UNIVERSIDADE DE SANTA CRUZ DO SUL
CURSO DE DIREITO

Carlos Mickael da Silva Santos

CRIMES INFORMÁTICOS: UMA ANÁLISE SOB A PERSPECTIVA DO DIREITO PENAL E PROCESSUAL PENAL

Santa Cruz do Sul
2021

Carlos Mickael da Silva Santos

CRIMES INFORMÁTICOS: UMA ANÁLISE SOB A PERSPECTIVA DO DIREITO PENAL E PROCESSUAL PENAL

Trabalho de Conclusão apresentado ao Curso de Direito da Universidade de Santa Cruz do Sul para obtenção do título de Bacharel em Direito.

Orientadora: Profa. Dra. Caroline Fockink Ritt

Santa Cruz do Sul
2021

Desistir não é opção.

AGRADECIMENTOS

Agradeço especialmente a minha tia, dinda e mãe, Maria Suzete Nunes da Silva, que sempre se preocupou com os meus estudos, tendo me incentivado e dado todo suporte que necessitei para chegar até aqui.

Igualmente, agradeço a minha avó, Aracy Nunes da Silva, os meus tios, Arno Lúcio Nunes da Silva e José Lauro Nunes da Silva, e a minha irmã, Cláudia Graziela da Silva Souza, que me deram todo apoio durante o período de formação na faculdade.

Da mesma forma, agradeço a minha noiva, Taís Rocha Castilhos, que esteve ao meu lado durante boa parte desta jornada, sendo ela a pessoa com quem pude contar para me dar o suporte necessário para enfrentar os momentos mais difíceis.

RESUMO

O presente trabalho possui como foco principal os crimes informáticos, em decorrência das suas particularidades que os diferenciam de delitos tradicionalmente cometidos no mundo físico, e a prova penal digital, a qual é dotada grande complexidade teórica e demanda cuidados especiais durante a fase investigatória devido a sua volatilidade. Outrossim, o trabalho objetiva compreender a forma como fenômeno social da criminalidade se manifesta no ambiente virtual, as questões práticas relacionadas a essa espécie de delito, os rastros que os crimes praticados nesse ambiente podem deixar e como evidenciar a ocorrência dessa espécie de crime através da prova obtida digitalmente. Nestes termos, indaga-se: como conceituar, identificar e caracterizar o crime praticado no ambiente virtual, bem como o material probatório decorrente do mesmo? Quais são os direitos suscetíveis de serem violados no decurso da produção da prova digital? Para isso, o método de abordagem utilizado é o dedutivo. É de fundamental importância o estudo do tema, visto que o uso inadequado de tecnologias e programas de computador reveste-se de um negativo fator criminológico de difícil controle. Como resultado, verifica-se o impacto das novas tecnologias no estudo do Direito, especialmente nos ramos penais.

Palavras-chave: Crimes informáticos. Internet. Investigações criminais. Provas.

ABSTRACT

The main focus of this work is computer crimes, as a result of their particularities that differentiate them from crimes traditionally committed in the physical world, and digital criminal evidence, which is endowed with great theoretical complexity and requires special care during the investigative phase due to its volatility. Furthermore, the work aims to understand how the social phenomenon of criminality manifests itself in the virtual environment, the practical issues related to this type of crime, the traces that crimes committed in this environment can leave and how to evidence the occurrence of this type of crime through proof obtained digitally. In these terms, the question is: how to conceptualize, identify and characterize the crime committed in the virtual environment, as well as the evidentiary material arising from it? What rights are likely to be violated during the production of digital evidence? For this, the approach method used is the deductive one. The study of the subject is of fundamental importance, since the inappropriate use of technologies and computer programs is a negative criminological factor that is difficult to control. As a result, the impact of new technologies on the study of Law is verified, especially in the criminal fields.
Keywords: Computer crimes. Criminal investigations. Evidences. Internet.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho monográfico visa efetuar um aprofundamento teórico-jurídico a respeito das características dos crimes informáticos, da origem dessa espécie delitiva, das divergências doutrinárias sobre as suas classificações e nomenclaturas, bem como se propõe analisar algumas de suas figuras típicas. Ademais, pretende-se analisar esses delitos na perspectiva dos institutos processuais penais, trazendo discussões doutrinárias em relação à territorialidade, a jurisdição, a competência e a prova penal.

Nesse sentido, objetiva-se compreender a forma como fenômeno social da criminalidade se manifesta no ambiente virtual, as questões práticas relacionadas a essa espécie de delito, os rastros que os crimes praticados nesse ambiente podem deixar e como evidenciar a ocorrência dessa espécie de crime através da prova obtida digitalmente.

Considerando que vivemos na chamada era digital, em que a maioria das informações trocadas entre as pessoas são feitas através de mecanismos cibernéticos, oriundos do surgimento da internet, espaço virtual no qual grande parte da sociedade passou a inter-relacionar-se, e onde também pôde-se observar a prática de crimes de diversas espécies, definidos como cibercrimes ou crimes informáticos; questiona-se: como conceituar, identificar e caracterizar o crime praticado no ambiente virtual, bem como o material probatório decorrente do mesmo? Quais são os direitos suscetíveis de serem violados no decurso da produção da prova digital? Para isso, realizar-se-á a pesquisa a partir do método dedutivo com procedimento monográfico. As técnicas de pesquisa utilizadas serão a bibliográfica e a documentação indireta.

A abordagem deste trabalho divide-se em três capítulos, o de número dois propõe-se a contextualizar o surgimento e o funcionamento da internet, além de objetivar compreender como surgiu o conceito de ciberespaço, normalmente atrelado à internet, espaço este utilizado para diversos fins, inclusive para a prática delitiva, sendo, portanto, um tema de suma importância para as ciências jurídico-criminais.

O capítulo de número três tem como objetivo conceituar os crimes informáticos, apresentando suas principais características, terminologias e como eles se diferenciam dos crimes já existentes no ordenamento jurídico pátrio. Além disso, propõe-se a discutir quais são os bens jurídicos suscetíveis de serem violados por

essa modalidade delitiva, bem como as suas classificações. Outrossim, discute-se a falta de harmonização dos sistemas jurídicos internacionais que não contam com uma solução para os entraves impostos pela transnacionalidade, problema que é um dos principais obstáculos enfrentado na investigação e punição desses delitos.

O capítulo de número quatro é destinado à análise das particularidades das provas no contexto do crime informático. Uma vez que os dados e as informações, no ambiente digital, podem não estar localizados, necessariamente, em apenas um lugar, o que os tornam suscetíveis de serem facilmente modificados ou excluídos, tornando o processo criminal mais difícil. Neste capítulo também são analisados aspectos técnicos específicos do material probatório digital e de como o exame de corpo de delito, com base nos preceitos processuais penais, é o mais adequado para se comprovar a prática de crimes informáticos. Além disso, faz-se um aprofundamento a respeito do instituto da prova, a função da mesma dentro do processo penal, a quem ela se destina, as prováveis limitações em sua aplicação e uma análise entre interesse público e privado, demonstrando que não há supremacia de um sobre o outro, mas uma relação de complementariedade e interdependência.

O estudo do tema em comento é de fundamental importância, visto que o uso inadequado de tecnologias e programas de computador reveste-se de um negativo fator criminológico de difícil controle. Como resultado, verifica-se o impacto das novas tecnologias no estudo do Direito, especialmente nos ramos penais.

2 ERA DIGITAL

A era digital, muito mais que um termo clichê, é a realidade vivenciada pela sociedade contemporânea, as tecnologias digitais ocuparam espaços importantes e essenciais na atual conjuntura social, figurando em vários setores da sociedade, como comércio, entretenimento, relacionamento, informação, política, entre outros. Os resultados verificados são notórios, tendo impacto direto na rotina dos indivíduos na busca de facilitar e melhorar as suas vidas.

As tecnologias digitais viabilizaram o surgimento de uma nova gama de produtos, uma nova forma de transmitir, acessar e arquivar informações, modificando o campo social, econômico e político. Não obstante, o aspecto mais relevante da tecnologia computacional não tem fim em si mesma, mas sim no potencial de formar redes inter-relacionais. Com o advento da internet no final da década de 1960, surgiu a possibilidade de se estabelecer conexão em rede, viabilizando construir, desmembrar, copiar, recompor e deslocar dados digitais, facilitando-se o acesso e a exibição de informações de diversos formatos de forma instantânea e rápida.

Da interconexão das diversas redes de dispositivos eletrônicos, surgiu o espaço virtual, o qual também podemos chamar de ciberespaço, que nada mais é do que um ambiente imaterial formado por uma grande infraestrutura tele comunicacional.

Para efeitos jurídicos, é primordial o estudo do ciberespaço devido à existência de uma série de atos criminosos passíveis de serem cometidos neste ambiente.

2.1 Sociedade e as tecnologias da informação e da comunicação

A sociedade, até chegarmos aos dias atuais, passou por diversas transformações, visto que o ser humano vem num constante processo de desenvolvimento, realizando significativas mudanças a sua volta. A humanidade saiu do modelo primitivo, tendo chegado à civilização, graças a obtenção de técnicas de domínio e aproveitamento dos recursos naturais, pois aprendeu a lidar com as adversidades da natureza. Verifica-se que o ser humano, ao longo da História, desde a Antiguidade, busca incessantemente desenvolver e aprimorar ferramentas e métodos que o auxilie em sua rotina nas mais diversas áreas (VAZ, 2012, p. 17), das quais destacamos as da comunicação e da informação.

Para caracterizar atualmente a sociedade é comum designá-la como sociedade da informação e da comunicação, que, pela perspectiva evolutiva histórica, viria a ser o modelo de sociedade observado após o período industrial ou moderno. Na prática, a sociedade da informação e da comunicação permeou o mundo com um grande fluxo de informações, o que acarretou na relativização das noções de território, visto que as barreiras de tempo e espaço concernentes à comunicação entre as pessoas foram superadas (KIST, 2019, p. 25).

A respeito da caracterização do referido modelo de sociedade, Gouveia (2004, p. 01, grifo nosso) faz a seguinte ponderação:

> a **sociedade da informação está baseada nas tecnologias de informação e comunicação** que envolvem a aquisição, o armazenamento, o processamento e a distribuição da informação por meios electrónicos, como a rádio, a televisão, telefone e computadores, entre outros. Estas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, económicos e políticos, criando uma nova comunidade local e global: a Sociedade da Informação.

Essa conjuntura social possui como característica principal a função desempenhada pelas tecnologias da informação e da comunicação, presente tanto na vida particular das pessoas como no contexto de suas atividades sociais, econômicas, políticas e culturais, o que levou a formação de uma comunidade local e, ao mesmo tempo, global, visto que essas tecnologias, especialmente as que funcionam via internet, aumentaram significativamente a forma de adquirir, armazenar, processar e distribuir informações por meio eletrônico (KIST, 2019, p. 26).

Verifica-se que nos últimos 30 anos os computadores deixaram de estarem restritos a ambientes avançados de pesquisa, sendo que passou a ocupar residências, tornando-se comum a sua presença no interior dos lares, bem como as informações que transporta, tendo fortalecido, dessa maneira, a comunicação entre as pessoas, atingindo todas as expressões sociais e culturais. Atualmente, mais do que nunca, parece mais real a possibilidade de a quantidade de mensagens digitais ultrapassarem, nos próximos anos, a comunicação física entre as pessoas, visto ao fácil acesso que se tem à internet (JEZLER JÚNIOR, 2019, p. 21).

A internet é um elemento único da atual infraestrutura da informação, devido a sua arquitetura aberta e compartilhada, sendo os seus serviços fornecidos por diferentes entidades (RODRIGUES, 2009, p. 30 apud JEZLER JÚNIOR, 2019, p. 22).

Ela possui influência global, portanto, abrange a atenção da sociedade moderna e também atrai a atenção da comunidade tecnológica, por apresentar a forma mais rápida de conectar as pessoas no mundo, sendo, por tanto, uma ferramenta poderosa de obtenção e disseminação de informações (JEZLER JÚNIOR, 2019, p. 22).

Portanto, devido ao ritmo acelerado do progresso tecnológico, o contexto social sofreu mudanças drásticas, sem precedentes em outro campo, em termos de aplicação de recursos tecnológicos e benefícios relacionados, o que cominou no encurtamento de distâncias e a substituição do átomo pelo bit (JEZLER JÚNIOR, 2019, p. 22).

Com relação a importância da internet em propiciar uma nova forma de comunicação entre as pessoas, Jezler Júnior (2019, p. 23-24), explana o seguinte:

> de maneira inédita, em uma análise histórica, o homem construiu um dispositivo capaz de dispensá-lo de toda comunicação direta. Ninguém duvida que a Internet se tornou objeto de um verdadeiro culto, com a promessa da pós-modernidade quanto a um mundo instantâneo, por meio do ciberespaço e da aldeia global. Trata-se de um novo traço socialmente lastreado na separação dos corpos e na coletivização das consciências.

Ademais, sobre o surgimento da internet, cabe destacar que ela “nasceu” no contexto da Guerra Fria, com uma estrutura completamente voltada para meio militar norte-americano. Por conseguinte, é na década de 70 que se tem o início da era eletrônico-digital (RODRIGUES, 2009 apud JEZLER JÚNIOR, 2019, p. 24).

Já no Brasil, as primeiras ações envolvendo o uso da internet se deram com a interligação de universidades e centros científicos do Rio de Janeiro, São Paulo e Porto Alegre aos Estados Unidos da América. No ano de 1989, surgiu o projeto da Rede Nacional de Pesquisa com a participação do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) com o objetivo de integrar e coordenar os trabalhos relativos a redes de comunicação no âmbito acadêmico, sendo que apenas em 1993 a internet alcançou outros setores da sociedade (JEZLER JÚNIOR, 2019, p. 24).

Como denota-se, a tecnologia da informação e da comunicação se caracteriza por um aglomerado de dispositivos físicos (*hardwares*) aliados a um conjunto de programas (*softwares*) que possibilitam o funcionamento daqueles. Associado a isso, a internet, a partir do seu advento e popularização, teve um papel impar na aplicação e desenvolvimento das tecnologias da informação e da comunicação, o que acabou

possibilitando aos seres humanos experimentarem uma nova forma de difundir e acessar um número imenso de informações, bem como estabelecer um novo método de comunicação capaz de dispensar a presença física entre os interlocutores.

