos", etc[12].

Assim como não há um consenso quanto à denominação dos crimes praticados na rede mundial de computadores, também não há um consenso quanto à classificação dos crimes virtuais. Os chamados crimes de computador surgiram nas últimas décadas do século XX, em meados dos anos 70, acompanhando o aumento na utilização dos computadores, sendo assim consideradas as condutas efetivadas através da utilização de um computador conectado ou não a uma rede[13].

Em meados da década de 1980, Tiedermann classificou os crimes de informática no âmbito dos delitos econômicos como: manipulações, espionagem, sabotagem e

---

[10] CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais.* São Paulo: Editora Saraiva, 2011, p. 46.
[11] COLLI, Maciel. *Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos.* Curitiba: Juruá Editora, 2010. P. 44.
[12] CRESPO, op. cit., p. 46.
[13] LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional.* São Paulo: Editora Atlas, 2011. p. 8.

furto de tempo[14]. 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).

Embora não exista uma unanimidade em relação à classificação dos crimes virtuais, a classificação mais comum é a de separar as condutas em que a informática é meio e as demais conduta. Para classifica-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), como também àquelas condutas consideravelmente perigosas, ainda não incriminadas no Brasil, cujos bens jurídicos atingidos são exclusivamente os sistemas informatizados[15].

Diante da diversidade de classificações dos crimes virtuais, a forma mais usual de se classificar os crimes digitais 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)"[16]. Neste sentido, Ivette Senise Ferreira e Vicente Greco Filho adotam a classificação que divide os crimes virtuais em crimes próprios[17], 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

---

[14] CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais.* São Paulo: Editora Saraiva, 2011. p. 60.

[15] MALAQUIAS, Roberto Antônio Darós. *Crime Cibernético e Prova – A investigação criminal em busca da verdade.* Curitiba: Juruá Editora, 2012. p. 60.

[16] CRESPO, op. cit., p. 62.

[17] 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.

instrumentos nas mãos dos criminosos e propiciou a formação de uma criminalidade específica da informática cujo alcance ainda não foi corretamente avaliado[18].

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.

1.2 Bens Jurídicos relativos à Informática – Criminalidade informática

Juntamente com vários benefícios e facilidades, a internet trouxe também alguns males e possibilitou o surgimento de novos delitos praticados através da rede mundial de computadores.

Uma pesquisa realizada pelo CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), grupo de respostas vinculado ao Comitê Gestor da internet no Brasil[19], aponta que em 2013 foram totalizados 352.925 incidentes no Brasil, dentre os quais tentativas de fraude, ataques a servidores Web, varreduras e propagação de códigos maliciosos[20].

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 definida.

---

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

[19] Comitê responsável por receber, analisar e responder incidentes de segurança envolvendo qualquer rede brasileira conectada à internet.

[20] CERT.br. Estatísticas dos incidentes reportados ao CERT.br. Disponível em: <http://www.cert.br/stats/incidentes/>,acessado em 08 de março de 2014

Devido a existência de lacunas da lei penal e da impossibilidade de se utilizar da analogia *malam partem* no direito penal, 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, enquanto, com a sociedade digital globalizada, outros bens jurídicos (difusos) passaram a ser afetados[21]. Neste 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 virtuais 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 sistemas de redes de computadores[24].

---

[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.
[24] CRESPO, op. cit., p. 56.

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

> "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, a criminalidade da informática está limitada a uma vinculação da utilização dos computadores, facilitada pela internet, 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.

1.3 Virtual versus Real

A internet, rede mundial de computadores, apresenta uma maior fragilidade e possibilidade de se praticar os cibercrimes, por se tratar de uma rede pública e de não ser regida por qualquer tipo de ordenamento, permitindo 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 cibercrimes por meio da internet pode envolver a multinacionalidade de sujeitos e bens"[27].

---

[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.

[27] COLLI, Maciel. Cibercrimes. *Limites e perspectivas à investigação policial de crimes cibernéticos.* Curitiba: Juruá Editora, 2010. p. 45.

O francês Pierre Levy entende 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].

No cotidiano, enquanto a realidade pressupõe algo tangível; a palavra virtual costuma ser empregada no sentido de irrealidade. 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 de Pierre Levy "ainda que não seja possível fixar o virtual em nenhuma coordenada espaçotemporal, o virtual é real" [29]. Não é correto, no entanto, tratar o mundo virtual como um mundo sem regras, na qual tudo é permitido, pelo simples fato de considerá-lo uma "não realidade"[30].

Assim, a virtualização é definida por Levy como o movimento inverso da atualização:

> "A atualização aparece então como a solução de um problema, uma solução que não estava contida previamente no enunciado. A atualização é a criação, invenção de uma forma a partir de uma configuração dinâmica de forças e finalidades. [...] A virtualização não é uma desrealização (a transformação de uma realidade num conjunto de possíveis), mas uma mutação de identidade, um deslocamento do centro de gravidade ontológico do objeto considerado: em vez de se definir principalmente por sua atualidade (uma solução), a entidade passa a encontrar sua consistência essencial num campo problemático"[31].

A ausência de um espaço demarcável não é suficiente para tornar a virtualização algo irreal. O fato da 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.

Nesse mesmo sentido, considerando que o virtual não corresponde à irrealidade, Paulo Marco Ferreira Lima afirma que a internet não pode ser considerada como uma terra sem lei, uma vez que as operações realizadas na internet são fundamentadas nos

---

[28] LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 2010. p. 49.
[29] Ibidem, p. 50.
[30] Ibidem, p. 50.
[31] Idem. *O que é o virtual?*. São Paulo: Editora 34, 2011. p. 17.

relacionamentos entre os seres humanos e, portanto, devem ser regidas obrigatoriamente pelos princípios gerais do direito. É dever do Estado coibir qualquer conduta sempre que as liberdades individuais ou interesse público forem lesionados. A conduta humana sempre será objeto do direito, ainda que realizada por intermédio dos computadores[32].

Diante desse cenário, cabe ao Direito acompanhar todas essas mudanças proporcionadas pela evolução tecnológica, uma vez que as evoluções no mundo social, econômico e político influenciam nos aspectos jurídicos, no sentido de discutir regulamentos e normas de forma a minimizar os conflitos entre os indivíduos que se utilizam deste meio, bem como os delitos praticados por tais indivíduos[33].

Não é a primeira vez na história que o Direito tem que acompanhar a evolução da sociedade. Todos os veículos de comunicação (imprensa, telefone, rádio, televisão), a partir do momento que se tornaram veículos 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 ordenamento jurídico e na sociedade"[34].

Os dispositivos criados pelo homem, computadores e suas redes, possuem uma natureza dúplice dependendo 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 dever do Estado prever mecanismos de prevenção e repressão das condutas ilícitas[35].

