UNIVERSIDADE FUMEC
FACULDADE DE CIÊNCIAS HUMANAS, SOCIAIS E DA SAÚDE
Programa de Pós-Graduação *stricto sensu* em Direito

MATHEUS DE ARAÚJO ALVES

CRIMES DIGITAIS:
ANÁLISE DA CRIMINALIDADE DIGITAL SOB A PERSPECTIVA DO DIREITO PROCESSUAL PENAL E DO INSTITUTO DA PROVA

Professor Orientador Doutor Sérgio Henriques Zandona Freitas

Belo Horizonte
2018

MATHEUS DE ARAÚJO ALVES

CRIMES DIGITAIS:
ANÁLISE DA CRIMINALIDADE DIGITAL SOB A PERSPECTIVA DO DIREITO PROCESSUAL PENAL E DO INSTITUTO DA PROVA

Dissertação apresentada ao Programa de Mestrado Acadêmico em Direito (*stricto sensu*) da Faculdade de Ciências Humanas, Sociais e da Saúde da Universidade FUMEC, como requisito parcial para a obtenção do título de Mestre em Direito.

Área de concentração: Instituições sociais, direito e democracia.

Linha de pesquisa: Esfera pública, legitimidade e controle.

Orientador: Professor Doutor Sérgio Henriques Zandona Freitas.

Belo Horizonte

2018

FICHA CATALOGRÁFICA

UNIVERSIDADE FUMEC

FACULDADE DE CIÊNCIAS HUMANAS, SOCIAIS E DA SAÚDE

Programa de Pós-Graduação *stricto sensu* em Direito

MATHEUS DE ARAÚJO ALVES

CRIMES DIGITAIS: ANÁLISE DA CRIMINALIDADE DIGITAL SOB A PERSPECTIVA DO DIREITO PROCESSUAL PENAL E DO INSTITUTO DA PROVA

Dissertação apresentada ao Programa de Mestrado Acadêmico em Direito (*stricto sensu*) da Faculdade de Ciências Humanas, Sociais e da Saúde da Universidade FUMEC, como requisito parcial para a obtenção do título de Mestre em Direito.

Orientador: Professor Doutor Sérgio Henriques Zandona Freitas (FUMEC)

Professor Doutor André Cordeiro Leal (FUMEC)

Professora Doutora Joana Rita Sousa Covelo Abreu (UMinho)

Professor Doutor Márcio Eduardo Senra Nogueira Pedrosa Morais (UIT)

Professor Doutor Vinícius Diniz Monteiro de Barros (PUC Minas)

Belo Horizonte, 17 de dezembro de 2018.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por proporcionar a realização de mais esse sonho, sendo fonte de inspiração e conforto nas dificuldades e de gratidão em todas as vitórias ao decorrer desta caminhada.

Aos meus pais, Marcus e Lúcia, pelo incentivo e apoio incondicional, sem medir esforços, durante toda minha vida. Esse momento é nosso e só está sendo possível graças ao amor e a educação que vocês me proporcionam.

Aos meus irmãos e familiares pela torcida de sempre, principalmente ao meu avô Jairo, que me motiva a ser sempre melhor, como pessoa e como profissional.

Agradeço também aos meus amigos, sempre presentes inclusive em meus momentos de ausência. A todos aqueles que conheci durante o curso do mestrado e que, mais do que colegas, se tornaram grandes amigos.

A Anna pelo amor, carinho e companheirismo de sempre, em todos os momentos. Minha eterna gratidão!

Ao professor Dr. Sérgio Henriques Zandona Freitas pelo exemplo de pessoa e pelas orientações não só acadêmicas, mas também de vida. Obrigado pela oportunidade de ter sido seu orientando e, principalmente, pela amizade e companheirismo construídos nesses dois anos.

Ao professor Dr. André Cordeiro Leal, pelos ensinamentos e orientações que, com imenso cuidado e gentileza, contribuíram de forma significativa para o conteúdo deste trabalho.

Aos professores Dra. Joana Rita Sousa Covelo Abreu, Dr. Márcio Eduardo Senra Nogueira Pedrosa Morais e Dr. Vinícius Diniz Monteiro de Barros, pela gentileza em aceitar compor a banca examinadora.

A todos que contribuíram, cada um à sua maneira, para a conclusão de mais essa etapa de vida. Obrigado de coração!

"Jamais considere seus estudos como uma obrigação, mas como uma oportunidade invejável para aprender a conhecer a influência libertadora da beleza do reino do espírito, para seu próprio prazer pessoal e para proveito da comunidade à qual seu futuro trabalho pertencer".

Albert Einstein

RESUMO

O avanço da globalização e das transformações da Era da Informação trouxeram mudanças significativas para a vida em sociedade. Apesar de encurtar distâncias de comunicação e otimizar a vida humana, também exerceu forte influência no campo dos delitos penais, mudando não só a forma de cometimento de crimes já previstos em leis, mas também inaugurando novas figuras delitivas que violam novos bens jurídicos. Os riscos e adversidades no chamado mundo real também se repetem no meio digital, uma vez que a internet é uma extensão da sociedade de risco atual. Com a possibilidade de acesso anônimo, o usuário é beneficiado com a sensação de privacidade, mas, por outro lado, tem-se a ideia de oportunidade para o cometimento dos crimes chamados digitais. Esta modalidade delitiva possui particularidades e divisões entre si, podendo ser: crimes digitais próprios e crimes digitais impróprios. Outra característica fundamental destes ilícitos é a volatilidade da sua materialidade, já que os dados e informações no ciberespaço não se encontram, necessariamente, em apenas um lugar, podendo ser facilmente modificados ou suprimidos. Entre as problemáticas dos crimes digitais, também está o desafio de se determinar o momento e o local da sua ocorrência, fato de importante implicação, uma vez que, de forma geral, o período de tempo entre a ação e o resultado é relativamente grande. Isso implica em diversas discussões a respeito de jurisdição e competência, em busca de teorias que melhor pacifiquem a questão e possam contribuir para uma efetiva persecução penal. Apesar da internet parecer uma rede imaterial, seu funcionamento depende da existência de uma infraestrutura real que, para ser acessada, precisa da atuação de provedores que, a partir de então, passam a deter as informações referentes aos usuários e seus comportamentos na rede. Com a entrada em vigor do Marco Civil da Internet, passa-se, então, a regular a atuação dessas empresas para que os dados pessoais e a privacidade dos usuários tenham a devida proteção legal. Os crimes praticados no ciberespaço, muitas vezes, não deixam vestígios e, com a obscuridade da internet, os autores desses ilícitos ficam impunes, devido à fragilidade do material probatório. Os elementos de prova, são voláteis e frágeis e, com isso, caso não sejam prontamente preservados, podem ser rapidamente danificados ou suprimidos, impedindo a devida investigação. O instituto da prova é dotado de uma grande complexidade teórica que comina em diversas implicações dentro do devido processo legal que, no ordenamento jurídico brasileiro traz diversas garantias e regulamentações para seu uso. O significativo crescimento dos crimes digitais é internacionalmente considerado como um grande problema da sociedade de risco e, com isso, necessita de um estudo aprofundado e de soluções globais para que sejam combatidos, fazendo com que as providências tomadas por países em seus respectivos territórios, ou por diferentes nações, sejam harmonizadas entre si, devido ao caráter transnacional do meio digital. Não se trata, dessa forma, de uma tarefa exclusiva do ramo do Direito, mas de um esforço conjunto em nível transnacional e transdisciplinar. Para isso, utilizar-se-á pesquisa bibliográfica por meio do método dedutivo.

Palavras-chave: Crimes Digitais. Instituto da Prova. Direito Penal. Direito Processual Penal. Sociedade de Risco.

ABSTRACT

The globalization breakthrough and the transformations in the Age of Information have brought significant changes to life in society. Despite shortening communication distances and optimizing human life, it has also had a very strong influence in the field of criminal offenses, changing not only the way of committing crimes that are already established by laws, but also unveiling new punishable figures that violate new legal assets. The risks and adversities in the so-called real world are also repeated in the digital environment, given that the internet is an extension of the current Risk Society. With the possibility of anonymous access, the user benefits from the sense of privacy, but, on the other hand, there's the idea of an opportunity to commit the so-called digital crimes. This punishable modality has peculiarities and divisions within itself, which may be: suitable or not suitable digital crimes. Another fundamental trait of these illegal actions is the volatility of their materiality, since all the data and information in the cyberspace are not, necessarily, located in one place, and may be easily modified or removed. Among the set of problems revolving around digital crimes, there is also the challenge to determine the time and place of its occurrence, an important fact, since, in general, the time period between action and result is fairly long. This implies in several discussions about jurisdiction and expertise, searching for theories that best pacify the question and may contribute to an effective criminal prosecution. Although the internet may seem like an immaterial network, its operation depends on the existence of a real infrastructure which, to be accessed, needs the action of providers which, from then on, take possession of information about users and their behaviors in the network. With the establishment of the Brazilian Civil Rights Framework for the internet, it is then, a matter of regulating the practice of these companies, so that the personal data and the privacy of users may have proper legal protection. Crimes committed in cyberspace, most of the time, leave no traces and, with the obscurity of the internet, the offenders go unpunished, due to the fragility of the evidences. The proof in the digital environment, of top of being volatile, is also very fragile and, with that, if not promptly preserved, can be quickly damaged or erased, preventing any proper investigation. The institute of proof is endowed with great theoretical complexity, which enforces several implications within the proper legal process that, in the Brazilian legal system, brings several guarantees and regulations for its use. The rapid growth of digital crimes is internationally considered a major problem of the Risk Society and, therefore, requires in-depth study and global solutions in order to be fought against, so that measures taken by countries in their respective territories, or by different nations, are combined among themselves, due to the transnational nature of the digital environment. It is not, therefore, an exclusive task of the law, but joined efforts between transnational and transdisciplinary levels. For this, bibliographic research will be used through the deductive method.

Keywords: Digital Crimes. Institute of Proof. Criminal Law. Criminal Procedural Law. Risk Society.

SUMÁRIO

1 INTRODUÇÃO

Os avanços tecnológicos experimentados pelo ser humano nas últimas décadas trouxeram mudanças significativas para a vida em sociedade, encurtando distâncias entre as comunicações e acelerando transformações sociais na era da informação. Entretanto, não foram só benefícios que surgiram com a revolução informática, esta também influenciou diretamente no campo dos delitos penais, mudando a forma de cometimento de crimes já previstos no ordenamento jurídico e inaugurando novas modalidades delitivas, além de novos bens jurídicos passíveis de proteção.

A possibilidade de anonimato no acesso, além de garantir uma maior privacidade para o usuário, pode também contribuir para aumento da possibilidade de criminosos agirem de forma desapercebida. Surgem, portanto, os crimes digitais que, diferentemente dos crimes cometidos no mundo material, possuem características próprias que os tornam ainda mais difíceis de serem investigados e coibidos. Enquanto no mundo real, tanto o autor quanto a vítima estão, necessariamente, próximos entre si quando ocorre o delito, nos crimes digitais pode existir um distanciamento espacial significativo, que dificulta a persecução penal e cria barreiras burocráticas muitas vezes intransponíveis que podem impedir qualquer condenação.

Assim, o presente trabalho pretende fazer um aprofundamento teórico-jurídico sobre as particularidades dos crimes digitais, a origem dessa modalidade delitiva, o contexto em que ela se inclui na sociedade de risco, as divergências doutrinárias a respeito de suas classificações e nomenclaturas e um exame de alguns de seus principais ilícitos.

Além do aprofundamento nas características inerentes à criminalidade digital, almeja-se fazer uma análise desses delitos sob a óptica dos institutos processuais penais vigentes, as discussões doutrinárias e jurisprudenciais em relação à territorialidade, jurisdição, competência e, principalmente, em relação ao instituto da prova.

Para isso, realizar-se-á pesquisa a partir do método hipotético dedutivo, com base em fontes doutrinárias, legislações e jurisprudências, tendo como marco teórico as obras destinadas aos crimes digitais de Spencer Toth Sydow e Marcelo Xavier de Freitas, e a Teoria Geral do Processo de Rosemiro Pereira Leal.

Dividindo-se a abordagem deste trabalho em capítulos, o de número 2 dedica-se a contextualizar o surgimento e o funcionamento da internet, além da relação entre os riscos presentes no meio digital e como eles podem influenciar na vida em sociedade.

O capítulo 3 é destinado a conceituar os crimes digitais, apresentar suas principais características, nomenclaturas e em que os diferem dos crimes já presentes no ordenamento

jurídico brasileiro. Além disso, propõe-se a debater sobre quais os bens jurídicos que são violados através desta modalidade delitiva, bem como as suas classificações, trazendo a discussão da falta de harmonização dos sistemas jurídicos internacionais que não possuem uma solução pacífica para as barreiras ocasionadas pela transnacionalidade, problema este que é a principal dificuldade enfrentada na investigação e punição destes delitos, contribuindo diretamente para o aumento da criminalidade digital.

O capítulo 4 faz uma análise sobre as particularidades das provas no âmbito dos crimes digitais. Uma vez que os dados e informações no meio digital não se encontram, necessariamente, em apenas um lugar, estas podem ser facilmente modificadas ou suprimidas, dificultando ainda mais a persecução penal. Traz-se também, neste capítulo, uma análise sobre os aspectos técnicos específicos do material probatório digital e de como o exame de corpo de delito, baseando-se nos preceitos processuais penais, é o meio mais adequado para se demonstrar sua prática. Ademais, faz-se um aprofundamento bibliográfico a respeito do instituto da prova, sua função dentro do processo penal, a quem se destina, as possíveis limitações em sua aplicação e uma análise entre interesse público e privado, em que não há a supremacia e prevalência prévia de um sobre o outro, mas uma relação de complementariedade e interdependência.

O capítulo de número 5 discorre sobre o Marco Civil da Internet que entrou em vigor no ano de 2014 e, apesar de deixar algumas lacunas, trouxe importantes implicações no estudo do direito processual penal informático e nos crimes digitais, pois esclareceu termos técnicos ainda controvertidos na doutrina e na legislação, além de regular o funcionamento das empresas provedoras de internet, com o objetivo de uma maior proteção dos dados e da privacidade dos usuários no território nacional.

O capítulo 6 traz o entendimento de que, apesar da internet ainda ser considerada por muitos como um território livre e impune, a realidade se mostra diferente. Diariamente o judiciário tem buscado coibir as atividades ilícitas praticadas no meio digital, ainda que de forma pontual, através da aplicação das leis penais e de legislações específicas. Ademais, traz a necessidade de se ter disposições claras das condutas no ordenamento jurídico para que a aplicação da lei penal possa ser feita de forma harmônica e em respeito aos princípios constitucionais.

Na conclusão, além de uma síntese dos capítulos acima descritos, destaca-se que, para um problema global como o dos crimes digitais é necessária uma solução também global, fazendo com que as providências tomadas por países em seus respectivos territórios, ou por diferentes nações em âmbito global, sejam harmonizadas entre si. Não se trata, portanto, de

uma tarefa exclusiva do Direito e nem apenas a necessidade de se tipificar no ordenamento jurídico determinadas condutas ilícitas, mas de um trabalho colaborativo em nível internacional e transdisciplinar para que esta modalidade delitiva seja devidamente coibida.

2 A ERA DA INFORMAÇÃO E A INTERNET

Com o crescente avanço do processo de globalização, a sociedade vem passando por uma nova espécie de revolução chamada por Guilherme de Souza Nucci de "revolução informática" ou "terceira revolução industrial" (NUCCI, 2017, p. 37). Baseada principalmente na informação, através da união entre o conhecimento científico e a produção industrial, vem possibilitando profundas evoluções no campo tecnológico de forma a encurtar distâncias e acelerar transformações sociais no período em que Marcelo Crespo chama de "era da informação" (CRESPO, 2011, p. 25).

Apesar desses vários avanços tecnológicos e descobertas científicas, a revolução informática também exerceu influência no cometimento de infrações penais, mudando não só o *modus operandi* de crimes já previstos no ordenamento jurídico pátrio, mas também inaugurando novas figuras delitivas, que serão discutidas no presente trabalho.

Falar de "era da informação" – também chamada pelo autor de "era tecnológica" ou "era digital" – é referir-se ao período pós-industrial que, apesar de suas bases se fundarem na década de 1970 (CRESPO, 2011, p. 25), com a invenção do microprocessador, das redes de computadores e do computador pessoal.

2.1 A FORMAÇÃO DA SOCIEDADE DA INFORMAÇÃO

A formação da Sociedade da Informação não se deu de repente, foi proveniente de um longo processo evolutivo iniciado na própria revolução industrial que, na Inglaterra de meados do século XVIII, consistiu em um conjunto de mudanças tecnológicas e estruturais com intenso reflexo na cadeia produtiva, seja em nível econômico ou social, alterando quase todos os aspectos da vida cotidiana da época ao espalhar-se pelo mundo a partir do século XX (MONTEIRO, 2010, p. 21).

Assim como na Revolução Industrial em que a classe burguesa procurava transformar a sociedade em seu benefício, Renato Leite Monteiro afirma que, desde os primórdios da civilização, o ser humano tem buscado aplicar suas capacidades mentais com o intuito de transformar e adaptar o meio em que vive, adequando-o sempre às suas necessidades (MONTEIRO, 2010, p. 21). E uma das principais necessidades humanas é a de se comunicar. Diversas evoluções aconteceram em diferentes campos do conhecimento, porém é necessário ressaltar que, nos ramos da informática, das telecomunicações e transmissão de dados, a velocidade desses avanços é significativamente maior.

Como supracitado, segundo os ensinamentos de José de Oliveira Ascensão, o termo Era/Sociedade da Informação teve suas primeiras referências na década de 1970 nos Estados Unidos e no Japão, onde se travavam discussões sobre como classificar a sociedade pós-industrial em que a informação desempenhava o papel principal da vida econômica, política e social das pessoas, das empresas e das nações da época (ASCENSÃO, 2002, p. 69). Esse novo conceito de sociedade surge da influência das tecnologias da comunicação e da informação na sociedade, acelerando os processos produtivos e de consumo, o que gera um intenso desenvolvimento econômico e a propagação do conhecimento em escalas até então inimagináveis.

Com o advento das primeiras unidades de processamento eletrônico de dados e a velocidade em que as informações eram transmitidas e tratadas, ao invés de papéis e livros de registro, os dados passaram a ser armazenados em forma de *bits (binary digits)*, que são unidades digitais binárias interpretadas pelos computadores. A partir daí, aparece o fenômeno da digitalização, no qual há o predomínio da difusão de dados agora de forma digital. Esse fenômeno foi fortemente influenciado pelo surgimento dos Computadores Pessoais (PCs) na segunda metade do século XX, o que ampliou o acesso, pelo público, às inovações digitais, possibilitando qualquer indivíduo de usufruir de tais avanços (MONTEIRO, 2010, p. 21). Renato Leite Monteiro salienta que, a necessidade de se disseminar essas informações e conhecimentos, acabou por pavimentar os caminhos para o surgimento de uma rede que ligasse, em escala global, os computadores entre si (MONTEIRO, 2010, p. 21), possibilitando a troca de dados entre eles chamada de internet.

2.2 O NASCIMENTO DA INTERNET

O que hoje se conhece como internet teve origem nos Estados Unidos no final da década de 1960 com o nome de ARPANET. Idealizada pela ARPA (*Advanced Research Projects Agency*), ligada ao Departamento de Defesa norte-americano, foi criada no auge da Guerra Fria sob o forte temor de um bombardeio nuclear pela União Soviética (PINHEIRO, 2006, p. 13). Com seu uso, até então, uma exclusividade das Forças Armadas, esta rede promissora tinha como propósito espalhar as pesquisas e os dados valiosos do governo dos Estados Unidos por diversos lugares do país – três computadores na Califórnia, nas Universidades de Stanford, Berkeley e na UCLA e um na Universidade de Utah –, ao invés de centralizá-los em apenas um servidor que pudesse ser danificado (PINHEIRO, 2006, p. 13-14). Nesse sentido, destaca o professor Spencer Toth Sydow:

> Assim, a ideia foi a de difundir a informação sem que houvesse somente um centro estratégico frágil, que, atacado, levaria a um caos desenvolvimentista, permitindo-se que a informação trafegasse mesmo que tivesse havido a perda de um ou alguns núcleos tecnológicos. Pode-se dizer, portanto, que a importância inicial da rede informática foi estratégica (SYDOW, 2015, p. 31).

Seguindo esse raciocínio, tinha-se, portanto, um sistema interligado em rede que continuaria funcionando mesmo se parte dele saísse do ar. Dessa forma, com a rede descentralizada, são utilizadas rotas alternativas para que as informações sejam devidamente entregues. Assim, caso seja danificado ou destruído um computador para qual determinado pacote de dados fora enviado, ele seria redirecionado para outra rota, unindo-se posteriormente aos demais pacotes para refazer, de forma integral, a mensagem original.

De acordo com Gimenes, para que essa rede funcionasse de forma eficaz, fora necessário criar um protocolo para que todos os computadores que estivessem a ela conectados pudessem entrar em sintonia, de forma que as mensagens não se perdessem pelo caminho. Dessa forma, foram criados programas para colocar este dispositivo em prática, como o NCP (*Network Control Protocol*), que foi o pioneiro da lista, inaugurando o projeto (GIMENES, 2013, p. 07).

Após diversas pesquisas e avanços tecnológicos na área de telefonia, que estava em expansão nos Estados Unidos, a ARPANET mudou do NCP para um novo protocolo, chamado de TCP/IP (*Transfer Control Protocol/Internet Protocol*), obtendo uma grande aceitação global por ser compatível com uma grande variedade de plataformas diferentes de computadores (GIMENES, 2013, p. 07).

Em meados dos anos 1980, a ARPANET passou a ser gerenciada pela NSF (*Nacional Science Foundation),* órgão do governo norte-americano. Com isso, visando aumentar o meio para que pudesse passar mais informações em um período menor de tempo, criaram-se cinco centros de supercomputação nos Estados Unidos, como evidencia Blum (2001, p. 23). Já em 1990, a ARPANET foi divida em MILNET (*Military Network*), dedicada exclusivamente à troca de dados militares, e a NSFNET (*National Science Foundation Network*), para uso acadêmico (MAZONI, 2009, p. 10).

Foi só em 1991 que a exploração comercial do serviço começou, após a internet ter sido disponibilizada para as pessoas comuns através das inovações criadas por Tim Bernes Lee. Cientista inglês, Tim trabalhava na *European Organization for Nuclear Research* (Organização Europeia para Pesquisa Nuclear) na Suíça, onde desenvolveu "um complexo sistema de documentos interligados que misturava texto, imagem, som e mídia e se inter-relacionava através da internet, por meio de ligações (*links*) que poderiam ser acionadas" (SYDOW, 2015,

p. 31), fazendo com que o usuário conectado à rede navegasse por diversos ambientes e plataformas com uma interface gráfica dinâmica e visualmente mais atrativa.

Essa tecnologia conquistou usuários por todo o mundo e recebeu o nome de *World Wide Web* (Rede Mundial de Computadores), também conhecida pelas letras "WWW". A partir daí a internet passou a ser utilizada nos mais variados segmentos sociais. No ramo da educação, os alunos passaram a fazer pesquisas escolares pelos computadores ao invés de livros enciclopédias; salas de bate-papo encurtaram distâncias entre pessoas de todo o planeta e as empresas descobriram ali uma forma de alavancar seus lucros através das publicidades e vendas online, transformando o ambiente virtual em um novo ramo de negócios.

Segundo Yvonne Jewkes, socióloga e professora de criminologia na Universidade de Leicester, a popularização dessa nova ferramenta foi tão vertiginosa que fez com que, em apenas três anos, a internet atingisse a marca de 50 milhões de usuários, número que somente foi atingido pelo radio após 37 anos e pela televisão, em 15 anos (JEWKES, 2002, p. 33).

No Brasil, a internet se desenvolveu com a criação da Rede Nacional de Pesquisa (RNP) em 1989, uma iniciativa do Ministério da Ciência e Tecnologia com o propósito de criar uma infraestrutura de serviços de internet que abrangesse todo o território nacional (MONTEIRO, 2010, p. 18). Nas palavras de Monteiro, "até 1995, essa rede se limitava a áreas de educação e pesquisa, data em que deixou de se restringir ao meio acadêmico para se estender aos demais setores da sociedade, consolidando, assim, a internet comercial no país" (MONTEIRO, 2010, p. 18).

No início do século XXI, a internet alcança seu auge como sendo o principal meio de acesso a informações e de comunicação entre as pessoas. De acordo com a pesquisa de Simon Kemp, mais da metade da população mundial conta com acesso à internet no ano de 2018, sendo mais de quatro bilhões de pessoas conectadas à rede, enquanto a população global é estimada em 7,6 bilhões de seres humanos (KEMP, 2018). Seu uso tornou-se algo inerente e imprescindível na vida das pessoas e no funcionamento da sociedade. "Toda essa evolução fez com que as relações comerciais, as administrações públicas e a sociedade em geral passassem a depender muito da eficiência e segurança da chamada tecnologia da informação" (CRESPO, 2011, p. 31).

O expressivo avanço da internet e das demais tecnologias de informação tornaram o mundo um lugar mais conectado e também mais dependente da informática, residindo aí sua maior vulnerabilidade. O uso indevido dos computadores tornou-se uma verdadeira ameaça global, sendo de suma importância a segurança dos sistemas digitais e das informações privadas de seus usuários. A sociedade da informação também é a sociedade de risco, como bem alertava

Ulrich Beck, ao se referir ao período atual em que a sociedade não mais consegue estipular os riscos do seu próprio desenvolvimento. Riscos esses que não atingem apenas bens jurídicos individuais, mas também a esfera coletiva (BECK, 2010, p. 25)

2.3 A SOCIEDADE DE RISCO INFORMÁTICA

O termo "informática" é comumente usado para descrever o emprego do tratamento automático das informações. Com isso, é possível entender a necessidade de uma linguagem padrão para que o uso, a transformação e a transmissão de dados e informações aconteçam de forma integral e universal. Dessa forma, com o passar dos anos e com a popularização da internet, cada vez mais aparelhos tecnológicos passaram a interagir e trocar informações entre si, assim como seus usuários.

Até o presente momento, não existe um "código de condutas ou comportamentos" transnacional na rede informática. No seu início, ainda em fase embrionária, apostava-se que as redes e seus usuários seriam capazes de se autorregular, o que hoje é mais do provado ser um mero equívoco. As informações e os dados transformados em *bits* passaram a ter um alto valor econômico e social, dada à essencialidade da internet no cotidiano do ser humano. Com isso, a rede passa a ser, cada vez mais, alvo de uma cultura delinquente em que não se consegue medir a dimensão do perigo em que se está exposto. A sociedade conectada está sob um constante risco.

O termo sociedade de risco foi desenvolvido inicialmente por Ulrich Beck que defende que, "para uma sociedade evoluir e haver continuidade na produção de riqueza são necessários o avanço tecnológico e a exploração de novas áreas. A crescente industrialização traz consigo, então, escolhas, e estas são relacionadas as consequências e, logo, a sacrifícios" (apud SYDOW, 2015, p. 38). A identificação desses custos sociais e de seus sacrifícios é feito pela economia, com o aval da sociedade que é consciente dos riscos, mas que busca constantemente mitigar os custos consequentes da modernidade.

