INSTITUTO VALE DO CRICARÉ
FACULDADE VALE DO CRICARÉ
CURSO DE DIREITO

IGOR AZERÊDO SOARES

CELERIDADE E EFICÁCIA DA INVESTIGAÇÃO POLICIAL EM CRIMES DIGITAIS CONTRA A HONRA

SÃO MATEUS
2020

IGOR AZERÊDO SOARES

CELERIDADE E EFICÁCIA DA INVESTIGAÇÃO POLICIAL EM CRIMES DIGITAIS CONTRA A HONRA

Trabalho de Conclusão de Curso apresentado ao Curso de Direito, da Faculdade Vale do Cricaré, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador Prof. Me Samuel Davi Garcia Mendonça

SÃO MATEUS

2020

IGOR AZERÊDO SOARES

CELERIDADE E EFICÁCIA DA INVESTIGAÇÃO POLICIAL EM CRIMES DIGITAIS CONTRA A HONRA

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade Vale do Cricaré, como requisito parcial para obtenção do grau de Bacharel em Direito.

Aprovado em _____ de _____ de 2020.

BANCA EXAMINADORA

_____

PROF. Me SAMUEL DAVI GARCIA MENDONÇA
FACULDADE VALE DO CRICARÉ
ORIENTADOR

_____

PROF.
FACULDADE VALE DO CRICARÉ

_____

PROF.
FACULDADE VALE DO CRICARÉ

SÃO MATEUS
2020

Dedico este trabalho à minha família, que sempre acreditou no meu potencial e me incentivou a ir cada vez mais além.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ter me sustentado e abençoado, principalmente com saúde, familiares e amigos, durante todo este período.

Aos meus pais, Célio e Cida, por todo apoio dado enquanto fui graduando neste curso, seja de forma financeira, psicológica, emocional, moral ou quaisquer outras.

Agradeço também à minha irmã Larissa pela companhia e parceria enquanto também cursava na mesma Instituição, por todos os conselhos passados através das experiências já vividas no curso.

Ao meu sobrinho Lorenzo, também, por cada sorriso, beijo, abraço e susto que me dava quando chegava da faculdade, que ansioso aguardava nossa chegada.

Agradeço também à minha noiva Caryne por toda companhia, incentivo, paciência e apoio a todo instante, me ajudando sempre a persistir além das dificuldades.

E aos meus amigos e colegas que me acompanharam durante estes anos, dia após dia, especialmente, Acsa, Cristiano, Jeremias, Mateus, Râmella e Raul.

A injustiça em qualquer lugar é uma ameaça à justiça por toda parte.

Martin Luther King Jr.

RESUMO

O presente estudo tem por objetivo constatar a eficácia e a celeridade no âmbito da investigação criminal realizada para esclarecer e solucionar os crimes praticados contra a honra. Com o surgimento da internet e a criação cada vez mais frequente de aparelhos tecnológicos que tornam a comunicação totalmente simultânea, delitos que já eram cometidos no "mundo real" passaram a ser praticados também em meio virtual. Por conseguinte, aproveitando-se da inocência de muitos usuários da rede virtual, os criminosos investem diariamente em novas formas de obter êxito em suas fraudes, atingindo diretamente a vítima e aos seus bens jurídicos, como ao patrimônio, à liberdade individual e, segundo este estudo, ao direito à honra. Entretanto, a apuração e resolução dos crimes praticados contra a honra em meio virtual carecem no que tange ao tempo demandado e eficácia pretendida, visto que, durante as investigações pelas autoridades policiais, são encontradas diversas dificuldades para produção de provas, tornando necessárias novas medidas tanto procedimentais, quanto legais para que se alcance o resultado esperado. Deste modo, foi realizada uma revisão bibliográfica, com fundamentação em livros de doutrinadores do Direito, artigos publicados, legislação brasileira civil, penal e constitucional. Os resultados obtidos neste estudo demonstram que a investigação policial para apuração dos crimes virtuais contra a honra não obtém a eficácia pretendida, nem tampouco tramita de forma célere. Porém, ainda são necessárias mais pesquisas acerca deste tema, especificamente no que tange à ofensa contra a honra em meio cibernético, visto que ao longo da realização deste estudo notou-se poucas fontes.

Palavras-chave: crimes virtuais; investigação; internet; honra.

ABSTRACT

The purpose of this study is to verify the effectiveness and speed in the criminal investigation carried out to clarify and solve crimes against honor. With the emergence of the Internet and the increasingly frequent creation of technological devices that make communication totally simultaneous, crimes that were already committed in the "real world" began to be practiced also in a virtual environment. Therefore, taking advantage of the innocence of many users of the virtual network, criminals invest daily in new ways to obtain success in their frauds, directly affecting the victim and his legal assets, such as property, individual freedom and, according to this study, the right to honor. However, the investigation and resolution of crimes committed against honor in a virtual environment lacks in terms of time demanded and intended effectiveness, since, during investigations by police authorities, several difficulties are encountered in producing evidence, making it necessary to take new measures both procedural and legal to achieve the expected result. Thus, a bibliographic review was carried out, based on the books of legal scholars, published articles, Brazilian civil, criminal and constitutional legislation. The results obtained in this study demonstrate that the police investigation for the investigation of virtual crimes against honor does not obtain the intended effectiveness, nor does it proceed quickly. However, there is still a need for more research on this topic, specifically regarding the offense against honor in cyber environments, since during the course of this study few sources were noted.

Keywords: virtual crimes; investigation; internet; honor.

SUMÁRIO

1 INTRODUÇÃO 9
1 A INTERNET 11
1.1 HISTÓRIA DA INTERNET 11
1.2 A INTERNET NO BRASIL 14
2 DOS CRIMES DIGITAIS 16
2.1 SURGIMENTO E DEFINIÇÃO DOS CRIMES DIGITAIS 16
2.2 CLASSIFICAÇÕES 18
2.3 INCIDÊNCIAS DOS CRIMES VIRTUAIS 22
2.3.1 Os crimes digitais mais comuns 22
2.3.2 A Lei Carolina Dieckmann 25
2.3.2.1 Dos fatos 25
2.3.2.2 Prós e Contras da Lei 12.737/12 27
2.3.3 Lei Azeredo - 12.735/12 30
3 CRIMES CONTRA A HONRA 33
3.1 DEFINIÇÃO DOS CRIMES CONTRA A HONRA 33
3.2 CALÚNIA 35
3.3 DIFAMAÇÃO 37
3.4 INJÚRIA 38
3.5 DISPOSIÇÕES GERAIS 40
4 A INVESTIGAÇÃO POLICIAL EM CRIMES DIGITAIS CONTRA A HONRA 43
4.1 O INQUÉRITO POLICIAL 43
4.2 TITULARIDADE DA AÇÃO PENAL 46
4.3 PROCEDIMENTOS DO INQUÉRITO POLICIAL 48
4.4 INVESTIGAÇÃO DOS CRIMES CONTRA A HONRA EM MEIO CIBERNÉTICO 51
4.5 MEIOS DE PROVA DOS CRIMES VIRTUAIS 53
4.6 MEDIDAS A SEREM TOMADAS EM CASO DE CRIME VIRTUAL 58
CONSIDERAÇÕES FINAIS 60
REFERÊNCIAS BIBLIOGRÁFICAS 62

1 INTRODUÇÃO

Com o surgimento e avanço da tecnologia e da internet, a sociedade em diversos locais do mundo passou a se adequar e aprimorar seus conhecimentos. Entretanto, concomitantemente a estes progressos, o mundo passou a sofrer com outro problema: os crimes virtuais. Indivíduos dotados de vasto conhecimento e inteligência no que tange à rede de internet começaram a se aproveitar dos "internautas" com o intuito de praticar diversos crimes e obter vantagens ilicitamente.

Diante destes acontecimentos, evidenciou-se a carência de proteção e a necessidade de previsão na Legislação Penal, tanto a brasileira, quanto as de outros países, para se considerar as práticas como crimes e punir os criminosos, evitando a ideia comum de que a internet é "terra sem lei".

Para tanto, após vários anos de suposta impunidade aos transgressores, o Estado Brasileiro tomou iniciativa, trazendo ao Regimento Penal Pátrio previsões legais através de leis como a chamada “Lei Carolina Dieckmann” (Lei 12.737/2012) e a denominada “Lei Azerêdo” (Lei 12.735/2012), em que adotaram-se medidas para tratar dos crimes de informática.

Porém, ainda que criadas as leis, faz-se necessário compreender que a apuração dos crimes praticados no ambiente informático é um tanto quanto burocrática e detalhista, necessitando de grande empenho por parte das autoridades e, por vezes, demandando de bastante tempo para sua conclusão.

Deste modo, questiona-se se a investigação policial para apurar os crimes praticados no meio virtual contra a honra de milhares de vítimas ocorre de forma célere e eficaz. Assim, o presente trabalho tem por escopo geral realizar a constatação no que está relacionado à celeridade e à eficácia da investigação policial em crimes digitais contra a honra.

Para alcançar tal entendimento, ao longo deste trabalho, serão tomados por objetivos específicos: apresentar e definir o surgimento da internet e dos crimes virtuais praticados por meio dela, além de suas incidências; conceituar os crimes contra a honra com as devidas previsões legais e, por fim, demonstrar as etapas investigativas que visam apurar os também chamados crimes cibernéticos, bem como os meios de prova cabíveis.

Parte-se da hipótese de que a investigação policial em crimes digitais contra a honra não alcança um objetivo eficaz por ausência de empenho para resolução, de

mais especificidade nas leis criadas, de instrumentos que viabilizem e, quando sim, demanda longo tempo.

Para fundamentar e obter os objetivos almejados, analisam-se os entendimentos firmados pela doutrina especialista em âmbito penal, civil e constitucional, bem como as previsões trazidas pela Legislação Brasileira, suas jurisprudências e artigos que tratam acerca do assunto discutido.

Sendo assim, no primeiro capítulo este trabalho abrangerá acerca da história da internet em geral, do surgimento dos primeiros dispositivos informáticos e suas características técnicas, além da chegada da internet ao Brasil e suas primárias finalidades.

Já o segundo capítulo se encarregará de apresentar a história dos crimes digitais, as nomenclaturas comumente utilizadas e seu conceito. Além do mais, neste conteúdo serão apresentadas as classificações doutrinárias dos crimes virtuais, tal como relatar alguns das condutas criminosas mais praticadas em meio informático.

Seguindo a fundamentação do trabalho em questão, no terceiro capítulo será dissertado sobre os crimes praticados contra a honra, identificando suas definições, as tipificações punitivas elencadas no Código Penal Brasileiro e suas devidas caracterizações e diferenciações.

Enfim, o terminativo capítulo terá por finalidade destacar e pormenorizar as etapas e procedimentos das autoridades policiais em investigação que almeje esclarecer e resolver os delitos praticados contra a honra.

Ao fim do trabalho, depreende-se que os objetivos são alcançados e o questionamento levantado obtém a resposta sugerida pela hipótese, de modo que se fazem extremamente importantes mudanças urgentes na legislação e na execução dos procedimentos de sanção para se ter uma eficácia e agilidade reais.

1 A INTERNET

1.1 HISTÓRIA DA INTERNET

A interligação de milhões de dispositivos informáticos, universitários, científicos, pessoais, militares ou comerciais, conectados entre si, formam a grande rede de comunicação universal denominada internet. Esta se comporta como um agrupamento de redes, concatenadas via linhas telefônicas, ligações por fibra ótica ou micro-ondas, satélites, entre outros (CASTRO, 2003).

Assim, a internet, desde seus primórdios, já abrangia uma série de áreas de atuação, auxiliando desde o âmbito pessoal até o profissional, seja para fins comerciais ou ainda para estudos e produções científicas, aperfeiçoando cada vez mais a rede de comunicação entre as pessoas.

O escritor Fontes (2006) analisa também neste prisma que a internet possibilita o acesso à informação de forma inovadora. Salienta ainda que, ainda que tenha adentrado no meio comercial apenas durante a década de 90, há grande diversidade de informações disponibilizadas em meio digital, como assuntos profissionais, educativos, para divertimento, pesquisas, entre outros. Compara também a rede digital de internet às revistas e jornais, onde é possível consultar uma série de informações, mas com aquela de forma bem mais veloz.

A internet, como se conhece hoje, repentina e simultânea, passou por diversas modificações ao longo dos anos. Desde o seu surgimento, em 1969, diversos fatores levaram à popularização da rede de internet, tornando a sociedade cada vez mais moderna e a incentivando a buscar conhecimentos e aprimorar seu uso.

O ano de 1946 foi marcado pela criação do primeiro computador eletrônico, que foi denominado pelo exército americano de Eletronic Numerical Integrator and Computer (ENIAC). A máquina possuía um peso aproximado de 30 toneladas e despendia um espaço de 140 metros quadrados. (ROCHA, et al., 2015).

O desenvolvimento do primeiro computador marcou e revolucionou a tecnologia e a história da sociedade internacional, levando praticidade em diversas funções do dia a dia, bem como ações bancárias, comunicativas, comerciais e laborais, entre outras. Em aspectos físicos, as máquinas atuais estão em constantes mudanças, cada vez menores, mais finos e/ou leves.

Segundo Paesani (2014), houve em 1969 um projeto por parte do Governo norte-americano, através do Departamento de Defesa ARPA (Advanced Research Projects Agency) – Agência de Projetos Avançados, chamado Arpanet, em que a Rand Corporation se encarregou de desenvolver um sistema de telecomunicações a fim de assegurar que, em caso de ataque nuclear russo (ou soviético, à época), perante a Guerra Fria, a comunicação crucial dos Estados Unidos não fosse corrompida.

