CENTRO UNIVERSITÁRIO – UNINOVAFAPI
BACHARELADO EM DIREITO

CARLOS FELIPE MELO E SILVA
DAVID JHONATAS AMORIM DE SOUSA
LUDMILA LEITE PIRES

SISTEMA DE PROVAS NOS CRIMES VIRTUAIS: os desafios da instrução probatória em ações penais relativas aos crimes virtuais no brasil

TERESINA
2023

CARLOS FELIPE MELO E SILVA
DAVID JHONATAS AMORIM DE SOUSA
LUDMILA LEITE PIRES

SISTEMA DE PROVAS NOS CRIMES VIRTUAIS: os desafios da instrução probatória em ações penais relativas aos crimes virtuais no brasil

Artigo de Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Centro Universitário UNINOVAFAPI, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Profº Me Sarah Maria Veloso Freire

TERESINA
2023

FICHA CATALOGRÁFICA

S586s

Silva, Carlos Felipe Melo e.

Sistema de provas nos crimes virtuais: os desafios da instrução probatória em ações penais relativas aos crimes virtuais no brasil / Carlos Felipe Melo e Silva, David Jhonatas Amorim de Sousa, Ludmila Leite Pires. – Teresina: Uninovafapi, 2023.

Orientador: Profª. Me. Sarah Maria Veloso. Centro Universitário UNINOVAFAPI, 2023.

29 p.; 23cm

Monografia (Graduação em Direito) – Centro Universitário UNINOVAFAPI, Teresina, 2023.

1. Internet. 2. Crimes cibernéticos. 3. Legislação. I. Título. II. Veloso, Sarah Maria.

Catalogação na publicação

Francisco Renato Sampaio da Silva – CRB/1028

CARLOS FELIPE MELO E SILVA
LUDMILA LEITE PIRES
DAVID JHONATAS

SISTEMA DE PROVAS NOS CRIMES VIRTUAIS: os desafios da instrução probatória em ações penais relativas aos crimes virtuais no brasil

Artigo de Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Centro Universitário UNINOVAFAPI, como requisito parcial para obtenção do grau de Bacharel em Direito.

Data de Aprovação: _____/_____/_____

BANCA EXAMINADORA

_____

Prof.ªMe SARAH MARIA VELOSO FREIRE

Centro Universitário - UNINOVAFAPI

(Orientadora)

_____

Profª titulaçãoxxxxxxxxxx

Centro Universitário - UNINOVAFAPI

(1º Examinador)

_____

Profª titulaçãoxxxxxxxxxxx

Centro Universitário - UNINOVAFAPI

(2º Examinador)

AGRADECIMENTOS

Em primeiro lugar, agradecer a Deus, por tudo que alcançamos até o presente momento, aos nossos pais, irmãos e famliares, por entederem nossas ausências, correrias e por muitas vezes, o afastamento por estarmos em busca de realizar nossas metas e alcançar nossos objetivos.

Com carinho, agradecer aos nossos professores, que fizeram de tudo para nos orientar e dedicaram do seu tempo para nos conduzir em direção ao futuro e ao nosso lado profissional, que sem dúvidas, fará toda diferença.

Finalizamos, agradecendo também ao nosso trio, por termos sidos fortes e resilientes nesse processo de formação, muitas vezes um dando força ao outro, para não desanimar e muito menos desistir do caminho até o presente em que chegamos.

RESUMO

O crime virtual é um crime que decorre da evolução tecnológica pela qual passa a sociedade contemporânea. Os avanços tecnológicos e as novas descobertas científicas trouxeram novas realidades para a humanidade, onde o espaço e a existência física não são base para o cometimento de atos ilícitos. Com a crescente demanda de crimes envolvendo meios cibernéticos, tem que ser voltado procedimentos que identifiquem melhor as infrações cometidas, pra identificar: quais os possíveis danos causados? Quais as vulnerabilidades identificadas? Quais as melhorias e medidas que possam ser adotadas pra cessar esse problema? Quais as medidas judiciais cabíveis a o criminoso? Assim o objetivo geral desse estudo foi analisar os obstáculos dos procedimentos investigativos, para a proteção estatal dos direitos dos usuários perturbados por tais delitos. Nesse deslinde, o método aplicado na pesquisa será o hipotético dedutivo, assim a pesquisa teve caráter bibliográfico com abordagem qualitativa e no que cerne aos objetivos, optou-se pela pesquisa exploratória. Concluiu-se que a velocidade da tecnologia e os mais diversos mecanismos de comunicação fazem com que meios de criminalidade e anonimato sejam criados e modificados diariamente. Diante das questões probatórias levantadas em nossa pesquisa, buscamos encontrar uma alternativa para que o Estado veja de forma adequada neste ambiente veloz e mutável, garantindo a proteção da privacidade individual, ao invés de desconstruir os direitos e garantias que foram obtidos.

Palavras-chave: Internet. Crimes cibernéticos. Legislação.

ABSTRACT

Virtual crime is a crime that stems from the technological evolution of contemporary society. Technological advances and new scientific discoveries have brought new realities to humanity, where space and physical existence are not the basis for the commission of illicit acts. With the growing demand for crimes involving cybernetic means, procedures that better identify the infractions committed, to identify: what are the possible damages caused? What vulnerabilities are identified? What improvements and measures can be taken to stop this problem? What legal measures are available to the criminal? Thus the general objective of this study was to analyze the obstacles of investigative procedures for the state protection of the rights of users disturbed by such crimes. In this way, the method applied in the research will be the hypothetical deductive, so the research had bibliographic character with qualitative approach and at the heart of the objectives, it was opted for exploratory research. It was concluded that the speed of technology and the most diverse communication mechanisms cause means of crime and anonymity to be created and modified daily. Given the probative issues raised in our research, we seek to find an alternative for the state to see adequately in this fast and changing environment, ensuring the protection of individual privacy, rather than deconstruct the rights and guarantees that were obtained.

Keywords**:** Internet. Cybercrimes. Legislation.

1 INTRODUÇÃO

O crime virtual é um crime que decorre da evolução tecnológica pela qual passa a sociedade contemporânea. Os avanços tecnológicos e as novas descobertas científicas trouxeram novas realidades para a humanidade, onde o espaço e a existência física não são base para o cometimento de atos ilícitos (Malaquias, 2012).

Hoje, com o rápido desenvolvimento da ciência e da tecnologia, a Internet tornou-se um livro aberto, ou seja, uma janela aberta para o mundo. Não é exagero dizer que pode ser considerado como uma das garantias básicas dos direitos das pessoas. Tal prelúdio se dá pelo simples fato de que, hoje, tudo gira em torno da informatização (Alves, 2018).

Grande parte do debate é sobre as vulnerabilidades que as pessoas enfrentam ao usar as redes sociais. No entanto, é importante ressaltar que, além de um grande número de dispositivos, esse ambiente que integra as pessoas ao contexto da computação global é composto principalmente por indivíduos de diferentes origens culturais e que trabalham com diferentes comportamentos (Schimidt, 2014).