As mudanças trazidas pela implementação e a difusão da internet trouxeram transformações sociais importantes, com isso, o que se observou foi a criação de um ciberespaço ou rede, que, como Lévy (2010, p. 17 apud JEZLER JÚNIOR, 2019, p. 26) define, “é o meio de comunicação que surge da interconexão mundial de computadores, tablets, smartphones e outros compartimentos eletrônicos”, tema este que passaremos a abordar no próximo tópico.

2.2 Ciberespaço

O termo ciberespaço foi utilizado pela primeira vez pelo escritor de ficção cientifica William Gibson no ano de 1984, para caracterizar um espaço não-físico composto por redes de computadores pelas quais circulavam diversas formas de informações (SILVA, W.M.P., [2011], http://www.sbsociologia.com.br/portal/index.php?option=com_docman&task=doc_download&gid=776&Itemid=171).

Santos (2018, https://knoow.net/ciencinformtelec/informatica/ciberespaco/), apresentando um conceito objetivo e atual, define o ciberespaço da seguinte forma:

> ciberespaço é um termo usado para designar um ambiente de relacionamentos criado de forma virtual através do uso dos meios de comunicação modernos, entre eles a Internet. Este ambiente tornou-se possível graças a uma grande infraestrutura técnica na área das telecomunicações, composta por cabos, fios, redes, computadores, etc. Genericamente, Ciberespaço ou espaço cibernético é um espaço que existe no mundo da comunicação onde não é necessária a presença física do Homem para se conseguir comunicar. É uma zona de relacionamentos diversos, onde impera a imaginação, necessária para a criação de uma imagem muitas vezes anónima, que interagirá com as demais. Por meio da tecnologia, os homens, mediados pelos computadores, passam assim a criar ligações e relacionamentos capazes de fundar um espaço de sociabilidade virtual, o Ciberespaço.

No mesmo sentido, Kist (2019, p. 62) afirma que não se pode ver no ciberespaço “um lugar com natureza física e geográfica, e sim, um ambiente virtual de relacionamento interpessoal”.

Com base nessa ideia básica, quando falamos em ciberespaço estamos nos referindo à rede global de infraestrutura de tecnologia da informação interconectada,

especialmente redes de telecomunicações e sistemas de informática utilizados para processamento de dados. Em particular ao que diz respeito aos sistemas de processamento de dados, há dois termos que merecem destaque: *Big Data* e *Cloud Computing* (KIST, 2019, p. 42).

O *Big Data*, no contexto da Tecnologia da Informação, representa um grande número de dados virtuais, complexos e heterogêneos, que vêm de múltiplas fontes independentes. O valor da análise adequada desse grande conjunto de dados permite prever tendências de negócios, definir estratégias e políticas para a prevenção de doenças, combater crimes, etc. Portanto, cientistas, empresários, profissionais de mídia e Governos estão todos interessados nas vantagens de um *Big Data* (KIST, 2019, p. 42-43).

O *Cloud Computing* ou computação em nuvem, por seu turno, ainda é uma realidade nova no campo da Tecnologia da Informação; o termo “nuvem”, por certo, é uma metáfora; para usar esses serviços é necessário somente que o usuário tenha uma máquina com acesso à internet. Para este trabalho, imperiosa se faz a definição de *Cloud Computing* apresentada pelo *National Institute of Standards and Technology* (NIST), que assim preceitua: a computação em nuvem é um modelo que permite o acesso à rede ubíqua de forma conveniente e sob demanda, afim de possibilitar o acesso a um aglomerado de recursos de computação configuráveis (por exemplo, rede, servidores, armazenamento, aplicativos e serviços), que podem ser rapidamente provisionados e liberados com o mínimo de trabalho de gerenciamento e interação com o provedor de serviço (KIST, 2019, p. 43).

Big Data e *Cloud Computing* possuem importante projeção para o campo jurídico, especialmente porque as evidências criminais podem estar armazenadas neles; se os indícios de prova forem encontrados, por exemplo, na nuvem, em que a localização geográfica pode ser totalmente diferente do local onde o agente executou o ato delituoso, bem como onde o crime produziu seus efeitos, ou da localização da vítima, surgem questões problemáticas e então passasse a questionar como determinar o local do crime e a competência jurisdicional para julga-lo, sendo que tudo isso se agrava quando essas questões estão atreladas a mais de um país (KIST, 2019, p. 44).

Fernando Miró Llinares, em seus estudos, propõe, para caracterizar o ciberespaço, algumas notas essenciais, como disposto abaixo.

Deslocalização geográfica, que consiste no fato de que o ciberespaço é onipresente geograficamente, ainda que funcionalmente encontre-se em todo lugar (LLINARES, 2011, p. 10-11).

Transnacionalidade, o ciberespaço é incompatível com as fronteiras de Estados, além disso, não pertence a nenhum Estado-nação específico, embora possa ser acessado a partir de qualquer um deles. Em outras palavras, a natureza transnacional do ciberespaço significa que não existem barreiras à comunicação e interação entre as pessoas, exceto aquelas estabelecidas pelos próprios usuários. O conteúdo postado em uma página da *web* alocada em um servidor localizado em qualquer lugar pode ser visualizado por inúmeras pessoas em diferentes lugares ao mesmo tempo. O resultado é a facilitação da comunicação e do fluxo de bens, pois o ciberespaço supera as barreiras causadas pela distância física (LLINARES, 2011, p. 11).

Neutralidade, o que significa que os usuários podem transferir e acessar livremente diversos conteúdos, e uma das consequências disso é a grande dificuldade em controlar as informações e os conteúdos veiculados pela Rede, pois esses dados se espelham rapidamente por um espaço de grandiosa dimensão e imensamente popularizado. E o mais grave de tudo isso é que, se eles forem nocivos a bens jurídicos, o ciberespaço possibilitará a potencialização dos danos (LLINARES, 2011, p. 11).

Ausência de centralização, o ciberespaço não possui um local específico de origem e difusão, pelo contrário, ele é substancialmente descentralizado. Esta situação decorre da arquitetura da Rede, em que não há um ponto central ou pontos que funcionem em centros locais, consequentemente, nenhum desses pontos pode isolar o outro, nenhum deles pode determinar a quem o outro se conecta, e a queda de um ponto não impede que as informações continuem a fluir pela Rede. É esse fator estrutural que impede uma autoridade, agência ou instituição central controlar o fluxo de informações. É exatamente por isso que a internet não está sujeita às leis nacionais de um único país, nem está sujeita a normas específicas aceitas por todos os países, o que caba resultando na pouca efetividade dos controles governamentais (LLINARES, 2011, p. 11-12).

Espaço anonimizado, apesar de haver manifestações no sentido de que o anonimato não é uma característica da internet e do ciberespaço, pois estaria cada vez mais fácil identificar os usuários a partir do endereço IP, a realidade é que essa

identificação não é tão fácil quanto parece. Com efeito, neste campo, é natural que os autores de atos criminosos visem ocultar e evitar as medidas judiciais que conduzam à sua identificação. Em suma, o ciberespaço é adequado para o anonimato; e se o anonimato pode ser considerado um atributo intrínseco da liberdade, no âmbito do Processo Penal, chega a ser calamitoso, devido as dificuldades que se tem para identificar o autor de um crime (LLINARES, 2011, p. 12-13).

2.3 Perspectiva jurídica do ciberespaço

Todo exposto acima vai determinar e impregnar os fatos que ocorrerem no ciberespaço e isso, consequentemente, envolve o crime. Cabe realçar a influência das Tecnologias da Informação e Comunicação no domínio jurídico, particularmente no Direito Penal e Direito Processual Penal. É notório que esses dois ramos do direito têm sido fortemente afetados pelas diversas peculiaridades do ciberespaço. As discussões mais relevantes e interessantes buscam determinar se é apropriado recorrer a soluções jurídicas desenvolvidas e amadurecidas para o mundo físico e ajustá-las à realidade virtual, ou, inversamente, se é preciso criar um estatuto jurídico próprio, com princípios e institutos adequados para o mundo virtual. A respeito dessa temática, vale ressaltar as conclusões obtidas por um Grupo de Trabalho criado pela Diretiva nº 95/46 da Comunidade Europeia[1], as quais convergiram no sentido de equiparar o ciberespaço ao mundo físico, porém só no tocante aos princípios fundamentais e as regras gerais, a respeito das especificidades identificadas, as normas legais devem considerá-las com o intuito de criar um Direito novo a respeito delas (KIST, 2019, p. 53-54).

No âmbito jurídico criminal, o estudo do ciberespaço é importante para compreender a ocorrência de crimes nesse ambiente. Assim sendo, na área do Direito Penal, merece destaque a questão referente a identificação dos crimes informáticos, ou seja, os crimes praticados no meio virtual. É notório que o ciberespaço, há algum tempo, vem sendo utilizado para a prática de crimes, contudo, é necessário que se

[1]"As Diretivas Comunitárias integram o Direito Comunitário, tratando-se de um dos atos normativos adotados pelas Instituições Comunitárias. São, portanto, atos emanados da autoridade comunitária competente, por meio do qual é fixado um resultado que o(s) Estado(s) destinatário(s) devem alcançar no interesse comum; a peculiaridade é que na Diretiva é estabelecido apenas o resultado, deixando às instâncias nacionais a competência para definir a forma e os meios adequados e necessários para tanto" (KIST, 2019, p. 54).

distinga as espécies de crimes praticadas nesse espaço, estando de um lado os crimes já previstos na legislação que, tão somente, são cometidos no âmbito virtual, ou seja, o bem jurídico já se encontra tutelado, sendo o que se verifica de novo é apenas o espaço em que ocorre o crime. E do outro lado, temos as condutas lesivas praticadas no ciberespaço que não se enquadram em nenhum tipo penal tradicional, isto é, tratam-se de uma novidade, que afetam novos bens jurídicos (KIST, 2019, p. 53-55).

Já na área do Direito Processual Penal, com relação ao ciberespaço, o que se alude é a questão da produção da prova penal e a definição do local do crime e, consequentemente a jurisdição penal competente. Com relação a primeira, há de se observar que o ciberespaço criou uma nova modalidade de prova, a digital, que, embora utilize institutos e princípios de produção e valoração da prova física, possui suas especificidades probatórias, com um procedimento a parte de recolha e posterior processamento, a fim de ser valorada em processos penais. No tocante a segunda, imperioso se faz observar que a obtenção de provas digitais se dá por meio de pesquisas no interior de sistemas informáticos, podendo essa pesquisa revelar que eventuais provas de um crime se encontram armazenados, por exemplo, em um servidor localizado em outro país e, assim, surge a discussão acerca da aplicação territorial ou extraterritorial das leis do país que está promovendo a busca dessas provas (KIST, 2019, p. 53, 55 e 56).

3 CRIMES INFORMÁTICOS

Com o advento do ciberespaço surgiram também os crimes informáticos, sendo que muitos delitos, que, até então, eram praticados inteiramente no âmbito físico, passaram a contar com o ambiente digital para serem aplicados, além disso, verifica-se também o surgimento de outros crimes com características totalmente peculiares em decorrência das condições propiciadas pelo ciberespaço. O fato é que os criminosos não deixaram de acompanhar as transformações das tecnologias da informação e da comunicação, tendo passado a utilizarem a estrutura das redes virtuais para cometer crimes das mais diversas espécies, os quais passamos a examinar detalhadamente.

3.1 Terminologia e conceito dos crimes informáticos

Primeiramente, vale observar que a terminologia utilizada para designar os crimes praticados em ambiente virtual pode alternar na doutrina a depender do autor, não havendo, dessa forma, entendimento unificado acerca da nomenclatura a ser utilizada para designar esses crimes, conforme atesta Rosa (2006 apud SOUZA NETO, 2009, p. 24):

> Klaus Tiedmann fala em “criminalidade de informática”, para designar todas as formas de comportamentos ilegais ou, de outro modo, prejudiciais à sociedade, que se realizam pela utilização de um computador. [...] Kohn utiliza computer criminals para designar que seus praticantes. Jean Pradel e Cristian Feuliard referem-se a “infiltrações cometidas por meio de computador”. Há ainda quem prefira a expressão “crimes de computador”, “cybercrimes”, “computer crimes”, “computing crimes”, “delito informático”, “crimes virtuais”, “crimes eletrônicos” ou, ainda, “crimes digitais”, “crimes cibernéticos”, “infocrimes”, “crimes perpetrados pela internet”, denominações distintas, mas, que, no fundo, acabam por designar basicamente a mesma coisa

No cenário nacional, há uma inclinação da doutrina em adotar a denominação crimes ou delitos informáticos, muito em decorrência da opção escolhida pelo legislador pátrio ao editar a Lei nº 12.737/12 (“Lei Carolina Dieckmann”), em que, no enunciado, estabeleceu que esta norma “dispõe sobre a tipificação criminal de delitos informáticos” (KIST, 2019, p. 63 e 64).

Já na esfera internacional, especialmente no âmbito europeu, a tendência segue no sentido de utilizar a nomenclatura cibercrime, exemplo prático disso se verifica em Portugal, país em que, desde 15 de setembro de 2009, vige a Lei nº 109, a qual o legislador denominou expressamente de “Lei do Cibercime”, lei esta que revogou outra norma que era intitulada como “Lei da Criminalidade Informática” (KIST, 2019, p. 63).

Da doutrina nacional, imperioso se faz destacar a opção adotada por Jesus (2016, p. 48), que afirma o seguinte: “ao tratarmos de ‘crime informático’, usamos tal nomenclatura justamente para demonstrar qual o bem jurídico protegido pelo Direito Penal, a informática, ou a privacidade e a integridade dos dados informáticos”.

O fato é que não há um consenso acerca do termo a ser utilizado para designar o crime praticado em ambiente virtual, contudo, por uma questão de padronização do presente trabalho, para nos referirmos àquele, será adotada a expressão crime informático.

Feita essa breve ponderação sobre a terminologia, passamos a conceituar o crime informático. Pode-se dizer que este se caracteriza em “todo ato em que o computador ou meios de tecnologia de informação serve para atingir um ato criminoso ou em que o computador ou meios de tecnologia de informação é objeto de um crime” (ALEXANDRE JÚNIOR, 2019, p. 343).