Para tanto, planejaram e constituíram pequenas redes locais, denominadas LAN, situadas estrategicamente pelo País, e interligadas através das chamadas WAN, que são redes de comunicação geográfica. Assim havendo, em caso de bombardeio e destruição de algum local por ataque nuclear, a *inter networking* permaneceria ligando as redes locais conectadas e asseguraria a comunicação entre as áreas não atingidas, permitindo que se protegessem (PAESANI, 2014).

Deste modo, com o intuito de, a princípio, se protegerem e manterem ligadas suas bases de comando, os Estados Unidos deram início às redes de transmissão e comunicação e deram um passo à frente, tanto em novidade tecnológica em tempos de guerra, quanto em questões comerciais e econômicas para o país.

Em meados da década de 70, tendo como intuito de encadear os diversos locais de pesquisas das forças militares americanas, nasceu nos Estados Unidos a famosa internet, através do Departamento de Defesa Norte-Americano. Este surgimento se deu em virtude dos inúmeros aprofundamentos acerca da informática e criação de computadores (TEIXEIRA, 2007).

Porém a finalidade da criação da internet encontra divergências entre alguns autores. Muitos autores entendem que ela foi criada com fins militares, para o desempenho norte-americano na guerra e em geral. Já outros, compreendem que a internet possa ter sido criada, por exemplo, visando o aprimoramento de pesquisas científicas. Acerca disso, corrobora Finkelstein (2008) apud Neto (2009, p. 19):

> Sem dúvida há boatos de que a ARPANET foi desenvolvida para fins militares, mas a tese dominante é a de que a Internet surgiu com o objetivo de pesquisa de um projeto da agência norte-americana ARPA. A conexão teve início ao interligarem-se os computadores de quatro universidades, passando, a partir disso, a ser conhecida como ARPANET. Em 1970, esse projeto foi intensamente estudado por pesquisadores, o que resultou na concepção de um conjunto de protocolos que é a base da Internet. Depois, o ARPA integrou redes de computadores de vários centros de pesquisa. Em 1986, a NSFNET, entidade americana NSF, interligou-se à ARPANET, o que deu finalmente origem às bases da atual Internet.

Já no ano de 1973, houve o registro do denominado Protocolo de Controle de Transmissão/Protocolo internet (protocolo TCP/IP) pelo responsável pelo projeto do Departamento de Pesquisa avançada da Universidade da Califórnia, Vinton Cerf, sendo este Protocolo uma codificação que permitia aos diversos networks incompatíveis por programas e sistemas contatarem-se entre si (NETO e GUIMARÃES, 2003).

Este mecanismo chamado TCP/IP proporcionou que dois computadores, quando unidos à rede, dialogassem entre si, num mesmo idioma, além de possibilitar com que as várias redes componentes da Arpanet se interligassem, formando uma imensa rede internacional de computadores, sendo assim chamada pela primeira vez de Internet.

Desta maneira surgiu a Internet, sendo hoje considerada como uma forma de comunicação que conecta milhões de computadores e redes por todo o mundo e possibilita o acesso a uma quantidade de informações quase inexaurível, fazendo com que toda desproporção de tempo e lugar sejam praticamente zeradas.

Porém, apesar de tantos avanços, a Internet só começou a se aproximar mais do jeito que é conhecida nos dias atuais no ano de 1989, quando foi criada a World Wide Web (WWW), que viabilizou a popularização de seu uso, facilitando ainda mais o acesso às informações disponíveis em rede.

O surgimento da World Wide Web, ou apenas Web, foi crucial para tornar a internet um grande canal de comunicação em massa. Foi desenvolvida no ano de 1989, em Genebra, Suíça, sendo composta por hipertextos, o que aprimora e favorece a navegação (NETO, 2009).

A World Wide Web, também chamada de W3 ou WWW — que pode significar "Rede de Alcance Mundial" ou "Rede Mundial de Computadores" é um artifício acessível através da internet baseado num sistema difundido de acesso a dados e informações, que são apresentadas na configuração de hipertexto. Neste tipo de configuração, as informações são apresentadas na página, ligando-se entre os documentos e outros objetos, como menus ou índices, situados em vários locais da rede (CASTRO, 2003).

No intuito de favorecer a utilização dos eletrônicos interligados à rede de internet, com inúmeras pessoas simultaneamente em mesmos sites, foi criada a World Wide Web, ou rede mundial de computadores, através da Organização Europeia Para

a Investigação Nuclear. Logo a Netscape, também norte-americana, visando a troca criptografada de mensagens, possibilitando maior segurança aos "internautas", lançou o "HTTPS", que significa Hyper Text Transfer Protocol Secure e, em português, protocolo de transferência de hipertexto seguro (WERNER, 2001 apud LIMA e DUARTE, 2020).

Com o passar do tempo e através do desenvolvimento tecnológico, o computador passou a ser utilizado pelos indivíduos e empresas como mecanismo para produzir, arquivar, remeter, transmitir arquivos e obter diversas informações e conteúdos. No intuito de favorecer o uso dessas diversas utilidades ofertadas pelo sistema informático, foram criados inúmeros programas de computador.

1.2 A INTERNET NO BRASIL

Após o surgimento, aprovação e popularização da Internet em terras estrangeiras, a tão tecnológica ideia chegou ao Brasil e começou a se desenvolver com o intuito de estabelecer conexões entre as universidades brasileiras e as estrangeiras.

O primeiro computador brasileiro foi criado ainda no ano de 1972, e foi chamado de “patinho feio”, desenvolvido pela Universidade Federal de São Paulo (USP). Já em 1979, houve a criação da Secretaria Especial de Informática e, 9 anos depois, em 1988, iniciaram-se os contatos para implantação da nova tecnologia no Brasil (WENDT e JORGE, 2013; NETO, 2009).

Tal contato se deu entre Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), o Laboratório Nacional de Computação Científica (LNCC), a Universidade Federal do Rio de Janeiro (UFRJ) e as instituições científicas americanas que já possuíam a tecnologia da Internet, começando assim a troca de informações e dados para implantação da novidade no Brasil. Segundo informações, o motivo do contato com os americanos era que estudantes brasileiros que retornaram dos Estados Unidos sentiram falta do intercâmbio mantido quando estudavam lá (WENDT e JORGE, 2013; NETO, 2009).

Em meados de 1992, a Secretaria Especial de Informática foi fechada, sendo criada para suas funções a Secretaria de Política de Informática. Houve ainda, no mesmo ano, a implementação da primeira rede ligada à internet, conectando as principais universidades brasileiras. Porém, ainda não era como nos dias atuais, não

haviam interfaces e somente podia ser utilizada para envio e recebimento de correios eletrônicos, os e-mails (WENDT e JORGE, 2013).

A internet passou a ser usada no Brasil por volta dos anos 90, apenas por Instituições de pesquisas e, logo após, por Universidades, perdurando deste modo até o fim de 1995, época em que a utilização comercial se estabeleceu através da implantação de um BackBone (ou "rede de transporte") lançado pela Empresa Brasileira de Telecomunicações (EMBRATEL), com um certo fomento para a sua disseminação na mídia, que investiu em tratar do assunto, fazendo uso também de novelas (BRANT, 2003).

Então, em 1995, o uso de comercial da internet foi autorizado e disponibilizado no país, atingindo a conexão uma velocidade de 9,6 Kbps. No mesmo ano, a fim de organizar e compor todas as iniciativas de prestação de serviços de internet do Brasil, propiciando melhor qualidade técnica, inovação e propagação dos serviços fornecidos, surgiu o Comitê Gestor de Internet no Brasil (CGI.br) (WENDT e JORGE, 2013).

Conforme observou Brant (2003), o Brasil, no ano de 2001, dispunha em torno de 6 milhões de usuários de internet, ao passo que, em todo mundo, havia aproximadamente 349 milhões de usuários. No mês de janeiro de 2003, já havia no país 22,4 milhões de usuários. Em contrapartida, nos Estados Unidos o número de pessoas utilizando a internet já atingia 120,5 milhões.

Desta maneira, o surgimento da internet nesta época trouxe para o Brasil uma série de melhorias, aperfeiçoando diversas áreas do país, como pessoais, técnicas, profissionais, científicas, dentre outras. No entanto, apesar dos inúmeros benefícios trazidos, a chegada desta tecnologia promoveu também a aparição e propagação da prática de crimes por estas novas vias.

2 DOS CRIMES DIGITAIS

2.1 SURGIMENTO E DEFINIÇÃO DOS CRIMES DIGITAIS

São denominados crimes cibernéticos, ou ainda crimes digitais, os atos tipificados legalmente e praticados através de dispositivos informáticos em geral, bem como computadores, celulares, tablets, dentre outros aparelhos. (WENDT e JORGE, 2013).

Em uma sociedade atual tão modernizada e empenhada na utilização de produtos tecnológicos e informáticos, tem sido cada vez mais comum a prática dos crimes cibernéticos. Para analisar a frequência destes atos, há de se perceber que nem todos que se utilizam das atividades disponíveis na rede de internet têm a consciência do perigo que correm a todo instante ou, se sabem, não se previnem corretamente.

Segundo informação publicada pelo Portal G1 (2020), a Polícia Civil do estado do Amazonas relatou a ocorrência de 1.675 crimes virtuais, apenas na primeira metade do ano corrente. As autoridades verificaram uma alta das práticas delituosas nos meses de maio e junho, e associaram o aumento deste tipo criminoso ao período de isolamento social causado pela pandemia do novo Coronavírus (COVID-19).

Já em outro estudo realizado pela SaferNet Brasil junto ao Ministério Público, e publicado pelo site Estado de Minas (2019), foram registrados no ano passado, todos os dias cerca de 366 casos de crimes virtuais no Brasil. Essa mesma pesquisa apontou também que em 2018 foram registrou-se 133.732 casos de crimes virtuais.

A chamada "era digital" adveio junto ao constante desenvolvimento tecnológico, crescente a cada instante, pelo mundo inteiro. A todo momento surgem novas tecnologias, novas redes sociais, novos aplicativos e abundantes formas de se utilizar a internet e seus componentes.

Porém, junto a esta nova era, novos problemas também surgiram por potenciais criminosos que visavam se aproveitar de novos meios para praticar crimes. Os "vírus" de computador, por exemplo, almejam acessar dados e informações pessoais, como senhas, dados bancários, etc.

É incerto saber qual foi a informação primordial acerca de um vírus criado virtualmente de forma que tenha dado partida para que, futuramente, iniciassem o cometimento de atos criminosos se utilizando desses vírus, que se desenvolveram cada vez mais ao longo dos anos. Há quem entenda que alguns programadores produziram, em meados de 1984, um jogo denominado Core Wars, jogo este que era preparado para sobrecarregar a memória do computador de outro jogador, se utilizando de reprodução, toda vez que era aberto. Sabe-se ainda que os mesmos criadores desse jogo desenvolveram o que atualmente entendemos de antivírus, que era utilizado para anular e excluir as reproduções realizadas com o Core Wars (WENDT e JORGE, 2013).

Já outros estudiosos entendem que Richard Skrenta foi o primeiro a produzir um vírus de computador, em 1982, ainda quando tinha quinze anos de idade, tendo o programa malicioso sido chamado Elk Cloner. Este vírus adentrava à máquina e apresentava um "poema" ao usuário, produzindo cópias de si mesmo no momento que fosse inserido um disquete na máquina. E ao se inserir este disquete em outra máquina, o processo se repetia novamente (WENDT e JORGE, 2013).

Também no ano de 1986, dois irmãos nativos do Paquistão, produziram um vírus de informática que foi chamado Brain. Este adentrava e invadia a área de inicialização do disco rígido da máquina, com o intuito de averiguar uma utilização não permitida de programa médico de monitoramento cardíaco que desenvolveram. Todavia, sofreu alterações maliciosas que o levaram a causar danos bem como um vírus a disquetes, espalhando-se rapidamente, e provocando lentidão na utilização do sistema, ocupando bastante memória das máquinas infectadas (QUINTO, 2011, apud LIMA e DUARTE, 2020).

Segundo Neto e Guimarães (2003), os criminosos consideraram o computador e a internet como potenciais meios de praticar os delitos pretendidos. Consideram que, além disso, o avanço tecnológico deu ensejo à criatividade dos transgressores penais, possibilitando um novo leque de práticas e condutas ainda não observados pela sociedade, ainda que reprováveis.

Os crimes virtuais, conforme Carneiro (2012), advieram por volta do século XX:

> A literatura científica internacional demonstra que o universo dos crimes informáticos teve seus primeiros indícios no século XX, mais precisamente em 1960 onde se deu as primeiras referências sobre essa modalidade de crimes nas mais diversas denominações, com maiores incidências em casos de manipulação e sabotagem de sistemas de computadores.

Neste mesmo sentido, também afirma Albuquerque (2006) que as primeiras ocorrências de delitos informáticos remontam à década de sessenta. Os computadores eram usados como meio de prática dos crimes virtuais, como, por exemplo, o estelionato. Nesta época, a imprensa começou a relatar os primeiros casos de crimes informáticos. Já a partir da década seguinte, iniciaram-se os primeiros estudos mais aprofundados acerca da criminalidade virtual.