Dessa forma, segundo Malaquias (2012), é possível identificar pontos vulneráveis nesse ambiente interativo não apenas como possíveis falhas de segurança dos dispositivos conectados, mas também a atitude criminosa de alguns criminosos, com conhecimento técnico suficiente. Atividades criminosas de usuários que se conectam à rede de maneira negligente.

A grande maioria das atividades criminosas nas redes sociais foi regulamentada no sistema legal, incluindo: difamação, difamação, danos, ameaças, vazamento de segredos, roubo, vandalismo, apropriação indébita, peculato, violação de direitos autorais, zombar de outros por motivos religiosos, apoiar a prostituição, atos escritos obscenos, incitação a crimes, apologia a crimes ou criminosos, identidades falsas, inserção de dados falsos em sistemas de informação, adulteração de dados em sistemas de informação, falso testemunho, exercício arbitrário das próprias razões, jogos de azar, crimes que ponham em risco a segurança nacional, terrorismo, drogas e tráfico de pessoas, preconceito ou discriminação de raça, cor, etnia, pedofilia, crimes contra a propriedade industrial, interceptação de comunicações, lavagem de dinheiro e pirataria de software (Alves, 2018).

Por ser um campo em crescimento e existirem muitas ferramentas para diversas áreas como lazer, profissional e educacional, tem sido utilizado como

ferramenta do crime. Tal como é utilizada para o aperfeiçoamento e avanço científico, a Internet também é utilizada para comportamentos típicos ilícitos, nomeadamente o cibercrime. Essas infrações penais articuladas no código penal são de natureza a causar determinados danos, que podem ser morais ou hereditários (Schimidt, 2014)

Nesse interim, a escolha do tema decorre de a necessidade dos pesquisadores aprofundarem seus conhecimentos sobre temas populares. Assim, dado que a Internet está evoluindo a cada dia, esta pesquisa também. Existem muitas maneiras de combater esses crimes virtuais, como a promulgação de leis para regular esses comportamentos e padronizar os métodos de coleta de evidências para promover a investigação e punição de criminosos virtuais. Com maior coerção, os criminosos pensarão duas vezes antes de usar a Internet como ferramenta para seus crimes, pois não estarão mais protegidos da impunidade e do anonimato.

Com a crescente demanda de crimes envolvendo meios cibernéticos, tem que ser voltado procedimentos que identifiquem melhor as infrações cometidas, pra identificar: quais os possíveis danos causados? Quais as vulnerabilidades identificadas? Quais as melhorias e medidas que possam ser adotadas pra cessar esse problema? Quais as medidas judiciais cabíveis a o criminoso?

Assim o objetivo geral desse estudo foi analisar os obstáculos dos procedimentos investigativos, para a proteção estatal dos direitos dos usuários perturbados por tais delitos. Nesse sentido, os objetivos específicos foram: conceituar a origem e como ocorrem os crimes cibernéticos; indagar como se classificam estes crimes cibernéticos; e examinar como ocorre a admissibilidade das provas nos crimes cibernéticos.

Nesse deslinde, o método aplicado na pesquisa será o hipotético dedutivo, pois irá trabalhar com hipóteses, evidenciando assim entendimentos cabíveis ao ordenamento jurídico nacional sobre tal tema. A pesquisa teve caráter bibliográfico, baseando-se em livros, revistas virtuais, artigos publicados, monografias, com o intuito de analisar as diferentes concepções adotadas sobre o tema. A abordagem foi qualitativa, por ter base teórica, sem levantamento de números ou análise de dados, com o objetivo de compreender a visão geral sobre o referido tema. No que cerne aos objetivos, optou-se pela pesquisa exploratória.

Este estudo revela sua vital relevância ao observar como a Internet tornou-se hoje uma tecnologia indispensável e de grande importância, considerada essencial

para a sociedade contemporânea, utilizando-a para os mais diversos fins. No entanto, esse moderno recurso tecnológico é extremamente atrativo para indivíduos que veem nesse ambiente virtual uma grande oportunidade para a prática de infrações penais, em detrimento de leigos que utilizam a Internet para realizar tarefas simples do dia a dia.

Embora os crimes cometidos nessa área estejam em processo de modernização, o ordenamento jurídico brasileiro permanece inerte a essa nova realidade da sociedade, deixando de determinar quais meios probatórios os operadores do direito podem utilizar no processo penal, daí a tentação. ferramentas da internet. Observa-se que a falta de leis que definam formas específicas de provar isso ajuda os criminosos a permanecerem anônimos e a escapar impunes. Perante esta situação, os operadores do direito recorrem aos mesmos meios de prova.

Portanto, para comprovar a autoria e o mérito de um crime virtual, as provas mais utilizadas hoje e consideradas válidas pelo ordenamento jurídico brasileiro são: perícia realizada em computadores utilizados por agentes criminosos, correspondência interceptada e vazamento de documentos eletrônicos são relação site.

Nesse caso, a escolha da temática alçada decorre de a necessidade dos pesquisadores aprofundarem seus conhecimentos sobre temas populares. Assim, dado que a Internet está evoluindo a cada dia, esta pesquisa também. Existem muitas maneiras de combater esses crimes virtuais, como a promulgação de leis para regular esses comportamentos e padronizar os métodos de coleta de evidências para promover a investigação e punição de criminosos virtuais. Com maior coerção, os criminosos pensarão duas vezes antes de usar a Internet como ferramenta para seus crimes, pois não estarão mais protegidos da impunidade e do anonimato.

Desse modo, a proposta do tema é evidenciada ao longo da explanação do presente trabalho, que usa a metodologia dogmático-jurídicos, o estudo reporta o Direito Penal e Processual Penal, focando nas leis específicas voltadas ao conteúdo virtual, levantando os conceitos gerais de como essas provas se comportam perante o processo.

O método aplicado na pesquisa será o hipotético dedutivo, pois irá trabalhar com hipóteses, evidenciando assim entendimentos cabíveis ao ordenamento jurídico nacional sobre tal tema. De acordo com Prodanov (2013) “O método hipotético-dedutivo é uma modalidade que se inicia com um problema ou lacuna no

conhecimento científico, passando pela formulação de hipótese e por um processo de inferência dedutiva, o qual testa a predição da ocorrência de fenômenos abrangidos pela referida hipótese.

A pesquisa terá caráter bibliográfico, baseando-se em livros, revistas virtuais, artigos publicados, monografias, com o intuito de analisar as diferentes concepções adotadas sobre o tema, de forma a absolver conhecimento da pesquisa, procurando assim bases teóricas para a estrutura da presente pesquisa.

A abordagem será qualitativa, por ter base teórica, sem levantamento de números ou análise de dados, com o objetivo de compreender a visão geral sobre o referido tema. No que cerne aos objetivos, optou-se pela pesquisa exploratória, cujo intuito é fornecer mais informações sobre o tema que será abordado de modo que seja possível o seu melhor entendimento, explanação e orientação, estabelecendo maior familiaridade com a questão central abordada, para fornecer dados básicos que possam contribuir para o desenvolvimento do projeto, com pesquisas aprofundadas sobre o objeto proposto (Pradanov, 2013).