A necessidade de criação de mecanismos de prevenção e repressão que suportem as particularidades e peculiaridades trazidas com a prática de novas condutas ilícitas através da internet não impõe a criação de um novo direito. O Direito Digital pode ser considerado uma evolução do próprio Direito, já que abrange todos os princípios e regras já utilizados atualmente, contudo, incluindo novas normas para o Direito, em todas as suas áreas.

---

[32] LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. São Paulo: Editora Atlas, 2011. p. XVI.
[33] CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais.* São Paulo: Editora Saraiva, 2011. p. 38.
[34] PINHEIRO, Patrícia Peck. *Direito Digital.* São Paulo: Editora Saraiva, 2013, p. 76.
[35] LIMA, op. cit., p. XVI.

Isto é, não há a necessidade da criação de um direito específico, direito da internet, que contemple todas as peculiaridades trazidas pela internet, apenas a necessidade de previsão dessas particularidades pelas áreas do Direito.

1.4 Legislação Brasileira e os cybercrimes

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[36].

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" [37]. 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" [38].

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 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

---

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

[37] SILVA, Marco Antônio Marques da Silva. *Acesso à Justiça Penal e Estado Democrático de Direito.* São Paulo: Ed. J. de Oliveira, 2001, p. 07.

[38] 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: 20 de abr. 2014.

autoria do Deputado Paulo Teixeira; e o projeto de lei nº 84/99, de autoria do Deputado Eduardo Azeredo[39].

Em decorrência de alguns episódios[40] 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)[41] e a regra da ação penal para esse crime (Art. 154-B)[42], 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

---

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

[40] Em meados de 2011, ocorreram vários ataques de negação de serviço a sites do governo brasileiro que ficaram instáveis até sair do ar. Ademais, a atriz Carolina Dieckmann teve 36 fotos roubadas por hackers de seus arquivos pessoais e divulgadas na internet.

[41] "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: 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: 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".

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

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:

> "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."[43]

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[44].

---

[43] 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: 23 mar. 2014.

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

2. PROVA

O desenvolvimento tecnológico permitiu o surgimento da chamada sociedade da informação[45] caracterizada pela dependência cada vez maior da eficiência e segurança da tecnologia da informação e dos recursos tecnológicos. Essa evolução não trouxe somente benefícios para a sociedade, mas também permitiu que a criminalidade se apresentasse sob novas formas até então desconhecidas[46].

A era da informação, além de facilitar o fenômeno conhecido como globalização, interferiu ainda na prática de delitos à distância. A evolução tecnológica gerou novas formas de práticas ilícitas. A lista de crimes é extensa, contudo, não basta apenas a inclusão de novos tipos penais, uma vez que outras inovações foram trazidas com o surgimento desses crimes como àquelas relacionadas à investigação probatória[47].

No presente capítulo será apresentado um breve relato sobre a questão da prova no processo penal, antes de adentrar as questões relativas as particularidades trazidas com os crimes digitais no que se refere à produção de provas. Não é objetivo do capítulo esgotar todas as questões relacionadas à Teoria Geral da Prova, mas apenas levantar alguns assuntos que possuem uma associação direta com os crimes virtuais. Serão apresentados os aspectos gerais referentes à prova, objeto da prova, incluindo os fatos que não necessitam de comprovação probatória, valoração das provas, bem como os meios de prova.

2.1 Aspectos Gerais

Uma ferramenta que possui grande importância para o direito é a constituição da prova[48]. Cabe às partes envolvidas no litígio não apenas alegar os fatos ocorridos, mas também demonstrá-los, a fim de convencer o magistrado sobre a veracidade de tudo aquilo que foi afirmado em juízo. No processo penal, o objetivo das partes que litigam em juízo é o

---

[45] Sociedade da informação é a expressão utilizada para definir a sociedade que se formou a partir da evolução tecnológica e da dependência cada vez maior da tecnologia em atividades do dia a dia. Nessa sociedade mais conectada, a informação não só ganhou mais valor, como também tornou-se um fator de poder.

[46] CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais.* São Paulo: Editora Saraiva, 2011. p. 27.

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

[48] 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: 16 mar. 2014.

convencimento do julgador através de uma reconstrução histórica dos fatos ocorridos tendo como base o conjunto probatório anexado aos autos[49].

O processo penal é um instrumento utilizado para reconstruir determinado fato histórico da forma mais aproximada possível da realidade. Quando considerado como um rito, a função do processo penal é instruir o julgador e, por meio da reconstrução histórica de um fato, proporcionar o conhecimento do magistrado. Neste caso, as provas são os meios utilizados para que essa reconstrução do passado seja feita[50].

Por meio principalmente das provas, o processo penal busca fazer uma reconstrução do passado de forma a criar condições para que o magistrado exerça sua atividade recognitiva em relação ao fato narrado na peça acusatória. O exercício dessa atividade será o ponto inicial para a produção de seu convencimento que será externado na sentença. Aury Lopes Jr. considera que tanto o processo penal quanto as provas nele admitidas integram o que ele chama de "modos de construção do convencimento do julgador" cujo objetivo é formar sua convicção e legitimar o poder contido na sentença[51].

A prova pode ser conceituada como um conjunto de ações praticadas pelas partes, juiz ou terceiros, destinadas a comprovar ao juiz a ocorrência ou inocorrência do fato, a veracidade ou não de uma informação. Isto é, "a prova é todo e qualquer meio de percepção empregado pelo homem com o objetivo de comprovar a veracidade de uma alegação"[52].

Fernando Capez afirma que um dos temas mais importantes da ciência processual é a prova. Em suas palavras "as provas constituem os olhos do processo, o alicerce sobre o qual se ergue toda a dialética processual"[53]. A inexistência de provas idôneas e válidas implica na impossibilidade de uma condenação. Esta só ocorrerá quando houver uma certeza acerca da culpabilidade que não é obtida através de suposições e alegações não comprovadas.

Para J. E. Carreira Alvim, a prova pode ser conceituada sob duas acepções distintas: no sentido objetivo e no sentido subjetivo. Objetivamente, as provas correspondem a todos os métodos utilizados para demonstração da existência ou não de um fato jurídico, ou aos

---

[49] TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. Curso de Direito Processual Penal. Salvador: Jus Podivm, 2012. p. 376.
[50] LOPES JR, Aury. *Direito Processual Penal.* São Paulo: Saraiva, 2014. p. 549.
[51] Ibidem, p. 550.
[52] CAPEZ, Fernando. *Curso de Processo Penal.* São Paulo: Saraiva, 2011. p. 344.
[53] Ibidem, p. 344.

métodos utilizados com propósito de esclarecimento da ocorrência para que o juiz conheça da verdade dos fatos. Subjetivamente, é a "convicção que se forma no espírito do juiz quanto à verdade dos fatos". A prova está intimamente ligada à demonstração da verdade dos fatos[54].