Como visto, quando Beck fala de "riscos", este quer dizer que, ao contrário da sociedade industrial clássica, na modernidade a ciência não consegue mais prever as consequências de sua evolução, já que os danos não são limitáveis a esfera local e tem, agora, uma abrangência global, provindo até mesmo de uma simples decisão humana (BECK, 2010, p. 25).

É justamente no âmbito desses novos e constantes riscos que se deve considerar a evolução tecnológica da informática e dos meios de comunicação. A criminalidade informática é uma forma de ilícito complexo em que não se consegue mensurar as dimensões de seu dano,

além das dificuldades de investigação, obtenção de prova e identificação dos infratores, como será discutido posteriormente neste trabalho.

2.3.1 Segurança do meio informático

Apesar de parte dos usuários não terem sempre a capacidade de perceber que a internet é uma mera extensão da sociedade, uma parcela dos mesmos riscos existentes no "mundo real" também incide no "mundo digital". As preocupações com a segurança de casas, empresas e repartições públicas são muito mais presentes na sociedade material do que no ramo informático onde, muitas vezes, a proteção de redes e computadores é negligenciada por parte de seus responsáveis que, mesmo não estando seguros, têm uma falsa sensação de estarem protegidos por um simples antivírus em seu dispositivo.

Neste sentido, entende Sydow que:

> O escudo que a tela do computador representa não raro traz ao usuário a sensação de segurança, dando aparência de inatingibilidade. Não estar exposto em suas fragilidades faz com que prevaleça a ideia de segurança e com que o ser humano tenda a agir com menos limites e mais ousadia em tal situação. A economia justifica tal conduta com a figura da moral hazard, ou risco moral (SYDOW, 2015, p. 41).

Com isso, é possível entender que a sensação de tranquilidade perante determinada situação faz com que o ser humano tenha comportamentos mais descuidados ou até arriscados, devido ao excesso de confiança no momento. Sentindo-se seguro, é comum ao indivíduo agir de forma menos cautelosa e isso também ocorre no ambiente virtual. Quando o usuário acessa *sites* sem se atentar aos requisitos de proteção ou quando acessa e-mails desconhecidos sem a devida atenção, o mesmo está se colocando em uma situação de risco que pode gerar-lhe intensos prejuízos.

Da mesma forma que a tecnologia trouxe aos usuários ampla liberdade de acesso à rede mundial de computadores, por outro lado lhes retirou a possibilidade de identificar plenamente as pessoas com quais se relacionam. Como bem destaca Sydow, é possível observar o cuidado que o cidadão comum toma para não conversar com estranhos na vida material; porém, em regra, esta cautela não é levada à vida virtual, aceitando-se a comunicação desconhecida com certa simpatia e surpresa (SYDOW, 2015, p. 46). A anonimidade do acesso possui uma natureza dúplice, dá à vítima a sensação de privacidade, mas, ao mesmo tempo, facilita a atividade criminosa.

De acordo com Emanuel Alberto Sperandio Garcia Gimenes, "o problema da segurança informática pode ser decomposto em vários aspectos distintos, sendo mais relevantes os seguintes: autenticação, confidencialidade e integridade" (GIMENES, 2013, p. 05).

Sendo assim, a autenticação se refere ao processo pelo qual é validada a entidade de um usuário, já a confidencialidade reúne as vertentes de segurança que limitam o acesso à informação apenas aos usuários previamente autorizados, sejam humanos ou virtuais. Por sua vez, a integridade permite garantir que a informação a ser processada é autêntica, ou seja, que não é corrompida. Com isso, essa diferenciação e essas medidas objetivam impedir ou ao menos diminuir uma série de crimes e atos ilícitos que podem ser perpetrados pelos meios informáticos.

Com isso, é possível observar que a modernização trouxe para a sociedade contemporânea diversas transformações. Porém, em boa parte das vezes, as transformações são proporcionalmente superiores à sua capacidade de adaptação e de controle jurídico. A ciência informática é seguramente a que proporciona maiores avanços e em velocidade mais exponencial, o que traz em si, desta forma, insegurança, uma vez que sua regulamentação é incapaz de acompanhar a evolução da tecnologia. Com isso, a Sociedade Informática é identificada como a sociedade de risco justamente porque essa falta de controle jurídico das possíveis ameaças e riscos só aumentam a sensação de insegurança.

3 A CRIMINALIDADE DIGITAL

No decorrer da evolução tecnológica em busca de mecanismos eficazes que pudessem facilitar a solução de cálculos matemáticos complexos, não havia evidências de que o ser humano pudesse querer manusear esse equipamento para colocar em perigo algum bem jurídico. Tanto no aperfeiçoamento dos computadores como no advento da internet, as tecnologias visavam aprimorar, de forma confiável, processos que demandavam muito tempo e mão de obra, além de encurtar distâncias, conectando entre si, dados e usuários.

Entretanto, é possível observar como os crimes praticados no ambiente virtual têm tido cada vez mais repercussão midiática por todo o mundo. Com isso, tem-se a falsa sensação de que essa modalidade delitiva seja um fenômeno recente, o que não é verdade. Os primeiros casos de crimes digitais conhecidos foram detectados nos anos de 1960, com o manuseio de dados, sabotagem, espionagem e uso ilegal de sistemas de computadores, como relata Luciana Boiteux (2004, p. 156). Na década de 1970, a controvertida figura do Hacker já era conhecida com o advento dos crimes de invasão de sistemas e violação de softwares, mas foi em 1980 que houve uma maior incidência dos crimes de pirataria, propagação de vírus, pedofilia e invasão de sistemas (GIMENES, 2013, p. 02). Já os anos de 1990 ficaram marcados pela atuação do até hoje conhecido mundialmente como o maior Cracker da história, Kevin Mitnick, que invadiu os sistemas da "Motorola, Nokia, Sun Microsystems e Fujitsu Siemens antes de ser finalmente pego pelo FBI" (GHEDIN, 2012) em 1995.

Com tantas mudanças ocorridas na sociedade por causa da evolução da tecnologia, a criminalidade[1] também acabou sendo afetada e sofreu algumas transformações significativas. A sociedade da informação possui um potencial lesivo bem diferente da época em que o Código Penal brasileiro (BRASIL, 1940) foi concebido, quando os bens protegidos eram, em grande parte, materiais e tangíveis. Conforme o tempo foi passando e essas mudanças ocorrendo, reformas e inovações legislativas sobrevieram como, por exemplo, as violações de propriedade imaterial e as violações à ordem econômica ou tributária. Contudo, nem sempre o ordenamento jurídico consegue acompanhar a velocidade das transformações sociais. Com isso, a

[1] Importante conceituar o que seja criminalidade, que não se confunde com o conceito de violência. Enquanto a violência é um constrangimento físico ou moral, a criminalidade é a expressão dada pelo conjunto de infrações que são produzidas em um tempo e lugar determinado. Logo, criminalidade está associada aos crimes, cujo conceito material deve ser obtido na Ciência Jurídica, que os definem como a conduta humana que lesa ou expõe a perigo um bem jurídico protegido pela lei penal (MIRABETE; FABBRINI, 2016, p. 185).

criminalidade acaba aproveitando das lacunas penais para incorrer em novas práticas delitivas. Neste sentido, escreve Marcelo Xavier de Freitas Crespo:

> Sendo o Direito um fenômeno cultural, deve acompanhar, de algum modo, a realidade temporal e geográfica em que se desenvolve, vez que as evoluções do mundo social, político e econômico influenciam os aspectos jurídicos. Além disso, deve-se considerar que a informática transformou-se em importantíssimo instrumento de informação e esta, por seu turno, tornou-se valioso bem econômico.
> Dessa forma, naturalmente surgem inquietações dos homens quanto às leis que venham a regular o desenvolvimento tecnológico. Isto porque os avanços das tecnologias impõem complexos problemas jurídicos a serem decifrados pelos operadores do Direito (CRESPO, 2011, p. 22).

Diferentemente do mundo material, no mundo digital não existem regras de conduta interna, o que facilita, muitas vezes, o cometimento de condutas reprováveis. A falta de controle na internet dá a qualquer usuário a possibilidade de agir delituosamente, enquanto a vítima não sabe de onde vem o ataque, quem a ataca, quais suas motivações e talvez nem a dimensão do dano sofrido em seu sistema.

3.1 ASPECTOS CONCEITUAIS E NOMENCLATURAS DOS CRIMES DIGITAIS

Tentar conceituar e dar nome aos crimes praticados por meio da rede mundial de computadores não é tarefa fácil, pois, no Brasil, não existe por parte da doutrina, uma terminologia considerada pacífica e nem majoritária. Dessa forma, é possível encontrar diversas denominações, dentre as quais: “crimes de computador”, “cibercrimes”, “crimes digitais”, “crimes informáticos”, “crimes eletrônicos”, “crimes virtuais”, “delitos informáticos”, dentre outros.

Dentre os autores que debatem sobre o tema-problema, Augusto Rossini (2004, p. 110) e Bonilha (2006, p. 84) utilizam a denominação “delitos informáticos” para aquelas condutas típicas e ilícitas, que constituem um crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, através da informática, em ambiente de rede ou fora dele, que ofenda de forma direta ou indireta a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade. Para Ramalho Terceiro (2005) e Gimenes (2013), os crimes praticados neste ambiente se caracterizam pela ausência física do agente ativo. Com isso, ficariam definidos como sendo “crimes virtuais”.

Por sua vez, Sandra Gouvêa prefere o uso da expressão “crimes por meio da informática”, justificando que os computadores não são os únicos instrumentos capazes de serem utilizados nas práticas delitivas (GOUVÊA, 2017, p. 54). Tulio Lima Vianna, considerando o bem jurídico, que entende tutelado, considera apenas duas possibilidades: “delitos informáticos” ou “delitos computacionais” (VIANNA, 2001, p. 9-10).

Já Deborah Fisch Nigri, utiliza a expressão “crime informático” para se referir ao ato lesivo cometido através de um computador ou de um periférico com a intenção de se obter uma vantagem indevida (NIGRI, 2000, p. 38). Essa denominação também é adotada por Spencer Toth Sydow (2015, p. 55).

Constata-se, pois, que não há consenso a respeito da nomenclatura dos delitos relacionados à tecnologia. Porém, determinadas expressões, apesar de serem utilizadas para tentar abarcar estas condutas, acabam por limitar a abrangência de tais delitos. Como exemplo, o termo “computador” que significa “dispositivo capaz de obedecer a instruções que visam produzir certas transformações nos dados, com o objetivo de alcançar um fim determinado” (CRESPO, 2011, p. 49). Ocorre que, os crimes praticados através da internet, não necessariamente são cometidos em computadores. Enquanto isso, a expressão “cibernético” se refere à “teoria das mensagens e dos sistemas de processamento de mensagens (em um estudo comparativo entre o funcionamento do cérebro humano e dos computadores) que se encontra em desuso há décadas” (CRESPO, 2015) e “virtual” é um termo utilizado para descrever algo que não existe na realidade material.

Com toda essa divergência doutrinária e tantas denominações que não conseguem abranger de forma satisfatória os delitos em questão, a expressão que soa mais adequada é a defendida por Marcelo Xavier de Freitas Crespo que utiliza do termo “crimes digitais” para se referir “tanto aos crimes tradicionais, já previstos na legislação, contra os valores que tradicionalmente reconhecemos como merecedores de proteção, praticados com auxílio da mais moderna tecnologia, bem como as condutas ilícitas passíveis de penas que se voltem contra os sistemas informatizados e os dados” (CRESPO, 2015).

Em outras palavras, os crimes digitais são todas as ações típicas, antijurídicas e culpáveis cuja prática envolva o processamento automático de dados ou sua transmissão, em que um computador conectado à internet seja o objeto ou o instrumento da ação delituosa, ainda que o crime pudesse ser praticado de outra forma. Essa expressão é a mais apropriada em razão do que se pretende referir, ou seja, aos dados que decorrem da eletrônica digital: “aquela em que os dados são convertidos nos números “0” e “1”, que formam o sistema binário, base para o armazenamento de dados, mais moderna e atualizada que a eletrônica analógica” (CRESPO, 2015).

3.2 CARACTERÍSTICAS DOS CRIMES DIGITAIS

Inicialmente, é imprescindível que se faça uma retrospectiva dentro do próprio Direito Penal para compreender o que vem a ser um crime. A Lei de Introdução ao Código Penal

brasileiro (Decreto-lei n. 3914 de 09 de dezembro de 1941) faz a seguinte definição de crime: "considera-se crime a infração penal a que a lei comina pena de reclusão ou detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração a que a lei comina, isoladamente, penas de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente" (BRASIL, 1941). De acordo com as lições de Bitencourt, essa lei, sem nenhuma preocupação científica, limitou-se apenas a diferenciar as infrações penais consideradas crimes daquelas que constituem contravenções penais, as quais se apresentam, tão somente, na natureza da pena de prisão aplicável. Dessa forma, os crimes sujeitam seus autores às penas de reclusão ou detenção, enquanto as contravenções, no máximo, incorrem em prisão simples (BITENCOURT, 2017, p. 310). Diferentemente dos Códigos Penais de 1830 (BRASIL, 1830) e de 1890 (BRASIL, 1890), esta lei não definiu o conceito de crime, deixando sua elaboração a cargo da doutrina nacional.

Dessa forma, parte significativa da doutrina conceituou o crime como sendo uma conduta típica, antijurídica e culpável, ou seja, uma ação ou omissão contrária ao direito, desde que existam imputabilidade, consciência potencial de ilicitude e exigibilidade e possibilidade de agir conforme os preceitos legais, como ensina Guilherme de Souza Nucci (2017, p. 147). Este conceito se aplica a todo e qualquer delito, sendo ele crime ou contravenção penal. Entretanto, os crimes digitais possuem características que não se manifestam nas condutas praticadas no mundo material.

No meio físico, tanto autor quanto a vítima estão, na maior parte das vezes, próximos entre si quando acontece o fato típico, como no exemplo cometimento de um crime de roubo, em que os sujeitos ativo e passivo não podem estar distantes. Com isso, é possível dizer que a criminalidade no mundo material seria mais simples de ser combatida, já que o infrator estaria limitado no espaço de atuação e cometeria apenas um delito (ou uma cadeia de crimes) por vez. Uma vez praticado o crime, cabe à polícia agir no local, focada no ambiente em que houve seu cometimento, como se percebe em parte do artigo 6º do Código de Processo Penal (BRASIL, 1941):

> Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
> I – dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais;
> II – apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;
> [...]
> VI – proceder a reconhecimento de pessoas e coisas e a acareações (BRASIL, 1941).

Entretanto, como aplicar o texto legal supracitado em delitos em que não se há nem local definido e nem palpabilidade? O questionamento surge porque a principal característica dos crimes digitais é que estes não conhecem fronteiras, ou seja, não estão limitados a um determinado espaço geográfico de atuação. Enquanto os infratores podem estar em um país, o objeto tutelado pode estar em outro e o resultado em uma terceira localidade. Com isso, dificuldades são percebidas no procedimento investigatório dessa modalidade delitiva, uma vez que a variação de fronteiras exige cooperação entre o sistema jurídico e policial de, em alguns casos, diversos países, o que pode ocasionar barreiras burocráticas intransponíveis que impedem qualquer condenação.

Nesse sentido, é possível dizer que a criminalidade no mundo físico segue padrões verificáveis, uma vez que, ao passo que a maioria dos delitos no mundo material apresenta um tempo e espaço que podem ser reconstituídos e delimitados, os crimes digitais funcionam de maneira distinta. Estes podem ocorrer em uma questão de segundos ou por dias seguidos. Neste sentido, Renato Monteiro exemplifica que:

> Uma invasão e a modificação de um sistema informático pode acontecer em um piscar de olhos enquanto que um ataque distribuído de negação de serviço pode levar horas, quiçá dias, recebendo a denominação de crime continuado, até mesmo de dano, pois pode levar a corruptela total de uma estrutura que sustenta o sistema financeiros de um país (MONTEIRO, 2010, p. 46).

Outra característica fundamental dos crimes digitais é a volatilidade da materialidade dos delitos. Como os dados e informações no meio digital não se encontram, necessariamente, em apenas um lugar, estes podem ser facilmente modificados ou suprimidos. Com isso, a simples demora na busca de tais registros pode comprometer sua existência, fato que tem comumente ocorrido com as empresas responsáveis por prover serviços computacionais e que, por ainda não existir uma previsão legislativa específica sobre a matéria, aduzem que o armazenamento dos dados de acesso por longos períodos depende de empenho e de custos elevados.

Não deixar qualquer tipo de vestígio que possa contribuir para delimitar a materialidade e a autoria de um crime digital é uma tarefa difícil. Desde que haja colaboração dos provedores de internet e celeridade na investigação, a identificação da autoria desta modalidade delitiva se torna plenamente possível. Porém, a dificuldade maior tem sido na punição dos infratores, por esbarrar na barreira criada pela legislação inespecífica e as fronteiras da transnacionalidade.

É necessário salientar também a elevada presença da chamada cifra negra do Direito Penal presente nos crimes digitais (ZAFFARONI, 2007, p. 75). Segundo Sydow, a falta de comunicação destes delitos se dá, primeiramente, pelo acanhamento do ofendido que acredita

que, por ter sido lesado por meio da informática, isso implicaria uma sensação de incapacidade de operar seu dispositivo tecnológico, gerando, assim, uma relutância em se expor. O segundo motivo, é em relação às pessoas jurídicas, principalmente as instituições financeiras e as lojas virtuais, com receio de que, se relatarem alguma violação de seu sistema de segurança digital, isso ocasionaria uma perda de confiança dos consumidores em utilizar ou contratar seus serviços. A terceira, e última, é a falta de punibilidade dos autores de crimes digitais, somando ao fato de que a reparação da vítima raramente ocorre (SYDOW, 2015, p. 60).

Apresentadas algumas das principais características desta modalidade delitiva, é possível verificar-se que conceitos como soberania, território, tempo e espaço do crime mudam de sentido quando se trata de crimes digitais. Não só novos riscos são criados com a evolução da tecnologia, mas também carecem de proteção penal, agora, novos bem jurídicos, que merecem a devida atenção.

3.3 BENS JURÍDICOS PASSÍVEIS DE PROTEÇÃO PENAL

Para Allegro, o ser humano, quando exposto à vida em sociedade, tende a valorizar determinados elementos que geram interesses e disputas por parte de outros indivíduos (ALLEGRO, 2005). Essa valoração é proveniente de diversos fatores, tais como a satisfação de necessidades, a realização de desejos ou sua escassez, por exemplo. Dessa forma, quando algo passa a ser valioso e requisitado, torna-se, assim, um bem. Surge, então, o interesse de tutelar esse bem que, no direito, ocorre por meio de sua normatização. “Protegido pela legalidade, esse bem passa a apresentar-se como um bem jurídico, e sendo protegido pelo legislador penal a doutrina considera-o como bem jurídico penalmente tutelado” (ALLEGRO, 2005).

A figura do bem jurídico conhecida atualmente teve sua devida importância no âmbito jurídico-penal manifestada somente após os conflitos que marcaram o período da II Guerra Mundial, como bem destaca Douglas Resende da Silva. Depois dos obscuros anos da vigência dos regimes nazista na Alemanha e fascista na Itália, passou-se a buscar, de maneira efetiva, limitar-se o poder punitivo do Estado, com o fim de evitar que o Direito Penal pudesse ser utilizado como instrumento de repressão e ataque contra aqueles que divergissem da posição ideológica dominante (DA SILVA, 2017).

Com isso, Claus Roxin buscou criar uma teoria do bem jurídico crítico ao legislador, impendido que este pudesse atuar de maneira arbitrária e violadora das liberdades individuais a partir da criminalização ilegítima de condutas que não afetam a vida em sociedade (ROXIN, 2014, p. 74-75).

O conceito de bem jurídico, então, advém com o objetivo de conter a crescente onda de criminalização de comportamentos considerados imorais ou contrários aos valores políticos e religiosos, limitando o âmbito de atuação do legislador e impondo, para que a criminalização seja legítima, uma missão de proteção de bens jurídicos (ROXIN, 2013, p. 02).

Nas palavras de Bianchini, Molina e Gomes, a concepção de bem jurídico remonta à ideia de:

> [...] bem relevante para o indivíduo ou para a comunidade (quando comunitário não se pode perder de vista, mesmo assim, sua individualidade, ou seja, o bem comunitário deve ser também importante para o desenvolvimento da individualidade da pessoa) que, quando apresenta grande significação social, pode e deve ser protegido juridicamente. A vida, a honra, o patrimônio, a liberdade sexual, o meio-ambiente etc. são bens existenciais de grande relevância para o indivíduo (BIANCHINI; GARCIA-PABLOS DE MOLINA; GOMES, 2009, p. 232).

Nesse sentido, Eugenio Raúl Zaffaroni e José Henrique Pierangeli entendem que "bem jurídico penalmente tutelado é a relação de disponibilidade de um indivíduo com um objeto, protegido pelo Estado, que revela seu interesse mediante a tipificação penal de condutas que o afetam" (ZAFFARONI; PIERANGELI, 2015, p. 462).

Seguindo o raciocínio da teoria de Roxin e o conceito dos demais autores apontados, é possível verificar que se buscava uma limitação à atuação do *ius puniendi* estatal. A criminalização de uma conduta, portanto, só seria viável e legítima se atentasse contra um bem jurídico digno de proteção. É dever do Direito Penal proteger esses bens jurídicos, a fim de garantir, dessa forma, que os cidadãos possam usufruir de condições necessárias para um desenvolvimento social pacífico e equilibrado, quando nenhum outro ramo do ordenamento jurídico fosse suficiente para garanti-lo.

Segundo Roxin, em relação à fonte dos bens jurídicos dignos de proteção penal, cabe à Constituição (BRASIL, 1988) definir o que deverá ser digno de tutela, "quais são os bens jurídicos eleitos, bem como deve perquirir se a punição a condutas atentatórias são proporcionais, não sendo legítimo usar o Direito Penal quando se pode manejar outro ramo menos gravoso" (DA SILVA, 2017).

Dessa forma, tem-se que a atividade legislativa de produção de tipos penais incriminadores só pode conferir proteção penal a bens jurídicos que estiverem em consonância com a Constituição da República Federativa do Brasil (BRASIL, 1988).

Em suma, destaca-se a importância de se conceituar o que são bens jurídicos e, consequentemente, questionar qual a função do Direito Penal, para que se possa, então, estruturar um sistema punitivo em consonância com Estado Democrático de Direito. Nesse sentido, é necessário que se observe atentamente as importantes transformações que a evolução

da informática vem causando na sociedade de risco e se questione: essas mudanças trouxeram novos bens jurídicos que demandam por tutela jurídico-penal?

3.3.1 Bens jurídicos peculiares à informática

Diante dos novos riscos que surgiram a partir da evolução da informática e dos meios de comunicação, o bem jurídico penal a ser tutelado passa a ter novos contornos. Dessa forma, pode-se dizer que quando se tratam de crimes digitais, as condutas delitivas atingem não só aqueles valores tradicionalmente protegidos, como a vida, a integridade física, o patrimônio e a fé pública, mas, também, as informações armazenadas (dados) e a segurança dos sistemas de redes informáticas ou de comunicação, como ressalta Marcelo Crespo (2011, p. 56).

Com isso, a informação passou a ter um papel preponderante na sociedade, como uma espécie de "mercadoria", sendo o principal bem jurídico a ser tutelado nos crimes digitais. Além das informações e dos dados, a confiabilidade e a segurança dos sistemas e redes informáticas e de comunicação também carecem de tutela por parte do Direito Penal. Porém, isso não quer dizer que a objetividade jurídica historicamente protegida deva ser deixada de lado, Marcelo Crespo (2011, p. 57) e Francisco Bueno Arús (1997, p. 190) consideram ser possível uma violação conjunta de bens jurídicos tradicionais e outros, peculiares à informática.

Dessa forma, pode-se dizer que os crimes digitais são pluriofensivos, ou seja, atingem dois ou mais bens jurídicos. Ao mesmo tempo em que há violação de bens jurídicos tradicionais, há, também, a necessidade de proteção de novos interesses provenientes da sociedade de risco. Com isso, não é correto "atrelar única e exclusivamente o meio pelo qual se pratica a conduta, devendo se constituir em torno da afetação da informação como bem jurídico protegido, primordial e basicamente, ainda que não de forma exclusiva" (CRESPO, 2011, p. 58).

Portanto, cabe o questionamento de qual seria o principal bem jurídico afetado quando se trata de crimes digitais. Seria a informação ou os sistemas informáticos e de telecomunicações? Para Enrique Rovira del Canto a informação seria esse bem jurídico principal e, secundariamente, os dados ou os sistemas. O autor parte da ideia de que os dados representem a informação em sua forma digital, ainda que com valores variáveis, enquanto os sistemas nada mais são que os mecanismos materiais de funções automáticas de armazenamento, tratamento e transferência (ROVIRA DEL CANTO, 2002, p. 72).

Considerando-se, portanto, tanto a informação quanto os sistemas informáticos ou os dados e seus respectivos papeis dentro da discussão dos crimes digitais, é necessário pensar em novos modelos de proteção dos bens jurídicos que sejam adequados e condizentes com as novas perspectivas da sociedade de risco.

3.4 CLASSIFICAÇÃO DOS CRIMES DIGITAIS

Quando se pretende estudar as nuances dos crimes digitais, discorrer sobre suas classificações é a tarefa mais árdua. Isto porque há uma grande variedade de entendimentos propostos por diferentes autores, também justificável pela constante evolução tecnológica que tende a mudar suas opiniões.

Levando-se em consideração o que já fora explanado sobre os bens jurídicos protegidos nesta modalidade delitiva, o mais correto seria considerar crime digital apenas aquelas condutas que viessem a atingir a informação ou algum sistema informático. A simples utilização do computador como meio para o cometimento de algum delito não deveria ser considerado um crime digital, mas um crime já previsto no ordenamento jurídico pátrio com um "novo" *modus operandi*. Entretanto, ficou convencionado pela imprensa nacional e por parte da doutrina que qualquer ilícito praticado com o uso da tecnologia, caracterizaria, portanto, um crime digital (CRESPO, 2011, p. 62).

Tendo em vista a alta popularidade acadêmica e social desta convenção, não há como ignorá-la neste trabalho. Dessa forma, entende-se como a melhor classificação, por ser a mais objetiva e passível de se encaixarem as condutas ilícitas mais modernas, aquela defendida por Ferreira (2000, p. 163), Greco (2004, p. 85) e Crespo (2011, p. 63), que diferenciam as condutas cometidas contra um sistema informático; daquelas condutas praticadas contra outros objetos jurídicos, utilizando-se do meio digital.

Dessa forma, pode-se dizer que toda conduta praticada contra algum bem jurídico informático como sistemas ou dados, são crimes próprios ou puros, enquanto aquelas outras condutas que são perpetradas contra bens jurídicos tradicionais, não relativos à tecnologia, são crimes impróprios (CRESPO, 2011, p. 63), como será explanado a seguir.