A base legal será versada sobre os artigos e ainda convenções que tratam do referido tema, como por exemplo, a Convenção de Budapeste que é um tratado internacional de direito penal e processo penal que visa os crimes praticados por meio digital, se utilizando a internet, além de projetos de lei, onde pode se mencionar a Lei Carolina Dieckmann, como também os crimes já tipificados no código penal.

2 CRIMES CIBERNÉTICOS: UM LEVANTAMENTO HISTÓRICO

Nenhum país que queira acompanhar o ritmo do mundo pode escapar da evolução da realidade do uso da tecnologia nos mais diversos campos da atividade humana. Para o Brasil, a situação não é exceção. Em 1961, o Instituto Brasileiro de Geografia e Estatística (IBGE) passou a utilizar computadores modelo UNIVAC1105.

Em 1964, foi criado o Centro de Processamento Eletrônico de Dados do Estado do Paraná, empresa pública que desempenha diversas funções relacionadas à tecnologia da informação, como consultoria em informática, desenvolvimento e manutenção de sistemas, e outras funções importantes para o crescimento da economia brasileira. Internet (Silva, 2016). Em 1965, a recém-formada Agência Federal de Processamento de Dados juntou-se à União Internacional de Telecomunicações por Satélite (INTELSAT), estabelecendo a Brasil Telecom como uma ferramenta estatal para intervir nos serviços de telecomunicações, mantendo um

monopólio.

Todo o processo de introdução das telecomunicações e do uso dos computadores culminou no primeiro computador brasileiro: o "Patinho Feio" da Universidade de São Paulo (USP). Em 1974, a Computadores Brasileiros SA (COBRA) foi constituída como empresa nacional pioneira no desenvolvimento, produção e comercialização de tecnologias na área de informática. Em 1979, foi criada a Secretaria Especial de Informática com um conceito protecionista como base de sustentação da Lei de Informática. Em 1988, o Brasil deu um grande passo no uso da Internet, conectando-se à Bitnet, transmitindo e-mails do Laboratório Nacional de Computação Científica (LNCC), da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e o Fundo Tutelar da Universidade do Rio de Janeiro (UFRJ).

Em 1992, foi implantada a primeira rede conectada à Internet no Brasil, interligando as principais universidades brasileiras. Em 1995, foi criado o Conselho Brasileiro de Governança da Internet (CGI.br) para coordenar e incentivar os esforços para o desenvolvimento de uma Internet com qualidade técnica, inovação e difusão de serviços. Uma das tarefas fundamentais do CGI.br é disseminar informações sobre o uso da Internet no país, como parâmetros para a determinação de políticas básicas de inclusão digital dos brasileiros (Adachi, 2009, p. 37).

À medida que a Internet cresce, também aumentam as ameaças aos recursos técnicos disponíveis na rede. O matemático John Von Neumann previu programas reprodutíveis de informações que mais tarde fundamentam vários problemas que surgem hoje na forma de código malicioso (Lovison, 2012).

É interessante observar a relação entre a diversão e a capacidade de criar coisas novas. Por exemplo, na década de 60, o jogo Core Wars era um código malicioso desenvolvido por programadores que, ao ser executado, sobrecarregava a memória das máquinas dos outros jogadores. Os criadores do jogo também inventaram o primeiro antivírus chamado Reaper, que funcionava limpando as cópias geradas pelo Core Wars (Medeiros, 2005, p. 09).

Em 1982, Richard Skrenta criou o Elk Cloner, considerado por muitos estudiosos como o primeiro vírus a infectar um computador. Esse código malicioso se espalha por meio de cópias de disquetes contaminados, uma técnica que pode levar a infecções generalizadas subseqüentes devido à facilidade de troca de dados em disquetes. Em 1983, o pesquisador Fred Cohen chamou os programas de código nocivos de "vírus de computador" em sua análise (Sppaford, 1994, p. 03).

Em 1986, dois paquistaneses criaram um vírus de computador chamado Brain. Os vírus fazem com que o sistema operacional funcione lentamente. Além de utilizar técnicas que dificultam a deteção, o vírus atinge o setor de inicialização dos discos e se espalha por meio de disquetes (descartados). Em 1988, o primeiro software antivírus foi lançado, tornando o sistema seguro contra vírus cerebrais. Aquele ano foi um marco em uma batalha que continua até hoje, na qual os vírus sempre encontram uma maneira de superar a tecnologia antivírus, muitas vezes antes mesmo de serem criados. Ao mesmo tempo, um worm de Internet foi lançado na Internet, infetando aproximadamente 6.000 computadores (Overill, 1998, p. 159).

Em 1989, o "Dark Avenger" rapidamente infectou computadores como uma tática furtiva para diminuir seus danos para que eles pudessem permanecer sem serem detectados por mais tempo. Em 1992, o vírus Michelangelo se tornou o primeiro vírus a causar um burburinho na mídia. O vírus sobrescreverá partes do disco rígido da vítima em 6 de março, aniversário do autor renascentista. Em 1994, a Polícia da Scotland Yard, no Reino Unido, registrou o primeiro caso de punição contra o autor do vírus. Nesse caso, o autor do vírus causador foi condenado a 18 meses de prisão (Overill, 1998, p. 159).

Em 1999, surgiu o vírus Chernobyl, que tornou o disco rígido e os dados do usuário inacessíveis, causando enormes prejuízos econômicos à China, Turquia e Coreia do Sul. Em 2000, o vírus da carta de amor varreu a Europa e os Estados Unidos em 6 dias, causando prejuízos de cerca de US$ 9 milhões (Santos,Camargo. 2013, p. 44).

Todas essas perdas econômicas exigem cada vez mais a reavaliação das estratégias de gerenciamento de segurança de computadores, a criação de novos paradigmas de prevenção e a atualização contínua das políticas de segurança. Com o avanço da tecnologia, surgiram novos meios de propagação de ameaças, permitindo que novos dispositivos acessem a internet. Em 2004, surgiu o primeiro vírus móvel chamado Cabir. O vírus se espalha via Bluetooth e esgota a bateria do telefone infectado (Leavitt, 2005).

Com o surgimento de uma série de novos meios de contaminação de códigos maliciosos, os desafios relacionados ao acúmulo e atualização de conhecimento e tecnologia são um potencial desafio para os órgãos policiais que buscam proteger os bens jurídicos mais importantes da sociedade, que também podem se tornar criminosos. para fins maliciosos.

3 CRIMES CIBERNÉTICOS NA ATUALIDADE

Do ponto de vista processual penal, o Estado tem o direito de punir as condutas que tenham condutas positivas previstas na lei penal e lesem os interesses de terceiros e os interesses sociais. Ainda que se configure crime, devem ser seguidos os devidos trâmites legais antes da aplicação das sanções previstas, ou seja, o princípio da impunidade.