Neste mesmo sentido, Magalhães Gomes Filho diz que o termo prova pode ser conceituado sob três óticas distintas: em primeiro lugar, a prova é utilizada tanto pelo magistrado quanto pelas partes, com o propósito de reconstruir os fatos históricos tal como ocorreram; em segundo lugar, a prova é utilizada como meio de prova para trazer as informações a respeito do fato ocorrido ao processo; em terceiro lugar, a prova equivale à certeza da convicção do juiz[55].

Assim, o estado de convencimento do juiz considerado juntamente com o material anexado no processo resultará na prova. Enquanto os fatos alegados constituem os objetos da prova; a busca pelo convencimento do juiz quanto à veracidade dos fatos representa a finalidade da prova. Contudo, é necessário considerar que não é a alegação de qualquer fato que pode ser considerado objeto da prova.

2.2 Objeto da Prova

Segundo Nestor Távora e Rosmar Rodrigues, o objeto da prova consiste nos "fatos que fundamentarão a ação e a defesa capazes de influenciar na decisão do juiz, na responsabilidade penal e na fixação da pena, necessitando, portanto, de adequada comprovação em juízo". Isto é, para que um processo tenha prosseguimento, todas as circunstâncias, fatos e alegações relacionados ao litígio, sobre os quais restarem o quesito da dúvida, devem ser demonstrados em juízo, de forma a viabilizar o julgamento.[56].

Contudo, somente os fatos relevantes, relacionados ao litígio, poderão ser considerados objetos da prova. Em respeito ao princípio da economia processual, o juiz deve dirigir o processo de forma a evitar que atrasos em seu curso ocorram em decorrência do requerimento de provas dispensáveis ou simplesmente protelatórias ocasionalmente feito pelas partes. Alguns fatos carecem de provas e outros não.

---

[54] ALVIM, J. E. Carreira. *Teoria Geral do Processo revista, ampliada e atualizada*. Rio de Janeiro: Editora Forense, 2009. p. 260.
[55] MAGALHÃES GOMES FILHO, Antônio. *Direito à prova no processo penal*. São Paulo: RT, 1997, p. 41.
[56] CAPEZ, Fernando. *Curso de Processo Penal*. São Paulo: Saraiva, 2011. p. 345.

Não necessitam ser provados os fatos notórios, também chamados de verdade sabida, pois já são de conhecimento público, já fazem parte da cultura de uma sociedade. Segundo Heráclito Antônio Mossim, "o fato notório é aquele de existência vulgarizada, indicando-se uma verdade irretorquível que deve ser aceita sem discrepância"[57].

Da mesma maneira, os fatos chamados axiomáticos ou intuitivos não serão objeto da prova, pois são aqueles que se demonstram por si só, que tem força probatória própria. São fatos evidentes que se impõem ao raciocínio, como decorrência natural de outros. Como, por exemplo, quando alguém se depara com um corpo putrefeito, é evidente que se trata de um cadáver[58].

Por fim, as presunções legais independem de prova. São conclusões extraídas da própria lei, podendo ser absolutas ou relativas. Enquanto estas invertem o ônus da prova; aquelas dispensam a produção de provas. As presunções absolutas não admitem prova em contrário, enquanto as presunções legais relativas já admitem[59].

Devem ser comprovados os fatos controvertidos, aqueles sobre os quais há discordância entre as partes; afirmados por uma das partes e negados pela parte contrária; fatos relevantes, aqueles que tenham relação com o litígio e que de alguma forma influenciam na decisão do juiz; fatos determinados, que devem apresentar características suficientes que o distingam de outros semelhantes[60].

Encerrada a instrução probatória e definidos os fatos que podem ser considerados como provas, caberá ao juiz analisa-los a fim de solucionar o litígio confirmando a existência ou não dos fatos alegados e da veracidade de tais fatos. Ao analisar as provas, o juiz deverá seguir determinado critério, dependendo do sistema de apreciação de provas adotado.

2.3 Sistemas de apreciação de provas

Os principais sistemas de apreciação das provas apresentadas durante o processo são: o sistema da íntima convicção, também conhecido como sistema da certeza moral;

---

[57] MOSSIM, Heráclito Antônio. *Compêndio de Processo Penal*. São Paulo: Manole, 2010. p. 306.
[58] TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. *Curso de Direito Processual Penal.* Salvador: Jus Podivm, 2012. p. 378.
[59] CAPEZ, op. cit., p. 345.
[60] ALVIM, J. E. Carreira. *Teoria Geral do Processo revista, ampliada e atualizada*. Rio de Janeiro: Editora Forense, 2009. p. 271.

o sistema da prova tarifada, também conhecido como sistema das regras legais; e, por último, o sistema da persuasão racional, também conhecido como sistema do livre convencimento motivado. Assim, a valoração das provas pelo magistrado sofrerá variações dependendo do método de apreciação utilizado. Segundo Nestor Távora, as regras de apreciação adotadas demonstram a transparência no ato de julgar, uma vez que revelam o porquê do convencimento do juiz, qual o direcionamento do magistrado quando da tomada de sua decisão[61].

De acordo com o sistema da íntima convicção, o juiz tem total liberdade para decidir e não está obrigado a motivar a sua decisão. Não há qualquer regra de valoração das provas, podendo o magistrado inclusive se utilizar de suas crenças pessoais para tomar a sua decisão. Este sistema é aplicado, como exceção, nas decisões proferidas pelos júri popular ao votar nos quesitos sigilosamente, sem a necessidade de fundamentação[62].

No sistema da certeza moral do legislador, a lei atribui um valor a cada prova, inclusive estabelecendo uma hierarquia entre elas, retirando qualquer liberdade do julgador de apreciação da prova. O juiz deve obrigatoriamente respeitar as regras estabelecidas, obedecendo ao sistema e aos valores impostos pela lei. Não há convicção pessoal do magistrado na valoração das provas. Um exemplo da aplicação desse sistema é a previsão do Artigo 158 do Código de Processo Penal. De acordo com esse artigo, a materialidade dos crimes que deixam vestígios deve ser comprovada com a realização de exame de corpo de delito. Não existe neste caso a possibilidade do magistrado optar por outra forma de comprovação, como a confissão, por exemplo[63].

O sistema adotado no Brasil é o sistema da persuasão racional pela qual o legislador tem liberdade para decidir e apreciar as provas, não havendo limitação a qualquer critério legal de fixação de valores probatórios, desde que o faça de maneira motivada (Artigo 155, CPP). Este sistema representa um equilíbrio entre os sistemas anteriores. Não existe uma hierarquia entre as provas e o julgador decide livremente de acordo com sua consciência. É

---

[61] TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. *Curso de Direito Processual Penal.* Salvador: Jus Podivm, 2012. p. 398.
[62] ALVIM, J. E. Carreira. *Teoria Geral do Processo revista, ampliada e atualizada.* Rio de Janeiro: Editora Forense, 2009. p. 278.
[63] CAPEZ, Fernando. *Curso de Processo Penal.* São Paulo: Saraiva, 2011. p. 383.

importante frisar que a liberdade do juiz não é absoluta, pois deve explicitar motivadamente as razões que o levaram a tomar determinada decisão[64].