3.4.1 Crimes digitais próprios

Os crimes digitais próprios são, portanto, aquelas condutas proibidas por lei cujos bens jurídicos infringidos são os sistemas informáticos e as informações automatizadas (dados). Também chamados de crimes digitais puros, essa classificação remete àquelas condutas que recaem sobre o próprio computador físicos e seus componentes (*hardware*) ou sobre o sistema operacional ou programas (*software*), prejudicando seu normal funcionamento. Entre os exemplos mais conhecidos de crimes digitais próprios estão: a intrusão informática, o "furto" de identidade virtual, a inserção de *malwares*, o *scamming*, o *spamming*, e a interceptação de e-mails.

3.4.1.1 Intrusão informática

Intrusão informática, também conhecida como "invasão de dispositivo informático" ou, ainda, "*hacking"*, refere-se ao acesso não autorizado de um usuário ao sistema alheio, com ou sem o objetivo de obter vantagem, seja ou não por meios ardilosos, violentos, ou até mesmo por conta de um subterfúgio que consiga enganar o legítimo detentor dos direitos relativos ao sistema, levando-o a permitir o ingresso, sob erro (SYDOW, 2015, p. 113).

A princípio, este delito fora pensado como sendo aquele em que o autor, com conhecimentos de informática, ataca sistemas fechados provocando aberturas e vulnerabilidades nos mecanismos de defesa. A partir daí, obteria acesso para ingressar nos sistemas informáticos alheios. Entretanto, após avançarem os estudos a respeito das técnicas de invasão, conclui-se que para que se obtenha acesso aos sistemas alheios não é imprescindível a presença de mecanismos de violação. Isto porque boa parte dos sistemas operacionais e programas de uso cotidiano são lançados no mercado com falhas lógicas de programação. Essas falhas, também chamadas de *bugs*, podem gerar brechas de segurança que levam a uma possível vulnerabilidade dos sistemas, permitindo que usuários mal-intencionados possam aproveitar-se dessas aberturas para quaisquer fins (SYDOW, 2015, p. 114).

Outra prática recorrente nas redes informáticas é a indução de vítimas futuras e eventuais a instalarem ou acessarem arquivos que geram falhas de segurança ou criam portas de acesso livre nos dispositivos alheios (SYDOW, 2015, p. 114). O exemplo mais conhecido é o do "Cavalo de Troia", um *malware* (programa malicioso) que se oculta em programas que parecem inofensivos, mas que, ao serem acionados, criam brechas para que o sistema possa ser invadido pelo delinquente. Por vezes, o usuário nem percebe que seu dispositivo tenha sido violado, uma vez que a ação delituosa acontece sem nenhuma violência, mas de forma ardilosa.

Também é prática comum que parte dos usuários, ao escolher senhas de acesso para suas contas de e-mail, sistemas operacionais ou até conta de banco, tenda a optar por combinações consideradas óbvias, como sequências simples de números, referências a datas comemorativas, números de documentos ou até seus próprios nomes (SYDOW, 2015, p. 114). Assim, a probabilidade de que alguém com o intuito de acessar sistema alheio, por tentativa e erro a partir de um prévio conhecimento pessoal do usuário, acaba sendo consideravelmente maior.

Dessa forma, o termo "invasão de dispositivo informático" não parece ser o mais adequado, uma vez que o substantivo dá a entender um ato violento praticado pelo *hacker*, o que não é necessariamente verdade, como apresentado (SYDOW, 2015, p. 113). Porém, é a

nomenclatura adotada pelo artigo 154-A do Código Penal brasileiro (BRASIL, 1940), que será posteriormente aprofundado.

Nesse sentido, a expressão que melhor representa este delito, por ter uma concepção mais abrangente, é a de "intrusão informática", que significa a "ação de se introduzir, sem direito ou por violência, ou, alternativamente, o ingresso ilegal, sem convite ou com consentimento viciado" (SYDOW, 2015, p. 114).

O dano causado pela conduta está, portanto, no fato de que o acesso e tudo o que está com ele relacionado são individuais, exclusivos e somente podem ter seu caráter íntimo e pessoal publicado por quem detém o direito de permissão do mesmo. Marcelo Xavier Crespo discorre no sentido de que o prejuízo restaria configurado na medida em que se viola privacidade e causa esforço para que se modifiquem políticas de segurança da informação (CRESPO, 2011, p. 67).

A intrusão informática, assim, viola a confidencialidade do acesso particular e, consequentemente, a segurança do dispositivo informático, gerando riscos e incertas ao usuário. Ao mesmo tempo, pode gerar outras consequências como a modificação de arquivos, cópia de segredos industriais e inserção de códigos maliciosos.

Como supracitado, o delito em questão passou a ser tipificado no ordenamento jurídico pátrio após ser sancionada a Lei nº 12.737, de 30 de novembro de 2012 (BRASIL, 2012) que introduziu ao Código Penal brasileiro (BRASIL, 1940) o artigo 154-A, que prevê:

> Invasão de dispositivo informático
> 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 (BRASIL, 1940).

O delito em questão possui estreita relação com os outros crimes digitais próprios, sendo, muitas das vezes, o meio pelo qual outros ilícitos possam ser cometidos, como os que serão apresentados a seguir.

3.4.1.2 "Furto" de identidade virtual

"Furto" de identidade virtual é a ato de apropriar-se das características e identificações de outra pessoa para fazer-se passar por esta, sem que tenha obtido a devida autorização legal (SYDOW, 2015, p. 115).

Uma das características mais marcantes do ciberespaço é a anonimidade, que propicia aos usuários a possibilidade conviverem e interagirem entre si sem ao menos ter a certeza de quem são na vida real. Essa insegurança levou os desenvolvedores responsáveis pelos ambientes virtuais a criarem sistemas de identificação presumida, em que cada usuário que o acessa se vê obrigado a fornecer seus dados pessoais para cadastramento.

Ao acessar a internet, o usuário gera um histórico de navegação que apresenta quais as páginas mais visitadas e quais as preferências de assuntos pesquisados, o que influencia na criação de um acesso personalizado de acordo com suas predileções. Com isso, é possível afirmar que cada pessoa tem uma identidade própria no ambiente virtual e seu acesso pode ser de grande valia para suas relações pessoais e profissionais (SYDOW, 2015, p. 116).

O delito em questão está ligado, portanto, à utilização não autorizada desta identidade virtual alheia, fazendo-se passar por ele para se relacionar com pessoas de seu convívio, enviar mensagens, induzir outras pessoas a compartilhar informações pessoais, apoderando-se da vida virtual da vítima para seu benefício, mesmo que não seja econômico.

Uma vez dada permissão a alguém para que se possam enviar mensagens em seu nome ou conversar utilizando-se do apelido de outrem, estas atitudes deixam de violar qualquer bem jurídico e, consequentemente, encaixar-se a esse tipo. Isso porque a anuência afasta o caráter ilícito da ação, já que, nesse caso, a identidade virtual está disponível. Portanto, para se configurar o delito de "furto" de identidade virtual, é imprescindível que não haja autorização ao se apropriar do uso de confiabilidade e de credibilidade alheias para proveito próprio.

Quando se utiliza do termo "furto", para Spencer Sydow, está-se diante de uma atecnia. Isto porque a legislação penal brasileira é regida pelos princípios da reserva legal e da

taxatividade, que exigem que todos os elementos objetivos, subjetivos e normativos estejam presentes para que se configure um tipo penal, o que não é o caso do furto (SYDOW, 2015, p. 117).

O artigo 155 do Código Penal brasileiro (BRASIL, 1940) prevê que será punível aquele que "subtrair coisa alheia móvel para si ou para outrem" (BRASIL, 1940). Porém, identidade virtual é um conceito abstrato, representado por uma quantidade de características e atributos, que não se pode considerar como coisa móvel. Mesmo a lei penal dando aos bens imateriais, como programas de computador, direitos autorais e até à energia elétrica, a equivalência de proteção dada aos bens móveis, a identidade virtual, por se tratar de uma legitimidade de acesso a um perfil traçado, ainda não se inclui em tais apontamentos (SYDOW, 2015, p. 117).

Mesmo se equiparando os dados às coisas, ou se considere que para o uso da identidade virtual alheia, seja necessário possuírem-se os dados existentes no dispositivo alheio, ainda assim o núcleo do tipo penal previsto no artigo 155 não estaria configurado. Isto porque os *bits* que compõem os dados são intangíveis, ou seja, são apenas representações de uma linguagem de programação a serem interpretadas pelo dispositivo informático, não sendo possível que haja sua subtração, mas somente sua cópia para outros dispositivos (SYDOW, 2015, p. 117). Nesse sentido, não é logicamente possível que um dado seja retirado da esfera de vigilância de alguém, pois, no caso em questão, com a cópia deste para outro dispositivo, não existe subtração/supressão, mas uma pluralidade de originais idênticos.

O uso da expressão "furto" se deu pela tentativa de importar o termo referente a essa conduta na língua inglesa, predominantemente chamada de *identity theft*. Porém, mesmo que a tradução se refira a "furto de identidade", essa passa a ser incompatível com o ordenamento jurídico brasileiro (SYDOW, 2015, p. 118). Isso ocorre porque a definição da palavra "theft" simboliza o delito de furto ou de roubo, porquanto trata de tomar conta de algo pertencente a outrem, sem seu livre consentimento. Entretanto, no Brasil, a lei penal determina que furtos ou roubos só poderão ocorrer com a subtração do bem jurídico em questão, por esse ser sempre único, ou de uso único ou pontual, como a energia elétrica. Dessa forma, tem-se um afastamento da característica plural dos dados informáticos, não sendo possível sua proteção devido à uma não adaptação do tipo penal ao bem jurídico.

3.4.1.3 Inserção de malwares

Dentre os vários e recorrentes modos desenvolvidos para se praticar crimes digitais, a inserção de *malwares* (códigos maliciosos) talvez seja o mais popular dentre eles, uma vez que

todos os usuários com acesso à rede mundial de computadores estão suscetíveis de serem vítimas deste delito.

Também denominado de inserção de código malicioso, o contágio e/ou sabotagem de dispositivo informático alheio modifica, altera ou até destrói seus dados. Isso porque os *malwares* são instruções inseridas em dispositivos alheios por meio de arquivos aparentemente inofensivos, que dão comandos que implicam em algum prejuízo para o usuário, seja na confidencialidade, disponibilidade e até integridade de seus dados (SYDOW, 2015, p. 122).

Spencer Toth Sydow, em sua obra, apresenta como o delito em questão é tratado no ordenamento jurídico-penal alemão e italiano:

> O Código Penal Alemão em seus arts. 202a, 303a e 303b, com maior abrangência, delineia como sabotagem informática: a) a obtenção ilegítima de dados protegidos contra acesso ilegal, para si ou para outrem, b) a alteração, supressão, transformação prejudicial ou apagamentos de dados feitos ilegalmente, e c) a interferência no processamento de dados que traga prejuízos substanciais, por meio da destruição, danificação, inutilização, remoção ou alteração de sistema de processamento de dados ou suporte de dados.
> [...] o Código Penal Italiano, em seu art. 635 bis, determina que merece intervenção do Estado aquele que destrói, degrada ou inutiliza, no todo ou em parte, sistemas telemáticos alheios, ou programas, dados ou informações alheios (SYDOW, 2015, p. 22-23).

Vários são os códigos maliciosos que podem causar danos aos usuários e à segurança digital. Dentre eles os principais e mais recorrentes são os vírus, os *worms*, os *rootkits*, *keyloggers*, *spywares* e os *adwares*.

Os vírus são segmentos de códigos de programação que se anexam a programas ou sistemas de modo a se propagar pelos dispositivos informáticos e contaminar outros sistemas que estejam em contato com este, através de e-mails ou compartilhamento de arquivos (CRESPO, 2011, p. 74). Criados para se autorreplicarem e serem difundidos automaticamente, os vírus nem sempre são prejudiciais, pois seu contágio pode apenas tornar o sistema operacional do dispositivo mais lento, já que sua elevada capacidade de se copiar e espalhar pelo sistema faz com que a memória do dispositivo acabe sendo consumida.

Os vírus são, aparentemente, como um *software* qualquer, a diferença está no fato de que, enquanto normalmente os programas visam um aumento de capacidade e produtividade do usuário, os vírus tendem a dificultar seu acesso. Assim como os vírus que atacam os seres humanos, a versão digital destes variam quanto ao seu grau de lesividade, podendo trazer ao usuário de um computador mero inconveniente de uso, bem como a total perda de dados e corrupção de arquivos (CRESPO, 2011, p. 75).

Os *worms* (vermes), assim como os vírus, ao acessar um sistema, se multiplicam, causando desde lentidão do dispositivo até perda de seus dados. A diferença, é que estes

possuem um contágio aperfeiçoado, pois são desenvolvidos para se propagarem automaticamente através da internet, acessando os serviços de e-mail da máquina, enviando cópias em anexos que chegam a toda a lista de destinatários do usuário infectado (SYDOW, 2015, p. 124). Ao se aproveitar da confiabilidade dada às mensagens enviadas pelo usuário hospedeiro, os e-mails contendo os *worms* são abertos, fazendo com que o processo de infecção recomece, agora em um novo dispositivo contaminado. Em alguns casos, esse *malware* pode possibilitar que a máquina infectada seja controlada remotamente, ou seja, que um terceiro leia arquivos, acesse contas e exclua programas (CRESPO, 2011, p. 75).

Rootkits é o nome dado a um conjunto de códigos maliciosos criado para camuflar a presença de determinados processos ou programas de serem detectados pelo sistema operacional, a fim de permitir acesso e controle de determinado dispositivo informático e seus dados. "*Root"* é expressão utilizada pelos usuários que possuem o controle total de um computador, enquanto "kit" corresponde às ferramentas necessárias para esse acesso (DIAS, 2013). Os *rootkits* podem ser adquiridos de diversas maneiras, mas, principalmente, por meio de algum cavalo de troia ou algum anexo contaminado de e-mail. Quando ocorre uma varredura de arquivos maliciosos por programas antivírus, os *rootkits* acabam modificando a forma de pesquisa, levando este programa a não acusar sua existência e, consequentemente, a sua remoção.

Keyloggers (registradores do teclado em inglês) são *softwares* espiões aptos a identificar ações dos usuários que estejam por eles contaminados e, em sequência, enviar ao seu programador tais informações. Dessa forma, os *keyloggers* são capazes de detectar e informar toda e qualquer tecla que tenha sido acionada pelo usuário infectado. Uma vez que o sujeito ativo recebe o arquivo contendo esses dados, este tem acesso à tudo que foi digitado pela vítima, como dados e senhas de acesso a programas, contas de e-mail e serviço bancário *online*. Com isso, há uma quebra na confiabilidade e disponibilidade dos serviços digitais, podendo trazer, também, prejuízos econômicos para aquele que teve sua intimidade atingida. Após a popularização dessa ferramenta maliciosa, os bancos passaram a substituir a digitação das senhas de acesso às contas por modalidades digitais de teclado, evitando que os correntistas fossem monitorados pelos *keyloggers* ao acionar seus teclados. Porém, os programadores desenvolveram os *screenloggers* (registradores de tela), programas que conseguem capturar também as telas visualizadas no dispositivo digital, bem como os movimentos do *mouse* (SYDOW, 2015, p. 122). Com isso, mesmo não sendo mais digitadas no teclado alfanumérico tradicional, os infratores continuaram monitorando e registrando as senhas utilizadas pelos usuários contaminados.

Os *spywares* (programas espiões) são códigos maliciosos que interagem de forma automática com os navegadores de internet para coletar as ações dos usuários, bem como suas preferências de acesso. Porém, estes podem ser desenvolvidos para encontrar e registrar informações sensíveis e confidenciais dos usuários – por exemplo, os dados de acesso bancário –, enviando-lhe para seu programador, que poderá causar-lhe algum prejuízo. Atuando de forma semelhante estão os *adwares* (programas de anúncios) que são uma modalidade de *spyware*, mas com o objeto específico de exibir, de forma automática, na tela do dispositivo, alguma propaganda específica, geralmente baseada nas preferências do usuário.

É possível observar, portanto, que cada vez mais os *malwares* são criados e disseminados. Dependendo de sua programação, estes podem proporcionar danos irreparáveis aos sistemas e aos usuários, bem como apenas criar dificuldades e lentidão de acesso. A inserção desses códigos maliciosos supracitados adquiriu maior relevância jurídica com o advento da Lei nº 12.737/2012 (BRASIL, 2012), mas sua contaminação, de acordo com a legislação penal vigente, só poderá ser considerada um fato típico, quando o agente o programa com a específica finalidade de atingir dados ou obter alguma vantagem ilícita, como bem aponta Sydow (SYDOW, 2015, p. 122).

3.4.1.4 Engenharia Social e Scamming

O *scamming* é gênero da modalidade delitiva que se utiliza do meio digital para obter alguma vantagem sobre a vítima, abarcando diversas espécies de condutas tais como o *phishing*, o estelionato e o *pharming*. Também chamado de truque de confiança, o *scamming* é o delito pelo qual o ofensor e o ofendido se comunicam de forma direta ou indireta, sendo que o primeiro tenta persuadir o segundo a praticar alguma ação, geralmente a entrega de informações pessoais ou a transferência de valores econômicos (SYDOW, 2015, p. 126). Quando praticadas no meio digital, essas ações recebem o nome de engenharia social (ou engenhosidade social), como conceitua Marcelo Crespo:

> O que se de denominou recentemente engenharia social há muitos anos já se chama ardil ou artifício fraudulento para o Direito Penal. Entende-se como engenharia social todo método de mascarar a realidade para explorar ou enganar a confiança de uma pessoa detentora de dados importantes a que se quer ter acesso. É o artifício intelectual para acessar informações sigilosas.
> [...] a engenharia social é arma para que se consigam informações sigilosas importantes, mas o faz sempre mediante artifício ou ardil, de forma sub-reptícia (CRESPO, 2011, p. 82).

As ações que pretendem explorar as vulnerabilidades das vítimas no ciberespaço têm o costume de see veiculadas através de e-mails ou sites atrativos que funcionam como verdadeiras

iscas, oferecendo vantagens ou atiçando a curiosidade do usuário. Entre essas ações há diversas categorias, como os esquemas de enriquecimento rápido, que prometem altas quantias de dinheiro para o usuário através de supostos sorteios que, para o recebimento do prêmio, exigem um depósito ou pagamento de taxas, ou ainda os esquemas que envolvem produtos falsamente valiosos, conhecidos como *gold-brick schemes*, que são ações com um duplo caráter lesivo, pois alguém oferece um produto com uma qualidade prometida, mas que, após o pagamento e a entrega, esse material se mostra falso (SYDOW, 2015, p. 126).

Além dos esquemas já citados, existe a recorrente modalidade em que sites de conteúdo pornográfico, por ter um elevado potencial atrativo proveniente do oferecimento de fotos e vídeos sobre o tema, são utilizados como iscas para usuários que, a fim de satisfazer seus desejos, são levados a páginas ou fornecem dados pessoais que permitem que o delinquente possa prosseguir na sua conduta, obtendo informações sensíveis que permitem que este pratique extorsões. Com a posse desses dados, o criminoso digital passa a exigir vantagem do usuário-alvo para, como exemplo, não levar a público uma situação de exposição, como uma preferência sexual, uma foto íntima, relações extraconjugais ou até mesmo extratos bancários contendo transações ilegais.

O principal exemplo de engenharia social é o *phishing* (ou *phishing scam*) que consiste na ação do autor que se faz passar por representante de alguma pessoa jurídica, igreja, ONG ou até mesmo entidades governamentais para obter a confiança do usuário e, posteriormente, induzi-la a fornecer informações sensíveis como número do cartão de crédito, senhas, dados de contas bancárias, ou, ainda, instigar a baixar e executar arquivos que permitam a futura subtração de dados ou acesso não autorizado ao sistema da vítima (CRESPO, 2011, p. 83).

Segundo Spencer Sydow, os principais golpes aplicados no Brasil são aqueles que envolvem:

> a) a alegação de que um documento do usuário foi cancelado (geral- mente CPF ou título de eleitor) e que ele deve informar uma ampla quantidade de dados e números pessoais; b) mensagens informando que o usuário deve pagar um boleto anexado para limpar seu nome, tendo-se em vista que está constante na lista de maus pagadores; c) com altíssima incidência, e-mails de bancos em que o usuário é remetido, ao clicar na mensagem, a sites-espelho, idênticos aos verdadeiros, mas fraudulentos e hospedados em servido- res fora do país, em que se solicitam dados do cartão de credito, senhas, números de segurança etc., para que possa haver saques, pagamentos e transferência; d) o envio de mensagens sentimentais que buscam tocar os leitores de um problema aparentemente real – inclusive com fotografias – como, por exemplo, uma criança que precisa de algum transplante, jovens que precisam de contribuições para continuar seus estudos e até mesmo falsas ONGs e falsas igrejas solicitando contribuições; e) links para que o usuário acesse sites de seu interesse etc. (SYDOW, 2015, p. 128).

Com isso, é possível perceber o quanto grande parte dos usuários está sujeita a ser vítima da prática de *phishing*, uma vez que os autores, cada vez mais ardilosos, induzem seus alvos a

cederem informações pessoais muitas vezes levados por um desejo de ajudar alguma causa, ou mesmo para satisfazer alguma fantasia, acabam sendo vítimas de crimes como o estelionato.

3.4.1.5 Interceptação de e-mails

A interceptação de e-mail representa a conduta de impedir-se que a mensagem enviada pelo remetente, através de correio eletrônico, seja recebida pelo seu destinatário. Segundo Spencer Toth Sydow, este delito só pode ocorrer por dois motivos, principalmente: "a) as mensagens são normalmente enviadas em mecanismos de proteção; e b) não há mecanismos/autoridades intermediadores que garantam a chegada correta das mensagens a seus destinos" (SYDOW, 2015, p. 133).

A Constituição da República Federativa do Brasil (BRASIL, 1988) consagrou em seu rol de direitos fundamentais a inviolabilidade das comunicações em geral. Porém, não de forma absoluta, uma vez que é autorizada, mediante ordem judicial, a interceptação telefônica que possa contribuir com a investigação policial.

Nesse sentido, a Lei nº 9.296/96 (BRASIL, 1996) que regulamenta as interceptações telefônicas autorizou, eu seu artigo 10, a interceptação de comunicação também em sistemas de informática e telemática, prevendo a tipificação da conduta de quem realiza as ingerências sem a devida autorização judicial ou em desconformidade com aquela já concedida (CRESPO, 2011, p. 86). Entretanto, por essa regulamentação ter sido feita através de lei ordinária, surgiram questionamentos sobre a possibilidade da Constituição (BRASIL, 1988) autorizar a ingerência nas comunicações que não sejam de natureza telefônica, por assim estar delimitado no seu texto:

> Art. 5º [...]
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

Outro questionamento é em relação ao termo "interceptar" que, segundo Sydow, significa colocar-se entre, na qualidade de obstáculo, ou seja, impedir que o curso dos dados se desenvolva, de modo a impedir que o destinatário obtenha acesso a eles (SYDOW, 2015, p. 134). Porém, conforme já explicado nos capítulos dedicados ao funcionamento da internet, quando se envia um e-mail, a rede fraciona a mensagem em diferentes pacotes de dados que vão ser remetidos quantas vezes forem necessárias até que seu destino seja atingido, de modo tal que todos os pacotes ao serem recebidos, são devidamente convertidos e reagrupados no destinatário.

Com isso, a mero acesso e leitura dos dados referentes a um e-mail por parte de um terceiro pode não impedir que o destinatário também receba a informação em uma remessa de pacotes de dados seguinte, fazendo com que a mensagem atinja seu destino perfeitamente. Dessa forma, haveria o afastamento da figura do artigo 10 da Lei nº 9.296/96 (BRASIL, 1996), que remete ao tipo apenas quando a interceptação impedir que a mensagem atinja seu destinatário (SYDOW, 2015, p. 134).

Marcelo Crespo afirma estar superada a discussão sobre a constitucionalidade da inclusão dos meios informáticos e telemáticos de comunicação no rol do artigo 5º, inciso XII, da Constituição da República (BRASIL, 1988), tendo em vista que a necessidade de se incriminar tal conduta vem do cumprimento dos preceitos da Convenção de Budapeste de 2001. Não há dúvidas de que este delito deva ser fortemente coibido, tendo em vista que cada vez mais depende-se dos meios digitais de comunicação para trato diário das relações pessoais e profissionais. Entretanto, para que sejam afastadas discussões doutrinárias como as supracitadas, o autor recomenda que a redação típica se apresente de forma diversa (CRESPO, 2011, p. 87).

3.4.2 Crimes Digitais Impróprios

Os crimes digitais impróprios são aqueles delitos que já encontram tipificação no ordenamento jurídico pátrio, mas que passaram a ser cometidos através do auxílio do meio tecnológico. Nesse sentido, de acordo com Emanuel Gimenes, são as condutas nas quais o computador é usado como instrumento para execução do delito, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados) (GIMENES, 2013, p. 09).

Diferentemente dos crimes digitais próprios, nessa modalidade delitiva, a norma penal não exige como condição para sua ocorrência o emprego de dispositivo informático, que surge de forma acidental, apenas como um meio de execução do delito (RONCADA, 2017, p. 177).

Por serem praticados por meio da tecnologia, alguns desses crimes acabam ganhando grande repercussão midiática, uma vez que geram sensações de insegurança e medo através de um "ameaça invisível", como fora discutido nos capítulos dedicados à sociedade de risco.