Para Lopes Jr. (2019), a apropriação de penas pelo Estado ocorre quando normas judiciais são aplicadas para eliminar represálias privadas, o que se relaciona com a ideia de evolução das penas, pronunciada por juízes imparciais cujos poderes são limitados por lei. Deste ponto de vista, a evolução do processo penal está intimamente relacionada com a evolução do próprio direito penal, devendo a aplicação das penas passar pelos devidos trâmites legais, tendo em conta a necessidade de tutela constitucional entre o processo penal e a aplicação das penas. Conduta e Conformidade. Porque esse procedimento não é mais visto como uma simples ferramenta a serviço do poder punitivo (direito penal), mas como um limitador do poder e proteção dos indivíduos a ele sujeitos.

Deve-se entender que o respeito às garantias fundamentais não pode ser confundido com a impunidade, e isso nunca foi defendido. O processo penal é um meio necessário para alcançar a punição de acordo com a lei. Sua existência, portanto, só será reconhecida se as regras e garantias garantidas pela Constituição (a regra do devido processo) forem rigorosamente observadas (Lopes Jr., 2019).

Nesta área, Coutinho (2009) assinala que na maioria dos ordenamentos jurídicos existem dois regimes de processo penal: o investigativo e o penal. Na definição dada pelos autores, interrogatório. É indiscutivelmente o maior instrumento legal que o mundo já viu; e sabe. Independentemente de suas origens, a Igreja é estruturalmente má e tem sido assim por mais de 700 anos.

Ou seja, o sistema de interrogatório apresenta a imagem do juiz, bem como o poder de gestão do juiz e a iniciativa das provas que repassa, não havendo contradição e bastando a defesa. Por outro lado, o sistema de acusação distingue claramente entre acusação e julgamento, há uma separação de funções na gestão da prova e os juízes tornam-se espectadores para poderem fazer julgamentos imparciais (Coutinho, 2009).

A Constituição de 1988 define o processo penal brasileiro como a persecução baseada na inconsistência e adequação da defesa, na imparcialidade da sentença e nas demais regras do devido processo legal. No entanto, deve-se considerar que no mesmo ordenamento jurídico penal, de acordo com o disposto no artigo 156, §§ 1º e 2º da Lei de Processo Penal, é conferido aos juízes o direito de conduzir o devido processo legal de interrogatório. (Lopes Jr, 2019). Características do interrogatório também podem ser observadas no inquérito policial, procedimento administrativo em que o acusado não participa de processos conflituosos, podendo financiar os destinatários da denúncia e instaurar processo criminal (Brener, 2020).

Este procedimento administrativo tem por finalidade apurar o autor do crime e as circunstâncias dos factos criminais aparentes, tem por fim fundamentar o procedimento ou a não persecução penal, só podendo existir factos puníveis, cuja finalidade sejam apenas crimes verdadeiros, apenas crime fato o que chamamos de Comportamento Criminoso (Lopes Jr., 2019).

Precisamente no atual panorama social, com o forte desenvolvimento do conhecimento humano, do risco e do progresso tecnológico, surgiram novas realidades e necessidades, entre as quais cresce uma forte necessidade de segurança face às ameaças tecnológicas, que acabam por afetar os crimes jurídicos na sociedade. Uma das ferramentas de escolha mais poderosas para proteger o controle social que as pessoas tentam evitar intervindo quando surgem novos interesses legítimos, como direitos suprapessoais com conteúdo descentralizado, proteção de dados, proteção contra atos ilegais e situações perigosas. criminalização é proteção penal (Arageo, 2015).

Devido a novas infrações penais, especialmente no ambiente online, a forma como a autoria ou a evidência substantiva é revelada apresenta desafios significativos para facilitar os processos criminais. Como resultado, o comportamento humano no reino virtual é complexo e não é facilmente compreendido pela aplicação da lei. Diante dessa complexidade, o crime informático apresenta novos tipos de comportamento não sancionados pelo direito penal clássico, levando todo o mundo a organizar e promulgar sua própria legislação para proteger usuários e sistemas informáticos (Castro, 2018).

Houve um atraso no que cerne a doutrina jurídica em comparação com o ritmo do desenvolvimento tecnológico, ainda mais quando se trata da taxonomia do cibercrime. A gama de crimes e a variedade de novas práticas tornam qualquer

classificação obsoleta devido ao ritmo acelerado de mudança dos padrões criminais (Greco Filho, 2000).

Ivette Senise Ferreira (2005) sugere uma direção para uma possível classificação dos crimes virtuais: atos contra sistemas de computador, atos contra computadores com subespécie e atos contra dados ou programas de computador. Atos cometidos por meio de sistemas de computador, incluindo violações de propriedade; violações da liberdade pessoal e violações de propriedade intangível.

Como não há integração em torno de uma classificação igualitária específica, as principais dividem o cibercrime em apropriado, impróprio, híbrido, genérico e puro. Essa classificação decerto e errado, mista, não deve ser confundida com a classificação existente no direito penal que utiliza os termos certo e errado para classificar crimes de acordo com sujeitos ativos.

No mundo virtual, o crime em si é um crime contra dados e contra a estrutura física de sistemas operacionais e programas de computador. Subdivide-se ainda em: 1. Crime puro, que se refere à falta de condições especiais exigidas pelo tipo, para que o crime não seja típico; os casos de resposta são aqueles em que o interesse legítimo protegido pela lei penal é a inviolabilidade das informações automatizadas crimes (Viana, 2003).

Damásio de Jesus (2016) se posiciona por esse raciocínio, uma vez que os crimes eletrônicos são aqueles cometidos por computadores e executados ou consumidos eletronicamente. Entre eles, a tecnologia da informação (segurança do sistema, propriedade da informação e integridade dos dados, máquinas e periféricos) é um objeto jurídico protegido.

Na categoria específica de crimes, há alguns exemplos, fraude eletrônica, invasão de equipamentos de informática, instalação de vírus, alteração de senhas, modificação de equipamentos eletrônicos. Os cibercriminosos concentram-se precisamente em dados, software e dispositivos eletrônicos. Marco Túlio Viana aponta essa classificação como: “Aqueles cujos interesses legítimos são protegidos pela lei penal atentam contra a inviolabilidade da informação automatizada” (Viana, 2000).

Outra classificação é para crimes em que os meios eletrônicos são apenas um dos meios de cometer crimes e, portanto, são definidos como crimes culposos. Essa classificação determina que o uso de aparelhos eletrônicos é apenas mais um meio de ferir normas, mas nem só por meio de aparelhos eletrônicos o ato pode ser praticado. Os crimes culposos são cometidos em ambiente virtual, mas ofendem um

espaço físico real e suas ações recaem sobre bens ou pessoas. No mundo virtual, esses crimes são moldados com o apoio do direito penal, equiparando sua aplicação às normas jurídicas aos crimes do mundo real (Damasio de Jesus, 2016).

Damásio de Jesus (2016) define crime culposo como crime eletrônico culposo é quando um agente usa um computador como meio para produzir um resultado natural, ofende o mundo físico ou espaço "real", ameaça ou fere outra coisa, não computacional ou miscelânea crime de computador Um crime que afeta o mundo real, mas usa um ambiente virtual devido à conveniência que ele traz. Peculato, fraude, difamação, calúnia, intimidação são considerados crimes dessa natureza. Nas palavras de Ivette Senise Ferreira e Vicente Greco, a classificação dada é a de dividir os crimes específicos em atos dirigidos contra interesses legítimos em informática, e crimes de improbidade como atos dirigidos contra interesses legítimos tradicionais (Ferreira, 2011).