Greco (2017) contribui que os crimes em questão, também chamados de crimes de computador, crimes via internet, entre outros, são não somente os que possuem por objeto um componente informático, como programas de computador ou arquivos e informações nele contidos, por exemplo, mas também - de forma mais comum - a prática de outros delitos elencados na Legislação, utilizando a informática como meio para o ato.

Portanto, a prática delituosa nestes casos pode ocorrer através de diversos meios e formas, não se limitando a atitudes diretamente interligadas à internet, componentes eletrônicos, sistemas e outros, mas também abrangendo a prática de crimes já conhecidos perante a sociedade, porém, através de meios digitais.

2.2 CLASSIFICAÇÕES

Conforme demonstrado anteriormente, as infrações cometidas no meio digital recebem uma série de nomenclaturas diversas, podendo ainda ser chamados de crimes eletrônicos, crimes da informática, crimes cometidos na internet, cybercrimes, fraudes eletrônicas ou delitos computacionais.

Por conseguinte, torna-se indispensável realizar uma classificação das várias espécies de crimes cometidos em âmbito informático. Acerca deste tema, há diversas classificações por parte da doutrina jurídica, visto que muito se discutem os entendimentos firmados pelos autores.

Os crimes digitais podem ser classificados em "crimes cibernéticos abertos" e "crimes exclusivamente cibernéticos", segundo Wendt e Jorge (2013). Já por outros autores, os crimes digitais são classificados, quanto ao tipo, como próprios ou impróprios, puros, impuros ou mistos, e, quanto ao sujeito da ação, classificam-se como sujeito ativo ou passivo da ação.

2.2.1 Crimes digitais abertos ou exclusivamente cibernéticos

Os crimes cibernéticos abertos são aqueles que podem ser cometidos através da utilização de computadores, sendo este um meio para a prática criminosa, ou ainda sem se utilizar de dispositivos informáticos, praticando o delito de forma "tradicional" (WENDT e JORGE, 2013).

Os crimes contra o patrimônio (furto, extorsão, etc.), contra a honra (calúnia, injúria, difamação), contra a propriedade intelectual (violação de direito autoral), entre outras práticas, são alguns dos exemplos de delitos que podem ser praticados tanto em meio digital, tornando-se um crime cibernético “aberto”, quanto fora das redes, cometidos através do meio “comum”.

Por outro lado, os "exclusivamente cibernéticos" são os crimes que somente podem ser cometidos mediante o emprego de computadores ou quaisquer recursos e meios tecnológicos que possibilitem a obtenção da vantagem indevida e ilícita. Exemplo desta prática é o crime de aliciamento, assédio, instigação ou constrangimento de criança praticado por qualquer meio de comunicação a fim de práticas libidinosas, conforme previsto no Artigo 241-D do Estatuto da Criança e do Adolescente (Lei 8069/90) (WENDT e JORGE, 2013).

2.2.2 Crimes digitais próprios ou impróprios

Para DAMÁSIO DE JESUS, os delitos virtuais próprios ou puros podem ser cometidos por computador ou dispositivos de informática e têm sua perpetração também no meio digital. Nesta categoria, o bem jurídico protegido é a própria informática, como dados, acessórios auxiliares, segurança de sistemas, titularidade de informações (apud ARAS, 2001).

O sujeito ativo utiliza-se do sistema informático do sujeito passivo, sendo este sistema usado como meio para a efetivação do crime pretendido. Assim, há tanto a invasão de dados não autorizados, quanto a intromissão em dados armazenados, a fim de alterar, modificar, imputar dados falsos para atingir o sistema do computador, sendo somente praticados através do uso do computador ou diretamente contra ele e componentes. (Almeida et al., 2015, p. 224)

Nesta perspectiva, Costa (1997) considera o chamado crime digital puro aquela prática ilícita que vise tão somente o sistema do dispositivo computacional, tanto pelo dano físico à máquina, quanto aos componentes técnicos e tecnologias do equipamento, bem como sistemas e informações.

Quanto aos crimes virtuais impróprios ou impuros, já são tipificados na Legislação Penal vigente, e são praticados utilizando-se de dispositivo informático como computador e da rede, servindo assim como meio para a prática do crime, o delito se consuma através da máquina. Portanto, os bens jurídicos tutelados neste caso são os já elencados no Direito Penal, como a honra, o patrimônio, etc. (ALMEIDA, 2015).

Assim colabora DAMÁSIO:

> [...] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens não-computacionais ou diversos da informática (apud ARAS, 2001).

Neste sentido, NETO e GUIMARÃES (2003, p. 69) analisam que:

> [...] a informática permite não só o cometimento de novos delitos, como potencializa alguns outros tradicionais (estelionato, por exemplo). Há, assim, crimes cometidos com o computador (*The computer as a tool of a crime*) e os cometidos contra o computador, isto é, contra as informações e programas nele contidos (*The computer as the object of a crime*).

Compreende-se, portanto, em relação aos crimes digitais impróprios ou impuros, que a prática delituosa torna a utilização dos dispositivos informáticos, internet e afins, apenas instrumentos no modo de execução para que se consume o crime. Neste caso, o objeto jurídico vislumbrado pelo criminoso já se encontra tutelado na legislação penal atual.

2.2.3 Sujeito ativo ou passivo

A responsabilização ao autor pela prática de crimes cibernéticos, bem como sua comprovação se fazem tão difíceis visto que não há a determinada presença física do sujeito ativo. Por este motivo, a fim de identificar e responsabilizar o cibercriminoso,

tornou-se necessário denominar grupos que atuam neste meio virtual, surgindo assim o termo hacker (ALMEIDA et al., 2015, p. 225 e 226).

Entende-se por hacker o indivíduo com conhecimentos técnicos aprofundados acerca de sistemas de informática, mas que não necessariamente se utilizam destes conhecimentos para a prática de atos ilícitos. Levando em consideração o vasto entendimento das redes e tecnologias, este pode ser utilizado tanto de forma positiva, quanto negativa (ALMEIDA et al., 2015, p. 226).

Daí, analisando as práticas de cada “espécie” de hacker, surge outra nomenclatura utilizada, como uma ramificação do gênero Hacker, qual seja o termo cracker, por volta do ano 1985, por hackers que não concordavam com a utilização do termo pela imprensa para designar os indivíduos que se utilizavam do conhecimento técnico para atos ilícitos (ALMEIDA et al., 2015, p. 226).

Hodiernamente, ainda há grande equívoco entre os termos cracker e hacker. Os hackers são sujeitos que se utilizam de seus entendimentos técnicos para interesse próprio, para fins de trabalho ou auxiliar pessoas físicas e/ou jurídicas. De outra forma, os crackers (*cracking* = quebra) utilizam seus conhecimentos de forma maldosa visando corromper e invadir redes e sistemas (SILVA e DINIZ, 2017, p. 4).

Geralmente, ambos são bem conhecedores de sistemas, tendo aprofundados fundamentos no que tange a dispositivos informáticos e afins. A principal diferença se pauta na finalidade das ações de cada um, visto que os hackers comumente empregam seu conhecimento para atividades positivas, enquanto os crackers motivam-se, em suma, por práticas ilegais e criminosas (Almeida et al., 2015, p. 226).

Há ainda para fins de classificação de hackers os denominados *lamers*, *wannabes* ou script-kid, que possuem conhecimentos limitados e não apresentam perigos de larga escala, provocando pequenos danos e são considerados leigos em relação às outras "categorias" de hackers; os phreakers, que investem na prática de crimes especificamente ao ramo de telecomunicações, além dos defacers, que focam em invadir e depreciarem páginas de internet, deixando suas marcas (ALMEIDA et al., 2015, p. 226).

Deste modo, compreende-se que os responsáveis, ou sujeitos ativos dos crimes cibernéticos, são os chamados crackers que, conforme citado, têm precipuamente o objetivo de causar malefícios a terceiros, haja vista possuírem vasto conhecimento técnico na esfera informática.

Por outro lado, o sujeito passivo é aquele que sofre o dano causado pelo criminoso, ou seja, é a pessoa física ou jurídica que tem seu bem jurídico violado. Nas espécies de crimes em geral, comumente se conhece o sujeito passivo do crime, porém nos crimes virtuais nem sempre isso acontece. O desconhecimento do sujeito passivo de crimes virtuais muitas vezes se dá pela não divulgação dos fatos, ou ainda pela ausência de denúncia para apuração do crime.

Em crimes contra pessoas jurídicas, por exemplo, em caso de grandes empresas que têm dados violados e invadidos por criminosos, muitas vezes não há divulgação do crime sofrido para evitar que se propague uma má fama da empresa, evidenciando falha em seus sistemas de segurança. Já no caso de pessoas físicas, ocorre que diversas vezes não almejam a ação penal pertinente por suposta falta de punibilidade do agente infrator ou por dificuldade no acesso à Justiça (ALMEIDA et al., 2015, p. 227).

2.3 INCIDÊNCIAS DOS CRIMES VIRTUAIS

2.3.1 Os crimes digitais mais comuns

O “mundo” da internet, ou espaço cibernético, é utilizado para a prática de cada vez mais crimes, atingindo grande parte dos usuários da tecnologia. Dentre os mais habituais, tem-se os crimes contra a liberdade individual, crimes contra a honra, crimes contra o patrimônio, fraudes a cartões de crédito, pornografia infantil, pirataria, dentre outras práticas delituosas.

Neste sentido, Lima e Duarte (2020) entendem que os crimes de informática mais comuns são os de atribuição de falsa identidade (art. 307, CP), pornografia infantil online (art. 241, ECA), divulgação indevida de dados sigilosos (art. 153, CP), estelionato eletrônico (art. 171, CP), alteração indevida de sistemas de informação do Governo (art. 313-A, CP), fraude bancária eletrônica (art. 155, CP), violação a direitos autorais (art. 164, CP), crimes contra a imagem e a honra (arts. 138 a 141, CP) e interceptação clandestina de dados (art. 10, lei 9296/96).

Em relação aos crimes contra a liberdade individual, são praticados com maior frequência os delitos de ameaça (art. 147 do Código Penal), inviolabilidade de correspondência (arts. 151 e 152 do Código Penal), divulgação de segredos (arts. 153

e 154 do Código Penal), disseminação de segredos compreendidos ou não em sistemas de informação ou banco de dados da Administração Pública (artigo 153, inciso I do Código Penal) (TAVARES e REIS, 2014).

Em se tratando dos crimes cometidos contra a honra da vítima, os mais recorrentes são o crime de calúnia, com previsão na Legislação Penal em seu artigo 138, a difamação e a injúria, também elencados no Código Penal, nos artigos 139 e 140, respectivamente (TAVARES e REIS, 2014).

Para Schaun (2018), analisando-se os delitos contra a honra, é um exemplo do crime de calúnia (art. 138) a divulgação em internet de fakenews, bem como a prática do chamado *cyberbullying* pode ser citada como exemplo para o crime de injúria (art. 140).

A prática dos crimes contra a honra citados se dá, normalmente, em virtude de a possiblidade do agente criminoso cometer o crime de forma que permaneça em anonimato, utilizando-se de sites, blogs, redes sociais, chats, e-mails e demais meios de interação no meio digital (TAVARES e REIS, 2014).

Considerando-se assim a posição de anonimato e a possibilidade de tornar a divulgação disseminada e alastrada rapidamente pela rede virtual, cabe ainda mencionar a majorante para os crimes contra a honra conforme trazido pelo legislador no artigo 141, inciso III do Código Penal:

> Art. 141 - As penas cominadas neste Capítulo aumentam-se de um terço, se qualquer dos crimes é cometido:
> [...]
> III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria.

O nascimento e desenvolvimento da Internet influenciaram grandemente nos negócios de programas de computador, de forma que aumentasse significativamente a oportunidade de utilização e reprodução dos softwares. Porém, esta reprodução se dá inúmeras vezes através do processo denominado pirataria.

> O delito de pirataria de software consiste em apropriação indébita e na conduta de vendas de programas de computador sem a devida licença do autor. A lei nº 9609/1998 dispôs sobre propriedade intelectual de programa de computador e sua comercialização no Brasil (TAVARES, 2007 apud TAVARES e REIS, 2014).

A pirataria de software é a reprodução e comercialização do material produzido por outrem, não possuindo o indivíduo os direitos autorais do material. Esta apropriação, em geral a título de pirataria, além de ser uma conduta criminosa, produz diversos prejuízos aos verdadeiros autores, tanto em relação à venda do produto, quanto ao esforço despendido no processo de criação do material.

Outros tipos de crime que são cometidos com grande frequência através da rede de internet são as fraudes aos usuários de cartões de crédito. Segundo Ramos (2007, apud TAVARES e REIS, 2014) a ausência de normativas concernentes ao uso de cartão de crédito na internet causa grandes prejuízos aos proprietários da forma de pagamento. O autor menciona ainda que qualquer indivíduo que possua ou gerencie um provedor de acesso possui a possibilidade de adentrar aos dados dos cartões e permitindo um uso indevido. Tal possibilidade se dá em virtude de que não somente o responsável pelo provedor possui o acesso aos dados, mas também qualquer um que saiba utilizar meios para colher os elementos apresentados na rede.

Em consequência da inocência e/ou desatenção de muitas das vítimas, tem se tornado também bastante comum o crime de estelionato eletrônico. As vítimas, muitas das vezes, confiam em anúncios e promoções desarrazoadas que lhes são apresentadas nas páginas de internet, e são levadas através dos *links* a páginas que estão configuradas para obter seus dados.