Entre os exemplos dos crimes digitais impróprios estão os crimes contra a honra, de ameaça, falsidade ideológica e estelionato. Como destaca Marcelo Crespo, nada mais são que os antigos delitos já tipificados no Código Penal (BRASIL, 1940), mas sob outro *modus operandi* (CRESPO, 2011, p. 88). Os delitos mais recorrentes envolvendo os meios digitais são:

a) Ameaça: crime previsto no artigo 147[2] do Código Penal (BRASIL, 1940) que consiste em intimidar ou amedrontar alguém mediante a promessa de causar-lhe algum mal injusto e grave. No meio digital, tem incidido de forma constante principalmente nas mais diferentes redes sociais.

b) Incitação e apologia ao crime: o Código Penal (BRASIL, 1940), no artigo 286[3], prevê punição para aqueles que incitam a prática de crimes, estimulando outras pessoas a praticarem algum delito. Já o artigo 287[4] considera como infração penal fazer apologia a um fato criminoso ou a autor de crime. Com isso, discussões em fóruns e redes sociais com tal conteúdo podem ser consideradas como ilícitos penais.

c) Violação de direitos autorais: entre os mais recorrentes estão os delitos de pirataria, que consiste em copiar ou vender produto sem a devida autorização do detentor dos direitos, previstos no artigo 184[5] do Código Penal (BRASIL, 1940). Segundo Crespo, além da pirataria, o uso de marcas e documentos encontradas com o auxílio da internet também podem configurar como um crime. A lei brasileira protege a propriedade intelectual dividindo-a em dois grandes ramos: a propriedade industrial, que faz referência às patentes, ao desenho industrial e às marcas; e os direitos autorais, referentes aos *softwares*, bancos de dados e composições artísticas (CRESPO, 2011, p. 89).

d) Falsidade ideológica e falsa identidade: no primeiro caso, há inserção de dados falsos ou omissão de algo que deveria constar, em documentos públicos ou particulares, com a intenção de prejudicar direito, criar obrigações ou alterar a verdade sobre fato juridicamente

---

[2] Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:
Pena - detenção, de um a seis meses, ou multa (BRASIL, 1940).
[3] Art. 286 - Incitar, publicamente, a prática de crime:
Pena - detenção, de três a seis meses, ou multa (BRASIL, 1940).
[4] Art. 287 - Fazer, publicamente, apologia de fato criminoso ou de autor de crime:
Pena - detenção, de três a seis meses, ou multa. (BRASIL, 1940).
[5] Art. 184. Violar direitos de autor e os que lhe são conexos:
Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa [...]
§ 2º Na mesma pena do § 1o incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
§ 3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:
Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa [...] (BRASIL, 1940).

relevante, como prevê o artigo 299[6] do Código Penal (BRASIL, 1940). No caso seguinte, presente no artigo 307[7] do mesmo diploma legal, uma pessoa se faz passar por quem ela não é, utilizando-se de dados e até mesmo de senha de um terceiro, em proveito próprio ou alheio, ou até para causar algum dano. A prática de tais delitos através do meio digital se dá, principalmente, com o surgimento e popularização de perfis falsos, conhecidos como *fakes*, que são usuários que se passam por outros, na maioria das vezes, famosos ou detentores de cargos importantes.

e) Crimes contra a honra: são os delitos de calúnia, difamação e injúria, presentes nos artigos 138, 139 e 140[8], respectivamente, do Código Penal (BRASIL, 1940). Honra se refere às qualidades físicas, morais e intelectuais de um indivíduo, fazendo-o ser respeitado no meio social e que diz respeito, ainda, à sua autoestima (CRESPO, 2011, p. 90). Nessa modalidade delitiva, os criminosos, motivados pelo anonimato, cometem os crimes através de chats, blogs, e-mails, dentre outros meios de postagem digital. Assim como nos crimes de ameaça, possuem incidência maior nas redes sociais, como, por exemplo, quando há divulgação de informações falsas que prejudicam a reputação de um terceiro.

f) Pornografia infantil: este crime muitas vezes é erroneamente chamado de "pedofilia", referindo-se aos atos de divulgação e armazenamento de imagens com conteúdo pornográfico envolvendo crianças e adolescentes. Termo este que também é comumente atribuído às relações sexuais de maiores com menores de idade. Entretanto, Marcelo Crespo ressalta que, tecnicamente, a pedofilia se refere a um transtorno da preferência sexual, uma parafilia (um transtorno sexual recorrente), não havendo um crime específico no Brasil com esta

---

[6] Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:
Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, se o documento é particular (BRASIL, 1940).

[7] Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave (BRASIL, 1940).

[8] Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
Pena - detenção, de seis meses a dois anos, e multa.
§ 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
§ 2º - É punível a calúnia contra os mortos [...]
Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
Pena - detenção, de três meses a um ano, e multa [...]
Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
Pena - detenção, de um a seis meses, ou multa.
[...]
§ 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:
Pena - reclusão de um a três anos e multa (BRASIL, 1940)

denominação, apesar de diversas situações envolvendo a exposição da sexualidade infantil encontrarem sanções penais (CRESPO, 2011, p. 90). O delito que se pretende aduzir é o presente nos artigos 240, 241, 241-A, 241-B e 241-C[9] da Lei nº 8.069/1990 que dispõe sobre o Estatuto da Criança e do Adolescente (BRASIL, 1990) e pune a produção, reprodução, venda, exposição, oferecimento e armazenamento, por qualquer meio, de fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

[9] Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
§ 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena [...]
Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
§ 1º Nas mesmas penas incorre quem:
I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
§ 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.
Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
§ 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
§ 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
I – agente público no exercício de suas funções;
II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
§ 3º As pessoas referidas no § 2o deste artigo deverão manter sob sigilo o material ilícito referido.
Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo (BRASIL 1990).

g) Racismo e preconceito: o crime de racismo[10], previsto na Lei nº 7.716/1989, (BRASIL, 1989) remete à prática, indução ou incitação de discriminação ou preconceito por motivo de raça, cor, etnia, religião ou procedência natural, mas de forma geral, não individualizada. Também são passíveis de sanção penal, de acordo com a referida lei, as condutas que impeçam acesso a lugares públicos, empregos, meios de transporte, clubes, bares, restaurantes, sempre por conta de preconceito de raça, cor, etnia, religião ou procedência nacional (CRESPO, 2011, p. 91). Com isso, postagens e discussões em grupos e comunidades nas redes sociais que disseminam tais ideias são consideradas condutas criminosas.

O rol apresentado acima traz apenas alguns dos principais delitos sofridos pelos usuários na rede mundial de computadores. É mister observar, também, que os crimes digitais impróprios também possuem grande incidência no âmbito empresarial, causando prejuízos significativos por conta de ataques de grupos especializados. O desenvolvimento tecnológico coloca à disposição das empresas diversas facilidades através de *softwares* que tendem a potencializar suas operações. Entretanto, com a dependência cada vez maior dessas tecnologias, novos riscos são gerados e a possibilidade do cometimento de crimes empresariais através da internet se torna maior. Entre os principais delitos sofridos pelas empresas estão: o vazamento de informações, a cópia ilegal de dados, o desvio de clientes, uso indevido da marca, pirataria e acesso a informações sigilosas para exploração de falhas de segurança e sabotagem de fluxo de dados.

---

[10] Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
Pena: reclusão de um a três anos e multa.
§ 1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo.
Pena: reclusão de dois a cinco anos e multa.
§ 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza.
Pena: reclusão de dois a cinco anos e multa.
§ 3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência:
I - o recolhimento imediato ou a busca e apreensão dos exemplares do material respectivo;
II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;
III - a interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores.
§ 4º Na hipótese do § 2º, constitui efeito da condenação, após o trânsito em julgado da decisão, a destruição do material apreendido (BRASIL, 1989).

3.5 DOS SUJEITOS ATIVOS DOS DELITOS

Os crimes digitais representam um novo paradigma no Direito Penal, em que Estados e organizações internacionais têm buscado compreender a criminalidade informática com suas peculiaridades (CRESPO, 2011, p. 94) sendo que, as discussões a respeito dos sujeitos ativos, estão entre os principais questionamentos.

Como fora visto no presente trabalho, um dos grandes problemas relacionados aos crimes digitais está no fato de ser difícil identificar quem seja o autor dos crimes, devido à extraterritorialidade dos delitos e a volatilidade do material probatório. Entretanto, apesar de toda a complexidade, é natural que a doutrina tente traçar um perfil médio para os criminosos que atuam na rede mundial de computadores.

A partir do momento em que se parte do pressuposto de que para o cometimento de grande parte dos crimes digitais há a necessidade de instrumentos informáticos, é preciso levar em conta que, no Brasil, a aquisição destes dispositivos exige algum poder aquisitivo. Também, para seu manuseio, é necessário que se desenvolvam habilidades de programação e manipulação de dados, além de ser importante a compreensão da língua inglesa para o amplo uso dos sistemas (SYDOW, 2015, p. 142).

Diante disso, apesar de ser difícil dizer que há um perfil biológico para um criminoso digital, é possível concluir que somente pessoas com certo poder aquisitivo e com certo grau de instrução em língua estrangeira e linguagem de computação são capazes de se mostrarem proficientes para a prática de boa parte dos delitos que exigem uma maior capacidade técnica, como afirma Spencer Toth Sydow (2015, p. 142).

Entre os autores que buscam fazer um estudo criminológico sobre esses sujeitos ativos, há quem busque em teorias subculturais e de *social learning* (aprendizagem social) a explicação para o perfil singular desses criminosos, como Tulio Lima Vianna que aduz:

> [...] o fato de uma pessoa tornar-se criminosa é determinado, em larga medida, pelo grau relativo de frequência e de intensidade de suas relações com os dois tipos de comportamento. Isso pode ser denominado processo de associação diferencial. Prega-se, por essa teoria, que a delinquência sistemática é aprendida em associação direta ou indireta com aqueles que já cometeram ilícitos anteriormente. Com relação aos crimes digitais próprios, antes de serem praticados, precisam ser aprendidos. Como invadir um sistema informático? Não se trata de ação comumente praticada pelas pessoas que encontramos no nosso cotidiano. Assim, o aprendizado é essencial. E uma importante observação é que, por mais que se diga autodidata, é preciso conhecimento técnico que depende da cultura cyberpunk. Explica-se: uma singela busca pelo termo "hacker" em um site de busca vai apresentar uma enormidade de páginas repletas de fóruns, dicas, técnicas que ensinam os passos iniciais para se tornar um delinquente informático. Predomina a ideia de que o conhecimento gera conhecimento, de modo que aparentemente não se propõe oferecer técnicas a alguém que não ofereça nada em troca (VIANNA, 2001, p. 27).

Certo é que, apesar de a criminalidade digital não exigir indivíduos com características particulares – afinal, diversos delitos podem ser perpetrados com pouca habilidade informática, como os crimes digitais impróprios –, ainda assim prevalece a exigência de que o delinquente de alto gabarito possua uma boa quantidade de conhecimento, especialmente naquelas condutas que envolvam programação e intrusão (SYDOW, 2015, p. 143). É nesse patamar que se enquadram os *hackers*, figuras conhecidas como sendo sempre os "vilões" da internet, embora haja uma série de denominações para identificar os autores das condutas ilícitas como se verá nos capítulos seguintes.

3.5.1 Os *Hackers*

O termo *"hacker"* se originou nos laboratórios de computação do MIT (Massachussets Institute of Technology) na década de 1970 (CRESPO, 2011, p. 95) e, desde então, é utilizado para representam aqueles indivíduos que possuem profundos conhecimentos de informática.

Entretanto, com o passar do tempo, os *hackers* passaram a ser injustamente conhecidos como sendo "criminosos virtuais", apesar de nem todo *hacker* desejar o prejuízo alheio, pois, em sua grande maioria, são usuários que dedicam boa parte do seu tempo a estudar e modificar *hardwares* e *softwares* com o fim de desenvolver novas funcionalidades no mundo da computação. Isso significa que, apesar de serem noticiados como "ameaças" no mundo digital, trata-se do oposto: os *hackers*, em sua maioria, utilizam seus conhecimentos de forma benéfica, buscando desenvolver ferramentas capazes de impedir o cometimento de delitos digitais.

O termo *hacker* é gênero no qual são espécies os *White Hats, Grey Hats* e os *Black Hats* que serão vistos a seguir.

3.5.2 Os *White Hats*, *Grey Hats* e *Black Hats*

Os termos vêm dos antigos filmes de faroeste, onde heróis e vilões eram diferenciados entre si dependendo da cor dos seus chapéus. Essa foi a forma utilizada para se referir aos "bons" e aos "maus" *hackers*. As expressões significam, em tradução livre, "chapéu branco", "chapéu cinza" e "chapéu preto", e indicam, respectivamente, os bons e os maus, aqueles que fazem o bem e os que praticam crimes (CRESPO, 2011, p. 95).

Dessa forma, os *White Hats*, também chamados de "éticos", seriam aqueles *hackers* que não possuem a intenção de violar algum bem jurídico, mas sim utilizar de suas habilidades para detectar erros e falhas que possam comprometer a segurança de alguma rede ou dispositivo informático. Esses usuários são contratados por empresas para ocuparem cargos de analistas de sistemas, especialistas em tecnologia da informação, entre outros.

Os *Grey Hats* simbolizam aqueles usuários que ora praticam atitudes solidárias e cautelosas, ora violam bens jurídicos (SYDOW, 2015, p. 50). Um exemplo comum são os *hackers* que, a princípio, mesmo agindo com boa intenção, realizam testes de segurança em alguma determinada rede de computadores antes de obter a devida permissão dos envolvidos.

Em sentido oposto estão os *Black Hats*, aqueles *hackers* especializados em praticar condutas lesivas que trazem prejuízos reais para os ofendidos, sendo considerados tão nocivos quanto os *Crackers*.

3.5.3 Os *Crackers*

O *Cracker* é aquele indivíduo que, utilizando de seus profundos conhecimentos de informática, procura "quebrar" (*crack)* sistemas de segurança para invadi-los a fim de obter alguma vantagem indevida. O termo utilizado para denominar esses criminosos foi escolhido pelos próprios *hackers*, por volta de 1985, com o objetivo de diferenciar, para a mídia e para os leigos, as atividades praticadas por cada um dos grupos.

É importante frisar que esses são os verdadeiros criminosos digitais, embora não sejam os únicos. Estes são responsáveis pela criação dos *cracks*, que são ferramentas utilizadas na quebra da ativação de um *software* comercial, facilitando a pirataria. São definidos como uma grande ameaça econômica na rede mundial de computadores, uma vez que são os responsáveis pelas práticas de fraudes bancárias e eletrônicas, furto de dados, golpes, entre outros (ARIMURA, 2016).

3.6 TEMPO E LOCAL DO CRIME

Determinar o exato momento da ocorrência de um delito é de fundamental importância na aplicação da lei penal para a solução de conflito temporal de normas, avaliação da imputabilidade do agente, aplicação de prescrição e análise das circunstâncias do crime (VIANNA, 2001, p. 96-97).

Entre as teorias que buscam estabelecer qual o momento do crime estão: a teoria da atividade, também chamada de teoria da ação, que diz estar consumado o delito no momento da execução da conduta; a teoria do resultado ou do evento, que leva em conta o momento de seu resultado; e a teoria mista ou unitária, que considera que o crime é cometido tanto no momento da conduta quanto no de seu resultado.

O Código Penal brasileiro (BRASIL, 1940), em seu artigo 4º, adotou a teoria da ação ou da atividade ao estabelecer que "considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado" (BRASIL, 1940). A opção pela teoria

da atividade visa impedir o absurdo de uma conduta, praticada licitamente durante o prazo de vigor de uma lei, poder ser considerada crime, em razão de o resultado vir a produzir-se sob o império de outra lei incriminadora (BITENCOURT, 2017, p. 244).

Importante ressaltar também que, nos crimes digitais de forma geral, muitas vezes o período de tempo entre a ação e o resultado é relativamente grande. Na já citada conduta de inserção de *malware*, por exemplo, a inserção de código malicioso ou sabotagem de um dispositivo informático alheio pode gerar resultados apenas tempos depois dessa inserção, quando o usuário acessar determinada página ou abrir um arquivo infectado.

Também existe a possibilidade de que o acesso não autorizado a sistemas computacionais seja praticado como um delito permanente. Para isso, basta que o agente, ao obter esse acesso, troque a senha do sistema invadido e impeça o acesso dos usuários autorizados. Nesse caso, a ação e o resultado, prolongar-se-ão até que o legítimo proprietário consiga reaver o controle do sistema (VIANNA, 2001, p. 98).

Em relação ao lugar do cometimento do crime, o Código Penal (BRASIL, 1940), no artigo 6º, consagrou a teoria pura da ubiquidade, também chamada de mista ou unitária, ao considerar "praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado" (BRASIL, 1940). Com essa teoria, evita-se que ocorram conflitos negativos de jurisdição e soluciona-se a questão do crime à distância, em que a ação e o resultado realizam-se em lugares distintos. Caso haja uma eventual duplicidade de julgamento, esta é superada pela regra presente no artigo 8º do mesmo código, que estabelece a compensação de penas, como uma modalidade especial de detração penal (BITENCOURT, 2017, p. 254).

Com isso, caso um crime digital como a intrusão informática seja cometido através da internet, e o agente se encontra em um país diferente do da vítima, a aplicação dessa norma se torna demasiadamente simples, desde que em ambos os países esse delito já se encontre penalmente tipificado. Como exemplo, nesse caso, pode-se tanto punir o agente que acessar a partir de um computador localizado no Brasil um sistema localizado no estrangeiro, quanto no caso de uma vítima no Brasil sofrer um ataque proveniente de um computador localizado em outro país (VIANNA, 2001, p. 99).

Entretanto, quando a conduta é típica em apenas um dos países, a solução se torna bem mais complexa. É plenamente possível de acontecer que a conduta seja típica no país em que o comando é dado, porém atípica no país onde acontece o resultado fático. Ou, ao contrário, ser atípica no país da ação e típica no do resultado.

Renato Leite Monteiro também levanta questionamentos sobre esta questão ao trazer o exemplo de um e-mail contendo um artefato malicioso que seja mandado de um determinado país para vários destinatários, que irão executá-los em locais diferentes, causando danos em vários países. Nesse exemplo, atos foram praticados em diversos locais com resultados que puderem ser percebidos em diferentes jurisdições (MONTEIRO, 2010, p. 48).

Em termos gerais, Monteiro afirma não haver critérios seguros que determinem em qual medida o local da prática de um delito ou local em que esse delito se consuma deva ser considerado como o local exato do crime, pois várias teorias são adotadas por diferentes países, e cada um tem competência para determinar se tem ou não autoridade para processar o delito em seu território. Os tratados internacionais também podem discorrer sobre a questão, em nível de cooperação, para que os atos delituosos sejam tratados onde o dano resultante for maior, ou onde possam ser encontradas melhores condições de investigação, para que a colheita de provas seja feita de forma mais adequada para serem fornecidas às demais jurisdições, que tomarão as medidas que julgarem necessárias (MONTEIRO, 2010, p. 49).

Em sentido contrário, Tulio Lima Vianna ressalta que a solução para essa questão deve partir do pressuposto de que as normas de caráter penal devam ser interpretadas sempre de forma restritiva. Com isso, caso haja duas interpretações possíveis e perfeitamente lógicas para um mesmo fato jurídico, o intérprete tem o dever de optar por aquela que menos restringir a liberdade do cidadão (VIANNA, 2001, p. 100).

> Ora, o art. 6º do CP, traz em sua redação a palavra "crime" e não "ação" ou "conduta". Se o crime será considerado praticado tanto no local da conduta quanto no lugar do resultado, necessário se faz que, para ser considerado crime, seja crime tanto no local da conduta quanto no do resultado (VIANNA, 2001, p. 100).

Já que a própria norma estabelece a teoria ubiquidade como característica do delito, ou seja, a teoria de que será crime no lugar da conduta e no do resultado, deve-se entender que só será crime se este for fato típico no lugar da conduta e no local do resultado. É fundamental, portanto, que a conduta esteja tipificada em ambas as legislações, sob pena de ofensa direita do princípio da legalidade (VIANNA, 2001, p. 100).

Para as condutas praticadas no Brasil, que são tipificadas no ordenamento jurídico brasileiro, mas que produzem resultados em países onde não são consideradas ilícitas, também se aplica o princípio da exclusiva proteção a bens jurídicos. Caso um Estado soberano entenda que a proteção de determinado bem jurídico não seja necessária, o Brasil não pode querer protegê-lo, quando o resultado ocorra nas fronteiras desse país, sob pena de violação do artigo

4º, inciso III, da Constituição da República Federativa do Brasil (BRASIL, 1988) (VIANNA, 2001, p. 101).

3.7 JURISDIÇÃO E COMPETÊNCIA

A internet por essência não possui fronteiras e assim foi projetada para que fosse acessada de qualquer parte do mundo. Isso quer dizer que fora criada uma realidade virtual sem barreiras físicas das delimitações territoriais dos países. As relações se multiplicaram exponencialmente com essa ferramenta que, apesar de ter um caráter global, esbarra em diferenças culturais refletidas nas variadas legislações. Um mesmo conteúdo, por exemplo, pode ter diversos tratamentos em diferentes países, sendo considerado legal em um e ilegal em outro, como visto no capítulo anterior (DOMINGOS; RÖDER, 2017, p. 62).

Devido à possibilidade de um crime digital ser cometido em mais de um país ou ser praticado em um e gerar resultado em outro, a sua investigação se torna mais complexa, uma vez que aumenta a dificuldade de se precisar o local onde estão as provas a serem angariadas e de se estabelecer qual a jurisdição responsável.

Quando se fala de jurisdição, refere-se, junto com o poder de legislar e governar, à expressão da soberania de um Estado. Poder este que é único, mas tem sua aplicação, por uma questão de ordem prática, repartida entre variados órgãos do corpo estatal (VIANNA, 2001, p. 101-102). Mirabete e Fabbrini ensinam que:

> Como poder soberano do Estado, a jurisdição é uma e, investido do poder de julgar, o juiz exerce a atividade jurisdicional. Sendo evidente, porém, que um juiz não pode julgar todas as causas e que a jurisdição não pode ser exercida ilimitadamente por qualquer juiz, o poder de julgar é distribuído por lei entre os vários órgãos do Poder Judiciário, através da competência. A competência, é assim, a medida e o limite da jurisdição (MIRABETE; FABBRINI, 2015, p. 136).

A competência é, portanto, o limite do poder de cada órgão jurisdicional. Vianna destaca que a distribuição dos poderes jurisdicionais do Estado se dá de acordo com a natureza do crime praticado, com a qualidade das pessoas incriminadas e com o local em que o delito foi praticado ou se consumou, ou ainda, com o local da residência de seu ator. Neste trabalho, importam a fixação da competência em razão da matéria e em razão do local do delito que serão melhor aprofundadas (VIANNA, 2001, p. 102).

Embora a internet pareça uma rede imaterial, seu funcionamento está condicionado à existência de uma infraestrutura real. Para que um usuário possa acessá-la, são necessários provedores de conexão de rede, que atribuem ao usuário um número IP (*internet Protocol*) utilizado para ingressar no ciberespaço. O conteúdo a ser acessado nessa plataforma, incluindo

os serviços de e-mail, redes sociais, ou outras formas de comunicação via internet, dependem justamente dessa estrutura disponibilizada pelos provedores que, a partir de então, passam a deter as informações referentes aos passos que os usuários percorrem na rede, como históricos de navegação, postagens e comunicações (DOMINGOS; RÖDER, 2017, p. 62).

São essas informações que as empresas provedoras de internet detêm que permitem, de forma precisa, desvendar um crime digital ou obter um material probatório para a elucidação de um crime do mundo material. Com isso, tem-se gerado por parte dos usuários e do Poder Judiciário, diversos pedidos para que estes sejam disponibilizados no curso de uma persecução penal, como será aprofundado no capítulo referente ao Marco Civil da Internet.

Uma vez que essas empresas podem possuir sede física em um país, mas armazenar seus dados em servidores em qualquer local do mundo, depara-se com a dificuldade de se estabelecer qual o local que teria competência para decidir acerca do fornecimento de tais informações. Ademais, cada ordenamento jurídico possui uma percepção própria a respeito da devida proteção da privacidade, o que reflete nas diferenças legislativas sobre os requisitos para o fornecimento legal de dados e informações de usuários. Somando-se a isso, tem-se a volatilidade da prova no meio digital, já que a enorme quantidade de conteúdos sendo transmitidos pela rede mundial de computadores faz com que a sua manutenção pelos provedores seja a menor possível, devidos aos elevados custos gerados pelo seu armazenamento (DOMINGOS; RÖDER, 2017, p. 63).

De acordo com Bertrand La Chapelle e Paul Fehlinger, existem quatro possíveis critérios que podem ser utilizados para definir qual a lei aplicável na obtenção de dados digitais, sendo eles: a lei do local em que está o usuário, do qual se pretende obter os dados; a lei do local onde estão os servidores que armazenam os dados; a lei do local de incorporação da empresa que presta o serviço; e a lei do local dos registradores de onde o domínio foi registrado (LA CHAPELLE; FEHLINGER, 2016).

Entretanto, todas as possíveis soluções apresentam obstáculos e podem entrar em conflito com as regras de aplicação da lei penal de cada ordenamento jurídico. A primeira opção, que obrigaria os provedores de internet a fornecerem informações nos termos da legislação do local onde está o usuário, pode se deparar com a complexa situação em que este usuário esteja em um determinado país, cometendo uma infração pela internet e produzindo resultado típico no país que necessita dos seus dados para investigação, mas utilizando-se de um provedor de internet com sede em um terceiro país (DOMINGOS; RÖDER, 2017, p. 64).

O segundo critério, que pretende utilizar as leis do local onde estão os servidores que armazenam os dados, e que tem gerado diversas discussões pelos provedores de internet, sob a

alegação de precisarem cumprir as leis de proteção de dados e privacidade, impõe uma difícil tarefa ao operador do Direito que necessita da prova digital. Isso ocorre devido à possibilidade de as informações estarem duplicadas em diversos servidores espalhados simultaneamente pelo mundo, ou até fragmentadas, armazenadas em locais distintos. Com isso, seria tornaria inviável de estabelecer precisamente o local em que determinado dado imprescindível para uma investigação criminal estaria armazenado (DOMINGOS; RÖDER, 2017, p. 65).

A terceira opção, que versa sobre a utilização da lei da região em que a empresa foi incorporada também tem seus obstáculos, quando o local onde o serviço está sendo prestado não coincidir com aquela da incorporação, uma vez que estariam sendo aplicadas leis estrangeiras no território nacional. Igual consequência é gerada ao se adotar a quarta opção, que trata da aplicação da legislação do país de origem do registrador de onde o domínio foi registrado, já que também resulta em uma aplicação de leis estrangeiras a fatos que possuem impacto no território nacional (DOMINGOS; RÖDER, 2017, p. 65).

Em suma, Fernanda Domingos e Priscila Röder ressaltam que todos os critérios apresentados por La Chapelle e Fehlinger, ao assumirem que, para o fornecimento de dados digitais, as empresas provedoras de internet devem obedecer aos parâmetros legais de variadas jurisdições do local onde os fatos ocorreram ou tiveram o serviço prestado, acarretam na necessidade de pedidos de cooperação internacional (DOMINGOS; RÖDER, 2017, p. 66).

3.7.1 Competência no ordenamento jurídico brasileiro

A Constituição da República Federativa do Brasil (BRASIL, 1988), em seu artigo 109, inciso IV, fixou a competência dos juízes federais em razão da matéria, isto é, da natureza dos delitos praticados, ao estabelecer que

> os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral (BRASIL, 1988).

Isto posto, Tulio Lima Vianna julga necessário ressaltar que a internet é um serviço público de telecomunicação e, como tal, se sujeita à regulamentação da ANATEL (Agência Nacional de Telecomunicações), sendo incontestável o interesse da União em protegê-la juridicamente. Dessa forma, os processos relativos a intrusão informática, quando praticadas através da internet, deverão ser conhecidos e julgados pela Justiça Federal (VIANNA, 2001, p. 102-103).

Em relação à hipótese prevista no artigo 109, inciso V, da Constituição da República Federativa do Brasil (BRASIL, 1988), ou seja, “os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente” (BRASIL, 1988), é preciso se atentar que as condutas tipificadas no artigo 241 do Estatuto da Criança e do Adolescente (BRASIL, 1990) e também o crime de racismo tipificado na Lei nº 7.716 de 5 de janeiro de 1989 (BRASIL, 1989), têm previsão em convenções internacionais de direitos humanos. Uma vez que a consumação do delito normalmente ultrapassa as fronteiras nacionais quando estes são praticados através da internet, a competência para julgamento também pertence à Justiça Federal (KUROKAWA et al., 2006, p. 41). Por outro lado, caso o agente não se utilize da internet para obter acesso não autorizado ao sistema computacional alheio, a competência passa a ser da Justiça Comum.