A tipificação dos crimes virtuais implica a obrigatoriedade do uso de meios eletrônicos na prática dos crimes, o que se denomina doutrina híbrida do crime. A vítima é a pessoa certa, portanto, o autor do crime direciona o ataque a uma determinada vítima para obter vantagem de bens pessoais como transferências sem autorização prévia, fraude bancária e quaisquer outros bens que possam ser retirados da vítima pela rede Criminoso. Considerando a importância dos interesses legítimos protegidos para além da inviolabilidade dos dados, trata-se de crimes decorrentes da invasão de equipamentos informáticos que adquiriram o estatuto de crimes especiais (Damasio de Jesus, 2016).

Por fim, os crimes cibernéticos são crimes de natureza formal, pois são consumidos no cometimento de atos criminosos, independentemente da ocorrência de consequências naturais. Vicente Maggio classifica-o como: Crimes ordinários (crimes que qualquer um pode cometer), Presença Múltipla (muitas vezes através de atos diversos), Comissionamento (resultados das atividades ativas dos agentes: “Invasão”, “Instalação”), e Omissão em casos excepcionais (quando o resultado deva ser impedido por pelos garantes – art. 13, § 2º, do CP), de forma vinculante (somente mediante a execução prevista no tipo de crime) ou gratuita (pode ser executada por qualquer meio de execução), conforme o caso, formal (é consumido sem produzir resultados naturalísticos, embora possa acontecer.

4 A LEGISLAÇÃO BRASILEIRA E A COMPETÊNCIA NOS CRIMES VIRTUAIS

A legislação nacional está sempre se adaptando às novas tecnologias, mas o mundo virtual muda muito rápido e está em constante mudança a cada dia. Devido à velocidade das mudanças sociais e tecnológicas, a burocracia politizada em que vivemos acaba tornando as regras feitas para situações cotidianas menos preventivas e punitivas, tornando as mudanças nas regras obsoletas.

Nesse sentido, citamos o posicionamento de José Luiz Bolzan de Morais e Elias Jacob de Menezes Neto (2014) de que um dos principais objetivos da vigilância é prever o comportamento futuro, seja por meio do poder público prever atitudes ou do setor privado prever a melhor maneira de ganhar dinheiro com publicidade. Os seres humanos são criaturas de hábitos, portanto, ao coletar uma variedade de informações durante um período suficientemente longo, padrões de comportamento, mudanças, preferências e interações sociais podem ser previstos.

No entanto, devido ao número crescente de novos crimes, essa proteção legal pode não ser suficiente. A norma jurídica é pragmática, diz apenas ações que se conformem aos princípios constitucionais do Art. 5º, XXXIX da Constituição Federal de 1988. Não observar o devido processo legal sem ser canonizado ou decretado não pode ser considerado crime.

Atualmente, existem cada vez menos normas de comportamento no ciberespaço, formando uma lacuna diante desse vasto mundo. As leis que impõem seu texto aos crimes virtuais são a Lei Comum 12.735/2012, 12.737/2012 e a Lei 12.965/2014. A Lei 12.737/2012 é baseada na Lei 84/1999, mas esta lei é muito rígida em termos de proteção individual. O grupo de gestão elaborou uma lei facultativa que estipula que os padrões criminais irão representar o comportamento no mundo virtual e apresenta uma nova legislação para definir os direitos e deveres dos internautas.

Para essa lei, Patrícia Peck (2013) delineou a prática de quem, por ganho indevido, instalar uma vulnerabilidade em um sistema de informação, como backdoor ou configuração, de forma que determinadas portas de comunicação com a Internet estejam sempre abertas. Em geral, os usuários de gadgets e dispositivos de computação são protegidos contra hackers e pessoas mal-intencionadas que abusam de sua confiança ou tentam deliberadamente se infiltrar em um dispositivo para obter dados de computador apropriados ou prejudicar seu proprietário, excluir ou alterar dados de forma que eles se tornem inúteis, mesmo íntimo e privado. Informações

como fotos, documentos e vídeos. As empresas têm proteções legais mais fortes contra a espionagem digital, pois o acesso a segredos comerciais legalmente definidos e/ou informações confidenciais agora também está sujeito à lei (Pinheiro; Haikal, 2013).

Agora que o projeto entrou na legislatura, há uma corrida para ajudar a aprovar a lei mais rapidamente. A atriz brasileira Carolina Dieckmann (Carolina Dieckmann) causou alvoroço na sociedade e na mídia após a exposição de fotos íntimas. A atriz foi hackeada e os invasores poderiam usar o material como moeda de troca, obtendo acesso a fotos e informações privadas. Os cibercriminosos abordaram a atriz para fazer uma barganha em troca de não divulgar o material obtido. A atriz não cedeu à chantagem, e suas fotos íntimas foram divulgadas, causando grande repercussão e grande constrangimento à vítima, pois os criminosos incluíram nas fotos a orientação sexual da atriz. Como resultado dessa reação e pressão pública sobre o legislativo, em 30 de novembro de 2012 foi aprovada a Lei Carolina Dieckmann.

O Estado prevê a possibilidade de invasão e está sujeito ao exercício de seus poderes punitivos de forma a garantir a prevenção dos referidos princípios constitucionais. A existência de mecanismos de segurança que protegem os dispositivos eletrônicos como antivírus, senhas e outras defesas digitais impede a maioria das invasões, porém, quando esses dispositivos são submetidos a violações simples dessas defesas, atos criminosos são cometidos.

Leis destinadas a complementar e alterar o diploma legal vigente: Alterações ao Decreto nº 2.848, de 7 de dezembro de 1940 - Código Penal, decreto nº 7.716 do Código Penal Militar e Decreto nº 7.716, de 5 de janeiro de 1989, que dispõe sobre a uso de meios eletrônicos, sistemas digitais ou similares e outras medidas implementadas contra sistemas informatizados e similares (Brasil, 2012).

O Marco Civil da Internet foi instituído no ordenamento jurídico em 2012/2014, mas foi afetado por uma onda crescente de ataques direcionados a sites oficiais de governos e empresas públicas. Buscar a proteção da informação é o primeiro passo para a criação do “Marco Civil da Internet” pela Lei nº 12. 965/14, cujas disposições ampliam ainda mais as garantias pessoais e as obrigações e direitos dos internautas no Brasil de utilizar a Internet. As leis pendentes foram objeto de longos debates ao longo do caminho, com discussões centradas na liberdade, privacidade e neutralidade da rede, ressaltando o papel da soberania nacional. Sendo a internet uma ferramenta para o cidadão exercer seu papel social por meio da liberdade de expressão, essa

exposição pode acarretar em violações da vida privada, o que foi uma das preocupações do Estado ao promulgar a Lei 12.965/2014.