Ao se considerar os três modelos de valoração das provas, nota-se que o sistema do livre convencimento motivado é um importante princípio a sustentar a garantia da fundamentação das decisões judiciais, em contrapartida ao radicalismo do sistema legal de provas, que correspondia a um sistema de valoração hierarquizada de provas, sem se importar com as particularidades de cada caso concreto; e do sistema da íntima convicção, caracterizado pelo excesso de discricionariedade e liberdade, uma vez que a decisão do juiz não precisava ser fundamentada e nem obedecer a critérios de avaliação das provas[65].

No sistema da persuasão racional não existem limites e regras abstratas de valoração, o juiz, ao formar sua convicção, obrigatoriamente deverá fundamentá-la. A liberdade do magistrado não é plena, o juiz não pode tomar suas decisões substituindo as provas por meras conjecturas, baseando-se somente em sua opinião[66].

Assim como não existe uma liberdade absoluta quando o juiz tem que decidir a respeito do litígio, necessitando fundamentar a sua decisão motivadamente, também não existe uma liberdade absoluta quando se trata dos meios de provas permitidos na busca da comprovação dos fatos alegados no processo.

2.4 Meios de Prova

Os meios de prova são todos os recursos que podem ser utilizados, direta ou indiretamente, para comprovar a veracidade dos fatos alegados. É tudo aquilo que pode ser utilizado para demonstrar os fatos alegados no processo.

Os meios de prova, nas palavras de Paulo Rangel, "são todos aqueles que o juiz, direta ou indiretamente, utiliza para conhecer da verdade dos fatos, estejam eles previstos em lei ou não"[67]. Essa ausência de previsibilidade em lei está relacionada ao princípio da verdade real, predominante no processo penal, a qual não há qualquer limitação à prova, permitindo assim a

[64] CINTRA, Antônio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. *Teoria Geral do Processo.* São Paulo: Malheiros Editores, 2009. p. 377.
[65] LOPES JR, Aury. *Direito Processual Penal.* São Paulo: Saraiva, 2014. p. 575.
[66] Ibidem, p. 576.
[67] RANGEL, Paulo. *Direito Processual Penal.* Rio de Janeiro: Lumen Juris, 2003. p. 417.

utilização de meios de prova não previstos em lei, desde que sejam legítimos e não afrontem o ordenamento.

O rol de provas admissíveis elencado no Código de Processo Penal é meramente exemplificativo. Assim, poderão ser utilizadas provas nominadas e inominadas na busca da verdade dos fatos. Enquanto estas representam as provas ainda não normatizadas no ordenamento; aquelas representam as provas já disciplinadas na legislação[68].

Juntamente com as provas nominadas, previstas no ordenamento jurídico, são admitidas excepcionalmente as provas inominadas, provas não contempladas na lei, para a demonstração dos fatos e circunstâncias do litígio em questão. Contudo, a utilização destas provas deve respeitar os limites constitucionais e processuais da prova, sob pena de ilicitude ou ilegitimidade dessa prova[69].

Provas ilícitas são aquelas que violam regra de direito material ou a Constituição no momento em que são coletadas. Todo cuidado é necessário a fim de evitar que as provas coletadas se tornem ilícitas, pois caso o sejam deverão ser desentranhadas, já que não são passíveis de repetição, pois o vício ocorre no momento em que foi obtida. Assim, uma prova ilicitamente admitida, ainda que produzida com observância aos limites constitucionais e processuais, será nula por derivação[70].

Em regra, no processo penal impera o princípio da liberdade probatória que implica na plena utilização de meios probatórios idôneos para formação da convicção do juiz, ainda que não estejam expressamente previstos no ordenamento. As limitações figuram apenas no campo das exceções. Deve-se observar, contudo, que mesmo quando não há previsão legal de determinado meio de prova para esclarecimento dos fatos, o meio probatório deve respeitar à dignidade humana e não pode atentar contra a moralidade, sob pena de invalidade[71].

O principal objetivo da prova judiciária é a reconstrução dos fatos investigados de modo a fornecer ao julgador uma verdade judicial capaz de fundamentar a sua decisão final. Desse modo, lhe são fornecidos todos os meios de prova que o permitam se aproximar o máximo

---

[68] TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. *Curso de Direito Processual Penal.* Salvador: Jus Podivm, 2012. p. 379.
[69] LOPES JR, Aury. *Direito Processual Penal.* São Paulo: Saraiva, 2014. p. 596.
[70] Ibidem, p. 608.
[71] TOURINHO FILHO, Fernando da Costa. *Processo penal.* São Paulo: RT, 2003. p. 221.

possível da verdade histórica dos fatos investigados, com o cuidado para não ultrapassar os limites do devido processo legal. Para Eugênio Pacelli, a base da estrutura do devido processo legal é formada pelo contraditório e pela ampla defesa que "ao lado do princípio da inocência, autorizam a afirmação no sentido de ser o processo penal um instrumento de garantia do indivíduo diante do Estado"[72].

O princípio da liberdade probatória não é absoluto. Embora, a liberdade na utilização de provas seja a regra, há limitações que figuram no âmbito da exceção. O parágrafo único do artigo 155 do Código de Processo Penal é um exemplo de limitação imposto na utilização dos meios de prova. Dispõe o artigo que "somente quanto ao estado das pessoas, serão observadas as restrições estabelecidas na lei civil" [73]. Outro exemplo de limitação está prevista no artigo 158 do mesmo código que exige o exame de corpo de delito para todos os crimes que deixam vestígios, afirmando ainda que a confissão do acusado não supre esse tipo de exame[74]. Nestes casos, a lei exige a obrigatoriedade da utilização dos meios de prova previstos no ordenamento.

Dentre as espécies de provas que podem ser utilizadas para demonstrar a existência do fato típico, bem como comprovar a veracidade desses fatos estão os exames periciais dentre os quais o exame de corpo de delito, exame de lesões corporais, exame grafotécnico, exame nos instrumentos da infração; o interrogatório do acusado, que permite que este demonstre a sua versão dos fatos; a confissão, admissão do suposto autor dos fatos que lhe foram atribuídos; os indícios e presunções; a busca e apreensão, etc.[75].