> A competência da Justiça Federal para processar e julgar a divulgação na internet de material pornográfico envolvendo crianças e adolescentes já foi reconhecida por quatro Tribunais Regionais Federais (1ª, 3ª, 4ª e 5ª Regiões) brasileiros. Esses acórdãos reconheceram presente o requisito da extraterritorialidade, uma vez que a visualização de imagens de pornografia infantil publicadas na internet pode, virtualmente, ocorrer em qualquer país do mundo (KUROKAWA et al., 2006, p. 41).

Diferentemente do Código Penal (BRASIL, 1940) – que adota a teoria pura da ubiquidade –, o Código de Processo Penal brasileiro (BRASIL, 1941), quanto à competência em razão do local da infração, aderiu à teoria do resultado. Assim, para se julgar o delito de acesso não autorizado a computadores, também chamado de intrusão informática, será fixada não pelo local onde foi originado o comando, mas sim, pela localização onde se encontra o sistema computacional invadido (VIANNA, 2001, p. 103).

Caso o sistema computacional esteja situado no Brasil, a competência, portanto, será do juízo deste local. Mas, se o comando partir de um sistema computacional no Brasil e resultar em um acesso não autorizado em computadores de outro país, a competência será do juízo do local onde foi dado este comando, aplicando-se o disposto no parágrafo 1º do artigo 70 do Código de Processo Penal brasileiro (BRASIL, 1941) que dispõe que: “se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução” (BRASIL, 1941) (VIANNA, 2001, p. 103-104).

No mesmo sentido será fixada a competência nos casos de tentativa, quando, tendo sido dado o comando no território brasileiro, não tenha se consumado no estrangeiro por motivos alheios à vontade do agente. Assim, a competência também será do juízo do local em que foi

praticado o último ato de execução, conforme consta no *caput* do artigo 70 do Código de Processo Penal (BRASIL, 1941).

Entretanto, se o delito fora tentado em país estrangeiro e seus resultados seriam produzidos no Brasil, deve-se aplicar o disposto no parágrafo 2º deste mesmo artigo 70 do diploma legal que diz que: "quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir resultado" (BRASIL, 1941). Nesses casos, portanto, a competência será do juízo onde estiver localizado o sistema computacional que fora ameaçado pela tentativa proveniente de país estrangeiro (VIANNA, 2001, p. 104).

De acordo com Adriana Shimabukuro Kurokawa et al., para os outros delitos que não tenham sido abrangidos pelas hipóteses anteriormente expostas – como exemplo, os crimes contra a honra de particular praticados através da internet –, estes deverão ser investigados e processados no âmbito das Justiças Estaduais, já que o fato de um crime ter sido cometido através da INTERNET não basta para justificar a competência da Justiça Federal (KUROKAWA et al., 2006, p. 42).

Em relação à obtenção de provas digitais que estejam estabelecidas na rede mundial de computadores, o legislador brasileiro foi sensível ao considerar o caráter volátil desse material probatório, que necessita de celeridade para chegar ao domínio dos agentes de investigação e justiça, para propiciar o rápido e efetivo processamento dessa modalidade delitiva. Dessa forma, o legislador optou por firmar a jurisdição brasileira a partir do conceito de serviço prestado em território nacional, pois, apesar da internet ter como característica a falta de fronteiras físicas, o seu ponto de ligação com o mundo real ocorre em território existente e delimitado de um país (DOMINGOS; RÖDER, 2017, p. 81).

Com isso, Domingos e Röder acreditam não haver, até o presente momento, melhor maneira de garantir a efetividade das investigações e dos processos que não seja forçando as empresas provedoras de internet a cumprir diretamente ordens judiciais de entrega de provas digitais, para que se possa afirmar a soberania do Estado em que as atividades dos provedores ocorreram (DOMINGOS; RÖDER, 2017, p. 81).

O melhor caminho a ser seguido, portanto, é o do entendimento entre os Estados para que estes harmonizem suas legislações com o objetivo de possibilitar uma investigação mais célere e efetiva. O ordenamento jurídico brasileiro apresenta uma solução baseada em conceitos, princípios e práticas já reiteradas pelo direito pátrio, adaptando à contemporaneidade (DOMINGOS; RÖDER, 2017, p. 82). Contudo, enquanto não haja um tratado internacional único que pacifique essa questão, cabe aos provedores de internet, detentoras das provas

digitais, cumprirem a legislação do local onde estas oferecem seus serviços, colaborando de forma efetiva para o andamento das investigações e a solução de conflitos.

4 O INSTITUTO DA PROVA E OS CRIMES DIGITAIS

Além da já apontada diversidade de classificações dos crimes digitais e seus variados sujeitos ativos, outra característica importante dessa modalidade delitiva são as particularidades relativas às provas e à identificação de seus infratores, sendo esta a sua maior dificuldade no que tange à investigação criminal.

Os crimes praticados no ambiente digital, em grande parte das vezes, não deixam vestígios e, com a obscuridade da rede mundial de computadores, os autores desses delitos ficam à sombra do anonimato. A prova nos crimes digitais é frágil e volátil, mas merece um maior aprofundamento, como será feito a seguir.

4.1 PROVA E PROCESSO PENAL

Nos ensinamentos de Aury Lopes Jr, o processo penal seria um instrumento de retrospecção em que há uma tentativa de se reconstruir, de forma aproximada, um determinado fato (LOPES JR, 2017, p. 285). Dessa forma, é pelas provas que se faz a reconstrução desse fato passado, ou seja, do crime em questão.

O instituto da prova, dentro do direito processual, possui alguns princípios conceituais, que Rosemiro Pereira Leal aponta como sendo estes: o princípio da indiciariedade, ou seja, da existência de elemento sensível na realidade objetiva; princípio da idearidade, que se relaciona com a apreensão, somatização e transmissão do elemento de prova através do intelecto e, por último, o princípio da instrumentalidade, na qual a materialização gráfico-formal desses elementos se dá pelos meios intelectivos ou técnico-jurídicos permitidos. Como exemplo, o autor utiliza-se do instituto da perícia judicial que, sendo um meio de prova autorizado por lei, deve ser feito através de um perito, pela coleta intelectiva de elementos de prova existentes na realidade objetiva, sendo seu lado o instrumento expositivo do trabalho feito (LEAL, 2018, p. 265).

Os sistemas históricos de apreciação de prova marcaram a evolução dos sistemas jurídicos, sendo o da certeza legal o mais primitivo destes, uma vez que a certeza dos fatos necessitava de manifestação da lei divina, ou seja, das revelações de Deus que eram chamadas de ordálias. Nesse período, a culpabilidade ou inocência de alguém era medida de acordo com o grau de suas virtudes, de sua santidade ou de seu poder místico. Aceitava-se o juramento como prova e os vencedores dos eventuais duelos eram escolhidos por decisão de Deus, que, para provar sua inocência, dava ao acusado bravura e força para vencer. Esse sistema foi, por

anos, a base do processo inquisitório, no qual o arbítrio das classes nobres era o comando de revelação de justiça divina (LEAL, 2018, p. 267).

Com o passar do tempo, passou a vigorar o sistema da livre convicção, que orientou o sistema de *common law*, baseado em juízos de equidade e conveniência por parte dos julgadores nobres, em que o interesse coletivo é sistematizado pelo *secundum conscientiam*, no qual o juiz pode julgar segundo sua própria consciência, independentemente do material probatório, e até contra este. Sobre este sistema, Rosemiro Pereira Leal discorre que:

> Os critérios desse sistema geraram o processo dispositivo que, ainda na Inglaterra e Estados Unidos, mostra-se exitoso pela hegemonia econômica que ostentam, dispensando leis prévias para assegurar direitos fundamentais de sobrevivência e dignidade econômica para a maioria de seus povos, porque estes vivem em padrões privilegiados pelo aprofundamento da miséria e dominação que infligem ao Terceiro Mundo (LEAL, 2018, p. 267).

Posteriormente, adveio o sistema de persuasão racional, baseado no princípio da reserva legal, no qual a convicção do julgador é condicionada a juízos *secundum legis*, ou seja, em conformidade com a legislação vigente. Foi esse sistema que proporcionou o surgimento do processo acusatório no âmbito do direito processual penal (LEAL, 2018, p. 267).

O instituto da prova é reconhecidamente dotado de uma complexidade teórica elevada, uma vez que provar é assumir a difícil missão de representar os elementos da realidade objetiva pelos meios intelectivos autorizados pela legislação. Segundo Rosemiro Pereira Leal, os meios de prova são lógico-jurídicos indicados na lei para que, através de conhecimentos, dos sentidos e técnica de demonstração, possam-se transportar os elementos de prova encontrados na realidade objetiva para os autos do procedimento. Os meios de prova são, dessa forma, argumentos lógico-jurídicos aptos a demonstrar a existência de elementos suscetíveis de sensibilização ou compreensão relacionados ao fato (LEAL, 2018, p. 267).

É presente doutrina processual uma diferenciação entre os conceitos de meio de prova e meio de obtenção de prova. Segundo Gustavo Henrique Badaró, meio de prova é, portanto, tudo aquilo que sirva para fazer uma reconstrução aproximada dos fatos alegados pelas partes, já os meios de obtenção de provas, que também podem ser chamados de meios de investigação ou de pesquisa de provas, implicam na restrição de direitos fundamentais do investigado e, na maior parte dos casos, nas liberdades públicas ligadas à sua privacidade ou, ainda, à liberdade de manifestação do pensamento (BADARÓ, 2016, p. 387).

Para Aury Lopes Jr, é a prova que permite a atividade recognoscitiva do juiz em relação ao fato ocorrido que está sendo narrado na peça processual. Na opinião do autor, o Processo

Penal e a prova integram os modos de construção de convencimento do juiz, que formará sua convicção e legitimará o poder da sentença (LOPES JR, 2017, p. 287).

Nessa linha de pensamento do autor, as provas seriam, portanto, elementos que permitem a reconstrução histórica e sobre os quais recai a tarefa de verificação das hipóteses, com o objetivo de convencer o magistrado. Michele Taruffo defende que, além dessa função persuasiva em relação ao juiz, as provas também servem para "fazer crer" que o Processo Penal determina a "verdade" dos fatos, porque é útil que os cidadãos assim o pensem, mesmo que na realidade isso não ocorra, e quem sabe precisamente, porque na realidade essa tal "verdade" não possa ser obtida, é que precisa-se reforçar essa crença (TARUFFO, 2002, p. 83).

Em sentido oposto, Rosemiro Pereira Leal discorre que:

> Desservem ao direito, na contemporaneidade, os estudos da prova, se concebida, como assinalado, em moldes judiciaristas, mediante avaliação de sua eficácia probante pelo "poder" da sensibilidade e talento da apreensibilidade jurisdicional. A afirmação de que a "prova tem por objetivo a verdade" demanda cogitações sobre a controvertida acepção de "verdade", porque a busca obsessiva da certeza há de se conter, em direito, nos limites dos meios de obtenção da prova legalmente permitidos (LEAL, 2018, p. 269).

Nas lições de Dário José Soares Júnior, existe um embate entre aqueles que defendem o princípio da verdade real ou material, como sendo de plena observância do Processo Penal, e aqueles que rejeitam este princípio, tratando-se de um mito que não possui acolhida no paradigma democrático, sendo apenas um triste legado de inquisitoriedade e autoritarismo (SOARES JÚNIOR, 2016, p. 270). Dentro desse segundo grupo, há uma divisão que consiste, primeiramente, naqueles que, como Luigi Ferrajoli, defendem não ser possível falar em verdade processual, nem mesmo num sentido aproximado (FERRAJOLI, 2002, p. 43), e aqueles que buscam substituir no Direito Processual Penal a ideia de verdade pela de determinação formal dos fatos, como Francesco Carnelutti, que afirma bastar um limite mínimo que seja à liberdade de busca da verdade pelo juiz, para que esse processo se degenere em mero processo de determinação (SOARES JÚNIOR, 2016, p. 271):

> A verdade é como a água: ou é pura ou não é verdade. Quando a busca da verdade material está limitada de tal maneira que esta não possa ser conhecida, em todo caso com qualquer meio, o resultado, seja mais ou menos rigoroso o limite, é sempre o de que já não se trata de uma busca da verdade material, senão de um processo de determinação formal dos fatos. De fato, sempre é possível que em determinados casos o limite atue no sentido de impedir o conhecimento da verdade material e de substituir esta com uma verdade jurídica ou judicial; sendo assim: esta eventualidade é suficiente para que não se possa atribuir o conhecimento da realidade dos fatos como resultado do processo de determinação (CARNELUTTI, 2001, p. 52).

No mesmo sentido, Michele Taruffo afirma que é inútil tentar fazer uma distinção entre verdade relativa (formal, processual ou objetiva) e verdade absoluta (material ou subjetiva),

uma vez que no processo a única verdade possível é aquela decorrente do acertamento do fato derivada dos dados cognoscitivos resultantes das provas (TARUFFO, 2009, p. 83). Isto posto, a verdade produzida nos limites processuais não constitui uma verdade diferente daquela que se pode descobrir sem as limitações preclusivas ou decorrentes das normas sobre ilicitude das provas, que serão vistas nos próximos capítulos. A verdade produzida no processo pode ser limitada ou incompleta, podendo até a atividade processual se esgotar sem que tenha sido produzida nenhuma verdade (TARUFFO, 2009, p. 84).

Para Soares Júnior, quando se fala de verdade, refere-se à um daqueles conceitos metafísicos, como são os conceitos de bom, belo e justo, contra os quais não há como se pronunciar, mas, no entanto, tentar desvendar-lhes a natureza pode ser uma tarefa infrutífera e sem sentido (SOARES JÚNIOR, 2016, p. 273). Para o autor, é por esse motivo que Ferrajoli se posiciona, de forma estratégica, no meio termo. Não acolhendo uma concepção subtancialista da verdade, pois a identifica como autoritarismo, decisionismo e inquisição, mas, ao mesmo tempo, não a descartando totalmente (SOARES JÚNIOR, 2016, p. 273), pois "se uma justiça penal integralmente "com verdade" constitui uma utopia, uma justiça penal completamente "sem verdade" equivale a um sistema de arbitrariedade" (FERRAJOLI, 2002, p. 38).

No Direito Processual Penal, a verdade lógica deve ser buscada, mas com o prévio reconhecimento de que se trata de uma estrutura munida de grande complexidade. A própria estrutura é regulada normativamente pela Constituição (BRASIL, 1988), que inadmite, nos processos, as provas obtidas por meios ilícitos. Os fatos, objetos de apuração, devem ser confrontados com normas das mais diversas tipologias, razão pela qual a atividade interpretativa ganha ainda mais relevância, sendo, no entanto, altamente influenciável pelas razões ideológicas, que condicionam o sistema (SOARES JÚNIOR, 2016, p. 276). Com isso, Ferrajoli reconhece essa dificuldade e afirma que a linguagem jurídica deva ser "tendencialmente isenta de termos vagos e valorativos", o que seria assegurado pelo "sistema das garantias da estrita legalidade e estrita jurisdicionalidade" (FERRAJOLI, 2002, p. 42). Segundo Soares Júnior, para evitar as tendências autoritárias, deve-se acolher a sentença de Karl Popper segundo a qual deve-se ser um buscador da verdade, mas não ser seu possuidor (SOARES JÚNIOR, 2016, p. 276).

Em suma, não se pode compreender a prova apenas como aquilo que contribui para instrução e convencimento do julgador, mas também um direito fundamental decorrente da cláusula do devido processo legal, na qual institui complexas garantias processuais que visam asseguram plenamente tanto a verificação quanto a refutação (SOARES JÚNIOR, 2016, p. 285), reconhecendo que não só o juiz, mas também as próprias partes são destinatárias desta

(FERRAJOLI, 2012, p. 105). Não se trata, portanto, de um axioma da verdade, porque, como nas palavras de Carnelutti, a finalidade da prova é a fixação formal do fato controvertido, condicionada por percepções obtidas e deduções extraídas de acordo com o ordenamento jurídico (CARNELUTTI, 2001, p. 45).

Uma vez constatada a ocorrência de uma infração penal, como no tema em questão são os crimes digitais e, levando-se em conta as características da espécie, envolvendo sensíveis aspectos técnicos e quase sempre uma identidade camuflada, já nasce a problemática da comprovação, pelos meios legais, da sua existência e de quem é a autoria.

Nesse instante, compete aos órgãos encarregados da persecução penal (Polícia Judiciária e o Ministério Público) colacionar as provas hábeis a demonstrar a materialidade e a autoria do fato, revelando pelos meios admitidos por lei, todos os elementos e circunstâncias fático-jurídicas descritas no tipo penal. Este é um requisito do sistema penal acusatório, adotado pela Constituição da República Federativa do Brasil (BRASIL, 1988), segundo qual incumbe ao órgão acusador estatal – ou ao particular, quando se trata de uma ação penal em que este é o titular – a demonstração cabal do ato infracional praticado, rompendo o presumível estado de inocência previsto no texto constitucional, em favor de toda pessoa humana ou entidade personalizada (RONCADA, 2017, p. 178).

A presença dos princípios do contraditório e ampla defesa reafirma a necessidade de garantir o direito à prova, pois é em decorrência deles que a prova se manifesta. Este é um direito subjetivo das partes que as permite levar ao juízo suas postulações e ser-lhes proporcionada a possibilidade de demonstrar a veracidade de suas alegações (DIAS, 2015).

Seguindo essa linha de pensamento, Rosemiro Pereira Leal entende que:

> Portanto, a "Lei Constitucional" é elemento e instrumento de prova da existência ou não do Estado de Direito. Se a lei é produzida por meio do devido processo legislativo, na acepção aqui estudada, é ela também elemento e instrumento de prova da existência do Estado de Direito Democrático. Quando o NCPC (art. 369) contempla "meios moralmente legítimos" e "livre" conjectura do juiz (art. 370) para se provarem fatos, além de cometer a impropriedade de afirmar a existência de uma moral válida sem norma jurídica definidora, permite coleta de prova numa realidade externa ao direito, em critérios personalíssimos e sumaríssimos (instantâneos), com negativa de vigência do princípio da legalidade estrita adotado pelo art. 5º, II, da CF/1988 (LEAL, 2018, p. 265).

A produção da prova está assegurada no artigo 5º, incisos XXXV, LIV e LV da Constituição da República Federativa do Brasil (BRASIL, 1988) e, como anteriormente ressaltado, constitui um direito fundamental consubstanciado no contraditório, na ampla defesa, no devido processo legal e no acesso à justiça (DA SILVA, 2017, p. 03). Porém, sua produção não tem um caráter absoluto, sendo sujeita a determinados limites, como será exposto a seguir.

4.2 LIMITES À PROVA

Ainda que haja a incontestável certeza da existência de um determinado elemento de prova isso, por si só, não autoriza a coleta da prova *contra legem*, ou seja, contra a legislação vigente. A liberdade de persecução probatória não é direito absoluto, tendo controle dos devidos meios indicados na lei para que se obtenha o instrumento de prova. Como explica Leal, em direito o ato de provar é representar e demonstrar, instrumentando, os elementos de prova pelos meios de prova. Trazendo como exemplo, a perícia, que é um meio de prova para o exame de elementos de prova com elaboração final do laudo, que é o instrumento de prova (LEAL, 2018, p. 270).

É possível observar, nos mais variados ordenamentos jurídicos, o princípio geral de que não se admitem provas ilícitas ou ilegítimas no curso de um processo, cuja diferença, para Denilson Feitoza Pacheco, está atribuída ao fato de as primeiras serem obtidas mediante violação de um direito material do investigado e as segundas em violação de normas processuais (PACHECO, 2006, p. 544). O artigo 5º, inciso LVI[11] da Constituição da República Federativa do Brasil (BRASIL, 1988) veda a realização procedimental das provas que sejam obtidas por meios ilícitos. Segundo o autor, esse princípio geral tem origem na jurisprudência dos Estados Unidos da América, sendo definido conforme a terminologia *exclusionary rules* (regras de exclusão), do qual resulta que tanto as provas ilícitas como as ilegítimas devem ser excluídas pelo processo, seja para preservar a inviolabilidade provada, preservar o confisco popular do Estado ou prevenir abusos policiais (PACHECO, 2006, p. 546).

> Desse princípio geral decorrem os seguintes subprincípios: a) *good faithe exception*, pelo qual excepcionalmente, uma prova ilícita pode ser mantida quando obtida de boa fé; b) *fruits of the poisonous tree doctrine* (doutrina dos frutos da árvore envenenada), que resulta também na exclusão das provas derivadas das ilícitas, conforme o caso *Silverthorne Co. v. U.S.,* 1920; c) *independente source limitation*, segundo o qual outra fonte independente da ilícita, como se viu no caso *Bynum v. U.S., 1960*, em que a polícia usou impressões digitais obtidas num processo anterior que havia sido anulado; d) *Inevitable discovery limitation*, também se mantém a prova quando por outro modo fatalmente se chegaria à descoberta, tendo a prova ilícita apenas a antecipado; e) por fim a chamada *purged taint limited*, em que a prova derivada da ilícita é mantida quando em certos casos se considera que tenha sido "descontaminada", por exemplo, em razão de uma confissão espontânea, como no caso *Wong Sun* v. U.S., 1963 (SOARES JÚNIOR, 2016, p. 280-281).

No Direito Processual Penal brasileiro, a jurisprudência do Supremo Tribunal Federal historicamente relutou a acolher plenamente essas regras de exclusão, optando por adotar o

[11] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]
LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos (BRASIL, 1988).

princípio da proporcionalidade, deixando a decisão para o juiz no caso concreto (SOARES JÚNIOR, 2016, p. 281). Porém o artigo 157[12] do Código de Processo Penal (BRASIL, 1941), após a nova redação trazida pela Lei nº 11.690 de 2008 (BRASIL, 2008), acolheu respectivamente a regra de exclusão, a teoria dos frutos da árvore envenenada e a teoria da fonte independente. Portanto, a prova ilícita deve ser desentranhada do processo, assim como aquelas que delas derivem, podendo ser mantida a que não tenha nexo causal com a primeira, ou a que pudesse ser reproduzida por fonte independente.

Dessa forma, com a obtenção ilícita do elemento ou do instrumento de prova, o ato se torna inexistente, uma vez que a prova se ressentiria de aspecto teórico de sua configuração legal que, no caso, é a licitude do meio empregado (LEAL, 2018, p. 270). Portanto, o ato não seria nulo, anulável e nem viciado, mas ausente, devida à supressão de licitude na estrutura de sua produção. Sua existência é, no máximo, capaz de gerar uma hipótese psicológica ou sentimento subjetivo de convicção que, por sua vez, são irrelevantes do ponto de vista epistemológico (POPPER, 1974, p. 48-49).

Além da regra constitucional supracitada que inadmite a obtenção de provas por meios ilícitos, vigoram também no Código de Processo Penal (BRASIL, 1941), algumas limitações que tornam o material probatório ilegítimo. Como exemplo, tem-se no artigo 155, parágrafo único, a determinação de que devem ser observadas as restrições da lei civil no que tange à prova quanto ao estado das pessoas, como nos casos de casamento, morte e parentesco que somente são provadas mediante suas respectivas certidões; outro exemplo está no artigo 158, que torna indispensável o exame de corpo de delito para as infrações que porventura deixarem vestígios, não podendo ser suprido pela confissão do acusado; o terceiro é exemplo é o do *caput* do artigo 479, que proíbe, durante o julgamento, a leitura de documento ou a exibição de objeto que não tiver sido juntado aos autos com a antecedência mínima de três dias úteis, dando-se ciência à outra parte.

Tendo em vista as principais características das provas no âmbito do processo penal e alguns exemplos de suas restrições, é necessário observar que, nos crimes digitais, a persecução

---

[12] Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.
§ 1º São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras.
§ 2º Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova.
§ 3º Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial, facultado às partes acompanhar o incidente (BRASIL, 1941).

probatória possui determinadas particularidades que precisam ser aprofundadas, principalmente no que tange à sua volatilidade.

4.3 A PROVA NOS CRIMES DIGITAIS

Diversos conceitos que antes serviam como base para interpretação dos fatos e das leis tiveram que passar por reformulações, com o intuito de se modernizarem e se enquadrarem à nova realidade. As novas situações jurídicas presentes na sociedade de risco e no mundo tecnologicamente globalizado exigem conhecimentos específicos por parte dos profissionais do Direito para que estes atuem em consonância com o momento atual.

Essas novas situações têm como origem as diversas ações que utilizam dos meios digitais para a execução de ilícitos que ferem direitos legalmente tutelados. Como já abordado neste trabalho, a maior parte dessas condutas praticadas pela internet e suas redes sociais já está prevista no ordenamento jurídico brasileiro com a devida tipificação penal, mas estas possuem particularidades que as distinguem do mundo material, uma vez que o meio onde o ilícito é perpetrado é o digital, a persecução penal e probatória passam a ser diferentes (DA SILVA, 2017, p. 06).

Enquanto no crime tradicional, praticado no mundo material, se encontram informações essenciais para sua investigação, como vestígios, indícios e testemunhas, nos crimes digitais, as evidências podem estar alocadas em inúmeros dispositivos como computadores, celulares, *pendrives*, provedores de internet, registros de equipamento de infraestrutura de rede como roteadores, firewalls e servidores de e-mail. O material probatório, além de volátil, é bastante variado, podendo ser arquivos digitais, registros de servidores, históricos de navegação, fotos, vídeos, e-mails, entre outros (SHIMABUKURO, 2017, p. 23).

Devido as particularidades das provas no meio digital, caso esta não seja prontamente preservada, pode ser rapidamente danificada, alterada ou até suprimida, impedindo qualquer investigação ou identificação do autor do delito. Com isso, a coleta do material probatório nos crimes digitais segue rigorosos critérios de preservação e controle para que não haja perda de sua veracidade (SHIMABUKURO, 2017, p. 23).

No Brasil, o órgão responsável pela atribuição de integridade, autenticidade e validade jurídica aos documentos eletrônicos é o Instituto Nacional de Tecnologia. Porém, nem todas as provas eletrônicas são admitidas como portadoras de validade jurídica, por terem a confiabilidade de sua prática questionada por parte da doutrina (MATOS, 2014). Sobre isso, Marco Antônio de Barros expõe que:

> Com efeito, se a infração penal for praticada por meio da internet, é necessário identificar a máquina utilizada. Nesse tipo de investigação o objetivo é descobrir o endereço IP (internet Protocol) do computador dentro de uma rede. E nem sempre isto será suficiente, pois há casos em que um único computador sirva a mais de uma pessoa, sendo então necessário identificar quem realmente o utilizou para a prática delituosa. Na apuração dos chamados crimes digitais, informáticos ou cibernéticos, ou de infrações penais praticadas mediante o uso de microcomputadores, os peritos costumam empregar a técnica "post-mortem". Ou seja, o sistema é examinado após o desligamento da máquina, situação em que cabe ao perito proceder à duplicação das mídias e à avaliação de evidências armazenadas e/ou recentemente apagadas (BARROS, 2011, p. 126).