Em conformidade à Agência Câmara de Notícias, o Projeto de Lei 3376/20 acresce ao Código Penal o crime estelionato virtual. O texto do Projeto, que segue em tramitação na Câmara dos Deputados, prevê que essa prática terá pena de reclusão, de 2 a 10 anos, e multa, que, se comparada ao estelionato “comum”, é penalizada com o dobro (AGÊNCIA CÂMARA DE NOTÍCIAS, 2020).

Ainda segundo a Agência, o tipo penal do estelionato virtual será reconhecido no caso de o criminoso invadir, adulterar ou clonar um aplicativo de mensagens imediatas e de chamadas de voz para celulares, bem como utilizando-se da internet, de aparelho de comunicação ou de sistema de informática (AGÊNCIA CÂMARA DE NOTÍCIAS, 2020).

A rede virtual da internet desempenha funções importantíssimas para os avanços da sociedade, da economia, do ramo universitário e científico, bem como de diversas áreas. Contudo, conforme visto, também é “palco” de inúmeras condutas criminosas, além das já mencionadas anteriormente, algumas já tipificadas em lei, outras não, e que está propícia a um surgimento de novas práticas a todo momento.

2.3.2 A Lei Carolina Dieckmann

2.3.2.1 Dos fatos

A Lei dos Crimes Cibernéticos (Lei 12.737/2012), conhecida como “Lei Carolina Dieckmann”, que alterou o Código Penal Brasileiro, foi decretada e sancionada para tratar da tipificação criminal dos crimes informáticos, tendo como incentivo um fato criminoso cometido contra a atriz cuja Lei comumente recebe o nome.

Segundo o jornal G1, da Globo, em maio de 2012, a atriz Carolina Dieckmann teve divulgadas na internet 36 fotos em que estava nua. Houve então, por parte dos criminosos envolvidos, extorsão para que a atriz despendesse a quantia de R$10 mil a fim de, supostamente, não haver a publicação das fotos (G1, 2013).

À época, levantou-se a hipótese de que as fotos haviam sido extraídas de um aparelho pessoal de Carolina Dieckmann levado para conserto tempos antes. Contudo, tal hipótese foi desconsiderada e concluiu-se que "hackers" invadiram a caixa de e-mails da atriz e obtiveram as fotos (G1, 2013).

Diante disto, em 30 de novembro de 2012, foi decretada e sancionada pela então Presidenta da República Dilma Rousseff a Lei 12.737/12, que acrescentou ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal os artigos 154-A e 154-B:

> Invasão de dispositivo informático
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações

> sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
>
> Ação penal
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Considerando-se que o tipo penal incluso no artigo 154-A supracitado é de caráter expresso e taxativo, qualquer indivíduo que cometer alguma das condutas elencadas enquadra-se para fins de punição, tanto no crime comum, quanto em suas formas qualificada e majorada.

Importante ainda salientar que, conforme previsão apresentada no texto do artigo 154-B, a representação é requisito essencial para o prosseguimento da ação penal nos casos dos crimes estabelecidos no artigo anterior. Há exceção, entretanto, apenas para os casos de cometimento de tais crimes contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Além disso, a Legislação Penal também passou a vigorar com nova redação dos artigos 266 e 298:

> Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

> Art. 266. [...]
>
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
>
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.
>
> Falsificação de documento particular
>
> Art. 298. [...]
>
> Falsificação de cartão
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

2.3.2.2 Prós e Contras da Lei 12.737/12

Um dos benefícios apresentados através da sanção da Lei dos Crimes Cibernéticos (Lei 12.737/2012) foi a inclusão do tipo penal "Falsificação de cartão" na relação de delitos elencados no Capítulo III - DA FALSIDADE DOCUMENTAL do Código Penal, mais especificamente no Parágrafo Único do artigo 298.

Através desta previsão, tornou-se o cartão de crédito ou débito equiparado ao documento particular, a fim de punir sua falsificação, seja de forma integral ou parcial. Esta alteração recai como um avanço, visto que somente era possível punir o autor do delito de clonagem de cartões e obtenção de dados como crime de fraude.

No entanto, apesar de providencial ao caso sofrido pela atriz, noticiado em diversos veículos de informação da época, a “Lei Carolina Dieckmann” recebeu diversas opiniões sobre seu texto, eficácia e outros pontos, por vezes positivos, mas muitos de forma negativa.

Algumas especificidades em relação à Lei 12.737/2012 são apontadas e discutidas como, por exemplo, a ausência de meios processuais que assegurem a sua efetividade. O duradouro processo de investigação dos crimes cibernéticos recebe ainda mais contrariedades quando os provedores de internet não guardam os dados e registros de IP (Internet Protocol) em banco de dados corretamente conforme deve ser feito e, quando há, torna-se um procedimento um tanto quanto burocrático.

Exemplo disto foi o caso ocorrido em 11 de fevereiro de 2015, em que o Juiz Luis Moura Correia, da Central de Inquéritos da Comarca de Teresina, no estado do Piauí, ordenou à operadora de telefonia e acesso à internet Vivo a suspensão das atividades do aplicativo de mensagens instantâneas WhatsApp no território nacional (HIGA, 2015).

Tal determinação se deu, segundo o próprio Magistrado, Correia (2015), no intuito de “garantir a suspensão do tráfego de informações de coleta, armazenamento, guarda e tratamento de registros de dados pessoais ou de comunicações entre usuários do serviço e servidores […] do WhatsApp, em que pelo menos um desses atos ocorra em território nacional” (HIGA, 2015).

Um dos pontos a serem observados é em relação ao art. 154-A do Código Penal Brasileiro, adicionado através da Lei 12.727/2012. Considerando-se que no referido artigo não há previsão de configuração do crime quanto à simples invasão do dispositivo móvel alheio, compreende-se que somente se dará se o criminoso praticar uma adulteração ou violação de mecanismo de segurança. Sendo assim, apenas pela invasão do dispositivo, não há crime, todavia, se o dispositivo possuir ferramentas de proteção como senhas, antivírus ou outros, configurar-se-á o crime previsto (SILVEIRA et al., 2017).

Outrossim, também são alvos de análises e críticas as penas cominadas pela “Lei Carolina Dieckmann”. As penas elencadas nos artigos 154-A, 154-B, 266 e 298 da Legislação Penal são consideradas sanções fracas, que não intimidam os criminosos e transmitem impunidade. Deste modo, ao invés de haver inibição à prática criminosa no meio digital, a pena imposta torna-se, por vezes, inofensiva ao infrator, não atingindo o Direito o objetivo principal de puni-lo (SILVEIRA et al., 2017).

No artigo 3º da Lei, que altera o artigo 266 do Código Penal, é prevista a aplicação de pena para a interrupção ou perturbação de serviços telegráficos, telefônicos, informáticos, telemáticos ou de informação de utilidade pública. Sendo assim, considera-se que se asseguram os serviços públicos, em detrimento ao amparo a sites particulares.

Do mesmo modo, também é objeto de análise da Lei 12.737/2012 a ausência de responsabilidade penal aos responsáveis pelos sites e redes sociais que hospedam as mais variadas espécies de crimes virtuais como calúnias, injúrias, difamações, dentre outros (CASTRO, 2013 apud SILVEIRA et al., 2017).

A Lei 12.965/2014, denominada Marco Civil da Internet, foi decretada e sancionada também pela Presidenta da República à época, Dilma Rousseff, em 23 de abril de 2014. Esta lei estabelece e norteia regras quanto ao uso da rede de internet no Brasil, estabelecendo deveres e direitos dos provedores de internet, bem como de seus usuários e do Estado.

O Marco Civil da internet veio como forma de proteção também à privacidade de dados, comunicações telefônicas, telegráficas, dando a estes a inviolabilidade de sigilo, nos termos que a Constituição Federal Brasileira descreve como direito e garantia fundamental:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Outro empecilho que há em relação à aplicação penal da Lei Carolina Dieckmann é a grande complexidade por parte das autoridades para descobrir e comprovar os autores dos delitos. Conforme a Lei do Marco Civil da Internet, 12.965/14, há obrigatoriedade aos provedores de preservar os dados de acesso e guarda-los durante 6 meses, sendo que poderá o Poder Judiciário requerer um armazenamento por período superior, dada a devida importância (SILVEIRA et al., 2017).

Nesta perspectiva, determina a Lei 12.965/14, em seu artigo 15:

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
>
> § 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
>
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os

> registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.
>
> § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
>
> § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

No entanto, apesar de haver a devida previsão legal, a concessão dos dados e registros solicitados aos provedores, inúmeras vezes encontra óbice por parte destes, que impõem diversas obstruções e se levanta enorme burocracia, levando até mesmo a disputas judiciais ineficientes. Assim sendo, a aplicação da Lei 12.727/2012 requer inúmeras providências para que seja realmente eficaz e sejam os criminosos punidos.

2.3.3 Lei Azeredo - 12.735/12

A Lei 12.735, de 30 de novembro de 2012 é oriunda no projeto de lei 84, proposto em 1999, pelo deputado Luiz Piauhylino. O PL continha em seus fundamentos a sanção para criminosos do âmbito digital e somente em 2003 foi aprovado pela Câmara (SILVA, 2014).

Posto isto, a referida Lei altera o Código Penal Brasileiro, bem como o Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, a fim de caracterizar como crime as atitudes cometidas através da utilização de sistema eletrônico, virtual ou semelhante, que sejam cometidos contra sistemas informatizados e semelhantes, e outras medidas.

A Lei Azerêdo, como ficou conhecida, recebeu este nome pois o PL 84/99 teve como seu relator o senador Eduardo Azeredo, tanto no Senado quanto na Câmara. O projeto foi discutido durante um longo período no Congresso Nacional, tendo sido aprovado apenas em 2003 e tramitando no Senado até o ano de 2008 (SILVA, 2014).

Ainda segundo Silva (2014), considerando-se todo o debate realizado acerca da lei dentro de tantos anos de tramitação, foram sancionados apenas 4 artigos do texto original do projeto, que possuía 23 artigos. Todavia, ainda sobre os 4 artigos foram vetados 2 deles, quais sejam os artigos segundo e terceiro, pela Presidenta Dilma Rousseff:

> A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:
>
> Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.
>
> Art. 2º (VETADO)
>
> Art. 3º (VETADO)
>
> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.
>
> Art. 5º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:
>
> "Art. 20. .....
>
> .....
>
> § 3º .....
>
> .....
>
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;
>
> ....."
>
> Art. 6º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Observa-se que uma das medidas que traz a Lei 12.735/12 é a determinação da instalação de delegacias especializadas para o combate de crimes virtuais. Apesar de ter sido chamada ironicamente de "AI-5 digital" em virtude dos assuntos problemáticos que trazia em seu texto, a previsão de seu artigo 4° sobre a estruturação das áreas especializadas contra os crimes virtuais foi bastante conveniente (CANAL CIÊNCIAS CRIMINAIS, 2015).

Contudo, a previsão sujeita-se à vontade do Poder Público para se estruturar e efetivar-se, através do empenhamento e capacitação dos profissionais de Polícia, e provimento de equipamentos necessários, para que as delegacias estejam hábeis a

atender apropriadamente ao público-vítima de crimes de informática (CANAL CIÊNCIAS CRIMINAIS, 2015).

A Lei Azerêdo, além do mais, alterou a Lei 7.716 de 1989, que é a lei..., adicionando ao seu artigo 20, § 3º, o inciso II, para prever a faculdade ao juiz de ordenar “a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio” nos casos dos delitos de prática, incitação ou induzimento à discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, praticados via meios de comunicação social ou publicação de qualquer natureza.

3 CRIMES CONTRA A HONRA

3.1 DEFINIÇÃO DOS CRIMES CONTRA A HONRA

A honra é direito fundamental do indivíduo, conforme previsão na Constituição Federal de 1988, não aceitando-se a possibilidade de ofensa à honra de outrem, por quaisquer que sejam os motivos e assegurando-se o direito de indenização por esta violação.

O legislador, ao editar o texto da Carta Constitucional, atentou-se a mencionar no título de Direitos e Garantias Individuais a inviolabilidade da intimidade, da vida privada, da honra e da imagem dos indivíduos, além de garantir à vítima o direito a indenização pelo dano material ou moral decorrente de sua transgressão, conforme lê-se em seu art. 5º, inciso X.

O resguardo ao direito à honra veio ao Direito Fundamental Brasileiro como uma forma de respeito ao cumprimento do princípio da dignidade da pessoa humana, princípio este consagrado também na Carta Magna, como fundamento da República Federativa pátria:

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
> [...]
> III - a dignidade da pessoa humana;

Neste sentido, o Supremo Tribunal Federal entende que “o princípio da dignidade da pessoa humana busca proteger de forma integral o sujeito na qualidade de pessoa vivente em sua existência concreta.” (ADI 5.543, REL. MIN. EDSON FACHIN, J., DJE, 2020).

Tratando-se propriamente do conceito de honra como bem tutelado pela Legislação Brasileira, para Edgard Magalhães Noronha, é definida “como o complexo ou conjunto de predicados ou condições da pessoa que lhe conferem consideração social e intima própria” (NORONHA, 1996, p.110 apud CAPEZ, 2014, p. 274).

André Rodrigues Marins aponta que “a tutela da honra, como bem jurídico autônomo, não se limita ao interesse exclusivo do indivíduo, na medida em que a preservação daquele valor repercute na convivência harmônica da coletividade em seu meio social” (MARINS, 2010).