A respeito do conceito de crime informático, Jesus (2016, p. 49) assevera o seguinte:

> conceituamos crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal.

Há na doutrina alguns autores que entendem que o crime informático se trata, por excelência, de um crime-meio, em que apenas há a utilização de um meio virtual para a execução do delito. Nesse sentido, destacamos o entendimento de Pinheiro (2007 apud JESUS, 2016, p. 50), que afirma o seguinte:

> não é crime-fim por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por *hackers*, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros.

Por outro lado, há também o entendimento que o crime informático pode ser considerado crime-fim, bem como crime-meio, o que nos parece mais adequado, já que cada vez mais se verifica a prática de crimes informáticos próprios. Frente a necessidade de tipificar esses crimes, foram, inclusive, editadas as Leis nº 12.735/2012 e nº 12.737/2012. Além do mais, é incorreto afirmar que só *hackers* ou *crackers* podem cometer um crime-fim informático, tema que abordaremos mais adiante ao nos determos mais especificamente sobre os sujeitos ativos (JESUS, 2016, p. 50).

É inegável que a maior parte dos crimes informáticos está vinculada a delitos que por si só não são necessariamente virtuais, mas tão somente o meio utilizado para execução da conduta delitiva. Tendo como exemplo, o estelionato e a pornografia infantil são os crimes mais comuns praticados na rede. Por outro lado, os crimes informáticos mais raros, porém crescentes, são os causados por códigos maliciosos, capazes de produzir, por exemplo, a negação de serviço, sequestro e roubo de informações privilegiadas. O fato é que, apesar do Direito Penal já tutelar certos bens jurídicos agredidos pela via virtual, os dados e a segurança dos sistemas e redes informáticos necessitam de uma proteção específica (JESUS, 2016, p. 50).

Assim, vislumbrasse que os crimes informáticos ocorrem através do emprego de dispositivos eletrônicos, que podem servir de meio para a prática de crimes tradicionais passiveis de serem executados de variadas maneiras, dentre elas, a eletrônica; a título de exemplo, podemos citar o crime de estelionato que, no âmbito virtual, pode ser cometido através de um aplicativo de mensagem instantânea. Por outro lado, o dispositivo informático pode ser o próprio fim do crime, como no caso de envio de um *software* para ser instalado no computador de uma vítima com o objetivo de prejudicar o funcionamento do dispositivo, danificar arquivos digitais, capturar informações e dados, dentre outros.

3.2 Classificação dos crimes informáticos

Assim como a nomenclatura a ser utilizada para se referir aos crimes praticados no ambiente virtual, também não há uma uniformização na doutrina a respeito da classificação dos crimes informáticos. Assim sendo, passamos a destacar abaixo aquelas mais conhecidas.

Tiedemann (1980 apud JESUS, 2016, p. 51), ao tratar dos crimes informáticos no âmbito dos delitos econômicos, classificou os mesmos da seguinte maneira: a) manipulações, as quais podem prejudicar a entrada (*input*), a saída (*output*) e o processamento de dados; b) espionagem, subtração de informações arquivadas, incluindo-se, além disso, o furto ou emprego indevido de *software*; c) sabotagem, destruição total ou parcial de programas; e d) furto de tempo: uso indevido de instalações de computadores por empregados desonestos ou estranhos.

Sieber (2008 apud JESUS, 2016, p. 51-52), ao emitir parecer para Comissão Europeia sobre crimes informáticos, os classificou assim: a) violação à privacidade; b) crimes econômicos, subdivididos em *hacking*, espionagem, pirataria em geral (cópias não autorizadas), sabotagem, extorsão e fraude; c) conteúdos ilegais e nocivos; e d) outros ilícitos, contra a vida, crime organizado e guerra eletrônica.

Briat (1985 apud JESUS, 2016, p. 52), por sua vez, classificou os delitos informáticos em crimes em que a informática é o meio para a prática delituosa e os que a informática é o próprio fim, estando estes divididos da seguinte maneira: a) manipulação de dados e/ou programas com o intuito de cometer uma infração já prevista pelas incriminações tradicionais; b) falsificação de dados de programas; c) deterioração de dados e de programas e entrave à sua utilização; d) divulgação, utilização ou reprodução ilícita de dados e de programas; e) uso não autorizado de sistemas de informática; e f) acesso não autorizado a sistemas de informática.

Canto (2002 apud JESUS, 2016, p. 53), apresenta uma das classificações mais amplas sobre delitos informáticos, que compreende: a) infrações à intimidade; b) ilícitos econômicos; c) ilícitos de comunicação ou difusão de conteúdos ilegais ou perigosos; e d) outros delitos.

Como aponta Jesus (2016, p. 53), a melhor classificação é a apresentada por Martine Briat, que distingue os crimes informáticos naqueles em que a informática é o meio para o cometimento de crimes contra bens jurídicos já tutelados pelo Direito Penal, e crimes informáticos propriamente ditos, em que a informática (inviolabilidade

de dados) é o próprio bem jurídico protegido. Sendo assim, tal classificação é a que mais se alinha ao próprio conceito de crimes informáticos, conforme exposto acima

Nessa toada, quanto a classificação dos crimes informáticos, podemos dividi-los da seguinte maneira: crimes informáticos próprios, que são aqueles em que o bem jurídico afetado é a própria tecnologia da informação. A legislação penal, para estes delitos, possui algumas lacunas, assim, necessitam de enquadramento algumas práticas delitivas; e crimes informáticos impróprios, em que a tecnologia da informação serve de meio para práticas delitivas, atingindo bens jurídicos já tutelados pela legislação penal. Nestes casos a legislação criminal já cumpre suficientemente bem o seu papel, visto que boa parte das condutas delitivas já se encontram previstas em algum tipo penal (JESUS, 2016, p. 53-54).

Além dessas duas classificações essenciais, temos também que os crimes informáticos podem ser classificados em: misto, quando ocorrem nos casos de crimes complexos em que há a proteção de mais de um bem jurídico, ou seja, de um bem jurídico informático e de outro bem jurídico diverso, estando cada qual protegido por um tipo penal; e mediato ou indireto, ocorre quando um delito informático é praticado com o intuito produzir os efeitos de um delito não informático. Como já mencionado, é comum que crimes informáticos sejam utilizados como meio para a prática de um delito-fim. A título de exemplo, podemos mencionar o caso em que o agente invade um sistema eletrônico e captura os dados bancários da vítima e saca o dinheiro que há na conta da mesma. Nesse casso, o agente apenas será punido pelo furto, delito fim, devido ao princípio da consunção (JESUS, 2016, p. 54).

No mesmo sentido, Kist (2019, p. 67), apresenta como mais adequado a classificação dos crimes informáticos em próprios e impróprios. O mesmo explana que alguns crimes só podem ocorrer em função da existência do ciberespaço, ou seja, os chamados crimes próprios ou puros. Esses crimes afetam os sistemas informáticos e as informações e dados neles contidos, por isso, é considerado um bem jurídico de natureza difusa, em que se propõe a criminalização de condutas que afetam a integridade, a disponibilidade e a confidencialidade das informações e dados neles constantes. De outro lado, temos os crimes capazes de serem praticados pelos meios convencionais e no mundo físico, mas que, no caso concreto, foram postos em prática no ciberespaço, motivo pelo qual são denominados como crimes informáticos impróprios ou impuros; são delitos praticáveis de várias formas, até mesmo por

intermédio de dispositivos informáticos, e os casos mais comuns são as ciberfraudes, as ameaças, ataques à honra por meio dos aparatos tecnológicos de comunicação, assédio sexual a menores, cyberbullying e o cyberstalking[2]. Como se denota, nessa criminalidade, o bem jurídico tutelado é a honra, o patrimônio, liberdade, intimidade, dignidade sexual, segurança, etc., todos os quais podem ser atingidos por atos criminosos praticados por meios físicos tradicionais.

3.3 Tipificação dos crimes informáticos

No Brasil, diferentemente de outros países, como, por exemplo, Portugal, que possui uma lei penal específica para tipificar os crimes informáticos (Lei nº 109/2009), não há um diploma legal único, próprio e específico para tais ilícitos, estando eles dispostos de forma esparsa entre variadas leis, das quais destacamos abaixo algumas delas (KIST, 2019, p. 70-71).

Lei nº 9.609, de 19 de fevereiro de 1998, a qual "dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências" (BRASIL, 1998, http://www.planalto.gov.br/ccivil_03/leis/l9609.htm). Em seu artigo 12 está tipificada a conduta de violar direitos de autor de programa de computador[3].

Lei nº 9.296, de 24 de julho de 1996, que regulamenta a parte final do inciso XII do artigo 5º da Constituição Federal, o qual versa sobre a interceptação da

---

[2] "O *stalking*, comum no âmbito da violência doméstica-conjugal, consiste em atos de perseguição e assédio persistente à vítima; as modalidades comuns dessa perseguição são chamadas telefônicas repetidas, envio de mensagens de voz ou texto, envio de cartões, cartas, flores ou presentes como forma de presença, observação da vítima a distância, com uso de dispositivo de escuta, de visão ou de localização, comparecimento inesperado no local de trabalho, estudo ou na residência, danos em objetos de valor sentimental ou animais de estimação. O *cyberstalking* consiste na prática desses atos de perseguição com o manejo de aparatos eletrônicos" (KIST, 2019, p. 69).

[3] "artigo 12. Violar direitos de autor de programa de computador: Pena - Detenção de seis meses a dois anos ou multa. § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena - Reclusão de um a quatro anos e multa. § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral. § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo: I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público; II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo. § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação" (BRASIL, 1998).

comunicação telefônica e telemática. Nesta Lei se destaca o artigo 10, o qual preceitua que “constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei” (BRASIL, 1996, http://www.planalto.gov.br/ccivil_03/leis/l9296.htm).

Lei nº 8.137, de 27 de dezembro de 1990, a qual “define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências” (BRASIL, 1990). O tipo penal a ser destacado nesta Lei é o disposto no artigo 2º, inciso V, que dispõe que constitui crime “utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública” (BRASIL, 1990, http://www.planalto.gov.br/ccivil_03/leis/l8137.htm).

Lei nº 9.504, de 30 de setembro de 1997, a qual “estabelece normas para as eleições” (BRASIL, 1997, http://www.planalto.gov.br/ccivil_03/leis/l9504.htm). Esta Lei estabelece em seu artigo 72 que:

> constituem crimes, puníveis com reclusão, de cinco a dez anos: I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes (BRASIL, 1997, http://www.planalto.gov.br/ccivil_03/leis/l9504.htm).

Lei nº 8.069, de 13 de julho de 1990, a qual “dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências” (BRASIL, 1990, http://www.planalto.gov.br/ccivil_03/leis/l8069.htm). Esta Lei teve sua redação alterada pela Lei nº 11.829/2008, que incluiu a redação daquela o artigo 241-A, que estabelece que constituiu crime:

> 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 (BRASIL, 1990, http://www.planalto.gov.br/ccivil_03/leis/l8069.htm).

Por sua vez, no Código Penal, há alguns dispositivos que também merecem destaque, quais sejam, artigo 153, § 1º-A, com redação dada pela Lei nº 9.983/2000, que estabelece que constitui crime “divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública” (BRASIL, 1940, http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm); artigo 154-A, introduzido pela Lei 12.737/2012, que tipifica penalmente a conduta de:

> invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita (BRASIL, 1940, http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm).

Além destes dispositivos, temos também no Código Penal, a respeito da temática ora tratada, os crimes praticados por funcionário público contra a Administração, dos quais se destacam os dispositivos acrescidos pela Lei 9.983/2000, sendo eles o artigo 313-A, que versa sobre a inserção de dados falsos em sistema de informações; artigo 313-B, que trata da modificação ou alteração não autorizada de sistema de informação; e artigo 325, § 1º, que estabelece que incorrerá no crime de violação de sigilo funcional quem “permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública” (BRASIL, 1940, http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm).

Assim, ainda que de forma dispersa, no Brasil se estabeleceu um catálogo de tipos penais para cobrir pelo menos uma parte dos crimes cibernéticos, composta, em sua grande parte, por fraudes bancárias eletrônicas, ataques de engenharia social (*phishing*), utilização indevida de redes sociais para a prática de difamação, calúnia ou ameaça, comprometimento de computadores, danos à rede, ataques de negação de serviço, uso ou acesso não autorizado a sistemas ou dados, etc. (KIST, 2019, p. 75).

Nas situações em que não existe tipos penais específicos para os crimes informáticos, é viável e necessário utilizar os dispositivos tradicionais, portanto, a título de exemplo, o artigo 155 do Código Penal poderá vir a ser utilizado para punir a subtração de conta bancária praticada de forma eletrônica, o artigo 171 do Código

Penal para punir o estelionato efetuada de forma virtual, o artigo 163 do Código Penal para reprimir o dano praticado contra dispositivo informático, os artigos 138, 139, 140 e 147, todos do Código Penal, para os ataques perpetrados contra a honra e ameaças executadas por meios eletrônicos, o artigo 151 para a violação de comunicações enviadas por correio eletrônico (*e-mail*), entre outros (KIST, 2019, p. 75).

3.4 Sujeitos dos crimes informáticos

Passamos, agora, a tratar sobre os sujeitos dos crimes informáticos. Geralmente os sujeitos ativos, os criminosos, são chamados de *hackers*, termo que surgiu, na década de 1970, nos laboratórios de informática do MIT (*Massachusetts Institute of Technology*) (CRESPO apud ALVES, 2020, https://ler.amazon.com.br/?asin=B08LXB27TH&language=pt-BR). No entanto, tal expressão é utilizada erroneamente, visto que estes nada mais são do que profundos conhecedores de sistemas informáticos e que sabem localizar vulnerabilidades de segurança em sistemas informáticos, podendo ser profissionais de segurança da informação ou pesquisadores, os mesmos utilizam seus conhecimentos para fins de aperfeiçoamento de sistemas de segurança, testando as vulnerabilidades destes, não utilizando, em regra, tais conhecimentos para fins ilícitos (JESUS, 2016, p. 59-60). Sobre o *hacker*, Nogueira (2008 apud DULLIUS, A.D.; HIPLLER, A.; FRANCO, E. L., 2012, http://www.conteudojuridico.com.br/consulta/Artigos/30441/dos-crimes-praticados-em-ambientes-virtuais), faz a seguinte ponderação:

> este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver quem consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual.