Com base nos preceitos dos artigos 158 a 184 do Código de Processo Penal (BRASIL, 1941), extrai-se a regra de que o meio de prova mais adequado para se demonstrar uma prática criminosa é o exame de corpo de delito, materializado por laudo pericial emitido por técnico habilitado na área de conhecimento científico, isso quando a infração penal deixar vestígios. Corpo de delito é o conjunto dos vestígios resultantes da infração penal, enquanto o exame de corpo de delito é a análise e o registro feito por peritos sobre esses vestígios (RONCADA, 2017, p. 180).

Com isso, seguindo o pensamento de Rodiner Roncada, tem-se a percepção de que não se faz prova da existência de crimes digitais sem o devido exame de corpo de delito, formalizado em laudo técnico pericial. Isso devida à execução do crime envolver aspectos técnicos específicos, que exigem conhecimento científico de informática para atestar a existência do delito penal. Ao juiz, independentemente do seu conhecimento na área, não é dada a possibilidade de suprir a ausência do exame pericial pelo seu próprio conhecimento científico, uma vez que isso comprometeria sua isenção e imparcialidade para julgar a causa, colocando-o na posição de produtor de prova e subtraindo, das partes, a possibilidade de contradizer, durante o curso do processo, a exposição dos fatos e suas respectivas consequências (RONCADA, 2017, p. 179-180).

Roncada destaca também que, nas regras processuais penais, inexiste uma hierarquização das provas, na qual o juiz fundamenta sua decisão através de livre apreciação das mesmas, não havendo preferência entre as fontes de conhecimento e nem vinculação aos laudos periciais, que possuem valor apenas relativo, como está previsto no artigo 188 do Código de Processo Penal (BRASIL, 1941).

Parte da jurisprudência tem admitido a dispensabilidade do exame pericial quando estiverem presentes outros elementos probatórios que sejam suficientes para atestar a materialidade de um crime (RONCADA, 2017, p. 181), o que relativiza os preceitos do supracitado artigo 158 do Código de Processo Penal (BRASIL, 1941). Entretanto, autores como Guilherme de Souza Nucci, advertem que a ocorrência da infração penal deve ser objetivamente

comprovada nos autos do processo, mediante a colheita direta ou indireta dos vestígios materiais, deles extraindo-se uma conclusão segura sobre a existência do crime, por meio de exame pericial, conforme determina este artigo (NUCCI, 2015, p. 68). A dispensa do exame de corpo de delito ocorreria, portanto, somente nos casos em que houvesse o desaparecimento dos vestígios materiais, podendo ser substituído pela prova testemunhal, conforme autorizado pelo artigo 167 do Código de Processo Penal (BRASIL, 1941).

Eugênio Pacelli ressalta que não se trata de uma questão de hierarquização das provas, mantendo-se o regime processual do livre convencimento motivado do magistrado, mas sim à especificidade de meio de prova, tendo o legislador escolhido um meio específico para a comprovação da existência do crime, garantindo ao acusado um sistema probatório criterioso para a afirmação da certeza e do convencimento (PACELLI, 2018, p. 332).

Ainda que não exista hierarquia entre os meios de prova, o artigo 158 do Código de Processo Penal (BRASIL, 1941), como já visto, foi categórico ao estabelecer que o exame de corpo de delito é indispensável nos casos de infração penal que deixem vestígios materiais, não podendo ser substituído por qualquer outra prova, nem mesmo a confissão do acusado, o que acarretaria nulidade absoluta do processo. O legislador aqui, teve como objetivo garantir ao acusado a formação da culpa pelos meios que melhor possam representar os fatos, mitigando a possibilidade de sobreposição de algum caráter subjetivo por parte do juiz (RONCADA, 2017, p. 182).

Com isso, nos crimes digitais, o exame de corpo de delito se torna necessário, pois não há como confirmar de modo seguro a sua ocorrência e seu alcance sem constatar o caminho lógico percorrido pelo autor dentro do ambiente digital, até mesmo determinando a origem dos atos executórios, primordiais para determinar a autoria do crime. Isso só seria possível através de um exame técnico em que os vestígios são analisados por profissional habilitado em informática e tecnologia da informação, que tem a função de elaborar uma opinião crítica e fundamentada sobre os fatos observados (RONCADA, 2017, p. 183).

A dispensa do exame de corpo de delito se dá apenas em situações extremamente excepcionais, como já fora apresentado neste trabalho. A primeira delas é desaparecimento dos vestígios, por destruição ou ocultação total dos objetos que compõem cenário do delito, o que autoriza a substituição da prova pericial por testemunhal, conforme artigo 167 do Código de Processo Penal (BRASIL, 1941). Nos crimes digitais os dados muitas das vezes independem do dispositivo desaparecido e podem ser úteis na elucidação da materialidade e da autoria, o que acarreta na necessidade de realizar-se o exame pericial indireto (RONCADA, 2017, p. 184).

Outra excepcionalidade é o caso dos fatos serem de conhecimento comum – que fazem parte da cultura geral da sociedade – e não necessitarem de exame pericial, pois estão ao alcance de qualquer pessoa, podendo ser comprovados através de qualquer meio. Nessa categoria estão diversos fatos do conhecimento popular relacionado os crimes digitais, como exemplo, o funcionamento prático da internet, o acesso público a manifestações individuais em redes sociais e a utilidade de algum software que não necessitam de análise pericial (RONCADA, 2017, p. 184).

Os crimes digitais não possuem normas próprias de caráter processual dispostas no ordenamento jurídico pátrio. Com isso, são aplicáveis a estas, as normas processuais previstas genericamente no Código de Processo Penal (BRASIL, 1941) e em leis especiais, como a Lei nº 12.850 de 2013, conhecida como Lei de Combate à Organização Criminosa (BRASIL, 2013). Como exceção, é importante ressaltar que o Marco Civil da Internet no Brasil (Lei nº 12.965 de 2015) (BRASIL, 2015), possui importantes instrumentos de apuração de crimes digitais previstos nos seus artigos 13, 15 e 22, que determinam que o servidor de conexão ou de aplicações da internet atenda à ordem judicial de acesso ao conteúdo dos registros (RONCADA, 2017, p. 185), como será melhor aprofundado em nos capítulos seguintes.

Na legislação brasileira inexiste impedimentos para a utilização de provas obtidas no meio digital. De acordo com o artigo 225 do Código Civil (BRASIL, 2002), "as reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão" (BRASIL, 2002). Nesse sentido, o Código de Processo Civil de 2015 (BRASIL, 2015) prevê que "as partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz" (BRASIL, 2015). Dessa forma, as provas obtidas no ambiente digital são aceitas, desde que respeitados alguns padrões técnicos para sua coleta e armazenamento, com o objetivo de resguardar sua integridade, validade e/ou licitude (DA SILVA, 2017, p. 08).

A evolução das tecnologias de informação refletiu de forma direta na também modernização das ferramentas para validação jurídica das provas, o que impulsionou o surgimento de uma especialidade conhecida como computação forense. A computação forense é uma das especialidades da ciência criminalística que aborda a investigação probatória e que pode ser definida como o "uso de técnicas analíticas e de investigação para identificar, coletar, analisar e preservar as provas/informação que é armazenada magneticamente ou codificada"

(DA SILVA, 2017, p. 10). Uma vez que a ciência forense é aquela que abriga a perícia forense aplicada à informática, por sua vez, essa pode ser definida como sendo a “aplicação de princípios das ciências físicas ao Direito na busca da verdade em questões cíveis, criminais e de comportamento social para que não se cometam injustiças contra qualquer membro da sociedade" (DA SILVA, 2017, p. 10).

Na computação forense, faz-se o uso de métodos científicos com o objetivo de preservar, coletar, validar, identificar, analisar, interpretar, documentar e apresentar as evidências digitais (DA SILVA, 2017, p. 10). Evidências essas que são todas as informações sujeitas ou criadas pela intervenção humana, que possam ser extraídas de um computador ou de qualquer dispositivo eletrônico. Com isso, o exame forense visa extrair as informações que identifiquem qualquer indício que possa estar relacionado ao caso em questão, permitindo que se formulem conclusões sobre o delito. Para o Código de Processo Penal (BRASIL, 1941), indício é a circunstância conhecida e provada, que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra circunstância.

Para a investigação de um crime digital, deve-se começar pelo levantamento das evidências e informações que, por ventura, possam servir de elemento de prova. Nessa modalidade delitiva, as evidências e informações estão armazenadas em meios digitais como um disco rígido de computador ou na memória de um celular. Essa investigação implica na atividade de exame pericial que resultará na prova pericial, produzida a partir de critérios científicos. Para Queiroz e Vargas, o laudo pericial é peça fundamental de um processo, que traduz, em sua totalidade, o que foi realizado pelo perito de forma clara e objetiva antes, durante e depois de seus estudos sobre o caso em questão (QUEIROZ; VARGAS, 2010, p. 29). Então, as informações presentes neste material possuem uma importante carga de vestígios para a desencadeamento e conclusão do processo criminal (DA SILVA, 2017, p. 11).

As provas encontradas no meio digital têm como característica o grande risco de perecimento, o que acarreta uma necessidade de maiores cuidados no seu processo de coleta, para que que seja garantida sua integridade. Entretanto, para que uma evidência possa ser, de fato, considerada parte do elemento probatório de um crime digital, é necessário que sejam respeitadas determinadas regras de aceitação, que Jorge Luiz Silva da Silva elenca:

> Assim deve seguir a regra da admissibilidade, que observa se há condições da evidência ser usada no processo. A regra da autenticidade, que verifica se a evidência é certa e de relevância para o caso. A regra da completude, pois a evidência não poderá causar ou levar a suspeitas alternativas. A regra da confiabilidade, que não permite a existência de dúvidas sobre a veracidade e autenticidade da evidência. E a regra da credibilidade, que significa a clareza, o fácil entendimento e a interpretação (DA SILVA, 2017, p. 11).

Assim como nos crimes tradicionais do mundo material, nos crimes digitais também deve ser seguido o procedimento adequado para a coleta da evidência para não comprometer sua validade. Embora a computação forense seja altamente precisa, se o procedimento para coleta de evidências for realizado de forma equivocada, pode tornar a prova ilícita ou inválida (DA SILVA, 2017, p. 11).

A criminalidade no ambiente digital deve ser combatida com as mesmas ferramentas oferecidas nas demais modalidades delitivas. Para tal, Mariana Maria Matos afirma serem necessárias unidades policiais especializadas nestes crimes, de modo a assegurar a manutenção da integridade das provas ao mesmo tempo em que se possibilitaria a adequação dos órgãos policiais à velocidade dos crimes digitais (MATOS, 2014). Com isso, o processo de investigação e julgamento de um crime digital deve ser pautado na ampla liberdade probatória outorgada às partes e no livre convencimento do órgão julgador para este possa apreciar essas provas, fundamentando os motivos de sua decisão (DIAS, 2015).

4.3.1 Supremacia do interesse público e limitação das provas no meio digital

Uma grande parte das investigações a respeito de crimes cometidos no ambiente digital exige que, para fim de prova, ocorra a quebra de sigilo da troca de mensagens eletrônicas entre os usuários através de *softwares* e aplicativos. Entretanto, esse tipo de mensagem instantânea é caracterizado por transitar de forma criptografada de um ponto ao outro, e, quando são entregues, estas são excluídas dos seus servidores, ficando guardadas apenas no dispositivo do próprio usuário. Os provedores alegam não poderem interceptar ou armazenar as mensagens trocadas pelos usuários dessas ferramentas uma vez que elas são decodificadas apenas no terminal recebedor da mensagem, ou seja, no aparelho celular do usuário (DA SILVA, 2017, p. 12).

Mensagens contidas em aplicativos como o WhatsApp têm servido como material probatório para instruir processos através da apreensão de celulares para desmantelar associações criminosas e investigar participações em outros crimes. Em julho de 2016, o judiciário determinou ao Facebook do Brasil, proprietário do aplicativo Whatsapp, que interceptasse as mensagens dos usuários alvos de uma investigação sobre tráfico de drogas. Como não houve o cumprimento dessa ordem judicial, o Tribunal de Justiça do Rio de Janeiro determinou, através da juíza Daniela Barbosa Assunção da Vara de Execuções Penais, a suspensão dos serviços de troca de mensagens em todo o país (COSTA, 2016).

Outro exemplo do uso da ferramenta para coibir o crime de tráfico de drogas é trazido por Jorge Luiz Silva da Silva:

> Ainda na intenção de forçar o provedor do serviço WhatsApp a fornecer as informações para a investigação de crime de tráfico internacional de drogas, com a interceptação das mensagens envidadas pelos investigados, o Juízo da 5ª Vara Federal da Seção Judiciária de Foz do Iguaçu/PR, no bojo do procedimento nº 5007896-78.2015.4.04.7002 determinou o bloqueio de valor em conta e a aplicação de multa diária até que a medida seja satisfeita. No julgamento em 19/07/2016 (MANDADO DE SEGURANÇA (TURMA) Nº 5031214-13.2016.4.04.0000/PR) pelo TRF4, deferiu em parte a medida liminar, apenas para determinar que, até o julgamento final do mandado de segurança, o valor bloqueado não fosse objeto de qualquer movimentação (DA SILVA, 2017, p. 12-13).

É possível perceber, portanto, que existe uma limitação no que tange à obtenção de provas pelo sistema judiciário nos casos em que envolvam crimes digitais. Quando se projetou a infraestrutura da internet e dos dispositivos que a acessam, foram implementados requisitos de criptografia e segurança para coibir as tentativas de acesso não autorizado, de invasão de sistemas computacionais e proteção de dados sensíveis dos usuários não só visando sua integridade, mas também garantindo o direito à privacidade constitucionalmente elencado.

O direito à privacidade está garantido no inciso X do artigo 5º da Constituição da República Federativa do Brasil (BRASIL, 1988) que diz serem "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988). Porém, existe a discussão em relação à força de tal princípio em relação a uma proposta de implementação de um sistema de monitoramento das comunicações dos aplicativos de redes sociais para atender as eventuais demandas judiciais (DA SILVA, 2017, p. 13).

Marcel Leonardi destaca que a privacidade possui um valor social, pois molda as comunidades sociais e fornece a proteção necessária aos indivíduos contra vários tipos de violações, o que possibilita que estes desenvolvam sua personalidade e devolvam à sociedade novas contribuições. O autor destaca que a individualidade deve ser incorporada ao conceito de bem comum, e não entendida como seu contraponto. Quando esta é separada do bem comum, tem seu valor diminuído, e o sopesamento de princípios tende a favorecer aqueles tradicionalmente relacionados a interesses coletivos (LEONARDI, 2012, p. 121).

O direito à privacidade não tem valor apenas para a vida privada de cada um, mas também para a vida pública e comunitária. Esta não deve ser entendida como uma proteção exclusiva de um indivíduo, mas um direito necessário para a manutenção do exercício da cidadania (LEONARDI, 2012, p. 122).

Quando se cogita a possibilidade de se implantar uma solução de monitoramento das comunicações de aplicativos de trocas de mensagens, existe uma reiterada discussão a respeito do direito à privacidade. A mera possibilidade de alguma forma de controle já é motivo para divergências, principalmente no que tange ao princípio da supremacia do interesse público que,

por possuir um conceito indeterminado, não apresenta uma abrangência pacificamente delimitada (DA SILVA, 2017, p. 15).

O entendimento a respeito do princípio da supremacia do interesse público varia entre o que se relaciona a um interesse que se contrapõe ao interesse individual e o outro, que defende englobar a soma dos interesses individuais, contemplando o conjunto de necessidades humanas indispensáveis na vida do indivíduo. É nesse segundo entendimento que se encaixa o conceito de Celso Antônio Bandeira de Mello que afirma se tratar do interesse resultante do conjunto dos interesses que os indivíduos pessoalmente têm quando considerados em sua qualidade de membros da sociedade e pelo simples fato de o serem (MELLO, 2018, p. 62).

Carlos Ari Sundfeld questiona o uso da expressão "supremacia", pois esta faz referência ao que está acima de tudo. Entretanto, para o autor, o interesse público não está acima da ordem jurídica, mas teria apenas uma prioridade em relação ao privado (SUNDFELD, 2012, p. 143). Gabriel de Araújo Lima, em sentido semelhante, argumenta haver uma contradição intrínseca na proposição deste princípio, pois se o interesse público contempla os interesses privados, o enunciado, sob o ponto de vista lógico, não poderia prever uma supremacia dos interesses públicos em relação aos interesses privados (LIMA, 2009, p. 125).

Em relação aos interesses públicos, Christiane Costa Assis argumento no sentido de haver, na concepção clássica, o entendimento de que a Administração Pública seria sua tutora, sem que houvesse a necessidade de participação da sociedade para sua definição. Com isso, o Estado seria uma entidade promotora dos interesses públicos entendidos como bem-estar dos indivíduos, cujo mecanismo de atuação seria o Direito (ASSIS, 2011, p. 110). Porém, a evolução dos sistemas jurídicos demonstrou que essa pré-concepção de interesse público não mais satisfaz os anseios da sociedade pluralista contemporânea, não se admitindo uma atuação exclusiva por parte do Estado na busca pela realização do interesse público, sendo necessário, também, que os particulares tenham participação ativa em sua construção (ASSIS, 2011, p. 110-111).

O interesse público, portanto, não deve ser um conceito estático, fechado em si, mas acompanhar as modificações da vida em comum e estar em consonância com as transformações da sociedade. Segundo Assis, partindo da proposta de Habermas, o verdadeiro conceito de interesse público é construído através do debate, no qual "a argumentação tem a forma de um concurso que visa aos melhores argumentos a favor de ou contra pretensões de validade controversas e serve à busca cooperativa da verdade" (HABERMAS, 2010, p. 250). Este debate deve acontecer de forma constante, pois é necessária uma abertura permanente para novas argumentações (ASSIS, 2011, p. 113).

> A esfera pública pode ser descrita como uma rede adequada para a comunicação de conteúdos, tomadas de posição e opiniões; nela os fluxos comunicacionais são filtrados e sintetizados a ponto de se condensarem em opiniões públicas enfeixadas em temas específicos. Do mesmo modo que o mundo da vida tomado globalmente, a esfera pública se reproduz através do agir comunicativo, implicando apenas o domínio de uma linguagem natural; ela está em sintonia com a compreensibilidade geral da prática comunicativa cotidiana (HABERMAS, 2010, p. 92).

A busca do interesse público na Teoria Discursiva do Direito de Habermas se apresenta, então, como uma alternativa democrática que possibilita ampla participação da sociedade na esfera pública, além de propor uma equiprimordialidade entre esfera pública e privada, sem que haja uma sobreposição de uma em relação à outra (ASSIS, 2011, p. 116). Quando se constata em sua teoria que a legitimidade das democracias constitucionais contemporâneas depende do reconhecimento de relação de interdependência entre os direitos humanos e a soberania popular, e entre autonomia pública e privada, é possível concluir que o supremacia do interesse público é efetivamente incompatível com o paradigma do Estado Democrático de Direito e, consequentemente, com a Constituição da República Federativa do Brasil de 1988 (BRASIL, 1988) (FISCHGOLD, 2011, p. 86).

Para Humberto Ávila, "*interesse público não é determinável objetivamente*" (ÁVILA, 2010, p. 86). É plenamente possível que as pessoas divirjam profundamente acerca do que seja o verdadeiro interesse da coletividade. O desacordo moral, filosófico e religioso é uma das características mais marcantes da sociedade contemporânea, com a qual a teoria política deve lidar (SOUZA NETO, 2006, p. 65). Para Marçal Justen Filho, "a solução do prestígio ao interesse público é tão perigosa para a democracia quanto todas as fórmulas semelhantes em regimes totalitários (o espírito do povo alemão ou o interesse do povo soviético)." (JUSTEN FILHO, 2016, p. 44). Sobre a dinamicidade do interesse público, Patrícia Baptista argumenta que:

> Ora apontado como o somatório de interesses individuais coincidentes, ora como uma grandeza autônoma, o interesse público mantém com os demais interesses existentes na sociedade uma relação de permanente tensão, sendo impossível afirmar, fora do caso concreto, o grau de conformação ou colidência entre eles.
> A questão do interesse público, enfim, nas palavras de Eros Roberto Grau, prossegue como a grande questão do direito administrativo. Apenas deve-se reconhecer que esse interesse público, mormente na versão corporificada na lei, não pode mais continuar monopolizando o direito administrativo. Antes, tal ramo do direito precisa evoluir para atuar como um instrumento eficaz de regulação de um espaço público marcado pela pluralidade de atores e de interesses em jogo, característica principal da sociedade contemporânea (BAPTISTA, 2003, p. 202-203).

Com isso, deixar a cargo da Administração Pública o monopólio da definição do interesse público não é cabível em uma sociedade democrática, mas, ao mesmo tempo, apenas identificá-lo ao interesse da coletividade e a o bem comum nada acrescenta ao debate

(MOREIRA NETO, 2014, p. 410). Diante da diversidade de interesses igualmente legítimos que se manifestam na sociedade, o conceito de interesse público deve ser pensado à luz de uma perspectiva procedimental, segundo a qual este não tem um conteúdo pré-estabelecido, ele é resultado de procedimentos democráticos de criação, execução e aplicação do Direito (JUSTEN FILHO, 2016, p. 45).

Para Bruno Fischgold, "o paradigma procedimental do Estado Democrático de Direito, tal como trabalhado por Habermas, leva a sério o pluralismo e, por isso, rejeita qualquer possibilidade de haver um modelo perfeito para a organização social" (FISCHGOLD, 2011, p. 88). Ele diverge dos paradigmas jurídicos anteriores uma vez que não antecipa mais um determinado ideal de sociedade, mas visa, essencialmente, estabelecer condições para que os cidadãos possam, sob determinadas regras, descobrir seus interesses e o melhor modo de preservá-los (FISCHGOLD, 2011, p. 89).

Dessa forma, o termo "interesse público" deve ser interpretado como resultado do exercício da autonomia pública dos cidadãos de uma determinada comunidade jurídica em um determinado contexto histórico. Consoante o entendimento do professor Marçal Justen Filho, o interesse público não é o pressuposto de decisões democráticas sim o resultado delas (JUSTEN FILHO, 2016, p. 45).

Com isso, é possível observar que – diferentemente do que pressupõe o princípio da supremacia do interesse público – inexiste uma abstrata relação de antagonismo entre tais interesses, mas sim uma relação de complementariedade e interdependência (FISCHGOLD, 2011, p. 91). Ou seja, o exercício da autonomia pública só é possível se a autonomia privada estiver igualmente garantida a todos os cidadãos, ao mesmo tempo em que a autonomia privada apenas estará preservada de forma efetiva se os cidadãos fizerem uso adequado da autonomia pública (HABERMAS, 2002, p. 293-294).

Em uma sociedade plural e complexa, na qual os direitos fundamentais como um todo consubstanciam condições que possibilitam a soberania popular, a devida proteção do interesse privado representa uma verdadeira finalidade pública, fundamentada no princípio democrático. Deve-se constatar, portanto, que a promoção do interesse público também representa uma condição possibilitadora da proteção jurídica do interesse privado (HABERMAS, 2002, p. 295).

Em suma, a falsa ideia de que o interesse público goza de primazia frente ao interesse privado, portanto, encontra-se baseada em um pressuposto incompatível com o Estado Democrático de Direito. Direitos individuais que protegem interesses privados e metas coletivas que protegem interesses públicos encontram-se incluídos de forma igual entre os objetivos da atividade estatal, justamente porque a Constituição da República Federativa do

Brasil (BRASIL, 1988) reconhece a interdependência existente entre as autonomias pública e privada no paradigma do Estado Democrático de Direito (FISCHGOLD, 2011, p. 93). Dessa forma, no anseio de satisfazer os direitos e necessidades da coletividade, não se pode deixar de reconhecer as legítimas prerrogativas dos interesses individuais. Visando principalmente a garantia ao respeito à liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição da República Federativa do Brasil (BRASIL, 1988), é que em 2014 foi promulgada a Lei nº 12.965, denominada como Marco Civil da Internet (BRASIL, 2014) e que será comentada no capítulo seguinte.

5 MARCO CIVIL DA INTERNET

Após quase três anos de tramitação, o PL nº 2126 se converteu na Lei nº 12.965 (BRASIL, 2014), conhecida como Marco Civil da Internet em 23 de abril de 2014 que "estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria (BRASIL, 2014)".

Inicialmente, concluiu-se que, para o legislador, a internet no Brasil se configura como um direito difuso e universal, ao dizer, no inciso I do artigo 4º, que seu acesso é direito de todos. Em seguida, o artigo 5º demonstra que há uma compreensão do fenômeno sociológico que supera o conceito limitado de que a internet é um ambiente acessível apenas por computadores. Ao utilizar-se da nomenclatura "terminal", demonstra a atenção da lei para abarcar todo dispositivo que possua potencial para ser meio de prática de condutas no meio digital (SYDOW, 2015, p. 275).

Spencer Toth Sydow ressalta a importância da Lei nº 12.965 (BRASIL, 2014) trazer definições e conceitos como o da conectividade, da portabilidade, da fragmentariedade e da divisibilidade, visto que o judiciário, em grande parte das vezes, não compreende os termos técnicos dos pedidos feitos pelos operadores do direito. Mesmo que a função primordial da legislação não seja explicar termos, a era digital da sociedade de risco exige que seus participantes compreendam melhor determinadas situações em que a realidade da rede está contida. Uma simples diferenciação entre "registro de conexão" e "endereço de IP" já gera impactos positivos na esfera judiciária (SYDOW, 2015, p. 275).

Com a entrada em vigor do Marco Civil da Internet, a operação das empresas que atuam na internet passa a ser mais transparente, a proteção dos dados pessoais e a privacidade dos usuários passam a ser garantidas por lei. Isso significa, por exemplo, que essas empresas que trabalham com os dados dos usuários com fins publicitários não poderão mais repassar suas informações para terceiros sem que haja o livre e expresso consentimento do usuário.

Importante também são os preceitos do inciso VI do artigo 7º que apresenta o direito de informação – já previsto no Código de Defesa do Consumidor (BRASIL, 1990) –, mas que agora é reiterado aos usuários nos termos em que devem ser prestadas "informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade" (BRASIL, 2014). Essa prerrogativa, faz com que seja reconhecida a circunstância de fragilidade do usuário

perante os outros atores do meio digital, além dos constantes abusos praticados pelos provedores para obter vantagens ilícitas dos usuários (SYDOW, 2015, p. 275-276).

Com o advento do Marco Civil da Internet, a proteção aos dados dos usuários passa a ter uma maior garantia e só pode ser quebrada mediante ordem judicial. Isso também significa que, caso o internauta queira encerrar sua conta em uma determinada rede social ou serviço *online*, este pode solicitar que seus dados pessoais sejam excluídos de forma definitiva, pois, após a Lei nº 12.965 de 2014 (BRASIL, 2014) ter entrado em vigor, é garantido ao usuário que seus dados lhe pertençam, e não à terceiros.