A questão dos meios de prova bem como outros aspectos da prova no processo penal está intimamente relacionados aos crimes virtuais. A celeridade e o dinamismo com que esses crimes se perpetuam na internet, acompanhando a evolução tecnológica pela qual passa a sociedade, acabam trazendo particularidades e obstáculos na solução de tais crimes. A necessidade de perícia especializada, assim como a dificuldade da prova de autoria são algumas

---

[72] OLIVEIRA, Eugênio Pacelli de. *Curso de processo penal.* Rio de Janeiro: Lumen Juris, 2008. p. 283.
[73] BRASIL. *Decreto-Lei no 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Brasília, 1941. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 20 abr. 2014.
[74] CAPEZ, Fernando. *Curso de Processo Penal.* São Paulo: Saraiva, 2011. p. 379.
[75] TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. *Curso de Direito Processual Penal.* Salvador: Jus Podivm, 2012. p. 402.

das questões que merecem ser revistas de forma a adaptar-se as mudanças trazidas com a evolução tecnológica.

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[76].

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"[77].

Os crimes informáticos, 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.

3.1 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 de

[76] MALAQUIAS, Roberto Antônio Darós. *Crime Cibernético e Prova – A investigação criminal em busca da verdade.* Curitiba: Juruá Editora, 2012. p. 59.
[77] CRESPO, Marcelo Xavier de Freitas. *Crimes Digitais.* São Paulo: Editora Saraiva, 2011, p. 159.

computadores. 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[78].

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 depositário eletrônico, através da intervenção humana ou não, em um formato inteligível ao ser humano[79].

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[80].

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[81].

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[82].

---

[78] 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: 20 abr. 2014.

[79] PINHEIRO, Patrícia Peck. *Direito Digital.* São Paulo: Editora Saraiva, 2013, p. 216.

[80] PEREIRA, Evandro della Vecchia. *Investigação Digital: conceitos, ferramentas e estudos de caso.* 2010. Disponível em: <http://www.infobrasil.inf.br/userfiles/26-05-S5-2-68766-Investigacao Digital.pdf>. Acesso em: 20 abr. 2014.

[81] PINHEIRO, op. cit., p. 233.

[82] 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: 20 abr. 2014.

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[83].

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[84]. Ademais, contribui para essa complexidade 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[85].

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[86].

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[87].

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"[88]. 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 do

---

[83] PINHEIRO, Patrícia Peck. *Direito Digital.* São Paulo: Editora Saraiva, 2013, p. 232.
[84] 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.
[85] MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012. p. 65.
[86] LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. São Paulo: Editora Atlas, 2011. p. 15.
[87] PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Editora Saraiva, 2013, p. 234.
[88] TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. *Curso de Direito Processual Penal.* Salvador: Jus Podivm, 2012. p. 383.

processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais"[89].

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 questionamentos que venham a surgir sobre a identidade da prova e a licitude de sua obtenção[90].

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[91].

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 feito

---

[89] BRASIL. *Decreto-Lei no 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Brasília, 1941. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 20 abr. 2014.

[90] COLLI, Maciel. *Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos.* Curitiba: Juruá Editora, 2010. P. 160.

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

pela mensagem na rede de computadores[92]. 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.

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[93].

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)[94].

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[95].

---

[92] MALAQUIAS, Roberto Antônio Darós. *Crime Cibernético e Prova – A investigação criminal em busca da verdade*. Curitiba: Juruá Editora, 2012. p. 80.

[93] COLLI, Maciel. Cibercrimes. *Limites e perspectivas à investigação policial de crimes cibernéticos*. Curitiba: Juruá Editora, 2010. P. 167.

[94] Ibidem, p. 170.

[95] QUEIROZ, Claudemir; VARGAS, Raffael. *Investigação e perícia forense computacional. Certificações, Leis processuais e estudos de caso*. São Paulo: Brasfort, 2010. p. 10.

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[96].

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.

3.2 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[97].

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[98].

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[99].

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 em

---

[96] MALAQUIAS, Roberto Antônio Darós. *Crime Cibernético e Prova – A investigação criminal em busca da verdade*. Curitiba: Juruá Editora, 2012. p. 83.
[97] OLIVEIRA, Eugênio Pacelli. *Curso de Processo Penal*. Rio de Janeiro: Lúmen Júris, 2011. p. 327.
[98] TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. *Curso de Direito Processual Penal*. Salvador: Jus Podivm, 2012. p. 376.
[99] MALAQUIAS, op. cit., p. 65.

se apropriar de senhas e códigos de acesso alheios e utilizá-los para aplicar golpes financeiros ou invadir sistemas por meio dessa identidade[100].

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 qualificação, é pressuposto essencial para a instauração da instrução processual penal[101].

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[102].

Uma das características das condutas ilícitas praticadas na internet é o anonimato on-line, uma vez que o ambiente virtual em que estes crimes são praticados são caracterizados pela ausência de espaço físico. Os criminosos que acessam a rede mundial de computadores se utilizam de técnicas para ocultar sua verdadeira identidade e conduta, podendo, assim, assumir qualquer identidade que não a sua. Segundo Maciel Colli, "o anonimato on-line fornece uma liberdade inatingível no mundo real"[103].

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[104].

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

---

[100] MALAQUIAS, Roberto Antônio Darós. *Crime Cibernético e Prova – A investigação criminal em busca da verdade*. Curitiba: Juruá Editora, 2012. p. 66.
[101] Ibidem, p. 64.
[102] Ibidem, p. 64.
[103] COLLI, Maciel. *Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos.* Curitiba: Juruá Editora, 2010. p. 45.
[104] COSTA, Levi Roberto; PEIXOTO, Hélvio Pereira. *Um método para sistematização do processo investigatório de análise da informação digital Fomentando a cognição na atividade policial*. 2011. Disponível em: <http://www.icofcs.org/2010/ICoFCS2010-FULL.pdf#page=20>. Acesso em: 26 abr. 2014.

identificação virtual, o IP descreve todo o tráfego de rede e acessos feito pelo usuário em determinado período[105].

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[106].

Toda investigação criminal deve considerar as evidências deixadas pelo 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[107].

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[108].

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, serão

---

[105] PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Editora Saraiva, 2013, p. 308.
[106] COLLI, Maciel. *Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos.* Curitiba: Juruá Editora, 2010. p. 45.
[107] MALAQUIAS, Roberto Antônio Darós. *Crime Cibernético e Prova – A investigação criminal em busca da verdade*. Curitiba: Juruá Editora, 2012. p. 65.
[108] PINHEIRO, op. cit., p. 79.

analisados 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[109].

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[110].

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.

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[111].

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.

---

[109] DIAS, Vera Marques. *A problemática da investigação do cibercrime*. 2012. Disponível em: <http://datavenia.pt/ficheiros/pdf/datavenia01.pdf#page=63>. Acesso em: 26 abr. 2014.

[110] IOCCA, Érica Cristiane. *Crimes cibernéticos e a sociedade atual.* 2012. Disponível em: <http://www.judicare.com.br/index.php/judicare/article/view/50/158>. Acesso em: 26 abr. 2014.