Os *hackers* também podem ser chamados de *white hats* (*hackers* de chapéu branco) *ou gray hats* (*hackers* de chapéu cinza), a depender da conduta dos mesmos. *White hat* é o termo utilizado para definir os *hackers* éticos, que utilizam seus conhecimentos para fazer o bem, agindo em consonância com a lei, a fim apenas de fortalecer e desenvolver a segurança de sistemas informáticos, os explorando com o conhecimento de seus responsáveis; já a expressão gray hat é utilizada para definir

os *hackers* que invadem sistemas sem que os seus responsáveis saibam, embora não façam isso com o intuito de danifica-los ou obter informações sigilosas, acabam incorrendo em ilicitude (JESUS, 2016, p. 59-60). Sobre white hat e gray hat, Russo (2013, p. 4 apud JESUS, 2016, p. 60) explana o seguinte:

> um hacker de chapéu branco primeiramente pede permissões a corporação ou empresa antes de testar a segurança de sites, *softwares* ou sistemas. Caso descubra alguma falha em sua exploração o mesmo alerta sigilosamente todos os envolvidos após comprometê-los. Já o *Hacker* de chapéu cinza não utiliza o seu acesso indevido para fins maléficos, mas caso ele acesse um sistema de segurança, o mesmo já está comprometido, fato que torna a ação do *Hacker Gray Hat* totalmente ilegal.

Por outro lado, temos o *cracker*, este sim, que igualmente possui grandes conhecimentos tecnológicos, utiliza dos mesmos exclusivamente para praticar crimes, sendo, por tanto, o autêntico criminoso da rede de computadores. Os *crackers* também são conhecidos como *black hats*, assim como os *hackers* são chamados de *white hats ou gray hats* (JESUS, 2016, p. 60). A respeito dos *black hats*, Assunção (2014, p. 34) faz a seguinte assertiva:

> "hacker do mal" ou "chapéu negro". Esse, sim, usa seus conhecimentos para roubar senhas, documentos, causar danos ou mesmo realizar espionagem industrial. Geralmente tem seus alvos bem definidos e pode passar semanas antes de conseguir acesso onde deseja, se o sistema for bem protegido.

Além dos *hackers* e *crackers* que cometem, por excelência, os chamados crimes informáticos próprios, temos ainda aqueles criminosos que, apesar de não possuírem grandes conhecimentos tecnológicos, cometem crimes informáticos, são sujeitos que possuem razoável conhecimento informático e que se valem do despreparo de suas vítimas para praticar crimes. Acerca disso, Jesus (2016, p. 58) afirma o seguinte:

> [...] muito se fala em "crimes de alta tecnologia" quando, na verdade, a tecnologia utilizada na maior parte dos casos é trivial, corriqueira, de fácil curva de aprendizagem, e com ferramentas disponíveis para venda e troca em redes IRC (*Internet Relay Chat*) e demais cantos da Internet. Horas de vídeos disponíveis na Internet podem conduzir pessoas a praticarem invasões com relativa facilidade. As vítimas comummente contribuem e cooperam ativamente para se tornarem vítimas, facilitando o trabalho do cibercrime. [...] Muito se comenta ou classifica-se o crime digital no conceito de colarinho branco, diga-se, crimes que somente pessoas com determinado *know-how* podem praticar, porém, é fato que tais premissas se minimizam a cada dia, onde cada vez mais pessoas sem sólidos conhecimentos em informática iniciam a prática delitiva, obtendo êxito.

Por seu turno, o sujeito passivo dos crimes informáticos pode ser uma pessoa física ou jurídica que tenha tido um bem jurídico afetado ou ameaçado através de um dispositivo informático (CARNEIRO, 2012, https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/). Com relação a isso, Nogueira (2008 apud SOUZA NETO, 2009, p. 29) afirma o seguinte: “qualquer um de nós pode ser vítima, todos nós que temos acesso a rede mundial de computadores estamos arriscados a sermos vítimas dos delitos informáticos”.

3.5 Local da prática do crime informático e os desafios inerentes à territorialidade da lei penal

Agora passamos a analisar as questões atinentes a territorialidade relacionada aos crimes informáticos, necessário se faz observar que os crimes informáticos não estão limitados as demarcações geográficas dos países, as fronteiras físicas não são empecilho para sua prática, bem como seus efeitos e consequências não estão adstritos ao espaço geográfico. Essas características dos crimes informáticos acabam, consequentemente, se refletindo nas questões relacionadas a definição do local do crime (KIST, 2019, p. 78 e 80).

O estudo acerca do local do crime é fundamental para que se defina a jurisdição competente para a interposição de uma ação penal. Neste ponto os crimes informáticos produzem alguns problemas jurídicos, pois os critérios geralmente usados para identificar a jurisdição competente de crimes cometidos no mundo real não se aplicam adequadamente aos crimes informáticos, visto que estes têm como característica o fato de poderem serem cometidos a distância, produzindo efeitos em local distinto, até mesmo em país diverso, gerando, assim, situações jurídicas plurilocalizadas e possivelmente conflitantes (KIST, 2019, p. 81).

Sobre o tema em análise, Ferreira (2001 apud Silva, P.S., 2015, p. 76) afirma o seguinte:

> a mobilidade dos dados nos sistemas de informática, que facilita largamente que os delitos sejam cometidos à distância, usando-se um computador num determinado país e ocorrendo os resultados em outro, bem como os atentado às redes de telecomunicações internacionais, que atravessam vários países,

> o uso indevido de programas importados, a necessidade de proteção dos exportados, tudo isso provocou a internacionalização da questão, que deve ser discutida pelos diversos países para a harmonização das normas penais aplicáveis e de outras medidas de caráter extra-penal.

O potencial de dispersão geográfica dos crimes informáticos pode causar problemas pela falta de uniformidade das condutas típicas entre os países. Pode ocorrer que em um determinado país a conduta delitiva não possua caráter criminoso, o que, teoricamente, reduziria o interesse deste Estado em puni-la, bem como poderia acarretar na falta de colaboração para a coleta de potenciais provas. Também é possível que o país de nacionalidade do autor do crime não esteja interessado em sua punição, nem coopere com outro país que pretenda concretizá-la, culminando, dessa forma, na recusa de extradição ou de execução da pena que for imposta no exterior (KIST, 2019, p. 82).

Por sua vez, o problema de definição da jurisdição competente ocorre quando a ação criminosa se encontra tipificada em mais de um país afetado por ela e cada um deles expressa interesse na persecução penal. Em outras palavras, quando o crime informático é praticado dentro da jurisdição de vários Estados soberanos e o comportamento é tipicamente previsto por cada um deles, é provável que mais de um dos países envolvidos demonstre interesse em avocar para si a competência para conhecê-la e julgá-la. Além disso, mesmo que as questões relacionadas à jurisdição internacional sejam superadas, podem surgir problemas na execução da penalidade imposta em país diverso daquele da nacionalidade ou da residência do agente (KIST, 2019, p. 83).

O problema da jurisdição nos crimes informáticos pode ser compreendido a partir de dois pontos de vista: pode acontecer que, sendo a conduta prevista tipicamente por mais de um país, nenhum deles demonstrem interesse na promoção da ação penal, ou, diversamente, ambos procurem promover a punição do agente infrator (KIST, 2019, p. 92).

Na primeira possibilidade, embora seja mais improvável de vir acontecer, resultará na falta de punição, o que é frustrante se levado em consideração o caráter preventivo e repressivo do Direito Penal. E, a este respeito, ainda que não seja pelo motivo do país não possuir interesse em punir a conduta do agente, observa-se que a impunidade perdura sobre os crimes informáticos, sobretudo porque é difícil determinar e identidade do autor e, mesmo que se identifique, muitas vezes essa

espécie de crime demanda a coleta de provas que se encontram em outros países, o que demandaria uma cooperação internacional, coisa que é pouco desenvolvida (KIST, 2019, p. 92-93).

Por outro lado, no segundo caso, o inconveniente reside na possibilidade de ocorrer o *bis in idem*, que consiste no fato do agente ser perseguido e punido mais de uma vez em decorrência do mesmo fato, o que é terminantemente vedado (KIST, 2019, p. 93).

No que tange à legislação brasileira sobre a questão relacionada a territorialidade, cabe pontuar que o Código Penal adotou a teoria da ubiquidade, conforme se observa na redação do seu artigo 6º, que considera o lugar do crime o local onde ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria se produzir o resultado. Assim sendo, ao se considerar, hipoteticamente, que um agente, que se encontra no estado do Rio Grande do Sul, tenha invadido um computador localizado no estado de São Paulo, teríamos como juízo competente para processar e julgar esse fato o do local onde está dispositivo invadido (JESUS, 2016, p. 61).

Por outro lado, a respeito das condutas ilícitas cometidas no exterior, não se aplicariam as normas brasileiras, tendo em vista a soberania do outro país, sendo que para esses casos demandaria extradição do infrator. Imperioso se faz observar que, em conformidade com o § 2º do artigo 70 do Código Processual Penal, quando os atos executórios tenham se verificado fora do Brasil, a competência será do local onde infração se deu ou foi consumada a ação delituosa (resultado). Ademais, no caso de crimes praticados por brasileiros no exterior e que façam vítimas em território pátrio, por motivos relacionados a soberania, a conduta deve ser considerada ilícita em ambos os países, além disso, deverá o agente adentrar em território nacional para que seja processado, forte no artigo 7º, inciso II, § 2º, *a* e *b*, do Código Penal (JESUS, 2016, p. 61-62).

De todo o exposto a respeito da territorialidade da lei penal como parâmetro de determinação da competência para julgamento dos crimes informáticos resta concluir que a mesma é insuficiente ou incapaz de dar conta de definir a jurisdição do crime informático. Na verdade, não basta dizer que o local do crime é onde ocorreu o comportamento delitivo ou se observou o resultado, porque, no caso concreto, as peculiaridades inerentes a esse tipo de infração penal, em especial a sua

plurilocalização, fazem com que em decorrência de um único fato sejam instaurados mais de um processo, ou até mesmo não seja instaurado nenhum, devido à dificuldade que se tem em definir qual das jurisdições pode ou deve atuar (KIST, 2019, p.101).

Outrossim, ao se tentar definir o Estado soberano capaz de avocar para si a competência para conhecer e julgar o crime, poderiam ser aplicados os critérios atinentes ao local de residência do agente, o local da prática dos atos executórios, o local do resultado, aí incluído também o desejado pelo agente em caso de tentativa, e o local de residência da vítima (KIST, 2019, p. 101).

Na perspectiva do crime tradicional, o uso do local da ação ou omissão geralmente se dá por ser o local onde o agente exterioriza sua vontade de cometer o crime e, portanto, é ali que o mesmo deve ser punido. Porém, no contexto da cibercriminalidade, esse padrão pode se mostrar ineficaz, visto que o agente, com o mínimo de conhecimento sobre legislação, poderá vir a escolher um local onde sua conduta criminosa não seja tipificada como crime e dessa forma se deslocar para lá. Portanto, esse critério permitiria ao agente escolher uma circunstância jurídica que exclui a responsabilidade criminal, pois o comportamento no local de atuação é atípico, o que impossibilitaria a persecução penal (KIST, 2019, p. 101-102).

Por outro lado, a justificativa para a escolha do local do resultado é que geralmente ali se encontram as evidências da ofensa criminal, o que facilita as investigações e os procedimentos. Porém, no crime cibernético, as evidências podem estar localizadas em um lugar completamente diferente do local do comportamento delitivo e do resultado, ou seja, porque os provedores de internet que podem coletar evidências de transmissão de dados estão espalhados em vários locais do globo terrestre (KIST, 2019, p. 102).

Ademais, o local de residência do agente pode ser insuficiente, especialmente quando o resultado do ato é verificado em outro país. Sendo que esse mesmo raciocínio também se aplica ao local de residência da vítima (KIST, 2019, p. 102).

Em suma, nas atuais circunstâncias, não existe uma solução acertada para determinar a jurisdição penal competente para os casos de crimes informáticos que ocorrem à distância ou em trânsito. Além de definir a jurisdição penal competente, também se verifica que os mecanismos de cooperação internacional para a coleta de provas necessitam ser aprimorados para os casos em que o processo instaurado

tramita em país diferente daquele onde se encontram as evidências (KIST, 2019, p. 102).

Portanto, como se infere, há a necessidade de que os países busquem uma cooperação internacional, a fim de julgar e punir os crimes informáticos, visto que a forma como são praticados e o meio utilizado para comete-los, podem potencializar o seu alcance, fazendo com que extrapolem o território nacional, atingindo outros países (SILVA, P.S., 2015, https://profmatheus.com/wp-content/uploads/2017/05/direito-crime-cibernetico.pdf).

E para que haja essa cooperação entre os países, os tratados e as convenções internacionais possuem papel fundamental para evitar que crimes de caráter transnacional fiquem impunes ou até mesmo que venham a ser punidos mais de uma vez, evitando-se, assim, o *bis in idem*. Especificamente sobre os crimes informáticos se destaca a Convenção de Budapeste, sobre a qual Jesus (2016, p. 55) faz as seguintes ponderações:

> de forma a conjugar esforços no combate aos crimes eletrônicos, foi realizada a chamada Convenção de Budapeste, acerca de cibercrimes, no âmbito do concelho da Europa. Trata-se, pois, de documentação de Direito Internacional Público, elaborada por comitê de especialistas, no escopo de que os países signatários implementem normas de direito material que façam frente ao crime cibernético. Assim, tem-se como um acordo internacional, firmado em 23 de novembro de 2001 por países da União Europeia, já contando com a adesão de Austrália, Japão e Estados Unidos, que fixa diretrizes às políticas nacionais e propõe a harmonização das legislações para que se possa combater o cibercrime de maneira eficiente.