No entanto, a lei estabelece regras para provedores de internet, sendo a mais relevante a proteção do direito à privacidade. Os provedores devem fornecer identidades de usuários em circunstâncias específicas, mas sempre por ordem judicial para proteger os direitos individuais e a privacidade. Acompanhando o marco civil da internet, a Lei 12.965/2014 traz questões como a obrigatoriedade dos provedores de serviços de internet manterem registros de conexão por um ano e registros de acesso por, no mínimo, seis meses.

A lei também beneficia os provedores ao responsabilizar os usuários pelo conteúdo que geram, a menos que esse conteúdo esteja em uma rede social que tenha sua própria gama de serviços. Em caso de veiculação de conteúdo criminoso nas redes sociais, o Provedor terá um prazo de remoção e, caso o conteúdo não seja removido, o Provedor responderá em qualquer juízo por qualquer dano causado pelo material publicado em suas páginas.

Há grandes divergências legislativas quanto à jurisdição condenatória do cibercrime, pois no mundo da informática o conceito de jurisdição é um tanto invalidado, pois a rede é um sistema global que perde limitações geográficas neste espaço sem fronteiras. Crimes multilocais ocorrem quando atos ou omissões ocorrem em locais incertos, criando uma cascata de conflitos jurisdicionais. O conflito existe porque os crimes podem ser cometidos em território nacional dentro de fronteiras internacionais, gerando conflitos de poder transfronteiriços (Pacheco, Lopes 2016).

O brasilismo usa teorias híbridas ou universais ao considerar formas de resolver conflitos de competência. As capacidades são definidas por onde ocorrem as violações, onde ocorrem as omissões ou ações, onde todas ou a maioria delas ocorrem simultaneamente e onde os resultados são produzidos (Silva, 2015).

As normas adotadas no artigo 6º do Código Penal são baseadas nos princípios da territorialidade, proteção, justiça universal, nacionalidade ativa e representação. Eugênio Pacelli (2010) Não deve haver conflitos no ambiente estatal porque há apenas uma jurisdição: como atividade e expressão do poder público, diz-se que há apenas uma jurisdição porque é uma intervenção estatal cujo objetivo é ação legal específica e, mais especificamente, ação legal em um caso criminal ou assunto de grande interesse para todos.

É necessário que a empresa armazene esse conjunto de informações por

motivos técnicos e administrativos, ou por norma legal a que está sujeita. Em alguns países, o armazenamento de conteúdo gerado na Internet é baseado em aspectos fiscais e econômicos. Por questões de segurança, esses servidores estão espalhados, seu conteúdo é replicado para vários cantos do globo, e suas informações são segmentadas e depois armazenadas para proteger o conteúdo de possíveis ataques de criminosos.

Supondo que a empresa provedora tenha o direito de fornecer os dados digitais, ela será responsável, para que possa fornecer todas as opções acima na ordem judicial final. Caso a empresa provedora não tenha fornecido conteúdo que facilite a investigação, responderá incidentalmente aos fatos após receber a notificação judicial e deverá retirar o conteúdo de sua notificação. Atendendo às condições de responsabilidade do prestador, deverá consultar a legislação aplicável.

Os juízes devem esclarecer os fatos lesivos e indicar quais providências devem ser tomadas. Após apresentar os conceitos básicos para a compreensão das peculiaridades típicas do comportamento do cibercrime, apontaremos o impacto dessas peculiaridades no processo penal, ou seja, no âmbito da investigação de casos de cibercrimes.

5 ADMISSÃO DE PROVAS EM CRIMES CIBERNETICOS

A prova é a ferramenta que se utiliza para tentar estabelecer a veracidade de uma alegação ou fato, portanto, todo fato existente no processo deve ser provado. A lista de crimes tem crescido consideravelmente, porém, não é suficiente incluir novos tipos de crimes, pois com o surgimento desses crimes vêm outras inovações, por exemplo relacionadas à investigação de provas (Pinheiro, 2013).

O conceito de prova não é derivado da lei, tem referências no pensamento científico geral. Surge no direito processual como forma de traduzir como o Estado/juiz e as partes se dispõem a provar suas pretensões em juízo, e para que a autoridade judiciária competente possa condenar o sujeito ou indultá-lo, dependendo de sua decisão. Dessa forma, o conceito de prova pode ser adotado como uma atividade designada para a coleta de elementos, que irão esclarecer os pontos contenciosos do processo e formar as convicções dos juízes (Cintra, 2010).

A prova no processo penal brasileiro pode ser conceituada como: uma série de atos praticados por uma parte com o objetivo de provar em juízo a ocorrência ou não

de um fato, a veracidade ou não de uma informação. Prova: “É todo e qualquer meio perceptivo empregado pelo ser humano para provar a veracidade de uma acusação” (Crespo, 2011).

Os elementos de prova são ainda divididos em cinco elementos distintivos: A coleta de provas refere-se ao uso de ferramentas de busca sujeitas à lei para coletar elementos de prova que serão submetidos ao tribunal; propostas de provas, que são baseadas na indicação das partes ao juiz de que serão intervenientes no processo os meios de prova pretendidos; a admissibilidade da prova, pela qual os magistrados aprovam ou rejeitam as provas já apresentadas; quais magistrados As provas e o valor produzidos no processo de ponderação de cada caso concreto, aquelas provas que mostram mais ou menos "valor" nos argumentos das partes e com o que são confrontadas, são persuadidas a tomar a decisão final (Aroca, 2005).

Quando o assunto for prova digital, coexistirá o mesmo paradigma e, nesse sentido, todo o ordenamento jurídico será justo, mesmo que sejam provas especiais, pois estão mudando a qualquer momento. A prova digital é descrita por Silva Rodrigues como: qualquer tipo de informação, com valor probatório, armazenada em repositórios eletrônicos digitais, ou transmitida em sistemas e redes de computadores ou redes de comunicação eletrônica, acessíveis privada ou publicamente, na forma binária ou em números (Silva Rodrigues, 2014).

Vera Dias, por sua vez, propõe um conceito que consideramos mais esclarecedor, categorizando-o como “informação que pode ser extraída de dispositivos eletrônicos (locais, virtuais ou remotos) ou redes de comunicação. verdadeiro, preciso e específico” (Dias, 2012).

Os crimes virtuais são diferentes dos crimes comuns, são mais difíceis de verificar do que os crimes comuns e exigem pessoal técnico especializado para rastrear e identificar os autores. Aprendemos que, em um ambiente de intrusão de rede tão mutante, somos constantemente atacados assim que entramos no ambiente virtual, e a maior dificuldade está em encontrar a origem da intrusão e o invasor. Somente quando o instigador e o autor do crime são identificados, a existência de responsabilidade criminal pode garantir a certeza da lei. Uma sensação de impunidade para o crime cibernético é palpável nas vítimas, enquanto os países lutam para rastrear os perpetradores de crimes.

No entanto, Ricardo José de Souza Silva, eminente doutor em tecnologia, comentou que como a Internet tem múltiplas camadas, as informações podem ser

armadas por cibercriminosos, pois há uma sensação de impunidade, em parte por estarmos em um ambiente virtual Restringindo as ações contra especialistas em infrações, por outro lado, amplia o estado de “aqui nada acontece” e, com isso, os crimes aumentam exponencialmente (Silva, 2018).