[111] IOCCA, Érica Cristiane. *Crimes cibernéticos e a sociedade atual.* 2012. Disponível em: <http://www.judicare.com.br/index.php/judicare/article/view/50/158>. Acesso em: 26 abr. 2014.

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[112].

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[113].

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[114].

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[115] 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 ser

---

[112] PINHEIRO, Patrícia Peck. *Direito Digital.* São Paulo: Editora Saraiva, 2013, p. 93.
[113] Ibidem, p. 93.
[114] MILITÃO, Renato Lopes. *A propósito da prova digital no processo penal.* 2013. Disponível em: <http://www.oa.pt/upl/{53f46e96-536f-47bc-919d-525a494e9618}.pdf>. Acesso em: 26 abr. 2014.
[115] A teoria da imputação objetiva é a atribuição de um resultado juridicamente relevante ao indivíduo que agiu por intermédio de uma conduta geradora de risco não permitido, ocasionando ameaça ou lesão a um bem jurídico tutelado pela norma penal.

indiciado 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." [116]

3.3 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[117].

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 prática da conduta delituosa, bem como a probabilidade do acusado ser o autor do crime[118].

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"[119], 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[120].

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 averiguação

---

[116] COLLI, Maciel. *Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos.* Curitiba: Juruá Editora, 2010. p. 92.
[117] MOSSIM, Heráclito Antônio. *Compêndio de Processo Penal. Curso Completo*. São Paulo: Manole, 2010. p. 84.
[118] OLIVEIRA, Eugênio Pacelli. *Curso de Processo Penal.* Rio de Janeiro: Lumen Juris, 2011. p. 115.
[119] BRASIL. *Decreto-Lei no 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Brasília, 1941. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 20 abr. 2014
[120] MOSSIM, op. cit., p. 84.

feita 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[121].

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[122].

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[123].

São características dos atos de investigação a ausência de certeza, já que se referem a uma hipótese e, portanto, estão impregnados de possibilidade e probabilidade; natureza pré-processual, já que servem de instrumento à investigação preliminar; servem para formar a

[121] OLIVEIRA, Eugênio Pacelli. *Curso de Processo Penal*. Rio de Janeiro: Lumen Juris, 2011. p. 115.
[122] MOSSIM, Heráclito Antônio. *Compêndio de Processo Penal. Curso Completo.* São Paulo: Manole, 2010. p. 91.
[123] LIMA, Renato Brasileiro. *Manual de Processo Penal*. Niterói: Impetus, 2011. p. 116.

opini delicti do acusador; servem para adoção de medidas cautelares pessoais, reais e de caráter provisional[124].

Os elementos informativos, apesar de não estarem sujeitos ao contraditório e a ampla defesa, são de fundamental importância para a persecução criminal, pois além de serem utilizados para formar a convicção do titular da acusação pública ou particular no oferecimento da peça acusatória; podem auxiliar o juiz na decretação de medidas cautelares[125].

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[126].

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[127].

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"[128].

Em regra, os elementos angariados durante a fase pré-processual só poderão ser aceitos como válidos e utilizados como base para uma sentença condenatória quando forem

---

[124] COLLI, Maciel. *Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos*. Curitiba: Juruá Editora, 2010. p. 107.

[125] MOSSIM, Heráclito Antônio. *Compêndio de Processo Penal. Curso Completo*. São Paulo: Manole, 2010. p. 95.

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

[127] BRASIL. *Decreto-Lei no 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Brasília, 1941. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 20 abr. 2014.

[128] TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. *Curso de Direito Processual Penal*. Salvador: Jus Podivm, 2012. p. 113.

repetidos na fase processual, assegurando o contraditório e a ampla defesa. Somente as provas colhidas sob a garantia do contraditório e a ampla defesa poderão ser aceitas como válidas[129].

Os atos de investigação não poderão ser utilizados pelo magistrado como único fundamento para uma possível condenação. Para que os elementos colhidos durante a fase de investigação sejam aceitos como fundamento em uma sentença penal condenatória, é necessário que sejam repetidos, quando possível, na fase processual. Isto é, no curso do processo penal a acusação só poderá se valer dos elementos colhidos durante o inquérito policial, utilizando-os como prova, quando estes forem convertidos em elementos probatórios através da chamada repetição de provas[130].

Contudo, existem provas que por sua volatilidade ou natureza não são passíveis de repetição. Um exemplo de prova caracterizada pela volatilidade são aquelas que, em decorrência de sua natureza, devem ser realizadas no momento em que foram descobertas sob o risco de perecimento. Neste caso, há necessidade de utilização de um instrumento incidental que permita a coleta antecipada de provas[131].

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 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

---

[129] TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. *Curso de Direito Processual Penal.* Salvador: Jus Podivm, 2012. p. 114.

[130] COLLI, Maciel. *Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos*. Curitiba: Juruá Editora, 2010. p. 109.

[131] LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. São Paulo: Editora Atlas, 2011. p. 109.

antes do início do processo ou em momento processual diverso daquele legalmente previsto. Estas provas são produzidas perante a autoridade judicial, com a observância do contraditório[132].

Os crimes virtuais são caracterizados principalmente pela efemeridade. Diante da prática de um cibercrime, são os dados armazenados no computador, na grande maioria dos casos, que servirão como provas do delito praticado. Para a localização de tais dados, conforme já exposto, é necessária uma atividade pericial especializada. Contudo, em algumas situações aquele que praticou o delito, poderá excluir os dados de tal forma que a localização destes se torna impossível até mesmo para peritos especializados. Por exemplo, quando além de excluir o arquivo o sujeito se utiliza de um procedimento chamado *disk-wiping*[133].[134]

A comprovação dos crimes cibernéticos não é tarefa fácil. É necessária qualificação técnica específica dos profissionais responsáveis pela verificação dos vestígios deixados quando da prática de um crime virtual, nem sempre presentes nos locais em que os crimes se consumam. A transitoriedade dos registros magnéticos exige que a realização das provas ocorra dentro de um curto período de tempo, a fim de evitar que detalhes sobre a prática do crime sejam perdidos[135].

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[136].

---

[132] LIMA, Renato Brasileiro. *Manual de Processo Penal*. Niterói: Impetus, 2011. p. 118.

[133] O *disk-wiping* é um processo que permite a gravação de informações no mesmo espaço em que existia um dado que foi deletado, mas que permanece armazenado no disco rígido de um computador sem referência de localização.

[134] COLLI, Maciel. *Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos*. Curitiba: Juruá Editora, 2010. p. 113.

[135] LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. São Paulo: Editora Atlas, 2011. p. 15.

[136] GRECO, Rogério. *Invasão de dispositivo informático - art. 154-a do código penal.* 2013. Disponível em: <http://atualidadesdodireito.com.br/rogeriogreco/2013/01/08/invasao-de-dispositivo-informatico-art-154-a-do-codigo-penal>. Acesso em: 29 abr. 2014.