Quanto às suas formas de análise, a doutrina se encarrega de classificá-las de diversas perspectivas, como em honra objetiva e honra subjetiva. A primeira, basicamente, se relaciona ao modo como um indivíduo é observado por outros, a forma como pensam dele, tratando de qualidades inerentes ao ser. Já a segunda, trata-se de como a própria pessoa se entende, o que pensa de si, o que causa sua estima.

Neste prisma, Prado (2008, p. 213, apud SOARES, 2020) pondera que:

> "A honra, do ponto de vista objetivo, seria a reputação que o indivíduo desfruta em determinado meio social, a estima que lhe é conferida; subjetivamente, a honra seria o sentimento da própria dignidade ou decoro. A calúnia e a difamação atingiriam a honra no sentido objetivo (reputação, estima social, bom nome); já a injúria ofenderia a honra subjetiva (dignidade, decoro)".

Também neste sentido, Capez (2014) tece suas observações acerca das diferenças entre a honra objetiva e subjetiva. Quanto à sua objetividade:

> Diz respeito à opinião de terceiros aos atributos físicos, intelectuais, morais de alguém. O sujeito acredita que goza no seu meio social, ou seja, é aquela que se refere a conceituação do indivíduo perante a sociedade. (CAPEZ, 2014).

Por outro lado, em relação à honra subjetiva, Capez (2014) sabiamente considera que:

> Refere-se à opinião do sujeito a respeito de se mesmo, ou seja, de seus atributos físicos, intelectuais e morais, em suma, diz com sua autoestima. Não importa a opinião de terceiros. (CAPEZ, 2014).

Não obstante, Fragoso (p.184 apud GRECO, 2014, p. 420) trata o entendimento das classificações de honra da seguinte forma:

> Na identificação do que se deva entender por honra, a doutrina tradicionalmente distingue dois diferentes aspectos: um subjetivo, outro, objetivo. Subjetivamente, honra seria o sentimento da própria dignidade; objetivamente, reputação bom nome e estima no grupo social. Essa distinção conduz a equívocos quando aplicada ao sistema punitivo dos crimes contra honra: não proporciona conceituação unitária e supõe que a honra, em seu aspecto sentimental, possa ser objeto de lesão. Como ensina Welzel, § 42, I, 1, o conceito de honra é normativo e não fático. Ela não consiste na fatual opinião que o mundo circundante tenha do sujeito (boa fama), nem na fatual

> opinião que o indivíduo tenha de si mesmo (sentimento da própria dignidade) (FRAGOSO, p.184 apud GRECO, 2014, p. 420).

Todavia, apesar das classificações apresentadas pelos estudiosos e doutrinadores, a segmentação da honra em subjetividade e objetividade torna-se uma, uma vez que uma completa o sentido da outra, formando um exclusivo conceito. Há, por fim, o entendimento e diferenciação em que a subjetividade da honra se dá através do que o indivíduo entende de si, enquanto a objetividade pauta-se na imagem deste perante a sociedade (MARTINS, 2017).

Aprofundando-se mais do que meras classificações, o Direito Brasileiro, brilhantemente, assegura a proteção à honra do indivíduo a fim de torná-lo amparado em sua vida privada. Entretanto, assim como ocorre com outros bens jurídicos, a honra sofre violações constantes, tendo como fatos tipificados como crimes a prática da Calúnia (art. 138), a difamação (art. 139) e a injúria (art. 138), todos elencados no Código Penal.

3.2 CALÚNIA

O crime de calúnia é tido como a conduta mais séria entre os previstos pela Lei no rol de delitos contra a honra. A caracterização se dá quando o criminoso efetua a atribuição a outrem de fato definido como crime, de forma que este acontecimento seja falso (MARTINS, 2017).

Ocorre que, ao analisar o tipo penal do crime de calúnia, compreende-se que a imputação falsa de "fato definido como crime", nos termos do artigo transcrito, deve basear-se em fato determinado. Não havendo o fato determinado, não se trata do crime em questão. Para fins de exemplo do fato, conforme citado, pode-se imaginar que "fulano" cometeu um homicídio contra "beltrano" durante o show em certa data.

> Calúnia
>
> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
>
> Pena - detenção, de seis meses a dois anos, e multa.
>
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.

Na hipótese de a conduta da calúnia ser praticada através de envio de e-mail na internet, todos os indivíduos que tiverem sido destinatários do e-mail, e o repassar, estarão também sujeitos a responder por coautoria, em virtude da previsão do § 1º do texto do artigo 138, que atribui a mesma pena do caput aos que, conhecendo a falsidade da imputação, a dissemina (CAMPANHOLA, 2018).

Além de dever o fato ser considerado crime, devidamente tipificado em lei, outro requisito essencial para a configuração penal do crime de calúnia é a falsidade da imputação. É necessário que o fato atribuído à suposta vítima seja um acontecimento falso ou há impossibilidade de se punir nas penas do artigo 138 do Código Penal.

Importante ressaltar que, em conformidade com Greco (2014), também se configurará o crime de calúnia quando houver veracidade do fato, portanto, ter havido, realmente, um acontecimento tipificado como crime, porém o criminoso associa falsamente a autoria do crime à vítima.

No entendimento de Damásio de Jesus (2007, p. 219), a respeito da caracterização da conduta de calúnia, extrai-se que:

> Constitui crime formal, porque a definição legal descreve o comportamento e o resultado visado pelo sujeito, mas não exige sua produção para que exista crime, não é necessário que o sujeito consiga obter o resultado visado, que é o dano a honra objetiva do agente.

Para fins de classificação do tipo de honra lesada, no caso do delito de calúnia, o bem jurídico amparado pela Lei Penal é a honra objetiva, de modo que se fere a reputação ou prestígio da vítima perante a sociedade, ou também a chamada boa fama (MARINS, 2010).

> § 2º - É punível a calúnia contra os mortos.
>
> Exceção da verdade
>
> § 3º - Admite-se a prova da verdade, salvo:
>
> I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
>
> II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
>
> III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

Importa ressaltar que, consoante ao § 2º do Art. 138, ainda que o ofendido seja pessoa morta, será cabível a punição pelo crime de calúnia. No parágrafo seguinte, apresentam-se as chamadas exceções da verdade, de modo que o responsável pela conduta delitiva tem a possibilidade de provar que o fato imputado ao outro não é inverídico, respeitadas as ressalvas mencionadas nos incisos do mesmo parágrafo.

3.3 DIFAMAÇÃO

Assim como ocorre em relação ao crime de calúnia, a conduta danosa considerada como difamação ofende a honra objetiva do indivíduo, provocando entendimentos de terceiros de forma que tenha seu prestígio abalado, em um meio social em que vivem (MARINS, 2010).

> Difamação
>
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
>
> Pena - detenção, de três meses a um ano, e multa.
>
> Exceção da verdade
>
> Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

Ao contrário do que ocorre no crime de injúria, para a tipificação do crime de difamação ocorre, bem como para a calúnia, a imputação de um fato. Há a necessidade da descrição de um acontecimento, sendo que, ausente o fato, a conduta não se configura difamação.

O momento de consumação do crime de difamação, do mesmo modo ao de calúnia, é aquele em que a informação inverídica passa a ser conhecida por terceiros, visto que é este o instante que a reputação da vítima se torna lesada, alcançando-se a circunstância essencial.

No tocante à caracterização da difamação, não há a imprescindibilidade de que o comportamento praticado seja caracterizado crime. Basta que haja a atitude que ofenda a moral ou reputação do indivíduo, ofendendo sua honra, não se considerando a veracidade da imputação (SOARES, 2016).

Acerca deste assunto, Damásio de Jesus (2007, p. 225) retifica:

> Enquanto a calúnia existe imputação de fato definido como crime, na difamação o fato é meramente ofensivo a reputação do ofendido. Além disso, o tipo de calúnia exige elemento normativo da falsidade da imputação, o que é irrelevante no delito da difamação. Enquanto na injúria o fato versa sobre qualidade negativa da vítima, ofendendo-lhe a honra subjetiva, na difamação há ofensa à reputação do ofendido, versando sobre fato a ela ofensivo.

Enquanto a pessoa jurídica não pode ser sujeito passivo nos crimes de calúnia e injúria, esta pode sofrer o tipo penal do artigo 139, compreendendo-se que a pessoa pode ter imputada a si um fato ofensivo à sua reputação. Para a calúnia ou injúria, por exemplo, não é possível esta adequação visto que para a injúria é necessário atingir a honra subjetiva, sendo esta ausente na Pessoa Jurídica pois não tem atributos morais, físicos, religiosos, intelectuais, inerentes ao ser humano. Já para a calúnia, seria necessário definir à pessoa fato definido como crime (MARINS, 2010).

Há ainda de se analisar que, para haver a exceção da verdade no caso do delito de difamação, requer, segundo o parágrafo único do artigo 139 do Código Penal, que a vítima seja funcionário público, e o fato ofensivo imputado a ele seja alusivo às funções exercidas. Portanto, provando ser verdadeiro o fato, ficará o acusado isento do crime de difamação.

3.4 INJÚRIA

A tipificação da conduta criminosa do artigo 140, qual seja o crime de injúria, somente se dará pelo simples julgamento com intuito de desprezar e atingir a dignidade ou decoro do tutelado. Assim sendo, não há de se falar em pessoa jurídica no polo passivo para crime de injúria (MARINS, 2010).

Em se tratando da espécie de honra atingida, a conduta praticada acomete a honra subjetiva do indivíduo, ou seja, o que o próprio ser pensa de si, não necessitando de que a ofensa tenha passado ao conhecimento do meio social da vítima (SOARES, 2016).

> Injúria
>
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
>
> Pena - detenção, de um a seis meses, ou multa.

O parágrafo primeiro do presente artigo é tido como causa de extinção de punibilidade por perdão judicial, conforme o art. 107, IX do Código Penal, e também nos termos de Nucci (2015. P. 798): “quando o Estado, diante de circunstâncias especiais, crê não ser cabível punir o agente” (ARGACHOFF, 2015).

> § 1º - O juiz pode deixar de aplicar a pena:
>
> I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
>
> II - no caso de retorsão imediata, que consista em outra injúria.

De modo oposto, BITENCOURT (2007. P. 560-561 apud ARGACHOFF, 2015), entende que a retorsão imediata tem natureza jurídica de exercício regular de um direito, equiparando o instituto com o desforço imediato conforme elencado no Código Civil.

> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
>
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.
>
> § 3o Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:
>
> Pena - reclusão de um a três anos e multa.

O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) amparou a vítima do crime de injúria prevendo três subdivisões do delito no artigo 140. O caput do artigo em questão trata da chamada injúria simples, que é mais branda. Já no parágrafo segundo do mesmo artigo, é prevista a denominada injúria real, em que o intuito do criminoso é macular a honra pessoal da vítima, se utilizando de violência ou vias de fato como meio de consubstanciar o ato. Por fim, no parágrafo terceiro, há elencada a injúria preconceituosa ou qualificada, baseada no uso, por parte do criminoso, de características inerentes à etnia, cor, raça, religião, origem ou condição de deficiência ou pessoa idosa. Estes dois últimos tipos de injúria são considerados os mais graves entre os três abrangidos.

Assim havendo, de maneira oposta ao que ocorre nas condutas de difamação e calúnia, para adequação do ato ilícito ao tipo penal previsto no artigo 140, não se faz necessária a imputação de fato determinado. Chamar certa pessoa de ladrão, via

de exemplo, de modo que ofenda a sua dignidade ou decoro, se configura crime de injúria, e não de calúnia, pois o indivíduo não narrou o fato em que ocorreu a atitude de ladroar.

Ainda em oposição às configurações dos demais delitos contra a honra previstos na Legislação Penal Brasileira, a injúria se consuma no momento em que o ofendido ou, neste caso, sujeito passivo, passa a conhecer a ofensa proferida pelo sujeito ativo, não havendo necessidade de que a ofensa seja pública (MARINS, 2010).

Marins (2010) também afirma que esta consumação também pode ser aplicada em caso de haver o criminoso praticado a injúria a crianças ou doentes mentais, sob condição de que estes possam entender o sentido ofensivo da imputação.

3.5 DISPOSIÇÕES GERAIS

Os artigos 141, 142, 143, 144 e 145 do Código Penal vêm, finalizando o capítulo V dos Crimes contra a Honra, trazer determinações gerais em relação aos crimes estudados anteriormente, quais sejam: calúnia, difamação e injúria. Tais disposições tratam de majorantes aos crimes, exclusão do delito, retratação, pedido de explicações e forma de procedência da ação penal acusatória.

> Disposições comuns
>
> Art. 141 - As penas cominadas neste Capítulo aumentam-se de um terço, se qualquer dos crimes é cometido:
>
> I - contra o Presidente da República, ou contra chefe de governo estrangeiro;
>
> II - contra funcionário público, em razão de suas funções;
>
> III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria.
>
> IV – contra pessoa maior de 60 (sessenta) anos ou portadora de deficiência, exceto no caso de injúria.

É adequado salientar que, em se tratando das majorantes previstas no Art. 141: o Chefe de Estado abrange não somente o chefe soberano, mas também o primeiro-ministro (I); é fundamental que a ofensa proferida seja em virtude da função pública da vítima e, se cometida estando o funcionário presente, pode ser tipificado o desacato (II); são meios que facilitam a divulgação, por exemplo, os sites, muros, outdoors,

imprensa, etc. (III); é necessário o conhecimento da condição de idoso ou portador de deficiência, por parte do autor do crime (IV) (DELMANTO, 2007).