Os empecilhos descobertos na investigação, bem como a falta de provas que demonstrem a persistência da conduta criminosa e quem seriam os agentes ativos causadores do dano, são desafios a serem superados, pois na maioria das vezes a prática não deixa vestígios que possam ser relatados. Tribunal. O Estado tem um papel regulador no auxílio à vida social, pois o que acontece no mundo virtual impacta diretamente no mundo real, e nas palavras de Ricardo Silva (2018), o processo regulatório nas redes virtuais visa organizar o fluxo de comportamento, atitudes e consequências das pessoas. No entanto, tais informações armazenadas, mediante autorização pessoal dos prestadores de serviços, podem afetar sua vida no mundo real, inclusive com a divulgação de informações sigilosas a instituições financeiras e agentes de consumo, o que por vezes pode levar a situações incômodas, principalmente no domínio social (Silva, 2018).

Devido à ocultação da rede virtual, os criminosos superaram o anonimato. Outro ponto de análise é a fragilidade das provas virtuais. Como as provas são facilmente perdidas e danificadas durante a investigação, é muito importante encontrar os criminosos durante a investigação. Por isso, a Direct Operations Os traficantes devem ter o mesmo conhecimento técnico ou mais avançado que os criminosos para identificar os autores do crime cibernético.

Da mesma forma, segundo Marcos Ferreira Lima, nessas investigações, o objetivo é descobrir os endereços IP (Internet Protocol) dos computadores da rede. Isso nem sempre é suficiente, pois em alguns casos um computador atende a várias pessoas e é necessário determinar quem realmente o está usando para cometer atividades criminosas. Os especialistas costumam usar técnicas "post-mortem" ao investigar os chamados crimes digitais, informáticos ou cibernéticos, ou crimes cometidos através do uso de microcomputadores. Ou seja, verifica-se o sistema após o desligamento da máquina, cabendo a especialistas a tarefa de copiar as mídias e avaliar as evidências armazenadas e/ou deletadas recentemente (Lima, 2011).

A velocidade vertiginosa com que os conteúdos aparecem e desaparecem na rede virtual possibilita a realização de investigações criminais e desempenha papel no esclarecimento de crimes. fornecendo evidências, ele aderirá a certos padrões. Na

International High-Tech Crime and Forensic Conference, Londres, outubro de 1999, o Digital Evidence Science Working Group apresentou definições, padrões e princípios para demonstrar à comunidade forense internacional a natureza da evidência digital e os caminhos investigativos a seguir, adotando, forma que possa garantir sua força probatória sem tocar em garantias básicas (FBI, 2016).

Uma das diretrizes afirma que, para sua completude, a testagem virtual deve apresentar uma linguagem simples para que possa ser aplicada de forma universal, deixando apenas os termos técnicos considerados essenciais e específicos. A fim de garantir a preservação das provas, os técnicos forenses colocam as provas coletadas no Repositório Global de Material Forense, que regista arquivos de diversos assuntos, como vídeo, áudio e imagens digitais, esses arquivos não são fixados em uma máquina de corrida, justamente para garantir proteção contra possíveis ataques de cibercriminosos (Caixeta, 2012).

Isto sugere que os crimes virtuais têm vieses próprios e que perante a deteção é necessário adaptar os modelos internacionais de forma a serem reconhecidos noutros países associados ao crime, devido ao caráter transfronteiriço do crime (Gandini, 2016). O espaço virtual é amplo, pensado para distribuir de forma otimizada cada programa utilizado, estabelecendo assim categorias que distinguem os elementos materiais e de hardware (provas eletrônicas) dos sistemas computacionais.

Essa distinção é útil na hora de desenhar o programa correto para lidar com cada tipo de prova, criando um paralelo entre as cenas de crime físicas e digitais (DEL PINO, 2012). A necessidade de atualizar as formas de investigação de crimes cometidos por meios informáticos fez com que surgissem especialistas especializados que recolhem informação de equipamentos informáticos para posterior investigação, sendo até então a melhor investigação este tipo de investigação remetida a peritos técnicos.

A prova virtual segue rígidos padrões de integridade e valor probatório, conferindo estabilidade à investigação. É fundamental que a produção dessas evidências seja uniforme em todas as etapas do processo forense digital, para que as evidências possam ser admissíveis no tribunal, evitando lacunas na força probatória que possam, no futuro, comprometer a segurança e os direitos pessoais, aspectos fundamentais do indivíduo, e suficiente para detectar e punir cibercriminosos (Oliveira, 2012).

Pela particularidade da prova digital, ela é instável e mutável, o que aumenta a

dificuldade de sua apreensão. Em muitos casos, os pesquisadores obtiveram um teste que posteriormente foi observado ter sido modificado consideravelmente em alguns aspectos, retido apenas em alguns aspectos, ou modificado em todos os aspectos, no sentido de que todos os recursos foram perdidos, Ele perde sua força probatória (Gandini, 2016).

O cibercrime é caracterizado pela periculosidade e variedade, o que dificulta as investigações, como a identificação e comprovação de fatos/crimes. É dever do legislador encontrar meios viáveis e eficientes de encontrar os autores de crimes fictícios para verificar tais autores devido ao imensurável perigo para as vítimas e às peculiaridades de tais infratores.

6 CONSIDERAÇÕES FINAIS

O avanço contínuo da tecnologia e a popularidade da Internet tornaram difícil para os legisladores definir certos atos criminosos, resolvendo assim a grande maioria dos casos de crimes virtuais. O objetivo principal do presente trabalho acadêmico foi identificar os desafios apontados pela doutrina diante dos sistemas de prova para crimes virtuais.

Apontou-se questões legais desde o momento da autoria, aquisição e manutenção do material probatório, e analisamos a legislação brasileira e como ela se comporta diante de tais crimes. Como todas as evoluções têm suas responsabilidades e benefícios paralelos, as ferramentas tecnológicas fazem parte do cotidiano da sociedade, e em busca dessa comodidade, o mundo moderno trouxe também novas práticas criminosas.

Considerando as características especiais dos crimes virtuais, como volatilidade e efemeridade, é difícil preservar e garantir a integridade das evidências durante o processo de investigação, exigindo que especialistas especializados coletem todos os materiais como base para a investigação. processo. Para o cibercrime, a coleta de provas é um elemento essencial para determinar os autores dos crimes. As diversas formas e ferramentas utilizadas nos crimes no mundo virtual tornam a perícia mais difícil. Portanto, o conhecimento profissional é essencial para extrair e preservar essas evidências.

Existem várias maneiras de evitar o uso indevido de dados necessários para fins de prova, uma das quais é fornecer provas com antecedência. Prevista como

medida excepcional no Código de Processo Penal, faz alusão direta às características dos crimes cibernéticos, pois muitas dessas provas não podem ser reproduzidas em juízo por se perderem na configuração espaço/temporal, lembrando que essas medidas devem respeitar contradições e ser devidamente defendida garantia.