A dificuldade probatória que caracteriza os crimes virtuais decorre da própria dinâmica da informática, no que se refere à forma como os dados são processados, que impede a detecção de determinada atividade ou processamento após a sua realização. Ademais, é resultado também da facilidade de se fraudar informações por meio da manipulação de programas e dados[137].

O grande problema para a investigação criminal, quando se considera a efemeridade dos dados armazenados no disco rígido de um computador, seja uma imagem, arquivo ou vídeo, é a localização desse dado que pode ser primordial para a confirmação da materialidade e indícios de autoria do cibercrime praticado[138].

Maciel Colli afirma que o problema para investigação criminal surgirá quando os vestígios (arquivos, dados) deixados pela prática do crime forem deletados e o espaço por ele ocupado for novamente ocupado por outros dados, impossibilitando seu rastreamento pela perícia especializada mesmo se utilizando das ferramentas *foresincs*[139] disponíveis[140].

Considerando a efemeridade e volatilidade dos dados que servirão como prova diante da prática de um crime virtual que surge a necessidade da utilização da produção antecipada de provas. No entanto, tal instituto é uma medida excepcional e só deverá ser utilizada quando presentes os pressupostos da relevância e da impossibilidade de repetição em juízo. Ainda que os pressupostos sejam cumpridos, a eficácia dessa medida está condicionada "aos requisitos mínimos de jurisdicionalidade, do contraditório, da possibilidade de defesa e da fiel reprodução da fase processual" [141].

Tantos o peritos especializados como os policiais responsáveis pelo flagrante em um cibercrime devem ter cautela na coleta dos dados armazenados, além de observar o atendimento dos pressupostos e requisitos da produção antecipada de provas, permitindo assim que estas sejam aceitas na fase processual. Nas palavras de Maciel Colli "É essencial que a

---

[137] GRECO, Rogério. *Invasão de dispositivo informático - art. 154-a do código penal.* 2013. Disponível em: <http://atualidadesdodireito.com.br/rogeriogreco/2013/01/08/invasao-de-dispositivo-informatico-art-154-a-do-codigo-penal>. Acesso em: 29 abr. 2014.

[138] COLLI, Maciel. *Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos*. Curitiba: Juruá Editora, 2010. p. 112.

[139] Ferramentas de perícia forense utilizadas em computadores para a recuperação de dados, coleta e análise de evidências.

[140] COLLI, op. cit., p. 113.

[141] LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional.* São Paulo: Editora Atlas, 2011. p. 109.

instrução probatória em juízo, regida pelo contraditório e a ampla defesa, oportunize colher elementos convincentes e robustos a fundamentar um decreto condenatório" [142].

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[143].

Neste sentido, Nestor Távora e Rosmar Rodrigues afirmam que "é necessário que a nossa legislação de forma mais clara discipline a produção antecipada de provas, medida cautelar das mais relevantes e que encontra parca ressonância no art. 225 do CCP" [144]. Tal medida ainda exige uma previsão mais robusta na legislação brasileira.

[142] COLLI, Maciel. Cibercrimes. *Limites e perspectivas à investigação policial de crimes cibernéticos*. Curitiba: Juruá Editora, 2010. p. 114.
[143] TAVORA, Nestor. ALENCAR, Rosmar Rodrigues. *Curso de direito processual penal*. Salvador: Editora JusPodivm, 2012, p. 114.
[144] Ibidem, p. 114.

CONCLUSÃO

A presente monografia teve como principal objetivo analisar os crimes virtuais sob a ótica do Direito Brasileiro, tratando das peculiaridades decorrentes dessa nova modalidade de crime que influenciam e dificultam a investigação criminal. A recente tipificação de algumas condutas delitivas não é suficiente para solucionar as dificuldades encontradas na resolução de tais crimes.

A evolução tecnológica e, consequentemente, a popularização da internet, fez com que a sociedade se tornasse cada vez mais dependente de seus recursos na realização das atividades diárias. A internet, além de ser o principal meio de comunicação atual, passou a ser um novo instrumento para prática de delitos já tipificados, bem como permitiu o surgimento de condutas ilícitas cujos bens jurídicos atingidos são as informações, dados e sistemas de computador.

No Direito, a constituição da prova é uma ferramenta importante para se averiguar o que realmente ocorreu quando da prática do delito. Por meio das provas, a partes envolvidas deverão demonstrar os fatos, e não apenas alegá-los, a fim de convencer o magistrado de sua veracidade. O processo penal será o instrumento utilizado na reconstrução histórica dos fatos, a fim de proporcionar o conhecimento do magistrado dos fatos tal como ocorreram.

Quando se considera os crimes digitais e suas particularidades, algumas características podem dificultar o processo de investigação tais como a efemeridade e a volatilidade dos dados transmitidos e armazenados nos computadores, que são utilizados direta ou indiretamente no cometimento de um crime virtual. Uma solução para assegurar a manutenção da integridade de vestígios e provas, bem como adequar os organismos policiais à velocidade dos crimes cibernéticos seria a realização de uma investigação preliminar por intermédio de unidades especializadas nesse tipo de crime.

Em um processo investigativo, a admissão e a coleta de provas são elementos essenciais para se chegar à autoria de um delito. A utilização de mecanismos tecnológicos na prática dos crimes virtuais dificulta a extração de provas, sendo necessária a intervenção de

peritos especializados para se atestar a autenticidade de determinados documentos, bem como extrair a prova de um computador.

Outra dificuldade encontrada em razão da utilização de recursos tecnológicos para a prática de crimes é a identificação do autor do crime. A correta individualização do acusado, sua identificação e qualificação, é uma grande preocupação quando se trata de crimes digitais, uma vez que o próprio ambiente em que as condutas delitivas são praticadas, ambiente virtual caracterizado pela ausência de espaço físico, facilita o chamado anonimato on-line. Ainda que este anonimato seja relativo, já que existe certa facilidade na identificação do computador de origem, por peritos especializados, a grande dificuldade está em associar o proprietário do computador com o sujeito que cometeu o delito.

Uma solução para a identificação do criminoso virtual, já que a investigação por meio de peritos especializados chega à identificação de um computador e não do autor do delito, seria a utilização da biometria ou de qualquer outro meio que se utilize de características fisiológicas mensuráveis para identificar um usuário. Outro meio seria a responsabilização do acusado somente se houvesse uma prisão em flagrante com o equipamento ligado.

Em decorrência de suas características, efemeridade e volatilidade, a comprovação dos crimes virtuais é muito difícil. A dificuldade probatória e a facilidade no encobrimento de dados demanda que a realização das provas nesse tipo de crime ocorra em um curto período de tempo, de forma a evitar que alguns dados essenciais para a comprovação do delito sejam perdidos. Por esse motivo, a investigação dos crimes virtuais está intimamente ligada à necessidade da produção antecipada de provas, previsto no Código de Processo Penal como uma medida excepcional a ser utilizada somente em casos relevantes quando não for possível a repetição em juízo, sempre observando a garantia do contraditório e da ampla defesa.