> § 1º - Se o crime é cometido mediante paga ou promessa de recompensa, aplica-se a pena em dobro.

Por fim das majorantes, o parágrafo primeiro prevê a aplicação do dobro da pena no caso de cometimento de algum dos crimes dos artigos 138, 139 e 140, a troco de paga ou prometimento de recompensa.

> § 2º - (VETADO).
>
> Exclusão do crime
>
> Art. 142 - Não constituem injúria ou difamação punível:
>
> I - a ofensa irrogada em juízo, na discussão da causa, pela parte ou por seu procurador;
>
> II - a opinião desfavorável da crítica literária, artística ou científica, salvo quando inequívoca a intenção de injuriar ou difamar;
>
> III - o conceito desfavorável emitido por funcionário público, em apreciação ou informação que preste no cumprimento de dever do ofício.
>
> Parágrafo único - Nos casos dos ns. I e III, responde pela injúria ou pela difamação quem lhe dá publicidade.

Acerca das excludentes de crime, com previsão no Artigo 142, Delmanto (2007) corrobora que a imunidade judiciária descrita no inciso I tem por objetivo proteger a liberdade de defesa em juízo aos procuradores e partes. Não se incluem a esta imunidade o Juiz, por não ser parte, tampouco as autoridades policiais e auxiliares.

Segue também afirmando que a imunidade de crítica da qual trata o segundo inciso ampara os proveitos da cultura e sujeição às críticas pelas quais podem receber os autores de obras. Quanto ao inciso III, a imunidade pelo conceito desfavorável de funcionário se dá pela indispensabilidade da manifestação ao interesse público, sendo possível a punição por exagero ou abuso (DELMANTO, 2007).

> Retratação
>
> Art. 143 - O querelado que, antes da sentença, se retrata cabalmente da calúnia ou da difamação, fica isento de pena.
>
> Parágrafo único. Nos casos em que o querelado tenha praticado a calúnia ou a difamação utilizando-se de meios de comunicação, a retratação dar-se-á, se assim desejar o ofendido, pelos mesmos meios em que se praticou a ofensa.

Para fins de retratação, aqui tratada como causa extintiva de punibilidade, o criminoso tenta reparar o dano manifestando que errou ao cometer o ato ilícito. A possibilidade jurídica se perfaz apenas nos delitos de difamação e calúnia, não abrangendo a situação de cometimento contra funcionário público no exercício de suas funções. O autor deve se retratar antes de ser dada a sentença, de forma cabal, expressa, através de pronunciamento nos autos, interrogatório, etc. e independendo de aquiescência da vítima (DELMANTO, 2007).

Neste sentido, segundo o Relator Desembargador Federal Francisco Cavalcanti:

> 1. Para os Tribunais Superiores, a retratação, prevista no art. 143 do CP, é restrita à ação penal privada relativa aos crimes de calúnia e de difamação, não se aplicando quando a pretensão punitiva é veiculada mediante ação penal pública condicionada e visa preservar a integridade dos órgãos estatais no exercício de suas funções.
> 2. Nos casos de ação penal pública incondicionada, a retratação não isenta de pena nem extingue a punibilidade do agente.
> 3. Recurso conhecido e provido para anular a sentença e determinar ao juiz monocrático o regular processamento do feito. (BRASIL, 2010, p. 496)

O pedido de explicações aludido no artigo 144 é aplicável se houver dúvida do animus de ofender ou a quem foi destinada a ofensa, sendo cabível o referido pedido, e tendo como autor da ação a suposta vítima. Torna-se uma ação preparatória para os trâmites penais, não possibilitando suspensão de prazo de decadência (DELMANTO, 2007).

> Art. 144 - Se, de referências, alusões ou frases, se infere calúnia, difamação ou injúria, quem se julga ofendido pode pedir explicações em juízo. Aquele que se recusa a dá-las ou, a critério do juiz, não as dá satisfatórias, responde pela ofensa.
>
> Art. 145 - Nos crimes previstos neste Capítulo somente se procede mediante queixa, salvo quando, no caso do art. 140, § 2º, da violência resulta lesão corporal.
>
> Parágrafo único. Procede-se mediante requisição do Ministro da Justiça, no caso do inciso I do caput do art. 141 deste Código, e mediante representação do ofendido, no caso do inciso II do mesmo artigo, bem como no caso do § 3o do art. 140 deste Código.

A ação penal para aplicação dos direitos tutelados no Capítulo dos Crimes contra a Honra, de acordo com o artigo 145 é a queixa, com exceção ao caso da chamada injúria real (art. 140, § 2º), se a violência praticada resultar em lesão corporal.

4 A INVESTIGAÇÃO POLICIAL EM CRIMES DIGITAIS CONTRA A HONRA

4.1 O INQUÉRITO POLICIAL

O inquérito policial é um procedimento investigativo determinado em virtude do cometimento de um descumprimento penal, de forma que nele ocorrem diversas medidas que têm por escopo a consecução de elementos probatórios que possibilitem ao sujeito ativo da ação sua propositura para sanção ao transgressor (LENZA, 2013).

É o agrupamento de diligências feitas pelo Poder de Polícia Judiciária, de natureza administrativa e estabelecido pela autoridade policial, para investigar um delito, bem como sua autoria, que visam possibilitar ao detentor da titularidade da ação penal a instauração em juízo contra quem lhe causou dano ou prejuízo (CAPEZ, 2012).

Assim, entende-se por inquérito policial as etapas administrativas e investigativas, provocadas por autoridade policial, para que sejam levantados materiais comprobatórios de autoria e materialidade de delito praticado e, deste modo, possibilitar ao titular da ação ou Ministério Público o oferecimento da queixa-crime ou denúncia cabíveis.

Em se tratando do intuito do Inquérito Policial realizado atualmente, afirmam Vargas e Rodrigues (2011):

> O inquérito policial reúne os resultados da investigação transpostos para a lógica e linguagem jurídicas, consistindo em um documento escrito e obrigatório previsto pelo Código de Processo Penal brasileiro. Nele, encontram-se agrupados, dentre outros: o registro da ocorrência realizado por policiais militares; laudos e exames confeccionados por peritos; ordens de serviços cumpridas por investigadores; depoimentos transcritos por escrivães; portarias e relatórios de delegados; manifestações de promotores, solicitando novas investigações ou autorizando a dilatação dos prazos; despachos de juízes sobre prisão; escuta telefônica e mandados de busca e apreensão; e, até mesmo, petições de defensores. Isso tudo com o aval dos carimbos e assinaturas que visam tornar esses registros, documentos de fé pública, isto é, com veracidade atestada pelo Estado.

Ainda que extremamente importante e colaborativo, o inquérito policial não é elemento essencial e indispensável ao prosseguimento da ação penal, de tal maneira que outros meios de prova e informações podem ser utilizados ao invés do procedimento administrativo, contanto que haja suficiência para o sustento da imputação (CAROLINO, 2017).

O Código de Processo Penal Brasileiro (Decreto-Lei 3689, de 1941) menciona, em seu artigo 4º, a quem cabe exercer o Poder de Polícia Judiciária, bem como estabelece o fim útil do procedimento policial:

> Art. 4º A polícia judiciária será exercida pelas autoridades policiais no território de suas respectivas circunscrições e terá por fim a apuração das infrações penais e da sua autoria.
>
> Parágrafo único. A competência definida neste artigo não excluirá a de autoridades administrativas, a quem por lei seja cometida a mesma função.

4.1.1 Características

Considerando-se os devidos objetivos almejados, o inquérito policial é uma diligência escrita, não podendo, deste modo, ocorrer investigação de forma verbal. Para tanto, todas as provas e informações colhidas durante o inquérito são convertidas à forma escrita ou datilografada, num único processo, sendo a datilografia rubricada pela autoridade policial.

A previsão da obrigatoriedade da forma escrita ou datilografada ao inquérito policial encontra-se na própria Lei Processual Penal, em seu artigo 9°: “Todas as peças do inquérito policial serão, num só processado, reduzidas a escrito ou datilografadas e, neste caso, rubricadas pela autoridade”.

Assim, não poderá o inquérito policial ser procedido com material gravado ou de meio oral, devendo a autoridade policial proceder a colheita de provas sempre reduzindo-a a termo, de forma que se cumpra a obrigatoriedade formal trazida em Lei.

Outra característica concernente ao inquérito policial é a necessidade de sigilo, a fim de que se apure o fato ou se por exigência do interesse social, assegurado, de tal modo, pela respectiva autoridade e, conforme a descrição do artigo 20 do Código de Processo Penal.

Ainda que a Constituição Federal ampare no artigo 5º, inciso XXXIII, o direito fundamental de acesso a informações pelos órgãos públicos, de interesse particular, coletivo ou geral, assegura também o sigilo às informações que remetam à segurança da sociedade e do Estado.

Porém, a autoridade do Ministério Público, bem como a Judiciária, não partcipam de tal sigilo. Já o advogado possui a possibilidade de acessar aos autos do

inquérito, todavia, havendo declaração em juízo de sigilo da investigação, terá de deixar de acompanhar o cumprimento dos atos procedimentais.

A autoritariedade presente no procedimento investigativo é determinação expressa no § 4º do Artigo 144 da Carta Magna Brasileira, estabelecendo que “às polícias civis, dirigidas por delegados de polícia de carreira, incumbem, ressalvada a competência da União, as funções de polícia judiciária e a apuração de infrações penais, exceto as militares.

É uma autoridade pública que conduz o inquérito policial, o chamado delegado de polícia de carreira. Apenas a autoridade policial terá o dever de promover o inquérito policial, considerando-se que o particular não possui discricionariedade necessária para instaurar o procedimento de caráter administrativo (CAROLINO, 2017).

O inquérito policial é um procedimento investigatório realizado através de órgãos oficiais, de modo que o particular não pode se incumbir de procedê-lo, mesmo que seja o ofendido o titular da ação penal acusatória. A possibilidade de desempenhar a incumbência investigativa caberá apenas aos órgãos oficiais e, assim, ao Poder Público, de modo que não possa a pessoa física ter tal papel. Esta particularidade atribuída ao inquérito policial é chamada de oficialidade (CAROLINO, 2017).

Já a oficiosidade do inquérito policial é pautada no entendimento de que a atuação das autoridades policiais no procedimento investigativo insubordina-se de quaisquer fomentos, de modo que a instauração do inquérito recebe caráter indispensável havendo uma transgressão penal, salvo em se tratar de ação penal pública condicionada e de ação penal privada. Esta previsão expressa-se baseada no princípio da legalidade ou obrigatoriedade (CAROLINO, 2017).

Além das características já mencionadas, o inquérito policial é também indisponível em razão da impossibilidade de arquivamento pela autoridade policial depois de sua instauração, e dispensável, considerando-se que não há obrigatoriedade na execução do inquérito policial, podendo ser utilizados outros meios de provas que apresentem suficientes evidências de autoria e materialidade.

Capez (2006 apud JÚNIOR, 2015) relata, acerca da dispensabilidade, que o “inquérito policial não é fase obrigatória da persecução penal, podendo ser dispensado caso o Ministério Público ou ofendido já disponha de elementos suficientes para a propositura da ação penal”.

Por fim, o inquérito policial é descrito também como inquisitivo em virtude da impossibilidade dada ao indiciado ou suspeito de exercer o contraditório ou ampla defesa. O procedimento administrativo colhe e apura provas, oferece recursos e alegações, entre outros procedimentos, todos de forma inquisitiva (CAROLINO, 2017).

Para ratificar o conhecimento que se trata da inquisitoriedade do inquérito penal, expõe Capez (2006 apud JÚNIOR, 2015):

> Caracteriza-se como inquisitivo o procedimento em que as atividades persecutórias concentram-se nas mãos de uma única autoridade, a qual, por isso, prescinde, para a sua atuação, da provocação de quem quer que seja, podendo e devendo agir de ofício, empreendendo, com discricionariedade, as atividades necessárias aos esclarecimentos do crime de sua autoria.

Assim, o procedimento investigativo é compreendido como interrogativo e sem possibilidade de apresentação do princípio constitucional do contraditório e ampla defesa nesta fase de inquérito policial presidido pelo Delegado de Polícia.

4.2 TITULARIDADE DA AÇÃO PENAL

A determinação do Ministério Público, na pessoa do promotor de justiça, é indispensável para a ação penal pública, que tem início a partir da peça inicial de processo chamada denúncia. A ação penal pública difere da ação penal privada no sentido de que esta última depende da iniciativa do particular e não do poder público (AGENCIA CAMARA NOTICIAS, 2008).

A definição de quais crimes serão tratados por ação penal pública ou ação penal privada parte da própria Lei. Para tanto, analisa-se a natureza do bem jurídico tutelado que tenha recebido dano. Sendo o bem jurídico algo de considerada relevância perante a sociedade, o crime será apurado sem depender da representação do ofendido. Porém, se tratando de crime relacionado à vida intima do ofendido, como nos crimes contra a honra, caberá a necessidade de iniciativa da parte lesada ou de seu representante legal, de modo que este não é um crime de ação pública, mas privada (AGENCIA CAMARA NOTICIAS, 2008).

O Código de Processo Penal traça em seu artigo 24 sobre os crimes de ação pública:

> Art. 24. Nos crimes de ação pública, esta será promovida por denúncia do Ministério Público, mas dependerá, quando a lei o exigir, de requisição do Ministro da Justiça, ou de representação do ofendido ou de quem tiver qualidade para representá-lo.
>
> § 1º No caso de morte do ofendido ou quando declarado ausente por decisão judicial, o direito de representação passará ao cônjuge, ascendente, descendente ou irmão.