Vale ressaltar que existem múltiplas formas de violação de direitos legais em um ambiente virtual, e o acesso à tecnologia facilita novos atos criminosos. O risco de sobrevivência social continua o mesmo: ao entrar no vasto mundo da Internet, enfrentando a intrusão dos usuários, eles se tornam cada vez mais diversificados e são usados para prejudicar a privacidade e trazer benefícios indevidos aos usuários.

Assim, considerando a importância da prova no processo, são exemplificados os meios de prova, o objeto da prova, a classificação e o sistema de valoração dessas provas no ordenamento jurídico brasileiro. São analisadas as relações específicas do sistema probatório no âmbito virtual, as questões relativas à autoria e aos meios periciais empregados nesses crimes. A investigação é a base do processo, e face à dificuldade de obtenção de provas no mundo online, procuramos soluções face à identificação transfronteiriça, dificuldade de recolha de prova pericial e adequação legal. crime.

Ainda como solução, apontamos que a perícia forense é um meio necessário deste tipo de crime, a coleta de materiais biométricos e fisiológicos pode identificar o suspeito devido a característica de tais provas perecerem no decorrer do espaço/tempo. Cibercriminosos, também aplaudimos a expertise dedicada a esse tipo de investigação, pois a realização da coleta de dados requer o uso de tecnologia, pois isso garantirá a avaliação e verificação das evidências em tribunal.

Os alvos dos cibercriminosos são diversos, novos crimes são criados a cada dia, e um banco de dados pode ser criado como base nacional de cibersegurança, com referência a parâmetros internacionais. Um sistema integrado composto por instituições interconectadas, como sociedade, empresas de valores mobiliários, instituições bancárias e centros de pesquisa.

Dado que os crimes virtuais atravessam as fronteiras nacionais, os bancos de dados nacionais serão vinculados aos bancos de dados globais, garantindo uma identificação mais eficiente do autor. Ressaltamos também que um projeto de lei semelhante à nossa solução está em tramitação no Parlamento, alterando partes da legislação para torná-la mais atual e eficaz.

Concluiu-se que a velocidade da tecnologia e os mais diversos mecanismos de

comunicação fazem com que meios de criminalidade e anonimato sejam criados e modificados diariamente. Diante das questões probatórias levantadas em nossa pesquisa, buscamos encontrar uma alternativa para que o Estado veja de forma adequada neste ambiente veloz e mutável, garantindo a proteção da privacidade individual, ao invés de desconstruir os direitos e garantias que foram obtidos.

REFERÊNCIAS

ALVES, Maria Hiomara dos Santos. **A evolução dos crimes cibernéticos e o acompanhamento das leis específicas no Brasil**. Jus.com.br. [S.l], Mar. 2018.

ARAÚJO, Viviane Souza. **A validade jurídica dos documentos eletrônicos como meio de prova no processo civil.** [S.l], 05 nov. 2007.

AROCA, Juan Montero. **La prueba e nel proceso civil**. 4. ed. Madrid: Thomson Civitas, 2005, p. 284.

BRASIL, **Lei nº 11.343, de 23 de agosto de 2006**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em: 22de mai. 2023.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Brasília, 1940.

BRASIL. **Decreto-Lei no 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Brasília, 1941.

BRASIL. **Lei 12.735, de 30 de novembro de 2012**. Dispõe sobre a tipificação de condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, Brasília, DF. 22 mai. 2023.

BRASIL. **Lei 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências., Brasília, DF. 22 mai. 2023.

CAIXETA, T. F. G, **Revista Segurança Digital** – 9° Edição, 2012. Disponível em: https://periciacomputacional.com/pericia-digital/. Acesso em: 22 maio. 2023.

CINTRA, Antônio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. **Teoria Geral do Processo.** São Paulo: Malheiros Editores, 2010.

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

DEL PINO, Dr. Santiago Acurio. **Manual de Manejo de Evidencias Digitalesy Entornos Informáticos.** Uruguai. 2016.

DIAS, Vera Marques. A Problemática da Investigação do Cibercrime. **Data Venia, Revista Jurídica Digital**, Ano 1, n. º 1, julho-Dezembro 2012, ISSN 2182-8242.

FBI. **U.S. Department of Justice. 2016.** Disponível em: https://www.fbi.gov/about-us/lab/forensic-sciencecommunications/fsc/april2000/swgde.htm/. Acesso em: 05 abr. 2023.

FERREIRA, Ivette Senise. **A Criminalidade Informática.** Direito e Internet - Aspectos Jurídicos Relevantes. Editora Edipro, 2011.

FERREIRA, Ivette Senise. **Direito & Internet: Aspectos Jurídicos Relevantes**. 2. ed. São Paulo: Quartier Latin, 2005, p. 261.

GANDINI. João Agnaldo Donizeti, SALOMÃO, Diana Paola da Silva e; JACOB Cristiane. **A Validade jurídica dos documentos digitais.** July, 2016.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet.** Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016.

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional.** São Paulo: Editora Atlas, 2011, p. 6.

LOPES JUNIOR, Aury. **Direito Processual Penal.** 10. ed. São Paulo: Saraiva. 2013.

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

MORAIS, José Luiz Bolzan de; MENEZES NETO, Elias Jacob de. **Marco Civil da Internet: A insuficiência do marco civil da internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance.** Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

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

OLIVEIRA, Eugênio Pacelli. **Curso de Processo Penal**. Rio de Janeiro. Úmen. Juris, 2012, p.328.

PACHECO, Gisele Freitas-COSTA; LOPES, Renato. **Crimes Virtuais e a Legislação Penal Brasileira. 2016**

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

PRODANOV, Cleber Cristiano. **Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico - 2ª Edição.** Editora Feevale, 20 de jun. de 2013.

RANGEL, Paulo. **Direito Processual Penal.** 20. ed. São Paulo: Atlas, 2012.

RODRIGUES, Benjamim Silva. **Direito Penal Parte Especial**. Tomo I, Direito Penal Informático Digital, Contributo para a Fundamentação da sua Autonomia Dogmática e Científica à Luz do novo Paradigma de Investigação Criminal: a Ciência Forense Digital e a Prova Digital. Coimbra Editora, Limitada. ISBN: 978-989-95779-5-4.

SILVA, Ricardo José de Souza. Delito Virtual: Um diálogo sobre as transgressões online do mundo real. **Delictæ: Revista de Estudos Interdisciplinares sobre o Delito.** Volume 2. Número 4. jan.- jun./2018 Belo Horizonte: Centro de Investigações Interdisciplinares sobre o Delito, 2018. Semestral ISSN: 2526-5180 (eletrônico). Direito – II. Periódicos – III. Brasil.

STRAZZI, Alessandra. **Crimes contra a honra - diferenças entre calúnia, difamação e injúria**, disponível em: https://alestrazzi.jusbrasil.com.br/artigos/130177918/crimes-contra-a-honradiferencas-entre-calunia-difamacao-e-injuria. Acesso em: 30 de abr. 2023

VIANA, Marco Túlio apud CARNEIRO, Adeneele Garcia**. Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais.** Rio de Janeiro: Forense, 2000, p. 65

VIANA, Marco Túlio. **Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais.** Rio de Janeiro: Forense, 2003, p. 13-26