O Brasil, embora não integre essa convenção, já legisla em consonância com esta no que tange aos crimes informáticos, porém, conforme já defendeu o Ministério Público Federal em audiência pública na Câmara dos Deputados, é necessário que o país adira a mesma, para que se possa “alinhar aos esforços internacionais na persecução desse tipo de crime e facilitar a cooperação internacional para a obtenção da prova digital” (MINISTÉRIO PÚBLICO FEDERAL - MPF, 2019, http://www.mpf.mp.br/pgr/noticias-pgr/mpf-defende-adesao-do-brasil-a-convencao-de-budapeste-emaudiencia-publica-na-camara; SILVA, P.S., 2015, https://profmatheus.com/wpcontent/uploads/2017/05/direito-crime-cibernetico.pdf).

4 PROVA DIGITAL

Além do exposto acima, outra particularidade dos crimes informáticos está atrelada à obtenção da prova e à identificação dos infratores, sendo estes um dos maiores desafios enfrentados no curso da investigação criminal.

A grande maioria dos crimes informáticos deixam vestígios muito difíceis de serem identificados em decorrência da forma como se estrutura rede mundial de computadores, o que facilita a ocultação dos criminosos, os quais, muitas vezes, obtém êxito em permanecer no anonimato.

Por consequência, imperiosa se faz a abordagem e o aprofundamento desse assunto, o qual passaremos a abordar logo abaixo.

4.1 A prova e o processo penal

O processo penal pode ser comparado à uma ferramenta retrospectiva em que se tenta reconstruir um determinado fato de forma aproximada. Portanto, é por meio das provas que se busca fazer a reconstrução desse fato passado (LOPES JÚNIOR, 2017, p. 285).

O instituto da prova tem alguns princípios conceituais no Direto Processual Penal, os quais Leal (2018, p. 265) destaca os seguintes: princípio da indiciariedade, que consiste na existência de elementos sensíveis na realidade objetiva; princípio da ideariedade, o qual está relacionado com a apreensão, somatização e transmissão dos elementos de prova através do intelecto; e princípio da instrumentalidade, em que a materialização gráfico-formal desses elementos acontece pelos meios intelectivos ou técnico-jurídicos permitidos. Para sintetizar os princípios na prática, o referido autor utiliza o exemplo do instituto da perícia judicial que deve ser realizada por um perito que irá realizar a coleta intelectiva de elementos de prova existentes na realidade objetiva, sendo o seu laudo o instrumento expositivo do trabalho realizado.

No decorrer da História verifica-se a evolução dos sistemas de apreciação da prova que marcaram a evolução dos sistemas jurídicos. O sistema da certeza legal é o mais antigo, nesse sistema a certeza do acontecimento dos fatos estava atrelada a manifestação de lei natural ou divina. “Legal”, nesse contexto, significa atributo da lei da natureza reveladora dos juízos de Deus, conhecido também como ordálias. Nessa

época, a culpa ou inocência de alguém era aferida de acordo com o grau de suas virtudes, de sua santidade ou de seu poder místico. O juramento era aceito como prova da certeza da fidelidade ou compromisso com a verdade. Eventualmente eram organizados duelos (a prova *per pugnam*), em que o vencedor era tido como o escolhido de Deus, o que provava a sua inocência. Esse sistema foi, por muito tempo, a base do processo de inquisitório, em que o arbítrio das classes nobres era a ordem de revelação da justiça divina (LEAL, 2018, p. 267).

No decorrer do tempo, surgiu o sistema da livre convicção, atrelado ao sistema *common law*, que tem como base os juízos de equidade e conveniência por parte dos julgadores, em que o interesse coletivo é organizado pelo *secundum conscientizam*, no qual o juiz pode julgar de acordo com sua própria consciência, estando desvinculado do material probatório (LEAL, 2018, p. 267).

Por fim, adveio o sistema da persuasão racional, fundado no princípio da reserva legal, pelo qual a convicção do julgador está vinculada a juízos *secundum legis*, isso quer dizer, a decisão a ser proferida pelo magistrado deve estar em conformidade com a legislação vigente. Foi a partir desse sistema que se formou as condições para o surgimento do processo acusatório no campo do Direito Processual Penal (LEAL, 2018, p. 267).

O instituto da prova tem uma alta complexidade teórica, pois a mesma carrega a árdua tarefa de expressar elementos da realidade objetiva através de meios intelectivos autorizados por lei. De acordo com Leal (2018, p. 265), os meios de prova são lógico-jurídicos indicados na lei para que, através de conhecimentos, dos sentidos e técnicas de demonstração, as evidências encontradas na realidade objetiva possam ser transferidas para os autos do processo. Portanto, os meios de prova são um argumento lógico-jurídico, que podem comprovar a existência de elementos relativos à compreensão relacionada ao fato em análise.

Há na doutrina processual uma distinção entre os conceitos de meio de prova e meio de obtenção de prova. No entender de Badaró (2016, p. 387), o meio de prova é tudo aquilo que sirva para a reconstrução aproximada dos fatos alegados pelas partes, por outro lado, os meios de obtenção de prova, que também podem ser chamados de meios de investigação ou de pesquisa de provas, implicam na limitação de direitos fundamentais do indivíduo investigado e, na maioria dos casos, na restrição

das liberdades públicas relacionadas à sua privacidade ou, até mesmo, à liberdade de pensamento e expressão.

Para Lopes Júnior (2017, p. 287), é a prova que permite ao juiz apurar os fatos descritos nos autos do processo. O autor acredita que o Processo Penal e as provas fazem parte dos modos de construção de convencimento do juiz, que formará sua convicção e legitimará o poder da sentença.

Nessa toada, as provas seriam elementos que possibilitam a reconstrução histórica dos fatos com a tarefa de convencer o magistrado durante a sua apreciação dos mesmos. Taruffo (2002, p. 83) defende que, além dessa função persuasiva em relação ao magistrado, as provas também servem para fazer crer que o Processo Penal determina a verdade dos fatos, pois é conveniente que os cidadãos assim pensem, mesmo que isso não aconteça na realidade, pois essa "verdade" na realidade não pode ser obtida.

Em sentido contrário, Leal (2018, p. 269) assevera 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.

Para Soares Júnior (2016, p. 270-271), há um conflito entre quem defende o princípio da verdade real ou material, que acreditam que este princípio está em plena consonância com o processo penal, e quem rejeita esse princípio, por ser um mito que que não tem acolhida no modelo democrático. Nesse segundo grupo, existe uma divergência entre aqueles que defendem que é impossível falar em verdade processual, mesmo em sentido aproximado e os que buscam substituir no Direito Processual Penal o conceito de verdade pela ideia de determinação formal dos fatos.

Nessa busca de substituição de conceitos, Carnelutti (2001, p. 52) afirma o seguinte:

> 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.

Na mesma senda, Taruffo (2009, p. 83-84) sustenta ser desnecessário fazer uma diferenciação entre verdade relativa (formal, processual ou objetiva) e verdade absoluta (material ou subjetiva), visto que no processo a única verdade atingível é aquela que decorre do acertamento do fato proveniente dos dados cognoscitivos extraídos das provas. A verdade obtida no decorrer do processo penal pode ser limitada ou incompleta, podendo inclusive a ação processual se esgotar sem que tenha sido produzida qualquer tipo de verdade.

No entendimento de Soares Júnior (2016, p. 273), quando se fala de verdade no processo, refere-se na realidade a ideias metafísicas, como são os conceitos de bom, belo e justo, contra os quais não tem como se pronunciar, mas, no entanto, tentar demonstra-lhes a natureza pode ser uma tarefa infrutífera e sem sentido.

No Direito Processual Penal, a verdade lógica deve ser buscada, mas de antemão deve-se ter a ciência de que se trata de uma estrutura munida de grande complexidade. Essa estrutura é regulamentada pela Constituição Federal, sendo que as provas obtidas por meios ilícitos não são reconhecidas no procedimento. Os fatos que são objeto de investigação devem ser confrontados com normas das mais diversas tipologias, razão pela qual a atividade interpretativa ganha maior relevância, sendo, contudo, demasiadamente influenciável por questões ideológicas, que acabam afetando o sistema (SOARES JÚNIOR, 2016, p. 276).

Em razão dessa influência interpretativa da norma, Ferrajoli (2002, p. 42) sustenta que a linguagem jurídica deve ser “tendencialmente isenta de termos vagos ou valorativos e de antinomias semânticas internas”, o que seria assegurado pelo “sistema das garantias da estrita legalidade e estrita jurisdicionalidade”.

Em resumo, a prova não pode ser entendida apenas como algo útil à instrução do processo e ao convencimento do juiz, mas também como um direito básico derivado da cláusula do devido processo legal, que estipula salvaguardas processuais complexas destinadas a garantir plenamente a verificação e refutação dos fatos (SOARES JÚNIOR, 2016, p. 285).

Portanto, a prova não se trata de uma máxima da verdade, pois a finalidade da mesma é a fixação formal do fato contravertido, condicionada por conhecimentos

obtidos e deduções auferidas de acordo com o ordenamento jurídico (CARNELUTTI, 2001, p. 45).

Após a apuração de ocorrência de um crime, tal como o tema em discussão que são os crimes informáticos, que carregam uma grande problemática que é o elevado grau de dificuldade para a identificação dos autores, surge o desafio atrelado a comprovação, pelos meios previstos em lei, da sua existência e de quem é a autoria.

Para isso, cabe aos órgãos encarregados da persecução penal a responsabilidade de coletar evidências que possam comprovar a materialidade dos fatos e a identidade do autor, a fim de revelar todas as circunstâncias fático-jurídicas descritas no tipo penal da forma permitida por lei. Esta é uma exigência do sistema penal acusatório adotado pela Constituição da República Federativa do Brasil, de acordo com esse sistema, cabe ao órgão acusador estatal (ou ao particular, quando se admitir a ação penal privada) a demonstração contundente do crime praticado, rompendo, dessa forma, o estado de inocência inerente a toda pessoa humana ou entidade personalizada, conforme previsto no texto constitucional (RONCADA, 2017, p. 178).

A existência dos princípios do contraditório e ampla defesa sustenta a necessidade de proteção do direito à prova, pois é justamente por esses princípios que a prova se manifesta. Este é um direito subjetivo das partes, permitindo-lhes levar ao juízo suas postulações e ter a oportunidade de provar a autenticidade de suas alegações (DIAS, [2015], https://danielhc.jusbrasil.com.br/artigos/219666930/os-meios-de-prova-no-processo-penal-brasileiro-e-sua-importancia).

Nessa mesma linha de pensamento, Leal (2018, p. 265) expões o seguinte:

> 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

O artigo 5º, incisos XXXV, LIV e LV da Constituição da República Federativa do Brasil garante a produção de provas e, conforme mencionado acima, constitui direito

fundamental consubstanciado no contraditório, na ampla defesa, no devido processo legal e no acesso à justiça (SILVA, J.L.S., [2016], p. 03). No entanto, sua produção não possui caráter absoluto, estando sujeita a certas restrições, conforme descrito a seguir.

4.2 Limites à prova penal

Ainda que seja inegável a existência de um determinado elemento de prova, isso, por si próprio, não permite a coleta da prova *contra legem*, ou seja, contra a legislação em vigor.

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. 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).

Nos mais variados ordenamentos jurídicos é possível notar o princípio geral de que não se admitem provas ilícitas e ilegítimas, sendo estas as logradas em decorrência de violação de normas processuais e aquelas as obtidas mediante violação de um direito material do investigado. O artigo 5º, inciso LVI, da Constituição da República Federativa do Brasil, proíbe a utilização procedimental das provas que sejam alcançadas por meios ilícitos. Esse princípio geral tem origem na jurisprudência do Estados Unidos da América e é definido de acordo com a terminologia *exclusionary rules* (regras de exclusão), da qual se conclui que tanto as provas ilícitas como as ilegítimas devem ser mantidas apartadas do processo, seja para preservar a inviolabilidade provada, preservar o confisco popular do Estado ou prevenir abusos policiais (PACHECO, 2006, p. 544 e 546).

Conforme leciona Soares Júnior (2016, p. 280-281), do princípio geral supramencionado 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

No âmbito do Direito Processual Penal brasileiro, a jurisprudência do Supremo Tribunal Federal sempre se mostrou relutante em aceitar integralmente essas regras de exclusão da prova, optando por adotar o princípio da proporcionalidade, cabendo aos juízes decidir em casos específicos. No entanto, o artigo 157 do Código de Processo Penal, após nova redação implementada pela Lei nº 11.690 de 2008, acolheu respectivamente a regra de exclusão, a teoria dos frutos da árvore envenenada e a teoria da fonte independente. Logo, a prova ilícita deve ser removida do processo penal, bem como aquelas que dela derivam, podendo-se manter a que não possua nexo causal com ela, assim como a que pudesse ser reproduzida por fonte independente (SOARES JÚNIOR, 2016, p. 281).

Portanto, com a obtenção ilegal do elemento ou do instrumento de prova, o ato probatório torna-se inexistente, pois a prova será afetada no aspecto teórico de sua configuração legal, neste caso, a licitude dos métodos utilizados (LEAL, 2018, p. 270). Na realidade, uma vez que a legalidade em sua estrutura de produção é suprimida, a prova não seria nula, anulável e nem viciada, mas inexistente. Sua existência só pode produzir, no máximo, uma hipótese psicológica ou um senso de crença subjetiva, que por sua vez é irrelevante do ponto de vista epistemológico (POPPER, 1974, p. 48-49).

Além da regra constitucional acima mencionada que não permite a utilização de provas obtidas por meios ilícitos, o Código de Processo Penal também contém algumas restrições que tornam ilegítimo o material probatório. Por exemplo, tem-se no artigo 155, parágrafo único, o qual determina que sejam observadas as restrições da lei civil para a comprovação do estado das pessoas, como nos casos de casamento, óbito e parentesco, que só podem ser comprovadas por meio das respectivas certidões; outro exemplo é o artigo 158, que preceitua ser indispensável o exame de corpo de delito para os crimes que eventualmente deixarem vestígios, não se admitindo a sua supressão em decorrência da confissão do acusado; por último, imperioso se faz o exemplo que se pode extrair do artigo 479, *caput*, que proíbe, durante o julgamento, ler documentos ou exibir itens que não foram anexados

ao processo com pelo menos três dias úteis de antecedência, dando-se ciência à outra parte.

Visto a demonstração das principais características da prova no processo penal e alguns exemplos de suas limitações, cabe destacar que, nos crimes informáticos, a persecução probatória possui algumas particularidades que precisam ser examinadas, especialmente no tocante à sua volatilidade.