Ao final do primeiro capítulo, concluiu-se que a criminalidade informática não foi somente responsável pelo aparecimento de novas condutas ilícitas praticadas com o auxílio de um 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.

Apesar da necessidade de discussão de novos paradigmas de forma a acompanhar as novas perspectivas de risco da sociedade da informação e da criação de

mecanismos de prevenção e repressão, uma vez que os crimes virtuais apresentam certas peculiaridades, não é necessária a criação de um direito específico, apenas a previsão dessas particularidades pela área do Direito. Além de questões relacionadas à tipificação das novas condutas, outras questões devem ser discutidas a fim de combater a criminalidade informática.

No segundo capítulo restou analisada a importância da prova como principal instrumento na busca da veracidade dos fatos de forma a convencer o magistrado quanto aos fatos alegados no decorrer do processo. As peculiaridades trazidas com a prática dos crimes virtuais tais como a velocidade e dinamismo com que estes crimes se perpetuam, estão intimamente vinculadas à investigação probatória. Ao se considerar a importância da prova no processo, bem como os seus elementos, conforme analisado no segundo capítulo, o capítulo três trouxe as questões específicas que relacionam a importância da prova com as particularidades propriamente relacionadas aos crimes digitais.

Do capítulo três, é possível concluir que ao se considerar os crimes virtuais e suas peculiaridades algumas questões relacionadas à investigação 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 mostram-se importantes no que tange às investigações dos crimes virtuais, portanto, diante da escassez de técnica e recursos humanos preparados surge a necessidade de especialização dos profissionais que atuarão neste tipo de investigação.

Conclui-se ainda, quanto à identificação de autoria que, apesar da facilidade de rastreamento do computador pela qual o crime foi praticado, há uma dificuldade em associar o computador ao sujeito ativo do crime. A utilização da biometria e a prisão em flagrante com o computador operante seriam soluções propostas a fim de solucionar tal problema. Ademais, considerando a efemeridade e volatilidade dos dados que servirão como prova do crime digital praticado, o instituto da produção antecipada de provas ganha importância, diante da possibilidade de perecimento das provas.

Assim, diante da análise do processo probatório no que diz respeito aos crimes virtuais, ficou evidenciado que o ordenamento jurídico brasileiro não necessita da regulamentação de novas leis, a inovação criminológica requer muito mais que um diploma legal regulamentando os delitos virtuais. É necessária a discussão das questões trazidas das

particularidades desse tipo de crime para se chegar a um procedimento investigatório mais apurado, com a criação de novas delegacias especializadas e no treinamento de profissionais no que se refere às investigações forenses, por exemplo.

REFERÊNCIAS

ALVIM, J. E. Carreira. *Teoria Geral do Processo revista, ampliada e atualizada*. Rio de Janeiro: Editora Forense, 2009.

ANTONIOLI, Leonardo. *Estatísticas, dados e projeções atuais sobre a internet no Brasil.* 2014. Disponível em: <http://tobeguarany.com/internet_no_brasil.php>. Acesso em: 05 mar. 2014.

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: 20 de abr. 2014.

BRASIL. *Decreto-Lei no 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Brasília, 1941. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 20 abr. 2014.

CAPEZ, Fernando. *Curso de Processo Penal*. São Paulo: Saraiva, 2011.

CERT.br. *Estatísticas dos incidentes reportados ao CERT.br.* Disponível em: <http://www.cert.br/stats/incidentes/>,acessado em 08 de março de 2014

CINTRA, Antônio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. *Teoria Geral do Processo*. São Paulo: Malheiros Editores, 2009.

COLLI, Maciel. *Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos.* Curitiba: Juruá Editora, 2010.

COSTA, Levi Roberto; PEIXOTO, Hélvio Pereira. *Um método para sistematização do processo investigatório de análise da informação digital Fomentando a cognição na atividade policial*. 2011. Disponível em: <http://www.icofcs.org/2010/ICoFCS2010-FULL.pdf#page=20>. Acesso em: 26 abr. 2014.

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

DIAS, Vera Marques. *A problemática da investigação do cibercrime*. 2012. Disponível em: <http://datavenia.pt/ficheiros/pdf/datavenia01.pdf#page=63>. Acesso em: 26 abr. 2014.

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

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

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

GRECO, Rogério. *Invasão de dispositivo informático - art. 154-a do código penal.* 2013. Disponível em: <http://atualidadesdodireito.com.br/rogeriogreco/2013/01/08/invasao-de-dispositivo-informatico-art-154-a-do-codigo-penal>. Acesso em: 29 abr. 2014.

IOCCA, Érica Cristiane. *Crimes cibernéticos e a sociedade atual.* 2012. Disponível em: <http://www.judicare.com.br/index.php/judicare/article/view/50/158>. Acesso em: 26 abr. 2014.

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

LÉVY, Pierre. *O que é o virtual?.* São Paulo: Editora 34, 2011.

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

LIMA, Renato Brasileiro. *Manual de Processo Penal*. Niteroi: Impetus, 2011.

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

LOPES JR. Aury. *Direito Processual Penal*. São Paulo: Saraiva, 2014.

MAGALHÃES GOMES FILHO, Antônio. *Direito à prova no processo penal*. São Paulo: RT, 1997.

MALAQUIAS, Roberto Antônio Darós. *Crime Cibernético e Prova – A investigação criminal em busca da verdade.* Curitiba: Juruá Editora, 2012.

MILITÃO, Renato Lopes. *A propósito da prova digital no processo penal.* 2013. Disponível em: <http://www.oa.pt/upl/{53f46e96-536f-47bc-919d-525a494e9618}.pdf>. Acesso em: 26 abr. 2014.

MOSSIM, Heráclito Antônio. *Compêndio de Processo Penal*. São Paulo: Manole, 2010.

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

OLIVEIRA, Eugênio Pacelli de. *Curso de processo penal*. Rio de Janeiro: Lumen Juris, 2008.

PEREIRA, Evandro della Vecchia. *Investigação Digital: conceitos, ferramentas e estudos de caso.* 2010. Disponível em: <http://www.infobrasil.inf.br/userfiles/26-05-S5-2-68766-Investigacao Digital.pdf>. Acesso em: 20 abr. 2014.

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: 23 mar. 2014.

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

QUEIROZ, Claudemir; VARGAS, Raffael. *Investigação e perícia forense computacional. Certificações, Leis processuais e estudos de caso*. São Paulo: Brasfort, 2010.

RANGEL, Paulo. *Direito Processual Penal*. Rio de Janeiro: Lumen Juris, 2003.

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: 20 abr. 2014.

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

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

TOURINHO FILHO, Fernando da Costa. *Processo penal.* São Paulo: RT, 2003.

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

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