Outra inovação é a garantia da privacidade das comunicações, que antes era restrito, não tendo validade para os serviços de e-mail, como exemplo. A partir de então, o conteúdo das comunicações privadas em meios eletrônicos passa a ter igual proteção de privacidade que já era prevista para os meios de comunicação tradicionais como cartas e conversas telefônicas. A criação expressa de valores como inviolabilidade do usuário e de suas comunicações e dados apresenta uma nova realidade merecedora de proteção. Cabe, portanto, ao Direito Penal legitimar valores para que determinados bens jurídicos protegidos possam surgir legitimamente (SYDOW, 2015, p. 276).

No que tange à forma como serão conduzidas as investigações policiais, Spencer Toth Sydow ressalta a importância de se fazer uma distinção entre os conceitos de "dados estáticos" e "dados dinâmicos". Os dados estáticos são os registros imutáveis que um usuário tem na rede, enquanto os dinâmicos são os dados de navegação, as conversas, registros de *download*, entre outros. Para o acesso aos primeiros, o inciso IV do artigo 3º da Lei nº 12.850 de 2013 (BRASIL, 2013), conhecida como Lei de Organização Criminosa, prevê que em qualquer fase da persecução penal, serão permitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção de prova: "IV - acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais" (BRASIL, 2013). Para os dados dinâmicos, a regra passa a constar no Marco Civil da Internet e estes ficam limitados a serem cedidos apenas mediante autorização judicial (SYDOW, 2015, p. 277).

O artigo 22 da Lei prevê que "a parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet" (BRASIL, 2014). Isso significa que o particular interessado também poderá requerer ao juiz competente, as informações estáticas e dinâmicas com o objetivo de formar o conjunto probatório. Entretanto, o tratamento é mais

rigoroso em relação ao particular frente às autoridades do Ministério Público, uma vez que o requerimento será considerado inadmissível caso não sejam explicitamente demonstrados os indícios da ocorrência do delito, a justificativa motivada da utilidade dos registros e o período ao qual os registros fazem referência (SYDOW, 2015, p. 277).

Em relação à competência para obtenção de informações em crimes digitais, o artigo 11 do Marco Civil, em total sintonia com as regras de territorialidade do artigo 5º do Código Penal (BRASIL, 1940), apresentou que:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> §1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> §2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> §3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> §4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo (BRASIL, 2014).

Outra inovação trazida pela Lei nº 12.965 (BRASIL, 2014) diz respeito à fixação do prazo de manutenção de registros de conexão de um ano para o administrador de sistema autônomo provedor de internet. A ausência de busca de tais registros em um prazo razoável gerava dificuldades na obtenção de elementos probatórios, então a lei criou uma situação de dilação de prazo de guarda, a partir da requisição cautelar de armazenamento por período superior ao *caput* do artigo 13. Os titulares desses pedidos são, de forma exclusiva, a autoridade policial, a autoridade administrativa e o Ministério Público. Essa titularidade também é garantida em caso de guarda de registros de acesso a aplicações de internet, em uma sistemática semelhante, porém com o prazo de 6 meses de guarda (SYDOW, 2015, p. 277).

O artigo 18 do Marco Civil da Internet fala de irresponsabilidade civil dos provedores de conexão em relação a danos provenientes de conteúdos gerados por seus usuários. Entretanto, no artigo 19, explica-se que haverá sim uma responsabilidade civil, mas somente nos casos de os provedores receberem ordem judicial e não tornarem indisponíveis os conteúdos apontados como ilegais. Porém, essas regras são irrelevantes para a seara penal, uma vez que os provedores são pessoas jurídicas e, no ordenamento jurídico brasileiro, há diversos limites

para responsabilização criminal de pessoas jurídicas. Apenas quando houver regras de responsabilidades penais que possam individualizar uma conduta e culpabilizar uma pessoa física é que poderão eventualmente atribuir alguma sanção, como em casos de estelionato e difamação (SYDOW, 2015, p. 278).

Entre as mudanças que a nova lei promove, uma das mais relevantes é justamente sobre a retirada de conteúdos impróprios do ar. Antes da sua promulgação, não havia uma regra clara sobre esse procedimento. A partir de então, a retirada de conteúdos do ar passa a ser executada mediante ordem judicial, com exceção dos casos de "pornografia de vingança". Aquele que for vítima de violações de sua intimidade, poderá solicitar a retirada do conteúdo diretamente aos sites ou serviços em que esses materiais estejam hospedados. Caso a retirada ocorra, os provedores de acesso deverão comunicar "os motivos e informações relativos à não disponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo" (BRASIL, 2014), como atesta o artigo 20 da Lei (CULTURA DIGITAL, 2014).

Spencer Toth Sydow ressalta que o legislador agiu de forma errada em ter restringido tais reações extrajudiciais apenas à lógica da sexualidade, já que este poderia ter aumentado seu alcance também para circunstâncias de violações de honra, moralidade, moralidade pública e outros bens jurídicos. Para tanto, bastaria apenas uma indicação da existência de possíveis expedientes não processuais para situações de iminente ou potencial violação de bens penalmente protegidos. Com a ausência de identificação, portanto, a questão permanece apenas civil (SYDOW, 2015, p. 278).

Em relação aos critérios de competência, a Lei nº 12.965 (BRASIL, 2014) estabeleceu que são os Juizados Especiais os responsáveis pela decisão a respeito da ilegalidade ou não dos conteúdos, antes que estes sejam retirados do ar. Os casos de ofensa à honra ou injúria passam a ter tratamento igual ao que acontece fora do meio digital e são analisadas pelo judiciário, com a garantia de que todos os pedidos sejam avaliados por um juiz, e não pelo provedor de internet.

Outro avanço trazido foi a garantia de neutralidade da rede, que faz com que provedores de acesso sejam obrigados a tratar todos os dados que circulam na rede mundial de computadores de maneira igual, sem distinguir conteúdo, origem, destino ou tipo de serviço. Com isso, um provedor não pode, por exemplo, beneficiar o fluxo de tráfego de um site ou um serviço em detrimento de outro, pois a neutralidade só poderá ser excepcionada nos casos de requisitos técnicos ou serviços de emergência. Dessa forma, pode-se garantir a liberdade de manifestação do pensamento, a livre concorrência na internet e a possibilidade de o usuário escolher qual conteúdo irá acessar (CULTURA DIGITAL, 2014).

Em suma, assim como conclui Sydow, apesar de esta lei ter deixado diversas lacunas, ela tem um papel importante no estudo do Direito Penal informático e dos crimes digitais (SYDOW, 2015, p. 279), pois contribui de forma significativa para a sua adequada interpretação e tenta responder parte dos questionamentos que ainda pairavam sobre o assunto.

6 CRIMINOLOGIA E RESPOSTA ESTATAL

O expressivo crescimento do número de conexões entre os computadores tem gerado, também, o crescimento da criminalidade no meio digital, com criminosos incentivados pelo anonimato e pelas dificuldades de investigação que ainda cercam essa modalidade delitiva.

A ONU (Organização das Nações Unidas) já reconheceu a problemática dos crimes digitais, uma vez que vários países ainda não adequaram seus ordenamentos jurídicos mediante a criação e atualização de seus tipos penais e procedimentos investigativos, que pudessem ser utilizados para coibir o crescimento destes delitos (ROSSINI, 2004, p. 86).

Para isso, Emeline Piva Pinheiro ressalta fazer uma avaliação dos bens jurídicos, preocupando-se em achar um meio termo entre a liberdade de informação e a proteção de dados pessoais, para que estes bens jurídicos tutelados por diplomas legais aplicados no mundo material, também tenham validade para o mundo digital. Isto posto, não se pode desejar que o Direito Penal tutele todos os bens relevantes para a sociedade, já que este deve ter caráter subsidiário, uma verdadeira *ultima ratio* (última alternativa), sob pena de falência do sistema (PINHEIRO, 2006, p. 27).

Uma das mais marcantes características da sociedade de risco é justamente a falsa crença de que o Direito Penal deva ser chamado a todo o tempo para atuar na vida dos cidadãos. Com isso, Emeline Pinheiro julga inegável se considerar que se vive, atualmente, um período de intensa inflação legislativa em que uma lei penal sobre crimes digitais só viria a aumentar a quantidade de leis já editadas e que não possuem eficácia. A expansão patológica do Direito Penal começa com a criminalização generalizada das mais mínimas ações, em flagrante descompromisso com o princípio da intervenção mínima do Direito Penal (PINHEIRO, 2006, p. 27). Luiz Flávio Gomes e Alice Bianchini afirmam que essa hipertrofia penal se agravou com o modelo social de Estado que, nas últimas duas décadas, influenciou diretamente no crescimento de incriminações cada vez mais abusivas, como a Lei dos Crimes Hediondos (BRASIL, 1990) que, segundo o autor, é ineficaz, já que não fez diminuir os crimes desta espécie (GOMES; BIANCHINI, 2003, p. 264).

Neste sentido, Salo de Carvalho disserta que:

> A alternativa ao Estado providência, portanto, passa a ser um Estado penitência, configurando uma máxima que parece ser a palavra de ordem na atualidade: Estado social mínimo, Estado penal máximo. Gesta-se, no interior dessa ideologia, uma saída plausível para aqueles que foram destruídos ou que nunca chegaram a ter cidadania: a marginalização social potencializada pelo incremento da máquina de controle social, sobretudo carcerária.
> [...]

> Exigiu-se da estrutura liberal (genealógica) do direito penal algo que dificilmente terá capacidade resolutiva, projetando severos índices de ineficácia. Desde esta perspectiva, pode-se afirmar a existência de uma 'Constituição Penal', idealizadora/instrumentalizadora de um Estado Penal, plenamente realizada (CARVALHO, 2006, p. 190).

Além do mais, existe a problemática da jurisdição e competência no ciberespaço, como foi aprofundado nos capítulos referentes ao assunto. Com o fato de o mundo digital não possuir fronteiras físicas, o conceito clássico de soberania estatal acaba sendo, de certa forma, relativizado, assim como é o do tempo. A integração mundial dos computadores pela internet passa a ser terreno fértil para a ação de criminosos que, munidos das tecnologias mais avançadas, atuem num espaço no qual as prescrições jurídicas nacionais não são suficientes, pois carecem de uma cooperação global para trazer resultados efetivos e duradouros. Augusto Eduardo de Souza Rossini destaca a necessidade de se tratar um problema global através de uma solução também global, fazendo com que as providências tomadas por países em seus respectivos territórios, ou por diferentes nações em âmbito global, sejam harmonizadas entre si, já que o meio digital é transnacional. Não se trata, portanto, de uma tarefa exclusiva do Direito, mas de um trabalho conjunto em nível internacional e transdisciplinar (ROSSINI, 2004, p. 24-25).

Não se pode negar, contudo, que quando há a possibilidade de violação de bens jurídicos dotados de importância maior, estes justificam a intervenção do âmbito penal. Por esse motivo, levando-se em conta o cenário de constante mudança social exposto anteriormente e, considerando as mais variadas dificuldades jurídicas surgidas em razão do desenvolvimento tecnológico, Marcelo Xavier de Freitas Crespo menciona uma linha de resposta para esta problemática, denominada teoria da lei da informação (CRESPO, 2011, p. 99).

Desenvolvida por Ulrich Sieber, a teoria da lei penal da informação traz a constatação de que, cada inovação tecnológica é seguida por uma adaptação dos delitos. Esse fenômeno é verificável especialmente pela observação das legislações estrangeiras e o modo que estas se desenvolveram. Além disso, esse processo se inicia de forma mais lenta e prossegue em passo crescente (ROVIRA DEL CANTO, 2002, p. 40).

Essa teoria propõe que a informação seja considerada como um terceiro elemento básico ao lado das coisas e da energia. Com isso, a informação passa a ser um novo bem econômico, cultural e político, além de um perigo em potencial. Como a informação possui a capacidade de modificação do cenário social por ser um fator ativo nas mudanças de sistemas de processamento de dados, torna-se necessário que o Direito Penal se adapte a ela,

reconsiderando-se os valores atribuídos a bens jurídicos imateriais, sem deixar de diferenciá-los dos bens materiais (CRESPO, 2011, p. 99-100).

Para Sieber, as informações não devem vincular-se às pessoas – como geralmente ocorre em relação aos bens materiais –, de modo que devem ser tratadas como bens públicos, fluindo de forma livre na sociedade, sem um caráter absoluto de proteção. Trata-se, portanto, de um paradoxo entre a liberdade de informação e seu fluxo restrito, sem se considerar apenas o interesse econômico do proprietário dessas informações, mas também os interesses de toda a coletividade por elas (apud ROVIRA DEL CANTO, 2002, p. 41-42).

Dessa forma, o direito de acesso às informações passa a ter uma maior significância, não apenas para as autoridades governamentais e judiciárias encarregadas da persecução dos delitos, mas também para os cidadãos, como se verifica na Lei nº 13.709 de 2018, também chamada de Lei de Proteção de Dados (BRASIL, 2018). Em suma, Ulrich Sieber afirma que, a disciplina legal para a informação não pode ser a mesma aplicada aos bens materiais, pois deve-se garantir proteção ao criador da informação, aos cidadãos expostos a ela e, também, ao seu acesso de forma que a propriedade intelectual, a intimidade e os direitos de acesso à essa informação passam a ser objeto de proteção legal e devem servir de base para as reformas legais referentes às sociedades de informação (apud ROVIRA DEL CANTO, 2002, p. 41-42).

Crespo traz à tona a ideia de que, na sociedade de risco, há o clamor por uma lei penal também de risco, pois as posturas doutrinárias tradicionais centradas nos bens jurídicos individuais são incapazes de solucionar os novos desafios da criminalidade, levando o Direito Penal a ter um caráter meramente simbólico. Isto posto, é necessário que haja uma renovação desse Direito Penal clássico, de modo a conferir respostas mais efetivas às carências da sociedade. É nesse momento em o autor afirma serem aplicadas as leis penais de risco, cuja técnica se baseia na aplicação de normas penais em branco, de modo a flexibilizar os tipos penais. Entretanto, tal aplicação, deve ser feita de forma ponderada, sem que haja exageros e discricionariedades, para que sejam respeitados a lei penal e o princípio da legalidade (CRESPO, 2011, p. 100-101).

Gustavo Testa Corrêa afirma que o ordenamento jurídico vigente não está conseguindo acompanhar o ritmo das inovações tecnológicas e de comunicação, sendo possível se deparar, dentro da legislação brasileira, com algumas lacunas, as quais o Direito tem o dever de suprir, mediante um esforço concentrado para compreender sua real necessidade (CORRÊA, 2008, p. 12). Quanto aos novos riscos derivados dessa evolução, Marcelo Crespo entende como legítima a incriminação de algumas condutas que configurem perigo abstrato, já que a informação,

dentro da sociedade de risco, passa a ter um valor supraindividual que necessita ser observado sob novas perspectivas (CRESPO, 2011, p. 101).

Para Gimenes, apesar de não estarem satisfatoriamente codificados em diplomas legais, dadas as particularidades dos crimes digitais, em especial os que utilizam da internet, estes já estão sendo adequados à legislação positiva existente, na qual encontram refúgio, ainda que incidental, variando a sua tipificação conforme o bem jurídico violado (GIMENES, 2013, p. 12-13).

Embora a internet ainda seja considerada por muitos como território livre e impune, na realidade é diferente. Diariamente o judiciário vem coibindo a sensação de impunidade presente no ciberespaço e combatendo a criminalidade digital com a aplicação do Código Penal (BRASIL, 1940), do Código Civil (BRASIL, 2002) e de legislações específicas como a Lei nº 9.296 de 1996 (BRASIL, 1996), que versa sobre as interceptações de comunicação em sistemas de telefonia, informática e telemática, e a Lei nº 9.609 de 1998 (BRASIL, 1998) que trata da proteção da propriedade intelectual de programas de computador (GIMENES, 2013, p. 13).

Segundo Antonio Garcia-Pablos de Molina, o estudo criminológico aponta três diferentes formas de prevenção de conflitos para qualquer espécie de infração penal: a prevenção primária, a secundária e a terciária, levando-se em conta, o critério etiológico (GARCIA-PABLOS DE MOLINA, 2006, p. 312-314).

A prevenção primária é aquela que visa combater que o delito seja cogitado, através de investimentos em educação, conscientização, emprego e assistência social para que, dessa forma, se consiga afetar a raiz social do conflito criminal, buscando inibir que ele venha sequer a se manifestar (SYDOW, 2015, p. 135). É importante ressaltar que a falta de direitos básicos e de condições mínimas de sobrevivência contribuem de forma direta para que os cidadãos excluídos socialmente sejam levados a cometerem delitos. Spencer Toth Sydow destaca o fato de países com menos oportunidades e com maiores índices de desigualdades possuírem a tendência de apresentar um maior índice de criminalidade, especialmente patrimonial. Com isso, a intervenção preventiva estatal deve focar nas diferenças sociais como origem do delito, investindo nos setores culturais, econômicos e sociais por longos períodos, de forma a criar um segmento social mais igualitário e consciente, em que os crimes deixam de ser ponderados como uma opção (SYDOW, 2015, p. 136).

Por sua vez, a prevenção secundária de Pablos de Molina atua no foco da experiência obtida a partir de uma análise empírica da criminalidade, após estudo do tempo e espaço em que os crimes são praticados com determinada frequência. Através da estatística e do conhecimento pragmático, o Estado tem melhores condições de prevenir o acontecimento dos

delitos, agindo geograficamente – diminuindo o tempo em que os semáforos ficam fechados, mantendo carros de polícia em cruzamentos específicos, melhorando a iluminação de vias e espaços públicos, entre outros – ou mediante políticas legislativas e policiais (SYDOW, 2015, p. 136). Estes atos produzem efeitos a curto e médio prazo, já que retiram o ambiente propício do delinquente, agindo no foco potencial da ação de forma a desestimular que a infração ocorra naquele local. Entretanto, essa prevenção tem caráter paliativo e possui um efeito de prorrogação do momento e da região do delito, uma vez que o criminoso buscará, em outros lugares, ambientes mais propícios para o consentimento de seus delitos (SYDOW, 2015, p. 136-137).

Por último, a prevenção terciária que, diferentemente das modalidades anteriores trazerem atitudes focadas em todos os cidadãos de forma genérica, esta é focada na figura do recluso condenado e na prevenção de reincidências. Através de programas de ressocialização e de reinclusão social, visa dar ao preso condições de, ao sair do estabelecimento prisional, ser capaz de enfrentar o desafio da realocação social e, dessa forma, não ser (re)incentivado a comentar novos crimes (apud SYDOW, 2015, p. 137).

Porém, este estudo da prevenção de Pablos de Molina trata de crimes denominados "reais", ou seja, aqueles cometidos no mundo material, dos quais, para que pudessem ser desenvolvidas estratégias de prevenção, foram necessários apontamentos de traços similares de tal esfera da criminalidade. Para Sydow, os crimes considerados "reais" são, respectivamente:

> a) cometidos com a presença física entre ofensor e ofendido;
> b) crimes em que a ação em regra ocorre na modalidade um contra um, ou seja, o contato do ofensor é direto com cada vítima;
> c) os que exigem o uso de força, presença e planejamento por parte do ofensor, que se expõe e se arrisca;
> d) os que se desenvolvem de acordo com uma lógica, vestindo-se de generalidades e estilos na prática (SYDOW, 2015, p. 137).

Quando se trata de crimes digitais, entretanto, a problemática reside no fato de que a prevenção primária se mostra incapaz, as características especiais ineficazes em relação às ações da prevenção secundária, enquanto a prevenção terciária somente tem motivo de existir em um novo conceito de ressocialização. O crime digital dispensa a presença física do agente, o contato direto com a vítima e o uso da força. Este ocorre a partir de uma ação contra uma ou várias pessoas, sem respeitar uma lógica ou estilo e passível de constantes modificações em suas táticas de cometimento (SYDOW, 2015, p. 138). Além disso, só é possível notar o crime digital após seu cometimento, o que permite ao autor apagar os rastros sobre sua ação e seu paradeiro, tendo em vista a volatilidade de seu material probatório.

Além das ineficiências já citadas, as prevenções primária e terciária também se mostram inócuas em relação a pessoa do delinquente virtual, uma vez que se acredita que o agente compreende o caráter ilegal de suas ações, tem um determinado grau de instrução e educação tecnológica e até boas condições sociais. No mesmo sentido, não se pode falar em necessidade de ressocialização para o criminoso voluntário que pratica o fato típico revestido de motivos que, em muitas vezes, não se encaixam em qualquer das teorias criminológicas, mas sem em teorias de anulação de responsabilidade ou de técnicas de neutralização, utilizadas pelos desviantes (SYDOW, 2015, p. 139).

As questões jurídicas advindas do incremento do uso da tecnologia informática são claramente complexas e não podem ser tratadas com a simples incriminação de determinadas condutas. A legislação do país deve ser revista não só no âmbito penal, mas de forma conjugada e colaborativa.

A lei penal sobre crimes digitais tem passado por mudanças significativas desde a década de 1970, quando as novas formas de cometimento de delitos trouxeram à luz questões que acarretaram reformas na lei (CRESPO, 2011, p. 34). Inicialmente, cumpre observar que, no ano de 2012, foram promulgadas duas leis que visam coibir a prática de crimes digitais, sendo elas a Lei nº 12.735 (BRASIL, 2012), também conhecida como Lei Azeredo, e a Lei nº 12.737 (BRASIL, 2012), popularmente chamada de Lei Carolina Dieckman (MACHADO; SILVA, 2013, p. 70).

A Lei nº 12.735 de 2012 (BRASIL, 2012) possui apenas duas disposições, sendo que uma delas se refere à uma determinação às autoridades policias de estruturação organizada no combate aos crimes digitais, enquanto a outra acrescenta a possibilidade de cessação de transmissões eletrônicas quando houver prática, induzimento ou incitação à discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.

Do outro lado, a Lei nº 12.737 de 2012 (BRASIL, 2012) teve larga repercussão nacional após a notícia do vazamento de fotos íntimas da atriz Carolina Dieckman pela internet, induzindo o pensamento de que houve uma significativa influência midiática na atuação do Poder Legislativo em tal caso. Luís Antônio Licks Missel Machado e Jardel Luís da Silva alertam para o perigo de tal ocorrência, uma vez que diante da seriedade que se espera quando se aborda a lei penal, não seria ideal que se cedesse às pressões sofridas pela imprensa, de forma que o debate se torna prejudicado, assim como, provavelmente, a qualidade do texto legislativo (MACHADO; SILVA, 2013, p. 70).

Com relação ao texto da lei, este insere artigos no Código Penal (BRASIL, 1940) que versam sobre os delitos de invasão de dispositivo informático – também chamado de intrusão

informática – (artigo 154-A), interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade público (artigo 266) e de falsificação de cartão (artigo 298, parágrafo único).

O crime de intrusão informática do artigo 154-A do Código Penal brasileiro (BRASIL, 1940) já foi discutido em capítulo próprio neste trabalho, ao se tratar de exemplos de crimes digitais próprios. Esta conduta, como visto, pode ocorrer por diversas razões, tais como pelo mero deleite em superar desafios técnicos de segurança e invadir a privacidade alheia, como, na hipótese mais grave, de intenção de manipular ou sabotar dados e informações. Com isso, esse delito assume uma especial relevância, pois pode ser considerado como um verdadeiro crime meio para a realização de diversos outros delitos. Entretanto, o legislador optou por não identificar as demais condutas, nem sequer aduzir formas específicas para seu combate, gerando certa insegurança jurídica (CRESPO, 2011, p. 171).

Além disso, existem diversos outros crimes cometidos através da internet, mas que encontram sua previsão legal em outras áreas criminais, além dos crimes digitais impróprios que já possuem tipificação na lei penal, mas que passaram a ser cometidos através do auxílio do meio tecnológico. Destarte, é possível observar que o Estado tem avançado ao prever algumas condutas criminosas, apesar que ainda há muito a ser feito em relação a uma efetiva proteção estatal quando se trata do ciberespaço (COLLI, 2010, p. 132). A ausência de disposições claras das condutas no ordenamento jurídico acaba agravando as dificuldades já existentes para a investigação dos crimes digitais, principalmente em relação ao sujeito, às provas, ao tempo e ao local do crime, que se tornam ainda mais complexos quando se trata desta modalidade delitiva.

7 CONCLUSÃO

O avanço do processo de globalização trouxe profundas evoluções no campo tecnológico, encurtando distâncias e acelerando transformações sociais na era da informação. Entretanto, apesar desses vários progressos, a revolução informática também exerceu forte influência no campo do Direito Penal, mudando não só a forma de cometimento dos crimes já previstos na lei penal, mas também inaugurando novas figuras delitivas e novos bens jurídicos.

Até o momento, não existe nenhuma espécie de "código de condutas ou comportamentos" transacional na internet. No seu início, no final da década de 1960 nos Estados Unidos, apostava-se que as redes e seus usuários seriam capazes de se autorregular, o que hoje pode-se constatar que não se passava de um mero equívoco. As informações e dados que circulam na rede passaram a ter um alto valor econômico e social, quando a internet passou a ocupar um espaço essencial na vida em sociedade. Com isso, a rede passa a ser, cada vez mais, alvo de uma conduta delinquente na qual não se pode, sequer, calcular a dimensão dos riscos em que se está exposto, típico de uma sociedade de risco.

Apesar de uma parcela dos usuários não perceber que a internet é uma mera extensão da sociedade, grande parte dos mesmos riscos existentes no mundo real também incidem no meio digital. A anonimidade do acesso, apesar de dar ao usuário comum a sensação de privacidade, por outro lado traz a ideia de oportunidade para o delinquente agir de forma desapercebida, o que contribui para o crescimento dos crimes digitais. Esta modalidade delitiva possui particularidades e complexidades em que não se consegue mensurar as dimensões de seu dano, além das dificuldades de investigação, obtenção e manipulação de prova, e também da identificação dos autores.

Os crimes digitais são, portanto, todas as ações típicas, antijurídicas e culpáveis cuja prática envolva o processamento automático de dados ou sua transmissão, em que um dispositivo conectado à internet seja o objeto ou o instrumento da ação delituosa, ainda que o crime pudesse ser praticado de outra forma. Diferentemente da criminalidade no mundo material, no meio digital existe um distanciamento espacial entre autor e vítima do delito, fazendo com que o crime digital seja ainda mais difícil de ser combatido. Com isso, dificuldades são percebidas no procedimento investigatório delitivo, uma vez que a variação de fronteiras pode exigir cooperação entre diferentes sistemas jurídicos de diversos países, o que também pode ocasionar barreiras burocráticas intransponíveis que impedem qualquer condenação.

Outra característica fundamental desses crimes é a volatilidade da materialidade dos delitos, já que os dados e informações no meio digital não se encontram, necessariamente, em

apenas um lugar, podendo ser facilmente modificados ou suprimidos. Entretanto, não deixar nenhuma espécie de vestígio que possa contribuir para a persecução penal de um crime digital é uma tarefa difícil. Caso haja colaboração dos provedores de internet e celeridade na investigação, a identificação da autoria se torna plenamente possível. A dificuldade é maior no que tange à punição desses infratores, estando aí a principal problemática dos crimes digitais, devido às barreiras criadas pela legislação inespecífica e as fronteiras da transnacionalidade.