Na Ação Penal Pública, o Ministério Público é o titular, conforme a disposição trazida no artigo 24 do Código de Processo Penal, já evidenciado, bem como no artigo 129, I, da Constituição Federal e artigo 100 do Código Penal. A ação penal pública pode ser classificada em Ação Penal Pública Condicionada ou Ação Penal Pública Incondicionada, também chamada de Plena.

A Ação Penal Pública Plena ou Incondicionada se baseia na atuação do Ministério Público de ofício, dispensando-se a obrigatoriedade da vítima ou representante manifestar a sua vontade.

Já na Ação Penal Pública Condicionada ocorre o que a doutrina definiu por "condição de procedibilidade" que se fundamenta na indispensabilidade da manifestação da vítima ou de requisição do Ministro da Justiça. Ausentes estas representações, não pode o Ministério Público proceder com a ação penal e não pode também ser instaurado o inquérito pela autoridade polícia, conforme se entende dos artigos 5º § 4º. C/c artigo 24 do Código de Processo Penal e artigo 100, § 1º do Código Penal.

Por outro lado, há também a ação penal privada, que consiste na iniciativa tomada pela própria vítima, que provoca a judiciário através de queixa-crime apresentada neste caso por um advogado, e não por meio do Ministério Público. Tal categoria também apresenta classificações, quais sejam a Ação Penal Privada Exclusiva, a Ação Penal Privada Personalíssima e a Ação Penal Privada Subsidiária da Pública.

A Ação Penal Privada Exclusiva é a espécie de ação penal privada em que há o requisito já estabelecido na legislação. Neste caso, se a vítima morrer ou for declarada sua ausência, poderá ser sucedido por seu cônjuge, descendente, ascendente ou irmão, que assumirá a titularidade do direito da ação intentada, conforme previsão legal situada no artigo 31, CPP e artigo 100, § 4º., CP.

Já a Ação Penal Privada Personalíssima também é prevista na Lei tal qual a ação penal privada exclusiva. Porém, na ação privada personalíssima, apenas a vítima tem a possibilidade de atuar como titular da ação, sendo que, havendo morte

ou declaração de sua ausência, há impossibilidade de substituição. Por conseguinte, será declarada a extinção de punibilidade por decadência, se ainda não tiver realizado o intento da queixa-crime, visto que não há mais quem o possa fazer, ou por meio da perempção, tendo já sido realizada a instauração do processo, visto que não há possibilidade de outro prosseguir em favor do falecido ou ausente

Para fins de exemplificação deste tipo de ação penal, havia o “Crime de Adultério”, que não é mais tipificado como crime pelo ordenamento jurídico brasileiro, revogado pela Lei 11.106/05. Atualmente, portanto, via de exemplo, há apenas uma possibilidade de ação penal privada personalíssima, com previsão no artigo 236, Parágrafo Único, CP que é o crime de “Induzimento a erro essencial e ocultação de impedimento” ao casamento.

> Art. 236 - Contrair casamento, induzindo em erro essencial o outro contraente, ou ocultando-lhe impedimento que não seja casamento anterior:
>
> Pena - detenção, de seis meses a dois anos.
>
> Parágrafo único - A ação penal depende de queixa do contraente enganado e não pode ser intentada senão depois de transitar em julgado a sentença que, por motivo de erro ou impedimento, anule o casamento.

Por fim, a Ação Penal Privada Subsidiária da Pública é cabível aos casos em que a legislação não define a ação como privada, e sim como pública. O que a torna privada é quando há inércia por parte do titular da ação penal, que é o Ministério Público, ou seja, o titular não toma as medidas cabíveis ao prosseguimento correto da ação. Para tanto, há o prazo de 5 dias para réu preso e 15 dias para réu solto para que Ministério Público se manifeste. Havendo, mesmo assim, inércia, permite-se à vítima, seu representante legal ou seus sucessores a possibilidade de intentar a ação penal privada subsidiária da pública, conforme expressão constitucional do artigo 5º., LIX, CF e dos artigos 100, § 3º., CP e 29, CPP

4.3 PROCEDIMENTOS DO INQUÉRITO POLICIAL

Segundo Capez (2012), a chamada notitia criminis, que significa notícia do crime, refere-se ao momento em que a autoridade policial toma conhecimento, seja

este involuntário ou incentivado, de um fato supostamente definido como crime. As investigações, portanto, partem desta informação recebida pela autoridade.

A partir, então, do conhecimento da notitia criminis pela autoridade policial, na pessoa do Delegado de Polícia, deverá este iniciar os procedimentos que norteiam a investigação e que consistem, nos termos do artigo 6º do Código de Processo Penal, em:

> I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais;
>
> II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;
>
> III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;
>
> IV - ouvir o ofendido;
>
> V - ouvir o indiciado, com observância, no que for aplicável, do disposto no Capítulo III do Título Vll, deste Livro, devendo o respectivo termo ser assinado por duas testemunhas que Ihe tenham ouvido a leitura;
>
> VI - proceder a reconhecimento de pessoas e coisas e a acareações;
>
> VII - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;
>
> VIII - ordenar a identificação do indiciado pelo processo datiloscópico, se possível, e fazer juntar aos autos sua folha de antecedentes;
>
> IX - averiguar a vida pregressa do indiciado, sob o ponto de vista individual, familiar e social, sua condição econômica, sua atitude e estado de ânimo antes e depois do crime e durante ele, e quaisquer outros elementos que contribuírem para a apreciação do seu temperamento e caráter.
>
> X - colher informações sobre a existência de filhos, respectivas idades e se possuem alguma deficiência e o nome e o contato de eventual responsável pelos cuidados dos filhos, indicado pela pessoa presa.

O inquérito policial será formalmente instaurado de ofício, através de portaria da autoridade policial, ao lavrar o flagrante, ao haver representação formal da vítima ou se requerer o Juiz ou Ministério Público, de forma que se reduzam a termo todas as peças do inquérito, em um só processo, conforme previsão legal (GRECO FILHO, 2012, apud CAROLINO, 2017).

A instauração de ofício do inquérito policial ocorrerá, obrigatoriamente, ainda que sem fomento pela parte, em todo o caso em que a autoridade souber imediata e diretamente do fato, através de comunicação oral ou escrita realizada por qualquer indivíduo (delatio criminis simples), mediante comunicação anônima (notitia criminis

inqualificada), através da atividade diária (cognição imediata) ou ainda se houver prisão em flagrante (CAROLINO, 2017).

> Art. 5º Nos crimes de ação pública o inquérito policial será iniciado:
>
> I - de ofício;
>
> II - mediante requisição da autoridade judiciária ou do Ministério Público, ou a requerimento do ofendido ou de quem tiver qualidade para representá-lo.

Assim sendo, seguindo o entendimento da legislação penal, a instauração do inquérito policial se torna uma obrigação, de modo que seja um compromisso da autoridade a partir que se conhece o fato delituoso. O Delegado de Polícia, então, determina a instauração do inquérito e ordena as medidas necessárias a serem cumpridas.

Também pode ser instrumento que leve o conhecimento do crime à autoridade através de uma notícia, bem como por informação de outros policiais, por meio de mídia jornalística, lavratura de boletins em sua circunscrição, conhecimento passado por terceiros, dentre outras formas.

Em relação à instauração do inquérito policial através da requisição do Ministério Público, Capez (2012) contribui que o termo "requisição" remete a ordem, de modo que, ao receber o delegado uma requisição de instauração de inquérito por parte do juiz ou promotor de justiça, ocorre a imprescindibilidade do início das investigações. Assim, é indispensável que haja a especificação no documento de requisição, do fato criminoso que deve ser apurado.

Deverão ainda os juízes ou tribunais, sempre que perceberem existência de crime de ação pública em processos recebidos, encaminhar ao Ministério Público as devidas documentações para que ofereça a denúncia cabível. Entretanto, ausentes os elementos essenciais para que a denúncia seja apresentada, pode a Autoridade Judiciária requisitar que se instaure um inquérito policial com o objetivo de apurar os fatos. A mesma regra cabe também ao Ministério Público, toda vez que identificar prática criminosa em algum auto.

O ofendido pela prática criminosa também pode requerer à autoridade, encaminhando a esta uma petição, o início das investigações para elucidar os fatos. Poderá haver este requerimento tanto em crimes de ação pública, quanto no caso de

crimes de ação penal privada, sendo que, neste, não há interrupção do prazo decadencial pelo requerimento, devendo a parte se atentar.

O oferecimento da representação é requisito essencial para a instauração do inquérito nos casos de crime de ação penal pública condicionada a representação da vítima ou representante legal. A demonstração do princípio da oportunidade expressa a ação penal pública condicionada até o instante de ser a denúncia oferecida.

Também deverá o inquérito policial ser instaurado no caso de auto de prisão em flagrante, considerando-se a sua lavratura na oportunidade de prisão de determinado indivíduo e que, constam em seu texto, as informações do crime e da prisão.

Toda vez que uma pessoa é apreendida em flagrante delito e conduzida até uma Delegacia de Polícia, ocorre a lavratura do respectivo auto de prisão e, assim, dá-se início ao inquérito policial para apuração, juntada de provas e resolução do crime cometido.

4.4 INVESTIGAÇÃO DOS CRIMES CONTRA A HONRA EM MEIO CIBERNÉTICO

Segundo Fogliatto (2019), ao se analisar que o êxito das investigações de crimes informáticos depende de rapidez, em virtude da precisão de se buscar informações dos provedores, que não as guardam por muito tempo, há de se apreciar que é praticamente nula a efetividade das investigações realizadas por delegacias especializadas em crimes digitais.

Na percepção de Eudes Quintino (2012, apud TAVARES e REIS, 2014), o passo inicial a ser tomado em caso de cometimento de crime digital é verificar quem sofreu o dano para, então, se apurar qual ação será cabível ao caso: ação penal pública condicionada a representação ou ação penal pública incondicionada.

Sendo adequada a incondicionada terá a possibilidade a autoridade policial de instaurar o inquérito e posteriormente poderá ser proposta a ação penal, logo que houver a informação do cometimento criminoso e para que sejam apurados a autoria e a materialidade delitiva.

Desta maneira, para que as particularidades do crime praticado sejam constatadas, não se faz essencial que a vítima tenha manifestado anteriormente, de forma expressa, sua vontade.

Sob outra perspectiva, consistindo a ação penal em pública condicionada a representação, conforme previsão legal que se perfaz em regra, costumeiramente aplicada em boa parte das ocorrências, há indispensabilidade da representação pela vítima, a fim de que possibilite ao representante do Ministério Público propor a ação penal concernente (TAVARES e REIS, 2014).

Por consequência, não havendo a representação por conta da parte vitimada, não há como haver, através do Ministério Público, a iniciativa de propor a ação penal. Deverá a vítima (ou responsável legal, sendo a vítima incapaz) realizar a representação à autoridade tempestivamente dentro de seis meses depois de apurada a autoria do crime, conforme previu o legislador penal no art. 38 do Código de Processo Penal, e no art. 103 do Código Penal (TAVARES e REIS, 2014).

Portanto, se perpassado o prazo legal de seis meses, de caráter decadencial, a pretensão da punibilidade será extinta de modo que o criminoso ficará sem receber a devida sanção pela conduta ilegal.

No entendimento de Wendt e Jorge (2013), a investigação de crimes virtuais ocorre, basicamente, em duas etapas: uma preliminar chamada técnica e outra de decorrência, denominada etapa de campo, onde há efetivamente uma investigação por autoridade policial.

A etapa técnica para apuração de delitos informáticos envolvem atividades com intuito de localizar a máquina usada para fins da prática do crime, entre eles: examinar os dados contados pelo sujeito passivo do crime e entender o acontecido; direcionar a vítima a fim de manter as provas da prática criminosa e protegê-la em meio informático; obter inicialmente provas na rede de internet; formalizar o acontecimento através de boletim de ocorrência ou registro, instaurando-se a ação cabível; apurar inicialmente as informações contidas no meio informático em relação à autoria do crime, e-mails, registros e domínios de sites; formalizar as relações de provas obtidas e apurações prévias; apresentar formalização ao Poder Judiciário visando liberação judicial para realizar interferência de acessos, conexões ou informações, além da possibilidade de informações de cadastro tidos pelos provedores; examinar os dados informados pelos provedores (WENDT e JORGE, 2013).

Entendem Lima e Duarte (2020) que a atividade investigativa para apuração dos crimes cibernéticos, considerando-se a sua precariedade de evidências, tem início a partir da instauração do inquérito policial, realizado após o conhecimento da autoridade policial em delegacia especializada em crimes contra internet, prosseguindo com a colheita de provas.

4.5 MEIOS DE PROVA DOS CRIMES VIRTUAIS

Comparando, de certo modo, ao Cadastro de Pessoa Física (CPF) utilizado no Brasil para identificação das inúmeras pessoas por meio de números, os computadores e dispositivos informáticos que se ligam à internet podem e também recebem identificação por intermédio do chamado IP, que se descreve em Internet Protocol ou, em português, Protocolo de Internet. Esta codificação é único e possibilita uma conexão no mundo virtual entre incomensuráveis dispositivos (BRAGA, 2019).

Também neste prisma, é firmada a compreensão de Teixeira (2013, p. 43 apud LIMA e DUARTE, 2020) de que "o endereço IP, também conhecido como endereço lógico, é um sistema de identificação universal onde cada computador possa ser identificado exclusivamente, independente da rede em que esteja operando" e pode ser utilizado a fim de se constatar a responsabilidade do criminoso através de seu IP.