4.3 A prova no âmbito dos crimes digitais

Os diversos conceitos apresentados acima que servem de apoio para a interpretação dos fatos e das leis precisaram ser submetidos por reestruturações, com o objetivo de se atualizarem e se adaptarem à nova realidade. As circunstâncias jurídicas atuais que se verificam sociedade e no mundo tecnologicamente globalizado demandam dos operadores do Direito conhecimentos específicos para que possam atuar de acordo com o momento atual.

Essas novas circunstâncias têm como causa as variadas ações delitivas que se valem dos meios digitais para a prática de ilícitos que ofendem direitos legalmente tutelados. Conforme abordado anteriormente no presente trabalho, a maior parte das condutas delitivas praticadas pela internet já está prevista no ordenamento jurídico brasileiro com a respectiva tipificação penal, contudo, há algumas condutas com particularidades que as diferem das executadas no mundo material, visto que o meio em que o ilícito é cometido é o digital, gerando, dessa forma, efeitos no campo da persecução penal e probatória (SILVA, J.L.S., [2016], p. 06).

Ao passo que no crime tradicional, executado no mundo material, há informações essenciais para sua investigação, como vestígios, indícios e testemunhas; nos crimes informáticos, os indícios podem estar alocados em diversos dispositivos como computadores, *pendrives*, celulares, provedores de internet, registros de equipamentos de infraestrutura de rede como roteadores, *firewalls* e servidores de *e-mail*. O aparato probatório, além de volátil, é demasiadamente diversificado, podendo conter arquivos digitais (imagens, vídeos, áudios, etc.), históricos de navegação, registros de servidores, *e-mail*, dentre outros (SHIMABUKURO, 2017, p. 23).

Levando em consideração as particularidades da prova digital, caso a mesma não seja rapidamente identificada e preservada, pode sofrer danificações, suprimida,

ou alterada, dificultando dessa forma qualquer tipo de investigação e identificação do sujeito ativo do crime. Para evitar isso, a coleta do material probatório deve seguir rigorosos critérios de preservação e controle para que não seja perdida a sua veracidade (SHIMABUKURO, 2017, p. 23).

Na doutrina há quem entenda que nem todas as provas eletrônicas são revestidas de validade jurídica (MATOS, 2014, https://marianamariam. jusbrasil.com.br/artigos/119753698/da-producao-e-colheita-de-provas-no-ambiente-cibernetico). Sobre isso, Barros (2011, p. 126) assevera o seguinte:

> 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.

Baseado nas regras dos artigos 158 a 184 do Código de Processo Penal, extrai-se a ideia de que o meio de prova mais apropriado para se demonstrar uma prática criminosa é o exame de corpo de delito, realizado por meio de laudo pericial emitido por técnico competente na área de conhecimento científico, isso, claro, quando houver vestígios. O corpo de delito é a soma dos vestígios decorrentes da infração penal, ao passo que o exame de corpo de delito é a análise e o registro produzido por peritos sobre esses vestígios (RONCADA, 2017, p. 180).

Nesse sentido, Rodiner Rocada entende não ser possível produzir a prova da existência de crimes informáticos sem o adequado exame de corpo de delito, formalizado em laudo técnico pericial. Isso porque a execução de crimes informáticos demanda conhecimento específico, o que, consequentemente, requereria um perito com propriedade científica nessa área para atestar a existência do delito penal. Ao juiz, independentemente do seu conhecimento informático, não é oferecida a possibilidade de suprir a ausência de exame pericial pelo seu íntimo conhecimento, visto que isso prejudicaria sua isenção e imparcialidade para julgar a causa, uma vez que o colocaria na posição de produtor da prova, o que impossibilitaria, no curso do

processo, que as partes contradissessem a exposição dos fatos e suas respectivas consequências (RONCADA, 2017, p. 179-180).

Cabe destacar que, pelas regras processuais penais, não há uma hierarquia das provas, podendo o magistrado fundamentar suas decisões pela livre apreciação das mesmas, não existindo preferência entre as fontes de prova, nem tão pouco vinculação aos laudos periciais, os quais possuem valor apenas relativo, conforme previsto no artigo 182 do Código de Processo Penal (RONCADA, 2017, p. 180).

Há na jurisprudência um entendimento que admite ser dispensável o exame pericial quando estiverem presentes no feito outros elementos de prova que sejam suficientes para assegurar a materialidade de um crime (RONCADA, 2017, p. 181). No entanto, doutrinadores como Guilherme de Souza Nucci, afirmam que a ocorrência de infração penal deve restar comprovada de forma objetiva nos autos do processo, por meio da coleta direta ou indireta de vestígios materiais, extraindo-se destes uma conclusão segura sobre a ocorrência do crime, por meio de exame pericial, de acordo com o que preceitua o artigo 158 do Código de Processo Penal (NUCCI, 2015, p. 68).

Nessa linha de raciocínio dos autores supracitados, o exame de corpo de delito somente seria dispensável em casos em que houvesse o completo desparecimento dos vestígios materiais, devendo ser substituído, nessas circunstâncias, pela prova testemunhal, conforme estabelece o artigo 167 do Código de Processo Penal.

Eugênio Pacelli reforça a ideia de não haver hierarquia entre as provas, visto que o legislador somente elegeu meios específicos, para cada circunstância, de comprovar a existência do crime, sendo o que impera é o regime processual de livre convencimento motivado do magistrado (PACELLI, 2018, p. 332).

Nessa esteira, mesmo que não haja hierarquia entre os meios de prova, o artigo 158 do Código de Processo Penal, conforme já exposto, foi claro ao normatizar que o exame de corpo de delito é imprescindível nos casos de infração penal que deixarem vestígios materiais, não podendo ser substituído sequer pela confissão do acusado. O legislador nesse ponto teve a intenção de garantir ao acusado a formação da culpa pelos meios capazes de representar da melhor forma os fatos, afastando a possibilidade de sobreposição de algum caráter subjetivo por parte do magistrado (RONCADA, 2017, p. 182).

Dessarte, nos crimes informáticos, o exame de corpo de delito é de suma importância, porque não há como ter certeza da ocorrência do delito e seu alcance

sem apurar o caminho lógico trilhado em meio aos atos executórios, de modo que tudo isso é essencial para determinar a sua origem e precisar de quem é a autoria. Isso só poderia ser alcançado por meio de um exame técnico em que os vestígios são analisados por profissional com conhecimentos na área da informática e tecnologia da informação, tendo o mesmo a função primordial de formar uma opinião crítica e fundamentada sobre os fatos examinados (RONCADA, 2017, p. 183).

Cabe acrescentar que prescindisse do exame de corpo de delito quando não restam vestígios da pratica delitiva, conforme mencionado anteriormente no presente trabalho, bem como quando os fatos forem de conhecimento comum, sendo, resumidamente, aquilo que faz parte da cultura geral da sociedade; nesse caso não há a necessidade de exame pericial, pois o conhecimento oriundo dos fatos está ao alcance de qualquer pessoa, podendo ser facilmente comprovado por qualquer meio. Relacionado aos crimes digitais é possível mencionar como fatos de conhecimento comum o funcionamento prático da internet, o acesso público a manifestações individuais em redes sociais e a utilidade de alguns *softwares* populares que não necessitam de análise pericial (RONCADA, 2017, p. 184).

Os crimes informáticos não possuem regras processuais próprias no ordenamento jurídico brasileiro. Portanto, aplicam-se a eles as regras processuais estipuladas genericamente no Código de Processo Penal e em leis esparsas, como a Lei nº 12.850 de 2013, denominada como Lei de Combate à Organização Criminosa. Como exceção, imperioso se faz observar que a Lei nº 12.965 de 2014, mais conhecida como Marco Civil da Internet, contém significativos instrumentos de apuração de crimes informáticos previstos nos seus artigos 13, 15 e 22, os quais estipulam que o servidor de conexão ou aplicação da internet acate à ordem judicial de acesso ao conteúdo dos registros (RONCADA, 2017, p. 185).

No ordenamento jurídico brasileiro não há impedimentos para a utilização de provas obtidas no meio digital. De forma favorável a utilização desse tipo de prova, estipula o artigo 225 do Código Civil (BRASIL, 2002, http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm) que:

> 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.

Nesse sentido, estipula o artigo 369 do Código de Processo Civil (BRASIL, 2015, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm) 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.

Por conseguinte, as provas digitais são aceitas pelo ordenamento jurídico brasileiro, desde que respeitados certos padrões técnicos para sua coleta e armazenamento, objetivando, dessa forma, resguardar sua integridade, validade e licitude (SILVA, J.L.S., [2016], p. 08).

O desenvolvimento das tecnologias da informação refletiu diretamente na modernização das ferramentas para validação jurídica das provas, o que promoveu o surgimento da computação forense. A computação forense é uma das principais áreas da ciência criminalística que aborda a investigação probatória e que pode ser definida, nas palavras de Silva, J.L.S. ([2016], p. 10), como sendo o “uso de técnicas analíticas e de investigação para identificar, coletar, analisar e preservar as provas/informação que é armazenada magneticamente ou codificada”. Visto que a ciência forense abriga a perícia forense aplicada à informática, a mesma, por sua vez, pode ser definida, conforme exprime Silva, J.L.S. ([2016], p. 10), como 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”.

Na computação forense são utilizados métodos científicos com o propósito de identificar, preservar, coletar, interpretar, analisar, validar, documentar e apresentar as evidências digitais. Essas evidências são todas as informações sujeitas ou criadas pela intervenção humana, que podem ser extraídas de um computador ou qualquer dispositivo eletrônico. Portanto, os exames forenses são projetados para extrair informações para identificar qualquer evidência que possa ser relevante para o caso concreto, a fim de tirar conclusões sobre o crime (SILVA, J.L.S., [2016], p. 10).

Em meio a investigação de um crime informático, a primeira atitude a ser tomada é a realização do levantamento das evidências e informações que possam ser usadas como elemento de prova. Nessa espécie de crime, as evidências e as informações são armazenadas em mídias digitais, como discos rígidos de computadores (também

conhecidos como HD, abreviatura de *hard disc*) ou a memória de celulares. A investigação importa na atividade de exame pericial que, consequentemente, resultará na prova pericial, formulada a partir de critérios científicos. O laudo pericial é de suma importância para o processo para traduzir de forma clara e objetiva o que foi feito pelo perito antes, durante e depois de seus exames sobre o caso em análise (QUEIROZ; VARGAS, 2010, p. 29). Portanto, as informações alcançadas e expostas nesse material possuem uma elevada carga de vestígios para o desenrolar e conclusão do processo criminal (SILVA, J.L.S., [2016], p. 11).

As provas descobertas no meio digital são caracterizadas pelo grande risco de virem a perecer, o que demanda, consequentemente, maiores cuidados no seu processo de coleta, para que seja preservada a sua integridade. Ademais, para que a evidência seja realmente considerada parte dos elementos probatórios da prova digital, certas regras de aceitação devem ser seguidas. Seguindo essa ideia, Silva, J.L.S. ([2016], p. 11) afirma o seguinte:

> 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.

Os crimes informáticos, da mesma forma que os crimes tradicionais do mundo material, demandam procedimentos adequados para a coleta das evidências, a fim de não prejudicar sua validade. Apesar da computação forense ser demasiadamente precisa, caso o procedimento adotado para a coleta de evidências for feito de forma errada, pode vir a tornar a prova invalida ou até mesmo ilícita (SILVA, J.L.S., [2016], p. 11).

A criminalidade no âmbito digital deve ser combatida com as mesmas ferramentas presentes nessa espécie delitiva, para isso, essencial se faz haver unidades policiais especializadas nesses crimes, com o intuito de garantir a manutenção da integridade das provas atrelado a ideia de possibilitar a adequação dos órgãos policiais à velocidade que se transforma os crimes digitais (MATOS, [2014], https://marianamariam.jusbrasil.com.br/artigos/119753698/da-producao-e-colheita-de-provas-no-ambiente-cibernetico). Com isso, o método de investigação e

julgamento de um crime informático deve ser guiado pela ampla liberdade probatória estendida às partes e no livre convencimento do órgão julgador para que este possa analisar as provas, fundamentando sempre os motivos de sua decisão (DIAS, [2015], https://danielhc.jusbrasil.com.br/artigos/219666930/os-meios-de-prova-no-processo-penal-brasileiro-e-sua-importancia).

4.4 Interesse público e interesse privado

A maioria das investigações sobre crimes cometidos no âmbito digital exige que, para efeito de prova, haja a quebra do sigilo da troca de mensagens eletrônicas entre os usuários através de *softwares*. No entanto, esse tipo de mensagem instantânea se caracteriza por ser transmitida de um ponto a outro de forma criptografada e, ao ser entregue, é excluída dos servidores dos provedores que intermediam essa comunicação, restando a mensagem armazenada apenas no próprio dispositivo do usuário. Os provedores alegam que não podem interceptar ou armazenar as mensagens trocadas entre os seus usuários porque elas são decodificadas somente no terminal que recebe a mensagem, ou seja, o aparelho celular do usuário (SILVA, J.L.S., [2016], p. 12).

Em julho de 2016, no Estado do Rio de Janeiro, o judiciário determinou ao Facebook do Brasil, proprietário do aplicativo WhatsApp, que realizasse a interceptação de mensagens de alguns usuários alvos de uma investigação criminal. Na oportunidade, frente a falta de cumprimento da ordem, a juíza Daniela Barbosa Assunção de Souza, da 2ª Vara Criminal de Duque de Caxias, determinou a suspensão dos serviços de troca de mensagens em todo país (JUÍZA DO RJ, 2016, https://www.conjur.com.br/2016-jul-19/juiza-manda-suspender-whatsapp-reclama-resposta-ingles).

O problema, como é possível perceber, está no fato de haver uma limitação no que se refere à obtenção de provas pelo sistema judiciário nos casos que envolvam comunicação digital. A infraestrutura da internet e dos dispositivos que a acessam foram projetadas pensando na implementação de requisitos de criptografia e segurança para dificultar as tentativas de acesso à conteúdo não autorizado, de invasão de sistemas computacionais e proteção de dados sensíveis dos usuários não só visando sua integridade, mas também assegurando o direito à privacidade

elencado no texto constitucional (ALVES, 2020, https://ler.amazon.com.br/?asin=B08LXB27TH&language=pt-BR).