Diante dos novos riscos que surgem a partir da evolução da tecnologia informática, o bem jurídico penal também passa por transformações. Ao se tratar de crimes digitais, pode-se dizer que as condutas delitivas atingem não só os valores tradicionalmente protegidos, mas também os dados armazenados (informações) e a segurança dos sistemas de redes informáticas ou de comunicação. A informação, então, passa a ter um papel preponderante na vida do ser humano, sendo o principal bem jurídico a ser tutelado nesta modalidade delitiva. Além dela, a confiabilidade e a segurança dos sistemas e redes informáticas e de comunicação também passam a fazer parte da tutela do Direito Penal.

Ao longo do presente trabalho discorre-se que o simples fato de um computador estar sendo usado como meio para o cometimento de um delito não deveria fazer com que este fosse considerado um crime digital, mas um delito já previsto no ordenamento jurídico pátrio com um diferente *modus operandi*. Porém, ficou convencionado por parte da doutrina e da imprensa nacional que qualquer ilícito que seja praticado com o uso da tecnologia o caracterizaria como um crime digital. Entretanto, fora necessária uma diferenciação entre os delitos praticados contra algum bem jurídico informático como sistemas ou dados e aqueles que são perpetrados contra bens jurídicos tradicionais, não relativos à tecnologia, chamados de crimes digitais próprios e crimes digitais impróprios, respectivamente.

Entre as problemáticas que envolvem os crimes digitais, determinar o momento e o local da sua ocorrência estão entre os maiores desafios. Em relação ao momento do crime, o Código Penal (BRASIL, 1940) adotou a teoria da atividade ao considerar praticado o delito no momento da ação ou omissão, ainda que seja diferente o momento do resultado. Isso possui importantes implicações no âmbito digital, uma vez que, de forma geral, o tempo entre a ação e o resultado é relativamente grande. Já em relação ao local do crime, a lei penal consagrou a teoria pura da ubiquidade, ao considerar praticado o delito no local em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria ter produzido o resultado. Com isso, caso um crime digital seja cometido através da internet, e o agente se encontre em um país diferente do da vítima, a aplicação dessa norma seria extremamente simples, desde que ambos os Estados possuam tipificação para esses delitos. Entretanto, quando a conduta é típica em

apenas um dos países, a solução é bem mais complexa, pois não existe uma solução pacífica dentro da doutrina e nem critérios seguros que determinem em qual medida o local da prática de um ilícito se consuma deva ser considerado o local exato do crime. Parte dos autores acredita que os tratados internacionais devem discorrer sobre a questão, em nível de cooperação, para que estes sejam tratados onde o dano resultante for maior, ou onde haja melhores condições de investigação. Por outro lado, existem autores que ressaltam que a solução para essa questão deva partir do pressuposto de que as normas de caráter penal devam ser interpretadas sempre de forma restritiva, optando por aquela que menor restringir a liberdade do cidadão.

O melhor caminho a ser seguido, portanto, é o do entendimento entre os diferentes países para que estes harmonizem suas legislações com o objetivo de possibilitar uma investigação mais efetiva. A falta de disposições claras e de harmonização entre os diferentes sistemas jurídicos em relação a essa modalidade delitiva é a principal dificuldade enfrentada ao se investigar um crime digital, o que contribui diretamente pelos baixos índices de punição de seus sujeitos ativos.

O ordenamento jurídico brasileiro apresenta uma tentativa de solução que se baseia em conceitos, princípios e práticas já reiteradas pelo direito pátrio, se adaptando ao atual momento. Porém, enquanto não houver um tratado internacional único que pacifique essa questão, cabe aos provedores de internet, detentoras das provas digitais, cumprir a legislação do local onde estas oferecem seus serviços, colaborando de forma efetiva para o andamento das investigações e a solução de conflitos

Apesar de a internet parecer uma rede imaterial, seu funcionamento está condicionado à existência de uma infraestrutura real que, para ser acessada, depende da atuação das empresas provedoras de conexão de rede que, a partir de então, passam a deter as informações referentes aos passos que os usuários percorrem na internet. São essas informações que permitem, de forma precisa, desvendar um crime digital ou obter um material probatório para a elucidação de um crime do mundo material. Com a entrada em vigor do Marco Civil da Internet no ano de 2014, a operação dessas empresas provedoras de internet passou a ser mais transparente, já que a proteção dos dados pessoais e a privacidade dos usuários passaram a ser garantidas por lei.

Com isso, toda e qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, passa a ser, obrigatoriamente, respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Outro avanço trazido foi a garantia de neutralidade da rede, que faz com que provedores de acesso sejam obrigados a

tratar todos os dados que circulam na rede mundial de computadores de maneira igual, sem distinguir conteúdo, origem, destino ou tipo de serviço. Apesar de ter deixado diversas lacunas, o Marco Civil da Internet possui um importante papel no estudo do Direito Penal informático e dos crimes digitais, pois contribui de forma significativa para a sua adequada interpretação.

Os crimes praticados no ciberespaço, em grande parte das vezes, não deixam vestígios e, com a obscuridade da rede mundial de computadores, os autores desses delitos ficam à sombra do anonimato, devido à fragilidade do material probatório. A prova no meio digital, além de volátil, é bastante variada, podendo ser arquivos digitais, registros de servidores, históricos de navegação, fotos, vídeos, e-mails, entre outros. Por causa de suas particularidades, caso esta não seja prontamente preservada, pode ser rapidamente danificada, alterada ou até suprimida, impedindo qualquer investigação ou identificação do autor do delito.

O processo penal é reconhecidamente um instrumento de retrospecção no qual há uma tentativa de se reconstruir, de forma aproximada, um determinado fato para transportar os elementos de prova encontrados na realidade objetiva para os autos do procedimento. Dessa forma, é através das provas que se busca fazer esta reconstrução aproximada do fato passado, ou seja, do crime. Entretanto, a prova não pode ser compreendida apenas como aquilo que contribui para instrução e convencimento do juiz, mas também um direito fundamental decorrente do devido processo legal, no qual institui complexas garantias processuais que reconhecem que não só o juiz, mas também as partes são destinatárias desta.

O Código de Processo Penal brasileiro (BRASIL, 1941), estabeleceu que o meio de prova mais adequado para se demonstrar uma prática criminosa é o exame de corpo de delito, caso a infração penal tenha deixado vestígios. Parte da doutrina defende que não se faz prova da existência de um crime digital sem o devido exame de corpo de delito, formalizado em laudo técnico pericial. Isso porque a execução do crime envolve aspectos técnicos muito específicos, que exigem conhecimento científico de informática para atestar sua existência. Entretanto, outros autores defendem que o exame pericial pode ser dispensado quando estiverem presentes outros elementos probatórios que sejam suficientes para atestar a materialidade do crime. De acordo com os preceitos do artigo 167 do Código de Processo Penal (BRASIL, 1941), a dispensa do exame de corpo de delito ocorreria, portanto, somente nos casos em que houvesse o desaparecimento dos vestígios materiais, podendo ser substituído pela prova testemunhal. Outra excepcionalidade é o caso dos fatos serem de conhecimento comum – que fazem parte da cultura geral da sociedade – e não necessitarem de exame pericial, pois estão ao alcance de qualquer pessoa, podendo ser comprovados através de qualquer meio. Nessa categoria estão diversos fatos do conhecimento popular relacionado aos crimes digitais, como por exemplo o

funcionamento prático da internet e o acesso público a manifestações individuais em redes sociais.

Para a que haja a devida coleta de provas em grande parte dos crimes cometidos no meio digital, muitas vezes é necessário que ocorra a quebra de sigilo da troca de mensagens entre usuários. Porém, isso gera questionamentos a respeito de violações de garantias individuais como a da privacidade. Entretanto, a privacidade não tem valor apenas para a vida privada de cada indivíduo, mas também para a comunidade. Esta não deve ser entendida como uma exclusividade individual, mas um direito necessário para a manutenção do exercício da cidadania e do interesse público.

Contudo, diferentemente da concepção clássica, o interesse público não pode ser compreendido como antagônico e nem superior ao interesse individual. Com a evolução dos sistemas jurídicos, a pré-concepção de que o interesse público seja promovido exclusivamente pelo Estado não mais satisfaz os anseios da sociedade pluralista contemporânea que carece de uma participação ativa em sua construção. Nesse sentido, o termo "interesse público" deve ser compreendido como resultado do exercício da autonomia pública dos cidadãos de uma determinada comunidade jurídica em um contexto histórico em que não haja uma relação de antagonismo entre público e privado – diferentemente do que institui o princípio da supremacia do interesse público –, mas sim uma relação de complementariedade e interdependência entre eles. O exercício da autonomia pública só é possível caso a autonomia privada esteja igualmente garantida aos cidadãos.

Além das particularidades referentes às provas no meio digital e das divergências entre os diferentes sistemas jurídicos responsáveis pela sua investigação, o expressivo crescimento do número de conexões entre os computadores tem gerado, também, o crescimento vertiginoso da criminalidade no meio digital e na complexidade de se combater esses delitos. A ONU (Organização das Nações Unidas) já reconhece a problemática dos crimes digitais, uma vez que vários países ainda não adequaram seus ordenamentos jurídicos mediante a criação e atualização de seus tipos penais e procedimentos investigativos, que pudessem ser utilizados para coibir o crescimento destes delitos. Para isso, é preciso tratar-se o problema fazendo com que as providências tomadas por países em seus respectivos territórios, ou por diferentes nações em âmbito global, sejam harmonizadas entre si, já que o meio digital é transnacional. Não se trata, portanto, de uma tarefa exclusiva do Direito, mas de um trabalho conjunto em nível internacional e transdisciplinar.

Apesar de a internet ainda ser considerada por muitos como um território livre e impune, na realidade se mostra diferente. Diariamente o judiciário tem buscado coibir a sensação de

impunidade no meio digital e combater a criminalidade através da aplicação das leis penais e de legislações específicas. Ainda que não estejam satisfatoriamente codificados em diplomas legais, estes já estão sendo, de forma pontual, adequados à legislação positiva existente. As questões jurídicas advindas do incremento do uso da tecnologia informática são claramente complexas e não podem ser tratadas apenas com a incriminação de determinadas condutas. A legislação nacional precisa ser revista não só penalmente, mas de forma conjugada e colaborativa. Além disso, é possível observar que o Estado tem avançado ao prever algumas condutas criminosas, apesar de que ainda há muito a ser feito em relação a uma efetiva proteção penal quando se trata do meio digital. A ausência de disposições claras das condutas no ordenamento jurídico acaba agravando as dificuldades já existentes para a investigação dos crimes digitais, principalmente em relação ao sujeito, às provas, ao tempo e ao local do crime, que se tornam ainda mais complexos quando se trata desta modalidade delitiva.

REFERÊNCIAS

ALLEGRO, Romana Affonso de Almeida. **Bens jurídicos:** o interesse estatal de tutelar bens jurídicos através de sua normatização. Disponível em: https://www.direitonet.com.br/artigos/exibir/2089/Bens-juridicos. Acesso em: 10 abr. 2018.

ARIMURA, Mayumi. **Saiba a diferença entre hackers, crackers, white hat, black hat, gray hat, entre outros.** 2016. Disponível em: http://www.egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros. Acesso em: 06 nov. 2018.

ARÚS, Francisco Bueno. **Els delictes relatius a la informática.** Barcelona: Stvdia Juridica, 1997. v. 13.

ASCENSÃO, José de Oliveira. **Direito da internet e da sociedade da informação:** estudos. Rio de Janeiro: Forense, 2002.

ASSIS, Christiane Costa. O Interesse Público na Teoria Discursiva do Direito. **Revista de Estudos Jurídicos da Unesp.** UNESP, v. 15, p. 109-117, 2011.

ÁVILA, Humberto. Repensando o "Princípio da Supremacia do Interesse Público sobre o Particular". In: SARMENTO, Daniel (org.). **Interesses públicos versus interesses privados: desconstruindo o princípio da supremacia do interesse público.** Rio de Janeiro: Lúmen Juris, 2010.

BADARÓ, Gustavo Henrique. **Processo penal.** 4. ed. Revista dos Tribunais. São Paulo. 2016.

BAPTISTA, Patrícia. **Transformações do direito administrativo.** Rio de Janeiro: Renovar, 2003.

BARROS, Marco Antonio. **A busca da verdade no processo penal.** São Paulo: Revista dos Tribunais, 2011.

BECK, Ulrich. **A sociedade de risco:** rumo a uma outra modernidade. São Paulo: Editora 34, 2010.

BIANCHINI, Alice; GARCIA-PABLOS DE MOLINA, Antonio; GOMES, Luiz Flávio. **Direito penal:** Introdução e princípios fundamentais. 2. ed. São Paulo: Revistas dos Tribunais, 2009. v. 1.

BITENCOURT, Cezar Roberto. **Tratado de direito penal:** parte geral, 23. ed. São Paulo: Saraiva, 2017. v. 1.

BLUM, Renato Opice. **Direito eletrônico:** a internet e os Tribunais. São Paulo: Edipro, 2001.

BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais.** São Paulo: Revista dos Tribunais, 2004.

BONILHA, Ínkari Coelho. **O tratamento jurídico-penal do acesso não autorizado a sistema informático**. 2006. Dissertação (Mestrado) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2006.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 28 dez. 2017.

BRASIL. **Decreto nº 847, de 11 de outubro de 1890:** Promulga o Código Penal. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/1851-1899/d847.htm. Acesso em: 04 dez. 2017.

BRASIL. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940:** Código Penal. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm. Acesso em: 06 nov. 2018.

BRASIL. **Decreto-Lei nº 3.689 de 03 de outubro de 1941:** Código de Processo Penal. 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei no 10.406, de 10 de janeiro de 2002:** Institui o Código Civil. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei no 11.690, de 9 de junho de 2008:** Altera dispositivos do Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, relativos à prova, e dá outras providências.Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11690.htm. Acesso em: 29 nov. 2018.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012:** Vigência Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012:** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013**: Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei no 9.034, de 3 de maio de 1995; e dá outras providências. 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12850.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014:** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2014. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei nº 13.105, de 16 de março de 2015:** Código de Processo Civil. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018:** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei nº 7.716, de 5 de janeiro de 1989:** Define os crimes resultantes de preconceito de raça ou de cor. 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L7716.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990:** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8069.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei nº 8.072, de 25 de julho de 1990:** Dispõe sobre os crimes hediondos, nos termos do art. 5º, inciso XLIII, da Constituição Federal, e determina outras providências. 1990. Disponível em: http://www.planalto.gov.br/CCivil_03/Leis/L8072.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990:** Dispõe sobre a proteção do consumidor e dá outras providências. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996:** Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm. Acesso em: 06 nov. 2018.

BRASIL. **Lei nº 9.609, de 19 de fevereiro de 1998:** Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 06 nov. 2018.

CARNELUTTI, Francesco. **A prova civil.** Tradução de Lisa Pary Scarpa. Campinas: Bookseller, 2001.

CARVALHO, Salo de. A ferida narcísica do direito penal: primeiras observações sobre as (dis)funções do controle penal na sociedade contemporânea. In: GAUER, Ruth M. Chittó (Org.). **A qualidade do tempo**: para além das aparências históricas: história, direito, filosofia, psiquiatria, antropologia e ciências sociais. Rio de Janeiro: Lumen Júris, 2004.

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

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet.** 4. ed. São Paulo: Saraiva, 2008.

COSTA, Rodolfo. **Justiça do Rio de Janeiro determina bloqueio do WhatsApp no Brasil.** 2016. Disponível em: https://www.correiobraziliense.com.br/app/noticia/tecnologia/2016/07/19/interna_tecnologia,540833/justica-do-rio-de-janeiro-determina-bloqueio-do-whatsapp-no-brasil.shtml. Acesso em: 06 nov. 2018.

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

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais:** do que estamos falando? 2015. Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando. Acesso em: 13 dez. 2017.

DA SILVA, Jorge Luiz Silva. **A prova nos crimes que se utilizam das redes sociais.** 2017. Disponível em: https://ajufesc.org.br/wp-content/uploads/2017/02/Jorge-Luiz-Silva-da-Silva.pdf. Acesso em: 06 nov. 2018.

DIAS, Daniel de Lélis. **Os meios de prova no processo penal brasileiro e sua importância.** 2015. Disponível em: https://danielhc.jusbrasil.com.br/artigos/219666930/os-meios-de-prova-no-processo-penal-brasileiro-e-sua-importancia. Acesso em: 06 nov. 2018

DIAS, Juliana Costa Santos. **O que são rootkits e como enfrentá-los.** 2013. Disponível em: https://www.kaspersky.com.br/blog/o-que-sao-rootkits-e-como-enfrenta-los/769/. Acesso em: 08 maio 2018.

DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Shreiner. **Obtenção de provas digitais e jurisdição na internet.** São Paulo: EMAG, 2017.

FERRAJOLI, Luigi. **Direito e razão:** teoria do garantismo penal. Tradução de Ana Paula Zomer, Fauzi Hassan Chouckr, Juarez Tavares, Luiz Flávio Gomes. São Paulo: RT, 2002.

FERREIRA, Ivete Senise. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). **Direito e internet:** aspectos jurídicos relevantes. Bauru: Edipro, 2000.

FISCHGOLD, Bruno. **Direito administrativo e democracia:** a interdependência entre interesses públicos e privados na Constituição da República de 1988. 2011. 111 f. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2011.

FREITAS, Andrea; CARNEIRO, Lucianne. **Justiça do Rio determina bloqueio do serviço do WhatsApp novamente.** 2016. Disponível em: https://oglobo.globo.com/economia/justica-do-rio-determina-bloqueio-do-servico-do-whatsapp-novamente-19744594. Acesso em: 06 nov. 2018.

GARCIA-PABLOS DE MOLINA, Antonio. **Criminologia**. 5. ed. rev. e atual. São Paulo: Revista dos Tribunais, 2006.

GHEDIN, Rodrigo. **Kevin Mitnick, o hacker mais notório do mundo, responde as perguntas que você sempre quis fazer.** 2012. Disponível em: http://gizmodo.uol.com.br/kevin-mitnick-o-hacker-mais-notorio-mundo-responde-perguntas-que-voce-sempre-quis-fazer. Acesso em: 28 fev. 2018.

GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais. **Revista de Doutrina da 4ª Região**, Porto Alegre, n. 55, ago. 2013. Disponível em: http://revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Acesso em: 24 out. 2017.

GOMES, Luiz Flávio; BIANCHINI, Alice. Globalização e direito penal. In: **Escritos em homenagem a Alberto da Silva Franco.** São Paulo: Revista dos Tribunais, 2003.

GRECO, Alessandra Orcesi Pedro. **A autocolocação da vítima em risco.** São Paulo: Revista dos Tribunais, 2004.

HABERMAS, Jürgen. **A inclusão do outro:** estudos de teoria política. Tradução de George Sperber e Paulo Astor Soethe. São Paulo: Edições Loyola, 2002.

HABERMAS, Jürgen. **Direito e democracia:** entre a facticidade e validade. 2. ed. Tradução de Flávio Beno Siebeneichler. Rio de Janeiro: Tempo Brasileiro, 2010.

JEWKES, Yvonne. **Policing the net:** crime, regulation and surveillance in cyberspace. 2002. Disponível em: http://readinglists.ucl.ac.uk/items/C6BAAD01-E764-1C05-E52A-F88C8703136E.html. Acesso em: 05 dez. 2017.

JUSTEN FILHO, Marçal. **Curso de direito administrativo.** 12. ed. rev., atual e ampl. São Paulo: Editora Revista dos Tribunais, 2016.

KEMP, Simon. **Digital in 2018:** World's internet users pass the 4 billion mark. 2018. Disponível em: https://wearesocial.com/blog/2018/01/global-digital-report-2018. Acesso em: 26 mar. 2018.

KUROKAWA, Adriana Shimabukuro et al. **Crimes cibernéticos:** Manual prático de investigação. São Paulo: Procuradoria da República No Estado de São Paulo, 2006.

LA CHAPELLE, Bertrand; FEHLINGER, Paul. **Jurisdiction on the internet**: from legal arms race to transnational cooperation. internet & Jurisdiction. Paper Series, n. 28, April 2016. Disponível em: www.internetjurisdiction.net. Acesso em: 11 mar. 2018.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

LIMA, Gabriel de Araújo. Teoria da Supremacia do Interesse Público: crise, contradições e incompatibilidade de seus fundamentos com a Constituição Federal. **Revista de Direito Administrativo e Constitucional**, Belo Horizonte, no 36, p. 123-153, abr./jun. 2009.

LOPES JR, Aury. **Direito processual penal.** 14. ed. São Paulo: Saraiva, 2017.

MACHADO, Luís Antônio Licks Missel; SILVA, Jardel Luís da. **Crimes digitais:** O aumento da complexidade das relações sociais e os novos espaços de intervenção estatal. 2013

MATOS, Mariana Maria. **Da produção e colheita de provas no ambiente cibernético.** 2014. Disponível em: https://marianamariam.jusbrasil.com.br/artigos/119753698/da-producao-e-colheita-de-provas-no-ambiente-cibernetico. Acesso em: 06 nov. 2018.

MAZONI, Ana Carolina. **Crimes na internet e a Convenção de Budapeste.** 2009. 65 p. Monografia (Bacharelado em Direito) - Faculdade de Ciências Jurídicas e Sociais – FAJS, Centro Universitário de Brasília – UNICEUB, Brasília, 2009. Disponível em: http://www.repositorio.uniceub.br/bitstream/123456789/257/3/20523632.pdf. Acesso em: 04 dez. 2017.

MELLO, Celso Antônio Bandeira de. **Curso de direito administrativo.** 33. ed. São Paulo: Editora Malheiros, 2018.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Código penal interpretado.** 9. ed. São Paulo: Atlas, 2015.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de direito penal.** 32. ed. São Paulo: Atlas, 2016. v. 1.

MONTEIRO, Renato Leite. **Crimes eletrônicos:** uma análise econômica e constitucional. 2010. 192 p. Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2010. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp142465.pdf. Acesso em: 04 dez. 2017.

MOREIRA NETO, Diogo de Figueiredo. **Curso de direito administrativo.** 16. ed. Rio de Janeiro: Forense, 2014.

NIGRI, Deborah Fisch. **Crimes e segurança na internet.** In Verbis, Rio de Janeiro: Instituto dos Magistrados do Brasil, Ano 4, n. 20, p. 34-41, 2000.

NUCCI, Guilherme de Souza. **Manual de direito penal.** 13. ed. São Paulo. Saraiva. 2017.

NUCCI, Guilherme de Souza. **Provas no processo penal.** 4. ed. Rio de Janeiro: Forense, 2015.

PACELLI, Eugênio. **Curso de processo penal.** 22. ed. São Paulo: Atlas, 2018.

PACHECO, Denilson Feitoza. **Direito processual penal:** teoria, crítica e práxis. Niterói: Impetus, 2006.

PINHEIRO, Emeline Piva. **Crimes virtuais:** uma análise da criminalidade informática e da resposta estatal. Porto Alegre: PUCRS, 2006. Disponível em: http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2006_1/emeline.pdf. Acesso em: 04 dez. 2017.

POPPER, Karl Raimund. **A lógica da pesquisa científica.** Tradução de Leônidas Hegenberg; Octany Silveira da Mota. São Paulo: Cultrix, 1974.

POPPER, Karl Raimund. **Conhecimento objetivo.** Tradução de Milton Amado. Belo Horizonte: Itatiaia, 1999.

QUEIROZ, Claudemir; VARGAS, Raffael. **Investigação e perícia forense computacional**: certificações, leis processuais, estudos de caso. Rio de Janeiro: Brasport, 2010.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **Crimes virtuais.** 2005. Disponível em: http://www.advogadocriminalista.com.br. Acesso em: 22 dez. 2017.

RONCADA, Rodiner. **A prova da materialidade delitiva nos crimes cibernéticos.** São Paulo: EMAG, 2017.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal.** São Paulo: Memória Jurídica, 2004.

ROVIRA DEL CANTO, Enrique. **Delincuencia informática y fraudes informáticos.** Granada: Comares, 2002.

ROXIN, Claus. **A proteção de bens jurídicos como função do direito penal.** Tradução de André Luis Callegari e Nereu José Giacomolli. 2. ed. Porto Alegre: Livraria do Advogado, 2013.

ROXIN, Claus. **Novos estudos de direito penal.** São Paulo: Marcial Pons, 2014.

SCOLANZI, Vinícius Barbosa. Bem jurídico e Direito Penal. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 17, n. 3129, 25 jan. 2012. Disponível em: https://jus.com.br/artigos/20939. Acesso em: 10 abr. 2018.

SHIMABUKURO, Adriana. **Cibercrime:** quando a tecnologia é aliada da lei. 2017. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 06 nov. 2018.

SILVA, Douglas Rodrigues da. **Por que se fala tanto em bem jurídico no direito penal?** 2017. Disponível em: https://canalcienciascriminais.com.br/bem-juridico-direito-penal. Acesso em: 10 abr. 2018.

SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. São Paulo: Revista dos Tribunais, 2003.

SOARES JÚNIOR, Dário José. **A crise dogmática do processo penal**. Belo Horizonte: Editora D'Plácido, 2016.

SOUZA NETO, Cláudio Pereira de. **Teoria constitucional e democracia deliberativa**: um estudo sobre o papel do direito na garantia das condições para a cooperação na deliberação democrática. Rio de Janeiro: Renovar, 2006.

SUNDFELD, Carlos Ari. **Fundamentos de direito público**. 5. ed. São Paulo: Malheiros, 2012.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas.** 2. ed. São Paulo: Saraiva, 2015.

TARUFFO, Michele. **La prueba de los Hechos**. Madrid: Trotta, 2002.

TARUFFO, Michele. **La símplice verità:** il giudice e la costruzione dei fatti. Rosima-Bari: Laterza, 2009.

UOL. **Hackers e Crackers:** quais as diferenças entre eles? 2017. Disponível em: https://seguranca.uol.com.br/antivirus/dicas/curiosidades/hackers_crackers_qual_a_diferenca_entre_eles.html#rmcl. Acesso em: 06 nov. 2018.

VIANNA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais:** fundamentos de direito penal informático. 2001. 241 p. Dissertação (Mestrado em Direito) - Faculdade de Direito da UFMG, Universidade Federal de Minas Gerais, Belo Horizonte, 2001. Disponível em: http://www.bibliotecadigital.ufmg.br/dspace/handle/1843/BUOS-96MPWG. Acesso em: 06 nov. 2018.

VIANNA, Tulio Lima. **Do delito de dano e de sua aplicação ao direito penal informático.** Alfa-Redi: revista de derecho informático, n. 62, set. 2003. Disponível em: http://www.alfa-redi.org/rdiarticulo.shtml?x=1289. Acesso em: 6 jan. 2018.

ZAFFARONI, Eugenio Raúl. **O inimigo no direito penal.** Rio de Janeiro: Revan/ICC, 2007.

ZAFFARONI, Eugenio Raúl; PIERANGELI, Jose Henrique. **Manual de Direito Penal brasileiro:** parte geral. 11. ed. São Paulo: Revista Dos Tribunais, 2015.