As mensagens contidas em aplicativos de mensagem instantânea acessadas a partir da apreensão de celulares vêm sendo utilizadas como material probatório em meio a instrução de processos penais com o objetivo de desarticular associações criminosas e investigar participações em outros crimes. Observa-se, no entanto, que essas mensagens não são obtidas de forma instantânea, mas sim em momento posterior, após a preensão do aparelho celular atrelado à investigação, quando então a autoridade investigadora, devidamente autorizada judicialmente, poderá acessar as informações contidas na memória do dispositivo telefônico. Diferentemente do que ocorre, por exemplo, em uma interceptação telefônica, em que o agente investigador consegue acompanhar em tempo real a conversa do alvo investigado.

A partir desse problema surge a questão atrelada ao suposto conflito entre a supremacia do interesse público e o interesse privado, se seria cabível relativizar o direito individual das pessoas de se comunicarem de forma segura em favor da possibilidade de se criar mecanismos capazes de interceptar essas comunicações quando se demonstrasse conveniente ao interesse coletivo.

O direito à privacidade está previsto no artigo 5º, inciso X, da Constituição Federal do Brasil (BRASIL, 1988, http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm) 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”. Contudo, há uma discussão a respeito da força de tal princípio em relação a uma proposta de implementação de um sistema capaz de monitorar as comunicações estabelecidas via aplicativos para atender as eventuais demandas do judiciário (SILVA, J.L.S., [2016], p. 13).

O direito à privacidade é valioso não apenas para a vida privada dos indivíduos, mas também para a vida pública e comunitária. Isso não deve ser entendido como a proteção exclusiva dos indivíduos, mas como um direito necessário para a manutenção da cidadania (LEONARDI, 2012, p. 122).

Ao considerar a possibilidade de implementar uma solução que monitora as comunicações de aplicativos de mensagens, existe uma reiterada discussão sobre o direito à privacidade. A mera possibilidade de implementação de alguma forma de controle já é motivo para divergências, principalmente no que tange ao princípio da

supremacia do interesse público, por se tratar de um conceito incerto e sem abrangência delimitada pacificamente (SILVA, J.L.S., [2016], p. 15).

O entendimento sobre o princípio da supremacia do interesse público diverge entre os que o relacionam como sendo um contraponto ao interesse individual e os que entendem se tratar de uma soma de interesses individuais, contemplando o conjunto de necessidades humanas indispensáveis na vida do indivíduo. Nesse segundo entendimento, aplica-se 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 membros da sociedade (MELLO, 2018, p. 62).

Para Carlos Ari Sundfeld, o interesse público não está acima da ordem jurídica, mas teria somente uma prioridade em relação ao privado (SUNDFELD, 2012, p. 143). No mesmo sentido, Gabriel de Araújo Lima, afirma haver uma contradição intrínseca na proposta desse princípio, pois se o interesse público engloba os interesses privados, o enunciado, sob o ponto de vista lógico, não poderia prever uma supremacia dos interesses públicos sob os interesses privados (LIMA, 2009, p. 125).

Na concepção clássica, há a compreensão de que a Administração Pública seria a tutora do interesse público, sem haver a necessidade de participação da sociedade para sua definição. Dessa forma, o Estado seria uma entidade fomentadora dos interesses públicos entendidos como bem-estar dos indivíduos, cujo mecanismo de atuação seria o Direito. No entanto, com a evolução dos sistemas jurídicos restou demonstrado que essa preconcepção de interesse público não mais satisfaz os anseios da sociedade pluralista contemporânea, não podendo-se admitir 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).

Em uma sociedade democrática não é apropriado deixar a cargo da Administração Pública o monopólio da definição do interesse público, mas ao mesmo tempo, apenas identifica-lo ao interesse da coletividade e ao bem comum não ajudará em nada o debate (MOREIRA NETO, 2014, p. 410). Em decorrência da diversidade de interesses que se manifestam na sociedade, o conceito de interesse público deve ser idealizado a partir de uma perspectiva procedimental, segundo a qual o mesmo não possui um conteúdo pré-estabelecido, sendo ele o resultado de procedimentos

democráticos de criação, execução e aplicação do Direito (JUSTEN FILHO, 2016, p. 45).

A interpretação do termo “interesse público” deve-se dar como sendo o resultado do desempenho da autonomia pública dos cidadãos de uma determinada comunidade jurídica em um certo contexto histórico. Dessa forma, o interesse público não se trata de pressuposto para decisões democráticas e sim o resultado delas (JUSTEN FILHO, 2016, p. 45).

Distintamente do que se possa pressupor, entre a supremacia do interesse público e o interesse privado inexiste uma abstrata relação de antagonismo, sendo o que existe é uma relação de complementariedade e interdependência (FISCHGOLD, 2011, p. 91). Isto é, o desempenho da autonomia pública só será possível se a autonomia privada estiver assegurada a todos os cidadãos, conjuntamente, a autonomia privada só estará resguardada de forma efetiva se os cidadãos fizerem o uso adequado da autonomia pública. É possível constatar que a promoção do interesse público representa, igualmente, uma condição possibilitadora de proteção jurídica do interesse privado (HABERMAS, 2002, p. 293-295).

Resumidamente, é incompatível com Estado Democrático de Direito a ideia de que o interesse público possui uma preferência frente ao interesse privado, tendo em vista que os direitos individuais que protegem interesses privados e metas coletivas que protegem interesses públicos situam-se de forma igual entre os objetivos da atividade estatal, justamente porque a Constituição da República Federativa do Brasil adota a ideia de interdependência entre as autonomias pública e privada no modelo de Estado Democrático de Direito (FISCHGOLD, 2011, p. 93). Portanto, a fim de satisfazer os direitos e necessidades da coletividade, não se pode afastar as legítimas prerrogativas dos interesses individuais. Com o intuito de garantir o respeito à liberdade de expressão, comunicação e manifestação de pensamento, nos moldes da Constituição da República Federativa do Brasil, foi promulgada a Lei nº 12.965 de 2014, conhecida como Marco Civil da Internet, a qual será analisada em alguns aspectos no próximo capítulo.

4.5 Marco Civil da Internet, análise de alguns aspectos

O Marco Civil da Internet, Lei nº 12.965, promulgada em 23 de abril de 2014, estabelece em seu artigo 1º (BRASIL, 2014, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm) “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”.

O legislador, no inciso I do artigo 4º da Lei nº 12.965/2014, ao afirmar que o acesso à internet é direito de todos, estabelece que a mesma no Brasil se caracteriza como um direito difuso e universal. Na sequência, no mesmo diploma legal, o artigo 5º exprime a ideia de que a internet não é um ambiente acessível somente por computadores, demonstrando, dessa forma, o fenômeno sociológico exercido por aquela. O legislador, ao utilizar a nomenclatura “terminal”, manifesta a intenção de abarcar todo dispositivo que potencialmente possa ser utilizado como meio de prática de condutas no meio digital (SYDOW, 2015, p. 275).

Outro dispositivo da lei em comento que traz preceitos importantes é o inciso VI do artigo 7º que ostenta o direito de informação, que, por sua vez, embora já se encontrasse previsto no Código de Defesa do Consumidor, assegura aos usuários o direito de lhes serem prestados (BRASIL, 2014, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm):

> 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.

Essa prerrogativa, reconhece a fragilidade do usuário perante os outros atores do meio digital, bem como os corriqueiros abusos praticados pelos provedores que visam obter vantagens ilícitas dos usuários (SYDOW, 2015, p. 275-276).

A parir do surgimento do Marco Civil da Internet, o que se verificou foi uma maior proteção dos dados dos usuários, os quais passaram a ter maiores garantias, como, por exemplo, de só poderem ter o sigilo de dados informáticos quebrado mediante ordem judicial. Com isso também constatasse que, se um internauta quiser encerrar sua conta em uma rede social ou serviço *online*, o mesmo poderá requerer que seus dados sejam excluídos de forma definitiva, porque o Marco Civil da Internet firmou o entendimento de que os dados pertencem ao usuário, e não à terceiros (ALVES, 2020, https://ler.amazon.com.br/?asin=B08LXB27TH&language=pt-BR).

O Marco Civil da Internet também inovou ao garantir a privacidade das comunicações, que antes era restrito, visto que não se estendia aos serviços de *e-mail*, por exemplo. Com isso, o conteúdo das comunicações privadas em meio eletrônico passou a ter igual proteção de privacidade que já era previsto em favor dos meios de comunicação tradicionais como cartas e conversas telefônicas. Esses valores expressos de inviolabilidade de dados dos usuários e de suas comunicações demonstra uma nova realidade digna de proteção. Logo, cabe ao Direito Penal legitimar valores para que determinados bens jurídicos sejam protegidos (SYDOW, 2015, p. 276).

A respeito das investigações policiais, no que se trata a forma como as mesmas serão conduzidas, importante se faz ressaltar a diferença entre os conceitos de “dados estáticos” e “dados dinâmicos”. Os dados estáticos consistem nos registros imutáveis que um usuário possui na rede, ao passo que os dinâmicos são dados de navegação, como conversas, registros de *download*, dentre outros. Para o acesso àqueles, o inciso IV do artigo 3º da Lei nº 12.850 de 2013, denominada como Lei de Organização Criminosa, estabelece que em qualquer fase da persecução penal, serão permitidos, sem prejuízo a outros já previstos em lei, os seguintes meios de obtenção de prova (BRASIL, 2013): “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”. Já para o acesso aos dados dinâmicos, o Marco Civil da Internet estabelece que estes poderão ser cedidos somente mediante autorização judicial (SYDOW, 2015, p. 277).

O artigo 22 da Lei nº 12.965 de 2014 (BRASIL, 2014, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm) estabelece 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.

Isso quer dizer que um particular que possuir interesse em acessar informações estáticas e dinâmicas com o propósito de obter um material probatório poderá requerer isso ao juiz competente. No entanto, o procedimento é mais rigoroso do que o enfrentado por autoridades do Ministério Público, visto que o requerimento será considerado inadmissível se não restarem demonstrados explicitamente os indícios

da ocorrência do delito, os motivos para a utilização dos registros e o período ao qual os registros fazem referência (SYDOW, 2015, p. 277).

A Lei nº 12.965/2014, em seu artigo 13, também inovou ao fixar o prazo de um ano de manutenção de registros de conexão por parte do administrador de sistema autônomo provedor de internet, a fim de possibilitar a obtenção de elementos probatórios mesmo após o decurso de um prazo razoável posterior a prática de um eventual delito. Os titulares do pedido são, exclusivamente, a autoridade policial, a autoridade administrativa e o Ministério Público. Essa titularidade também é assegurada em caso de guarda de registros de acesso a aplicação de internet pelo prazo de seis meses, nos termos do artigo 15 da mencionada Lei (SYDOW, 2015, p. 277).

O Marco Civil da Internet também estabeleceu a possibilidade de retirada de conteúdos impróprios expostos na internet. Anteriormente, não existia uma regra clara a ser adotada para esse procedimento. A partir de então, a remoção de conteúdos da internet poderá ser executada mediante a ordem judicial, excetuado os casos de “pornografia de vingança”. Nestes casos, a vítima que teve sua intimidade violada poderá solicitar diretamente aos sites ou serviços em que estejam alocados esses materiais para que procedam com a remoção do conteúdo. Em caso de remoção do conteúdo, os provedores de acesso deverão comunicar ao responsável pelo conteúdo, se tiver o contato do mesmo, conforme estabelece o artigo 20 da Lei em comento (BRASIL, 2014, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm), “os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo”.

Em síntese, embora o Marco Civil da Internet tenha deixado diversas lacunas, ele possui um papel importante no estudo do Direito Penal atrelado a matérias informáticas, visto que contribuí de forma significativa para adequada interpretação da norma, bem como tenta solucionar alguns questionamentos que ainda existiam sobre o assunto (SYDOW, 2015, p. 279).

5 CONCLUSÃO

Através do presente trabalho, objetivou-se realizar uma abordagem sobre o desenvolvimento do processo tecnológico e seus impactos na vida das pessoas, que possibilitou encurtar distâncias, ainda que de forma virtual, e acelerar as transformações sociais na era digital. Atrelado a isso, buscou-se, sobretudo, demonstrar os impactos exercidos pela revolução informática no campo do Direito Penal e Processual Penal.

Diante disso, foi feita a abordagem de questões atinentes aos novos meios de cometimento de crimes tradicionais através do ciberespaço, o surgimento de novos bens jurídicos oriundos dessa nova realidade tecnológica, a territorialidade da lei penal em decorrência das particularidades dos crimes informáticos e a coleta e formação do material probatório no âmbito digital.

Desde o momento em que a internet passou a ocupar um espaço indispensável na vida em sociedade, as informações e os dados vinculados na internet passaram a ter um alto valor econômico e social. Dessa forma, a internet está se tornando cada vez mais alvo de comportamentos ilegais.

Embora o anonimato do acesso traga uma sensação de privacidade para os usuários comuns, também forma perfeitas condições para os criminosos possam agir sem serem notados num primeiro momento, o que contribui para o crescimento do crime informático. Esse tipo de crime é peculiar e complexo, trazendo grandes dificuldades para a investigação, obtenção e manipulação das provas, bem como identificação dos autores.

Tendo em conta os novos riscos decorrentes do desenvolvimento da tecnologia informática, os bens jurídicos criminais também estão sujeitos a mudanças. Ao lidar com o crime informático, pode-se dizer que o comportamento criminoso não afeta apenas o valor tradicionalmente protegido, mas também os dados armazenados (informações) e a segurança do computador ou do sistema de rede de comunicação. A partir daí, a informação passa a ter um papel preponderante na vida humana e a ser um bem jurídico que demanda proteção nessa espécie criminosa. Além disso, a confiabilidade e a segurança dos sistemas e redes de computadores também demandam tutela do Direito Penal. No decorrer do presente trabalho destacou-se que a classificação mais adequada dos crimes informáticos é aquela que os diferencia

entre os delitos cometidos contra algum bem jurídico informático próprio, como dados ou sistemas, e os praticados contra bem jurídico tradicional, não relacionado à tecnologia, através de meios digitais, sendo estes denominados crimes informáticos impróprios e aqueles crimes informáticos próprios.

Ao contrário dos crimes cometidos no mundo físico, no ambiente digital, normalmente, há uma distância espacial entre o autor do crime e a vítima, o que torna mais dificultoso o combate ao crime informático. Desta forma, dificuldades são enfrentadas em meio aos procedimentos de investigação criminal, porque as mudanças nas fronteiras nacionais podem exigir a cooperação entre diferentes países com sistemas jurídicos distintos, o que pode causar obstáculos burocráticos intransponíveis que impossibilitam a condenação.

Dos desafios relacionados aos crimes digitais, determinar o local da sua ocorrência está entre os mais desafiadores. Sobre isso, no Brasil, a lei penal adotou a teoria da ubiquidade, em que se considera praticado o crime no local onde ocorreu a ação ou omissão, no todo ou em parte, assim como onde se produziu ou deveria ter produzido o resultado.

Portanto, seguindo essa teoria, se o crime informático for cometido pela internet, e o perpetrador e a vítima estiverem localizados em países distintos, a aplicação da norma será muito simples, desde que ambos os países tipifiquem a conduta como crime, restando, neste caso, ter o cuidado para que não venha a ocorrer o *bis in idem*. Porém, quando o comportamento é típico em apenas um dos países envolvidos, é que surge o grande problema, pois não há uma solução pacífica na doutrina e nem critérios seguros capazes de determinar qual medida deve ser adotada. Ao nosso ver, a solução mais adequada deve se dar através de tratados internacionais que discorram sobre essa questão, estabelecendo a cooperação entre os Estados envolvidos, para que se possa criar condições investigatórias ao país interessado na persecução penal, a fim de que este obtenha todo material que necessita e que por ventura esteja armazenado no exterior.

Os crimes informáticos têm como característica essencial a volatilidade da sua materialidade, pois os dados e informações do ambiente digital não se encontram obrigatoriamente reunidos em um único local, podendo ser facilmente modificados ou suprimidos. No entanto, não deixar absolutamente nenhum rastro que possa ser utilizado no curso da persecução penal é algo muito difícil. Se houver cooperação do

provedor de internet e a investigação for rápida, é perfeitamente possível determinar a identidade do autor. A prova no âmbito digital, além de volátil, é muito heterogênea, podendo ser composta por registros de servidores, arquivos digitais, históricos de navegação, vídeos, fotos, e-mails, entre outros. Em razão das peculiaridades desse tipo de prova, caso a mesma não seja rapidamente preservada, pode acabar sendo danificada, alterada ou suprimida, o que dificultaria qualquer investigação ou identificação do autor do delito.

O processo penal é um instrumento retrospectivo, que tenta reconstruir um determinado fato de forma aproximada, de modo a transferir para os autos do processo as evidências encontradas na realidade objetiva. Portanto, é por meio das evidências que se busca essa reconstrução aproximada dos eventos passados, ou seja, o crime. No entanto, a prova não pode ser entendida como aquilo que contribui apenas para a instrução e convencimento do juiz, mas também como um direito básico derivado do princípio do devido processo legal, que prevê garantias processuais as partes, preceituando que não só o juiz, mas também as mesmas sejam destinatárias da prova.

O Código de Processo Penal elegeu o exame de corpo de delito como meio de prova mais adequado para demonstrar uma prática criminosa nos casos em que se verifique a existência de vestígios. Parcela da doutrina defende a tese de que não há prova do crime informático sem o respectivo exame de corpo de delito, consubstanciado em laudo técnico pericial. A justificativa apresentada pelos doutrinadores que defendem essa tese se dá no sentido de que esse tipo de crime envolve questões técnicas muito específicas, que demandam conhecimento científico de informática para assegurar sua existência. Contudo, outra parcela de doutrinadores defendem a tese de que que o exame pericial pode ser dispensado quando houver outros elementos de prova que sejam capazes de atestar a materialidade do crime. O Código de Processo Penal, em seu artigo 167, estabelece a dispensa do exame de corpo de delito somente em casos de desaparecimento dos vestígios materiais, podendo, neste caso, ser substituído pela prova testemunhal. Outra exceção se dá no caso dos fatos serem de conhecimento comum e não necessitarem de exame pericial, devido ao fato de estarem ao alcance de qualquer pessoa, podendo ser comprovados através de qualquer meio.

Para que ocorra a coleta de provas na maioria dos crimes praticados em ambiente digital, é necessário muitas vezes que ocorra a quebra do sigilo de troca de mensagens entre usuários. No entanto, isso provoca um questionamento sobre a violação de garantias individuais como a da privacidade. Ressalta-se que a privacidade não importa somente para um único indivíduo, mas para o coletivo, sendo, por tanto, um direito indispensável para a manutenção do exercício da cidadania e do interesse público.

Diferentemente da concepção clássica, o interesse público não pode ser visto como algo antagônico e nem superior ao interesse individual. Com o desenvolvimento dos sistemas jurídicos, o estereótipo de que o interesse público seja gerado exclusivamente pelo Estado não mais atende os anseios da sociedade que demanda uma participação ativa em sua construção. Nesse sentido, o termo interesse público deve ser tido como o resultado do desempenho da autonomia pública dos cidadãos de uma determinada comunidade em um contexto em que não haja controvérsia entre público e privado, mas sim uma relação de complementariedade e interdependência entre eles.

Ainda que a internet seja considerada por muitas pessoas como um ambiente sem lei, sendo propicio a impunidade, a prática se mostra diferente. Mesmo que as normas sobre o tema não estejam satisfatoriamente disciplinadas, vem sendo feito um trabalho de adequação à legislação positiva existente. As questões jurídicas decorrentes do incremento do uso da tecnologia informática são visivelmente complexas e não devem ser tratadas somente com a incriminação de certas condutas. A legislação pátria precisa ser revista não apenas penalmente, mas de forma conjugada e colaborativa. Ademais, observa-se que o Estado tem avançado ao prever algumas condutas criminosas, embora ainda tenha muito a ser feito para se alcançar uma efetiva proteção penal quando se trata de meio digital.

REFERÊNCIAS

ALEXANDRE JÚNIOR, Júlio César. Cibercrime: um estudo acerca do conceito de crimes informáticos. **Revista Jurídica da Faculdade de Direito de Franca**, Franca, SP, v. 14, n. 1, p. 341-351, 2019. Disponível em: http://www.revista.direitofranca.br/index.php/refdf/article/view/602. Acesso em: 13 set. 2021.

ALVES, Matheus de Araújo. **Crimes digitais:** análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova. São Paulo, SP: Dialética, 2020. *E-book*. Disponível em: https://ler.amazon.com.br/?asin=B08LXB27TH&language=pt-BR. Acesso em: 13 de set. 2021

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

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do hacker ético**. 5. ed. Florianópolis, SC: Visual Books, 2014.

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

BRASIL. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 13 set. 2021.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 13 set. 2021.

BRASIL. **Lei nº 8.137, de 27 de dezembro de 1990**. Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. Brasília, DF: Presidência da República, [2011]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8137.htm. Acesso em: 13 set. 2021.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 13 set. 2021.

BRASIL. **Lei nº 9.504, de 30 de setembro de 1997**. Estabelece normas para as eleições. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 13 set. 2021.

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. Brasília, DF: Presidência da República, [1998]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 13 set. 2021.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 13 out. 2021.

BRASIL. **Lei nº 12.850, de 02 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. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 13 out. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 out. 2021.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 13 out. 2021.

CARNELUTTI, Francesco. **A prova civil**. Tradução: Lisa Pary Scarpa. Campinas, SP: Bookseler, 2001.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Âmbito Jurídico**, [*s.l.*], abr. 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 13 set. 2021.

DIAS, Daniel de Lélis. Os meios de prova no processo penal brasileiro e sua importância. **Jus Brasil**, [*s.l.*], [2015]. Disponível em: https://danielhc.jusbrasil.com.br/artigos/219666930/os-meios-de-prova-no-processo-penal-brasileiro-e-sua-importancia. Acesso em: 13 out. 2021.

DULLIUS, A.D.; HIPLLER, A.; FRANCO, E. L. Dos crimes praticados em ambientes virtuais. **Conteúdo Jurídico**, [*s.l.*], ago. 2012. Disponível em: http://www.conteudojuridico.com.br/consulta/Artigos/30441/dos-crimes-praticados-em-ambientes-virtuais. Acesso em: 13 set. 2021.

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

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, DF, 2011. Disponível em: https://repositorio.unb.br/handle/10482/8732. Acesso em: 13 out. 2021.

GOUVEIA, Luís Manuel Borges. Sociedade da informação: notas de contribuição para uma definição operacional. **Universidade Fernando Pessoa**, Porto, Portugal, nov. 2004. Disponível em: http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf. Acesso em: 13 set. 2021.

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

JESUS, Damásio de. **Manual de crimes informáticos**. 1. ed. São Paulo, SP: Saraiva, 2016. *E-book*. Disponível em: https://stream2.docero.com.br/pdf_dummy/eyJpZCI6IjQ4OTcxMyIsIm5hbWUiOiJNQU5VQUwgREUgQ1JJTUVTIElORk9STUFUSUNPUyIsImV4dGVuc2lvbiI6InBkZiIsImNoZWNrc3VtX2lkIjoiNTIzNTQzMyJ9?. Acesso em: 13 set. 2021.

JEZLER JÚNIOR, Ivan. **Prova penal digital: tempo, risco e busca telemática**. 1. ed. Florianópolis, SC: Tirant Lo Blanch, 2019.

JUÍZA DO RJ manda suspender WhatsApp e reclama de resposta em inglês. **Consultor Jurídico**, [s./.], 19 jul. 2016. Disponível em: https://www.conjur.com.br/2016-jul-19/juiza-manda-suspender-whatsapp-reclama-resposta-ingles. Acesso em: 13 out. 2021.

JUSTEN FILFO, Marçal. **Curso de direito administrativo**. 12. ed. rev. atual. e ampl. São Pulo, SP: Revista dos Tribunais, 2016.

KIST, Dario José. **Prova digital no processo penal***.* 1. ed. Leme, SP: JH Mizuno, 2019.

LEAL, Rosemiro Pereira. **Teoria geral do processo:** primeiros estudos. 14. ed. Belo Horizonte, MG: Fórum, 2018.

LEONARDI, Marcel. **Tutela e privacidade na internet**. 1. ed. São Paulos, SP: Saraiva, 2012.

LIMA, Gabriel de Araújo. Teoria da Supremacia do Interesse Público: crise, contradições e incompatibilidades de seus fundamentos com a Constituição Fderal. **Revista de Direito Administrativo e Constitucional**, Belo Horizonte, MG, n. 36, p. 123-153, abr./jul. 2009.

LLINARES, Fernando Miró. La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. **Revista Electrónica de Ciencia Penal y Criminologia**, [*s./.*], p. 07-55, 2011. Disponível em: http://criminet.ugr.es/recpc/13/recpc13-07.pdf. Acesso em: 13 set. 2021.

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

MATOS, Mariana Maria. Da produção e colheita de provas no ambiente cibernético. **Jus Brasil**, [*s.l.*], [2014]. Disponível em: https://marianamariam.jusbrasil.com.br/artigos/119753698/da-producao-e-colheita-de-provas-no-ambiente-cibernetico. Acesso em: 13 out. 2021.

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

MINISTÉRIO PÚBLICO FEDERAL (MPF). MPF defende adesão do Brasil à Convenção de Budapeste em audiência pública na Câmara. **MPF**, Brasília, DF, jun. 2019. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/mpf-defende-adesao-do-brasil-a-convencao-de-budapeste-em-audiencia-publica-na-camara. Acesso em: 13 set. 2021.

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

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

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

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

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

QUEIROZ, Claudemir; VARGAS, Raffael. **Investigação e perícia forense computacional**: certificações, leis processuais, estudos de caso. 1. ed. Rio de Janeiro, RJ: Brasport, 2010.

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

SANTOS, Sofia. Ciberespaço: Noções e origem do termo Ciberespaço. **Knoow.net, Enciclopédia temática**, [*s.l.*], fev. 2018. Disponível em: https://knoow.net/ciencinformtelec/informatica/ciberespaco/. Acesso em: 13 set. 2021.

SHIMABUKURO, Adriana. Cibercrime: quando a tecnologia é aliada da lei. *In*: MUTA, Carlos (org.). **Investigação e prova nos crimes cibernéticos**. 1. ed. São Paulo, SP: EMAG, 2017. p. 17-31. *E-book*. Disponível em: https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 13 out. 2021.

SILVA, Jorge Luiz Silva da. A prova nos crimes que se utilizam das redes sociais. **Ajufesc**, [*s.l.*], [2016]. Disponível em: https://ajufesc.org.br/wp-content/uploads/2017/02/Jorge-Luiz-Silva-da-Silva.pdf. Acesso em: 13 out. 2021.

SILVA, Patrícia Santos. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais**. 1. ed. Brasília, DF: Vestnik, 2015. *E-book*. Disponível em: https://profmatheus.com/wp-content/uploads/2017/05/direito-crime-cibernetico.pdf. Acesso em: 13 set. 2021.

SILVA, Wanderlice Maria Pereira da. **As estruturas sócio-antropológicas do ciberespaço**, [*s.l.*], [2011]. Disponível em: http://www.sbsociologia.com.br/portal/index.php?option=com_docman&task=doc_download&gid=776&Itemid=171. Acesso em: 13 set. 2021.

SOUZA NETO, Pedro Américo de. **Crimes de informática**. 2009. Monografia (Bacharel em Direito) – Universidade do Vale do Itajaí, Itajaí, SC, 2009. Disponível em: http://siaibib01.univali.br/pdf/Pedro%20Americo%20de%20Souza%20Neto.pdf. Acesso em: 13 set. 2021.

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

SUNDFELD, Carlos Ari. **Fundamentos de direito público**. 5. ed. São Paulo, SP: Saraiva, 2015.

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

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

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

VAZ, Denise Provasi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório**. 2012. Tese (Doutorado em Direito Processual) – Faculdade de Direito, Universidade de São Paulo, São Paulo, SP, 2012. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/pt-br.php. Acesso em: 13 set. 2019.