Para se atingir a finalidade de encontrar o autor de crimes virtuais, qualquer informação pode ser relevante. Os aparelhos e máquinas normalmente produzem informações que são alocadas e guardadas em algum banco de dados, através de mensagens e códigos criptografados, por meio dos Protocolos e de Internet (IP) das máquinas usadas para o crime. Desta forma, a autoridade policial colhe as informações e as provas mantendo-as em segurança e sem alterações para que sejam suporte para resolução do crime (TEIXEIRA, 2013 apud LIMA e DUARTE, 2020).

Por conseguinte, o Protocolo de Internet é, em virtude das particularidades presentes, uma das formas utilizadas para apuração e identificação de criminosos via internet. Todavia, é neste momento de conseguir o endereço de IP que aparecem as adversidades uma vez que há relevante burocracia para se obter as informações de quem utilizava a rede específica no momento exato da prática criminosa, por mais que seja possível a descoberta através de provedores de sites e de internet, além de poder

o criminoso se utilizar de softwares e afins que alteram e burlam a codificação do IP (BRAGA, 2019).

Dentre as possibilidades de indícios advindos das averiguações de crimes cibernéticos, compreende-se por mais relevante para a conclusão e apuração do crime investigado a obtenção do endereço de IP do criminoso (DORIGON, 2018).

A apresentação de prova convincente e certeira em casos de prática de crime em meio informático é um tanto quanto difícil, além de necessitar de grande tempo, empenho e qualificação profissional. Para a apuração do caso concreto há, entre outros procedimentos, a distinção entre a legitimidade de acesso e o provável acesso criminoso, a constatação do meio utilizado para invasão, verificação de informações de sistemas e redes a fim de encontrar o endereço de IP (Internet Protocol) responsável pelo acesso onde realizou a prática criminosa (ALCÂNTARA, 2014).

Tendo sido obtida a informação do Protocolo de Internet se faz necessária a identificação e fornecimento das informações pelo provedor utilizado na data e horário do crime. Entretanto, esta obtenção é muitas vezes burocrática e tardia, visto que esta localização de endereço virtual pode ser burlada pelos chamados crackers, ou ainda em consequência da falta de armazenamento das informações de acesso dos clientes, por parte dos provedores (ALCÂNTARA, 2014).

Tendo sido encontrada e identificada a máquina que estava conectada ao Protocolo de Internet utilizado para a prática do crime a apurar, inicia-se a chamada etapa de campo, onde serão dirigidas ao local as autoridades policiais para promover os procedimentos necessários à elucidação do caso (WENDT e JORGE, 2013).

No tocante à apresentação de provas em processo, prevê o Código de Processo Civil Brasileiro, em seu artigo 369 que serão admitidas as provas, em observância aos meios legais, assim como os moralmente legítimos, de forma a se provar a veracidade dos fatos alegados.

O intuito real das provas em processo é de convencer o magistrado acerca o assunto abordado pela ação proposta e, deste modo, sendo as provas físicas, devem possuir autenticação, segundo previsão no Código Civil e o Código de Processo Penal, ou, na ausência da imprescindibilidade, se fazem necessárias as devidas assinaturas (LIMA e DUARTE, 2020).

Neste sentido, corrobora Nucci (2019, p.15):

> Convencendo-se disso, o magistrado, ainda que possa estar equivocado, alcança a certeza necessária para proferir a decisão. Quando forma sua convicção, ela pode ser verdadeira (correspondente à realidade – verdade objetiva) ou errônea (não correspondendo à realidade – verdade subjetiva), mas jamais falsa, que é um “juízo não verdadeiro”. Sustentar que o juiz atingiu uma convicção falsa seria o mesmo que dizer que o julgador atingiu uma “certeza incerta”, o que é um contrassenso.

O emprego da internet como instrumento de prova tem surtido inúmeros efeitos positivos por todo o Poder Judiciário, sendo utilizada cada vez mais continuamente em processos. Consoante ao entendimento de Romano (2011), a comprovação virtual, ou prova eletrônica é um agrupamento de dados organizados em um seguimento de bits e confiada a uma base física digital.

Para lograr êxito na comprovação da prática delituosa, é recomendado que o ofendido busque o quanto antes preservar as provas para que se apure os fatos. Se praticados, por exemplo, via redes sociais, e-mails ou sites de bate papo, os crimes deixarão a prova escrita e pode a vítima realizar a impressão do material probatório ou pode salvar o conteúdo ofensivo, atentando-se sempre à preservação do cabeçalho. Estas provas podem ser salvas em mídias como CD-R ou DVD-R, formatos que não permitem mudanças.

Porém, salienta-se que estes elementos, por si só, não possuem valor probatório em juízo. Para que obtenham tal caráter, o ideal é que seja realizada uma ata notarial, que consiste num documento lavrado pelo profissional cartorário, dotadod e fé pública, que dará a credibilidade necessária para ser a prova apresentada em juízo.

Em se tratando da prática de infrações penais praticadas contra a honra, há algum tempo era realizada pessoalmente, oralmente ou de forma escrita. Porém, atualmente, em proveito de inúmeras tecnologias criadas continuamente, há cada vez mais facilidade no cometimento dos crimes virtuais pois o criminoso pode, ainda anonimamente, se utilizar de redes sociais, mensagens, e-mails e muito mais para desonrar alguma pessoa.

A apuração de autoria para identificação do responsável pela prática criminosa no meio virtual se limita, de certa forma, ao próprio âmbito digital. Assim, além da identificação do endereço de IP da máquina utilizada para a prática do crime, ocorre de a autoridade policial solicitar judicialmente a quebra de sigilo telemático com a devida interceptação telefônica, nos termos da Lei 9.296, de 24 de julho de 1996.

A interceptação telefônica é um dos meios relevantes para a comprovação da prática de crimes virtuais, especialmente os cometidos contra a honra, levando-se em conta que, hodiernamente, muitas das ofensas à honra são praticadas através do aparelho celular, por meio de ligações, de redes sociais como o Whatsapp, por exemplo.

Porém, como descrevem Wendt e Jorge (2013), não é admitida a aplicação da lei de interceptação telefônica para se colher os dados de acesso:

> De um modo equivocada, muitas vezes a quebra de sigilo telemático é indeferida pelo poder judiciário sob o argumento de que não respeita os requisitos relacionados com as referidas normas. Por exemplo, nos casos de crimes contra honra praticados por meio da internet, em que o juiz de direito equivocadamente indefere a representação para a quebra de sigilo telemático e argumenta que a pena para o crime é de detenção, enquanto a lei de interceptação telefônica exige a pena de reclusão.

Entretanto, pode ser alegado pela autoridade policial os artigos 22 e 23 do chamado Marco Civil da Internet (Lei 12.965 de 2014) que, independentemente da pena de reclusão ou detenção, atenta-se a apreciar as fundadas evidências da ocorrência do fato criminoso, a motivação plausível da solicitação para fins de investigação criminal e o período pertinente aos registros:

> Art. 22. 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.
>
> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
>
> I - fundados indícios da ocorrência do ilícito;
>
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
>
> III - período ao qual se referem os registros.
>
> Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

A solicitação de quebra de sigilo na comunicação de mensagens virtuais entre usuários de aplicativos como o Whatsapp, Facebook é constantemente solicitada. Considerando que estes serviços de comunicação são pautados por um envio

criptografado chamado "ponta a ponta", faz-se necessária a interceptação nos provedores de internet ou aplicativo. Contudo, esses procedimentos para facilitar a apuração do crime encontram, por vezes, empecilhos por receberem dos provedores a informação de ausência de armazenamento das mensagens ou que, ainda, não há instrumentos para interceptar as mensagens (SILVA, 2017).

Portanto, vários são os empecilhos impostos às investigações e a seus profissionais quando em busca de apurar os chamados crimes virtuais. Entre os já citados, como a indisponibilidade de dados e concessão de acessos pelos provedores, a negativa da concessão da interceptação telemática e telefônica, são também problemas encontrados para se resolver tais delitos a fraude na identificação do número de IP, a falta de investimentos para capacitação técnica dos profissionais responsáveis e a Cloud Computing.

Em se tratando das fraudes mediante os Protocolos de Internet (IP), os criminosos se utilizam dos chamados proxies ou ainda locais públicos como lan houses ou até mesmo as redes Wi-Fi disponíveis. Os proxies são utilizados para intermediar os pedidos de seus usuários, conectando este e o conteúdo a ser vislumbrado. São feitos com o objetivo de ocultar o verdadeiro endereço de IP de quem está usando, para que este seja protegido de ataques praticados em meio virtual. Porém, boa parte se utiliza deste mecanismo para se tomar por anônimo e praticar crimes, dificultando a identificação do criminoso (CAMPANHOLA, 2018).

Ao se utilizar dos proxies de forma anônima, não são deixados rastros, protegendo as informações pessoais ou o local de onde foi acessado, tornando o mecanismo colaborativo ao criminoso. Deste modo, ao esconder as informações de acesso, as investigações de crimes praticados no meio cibernético se tornam ainda mais complicadas.

Outra forma de atrapalhar os procedimentos investigativos contra os crimes de informática, nos termos de Dorigon e Soares (2017):

> [...] é a chamada cloud computing, conhecida como computação nas nuvens, sendo este o serviço que permite o acesso e a consequente execução de arquivos e programas diretamente pela internet, permitindo o acesso de todas as funcionalidades de um computador pessoal. Assim, os dados almejados não precisam estar, necessariamente, no computador do usuário, permitindo que este execute as mais diversas atividades, como acessar um arquivo de mídia ou executar um programa, sem que o tenha em seu computador, por meio de qualquer dispositivo de informática que possua acesso com a rede mundial de computadores.

Por outro lado, a capacitação técnica dos profissionais responsáveis pelas investigações e apuração dos crimes virtuais deve ser amplamente levada em consideração. O meio digital é cada vez mais rápido, a internet se torna a todo instante mais avançada e moderna.

Em virtude das constantes atualizações das tecnologias utilizadas pelos criminosos, é necessária também essa constância no preparo dos agentes que, algumas vezes, não conhecem as novidades da tecnologia para prestar a proteção da população de forma mais eficiente (CAMPANHOLA, 2018).

Entretanto, além da qualificação técnica dos profissionais, é preciso também se adequar às novas tecnologias e equipamentos, aparelhamentos úteis e cabíveis que sejam melhores para a execução dos procedimentos investigativos, de modo que o Estado não fique "um passo atrás" dos criminosos (CAMPANHOLA, 2018).

Os crimes cometidos contra a honra do ofendido, quando praticados em meio cibernético, equiparam-se aos demais delitos virtuais no que tange à dificuldade para sua resolução, visto que recebem uma série de impedimentos e dificuldades para colher as provas cabíveis e sancionar o criminoso.

4.6 MEDIDAS A SEREM TOMADAS EM CASO DE CRIME VIRTUAL

A responsabilidade para apuração e enfrentamento aos crimes cibernéticos ficou atribuída a delegacias especializadas, através da já citada Lei 12.735 de 2012, chamada também Lei Azeredo, que estabeleceu a instalação de “[...] setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado”.

Há algumas delegacias especializadas em crime digitais espalhadas pelo Brasil e, se não houver na cidade do ofendido, poderá ele se dirigir à delegacia mais próxima para informar o sofrimento do crime. Porém, é importante ressaltar que a preservação das provas é essencial para condução da investigação, não sendo indicada, por exemplo, a atitude de reiniciar (chamado reset) o aparelho após a invasão, que pode levar à extinção dos elementos de prova que seriam utilizados para comprovar a prática e punir o criminoso.

Portanto, se o indivíduo tiver sido alvo de um crime informático, deverá proceder imediatamente com a devida proteção e coleta das provas do ocorrido, pois é bem provável que o criminoso possa excluí-las, e após, proceder com a devida informação à autoridade policial, lavrando um boletim de ocorrência para que as medidas administrativas, investigativas e judiciais sejam tomadas.

CONSIDERAÇÕES FINAIS

Ao se iniciar o presente trabalho, verificou-se que a investigação policial para resolver e findar os crimes praticados em meio informático demanda de bastante tempo e que, por vezes não ocorre a eficácia pretendida.

Assim como outros crimes que passaram a ser praticados em âmbito virtual, os crimes contra a honra também passam pelos mesmos problemas, possibilitando muitas vezes ao infrator certa impunidade. Deste modo, fez-se necessária esta pesquisa para estudar sobre a eficácia e a celeridade da investigação policial em crimes digitais contra a honra.

Diante disso, este trabalho teve por objetivo geral constatar a celeridade e a eficácia despendidos perante a investigação policial em crimes contra a honra, de modo que foi alcançado, pois foram demonstradas várias lacunas a serem preenchidas para que o procedimento investigativo ocorra de melhor forma.

O objetivo inicial da primeira etapa do trabalho foi expor e explanar acerca do surgimento da internet e dos crimes virtuais praticados por meio dela, além de suas incidências, tendo sido cumprido.

Para seguimento ao foco principal da pesquisa, conceituaram-se os crimes contra a honra com as devidas previsões legais, explicando cada espécie penal para fins de compreensão.

Por último, restaram demonstradas as etapas investigativas que visam apurar os crimes de informática, externando como é intentado, como se procede e quais as formas de prova a serem utilizadas.

A hipótese de que a investigação policial em crimes digitais contra a honra não chega a um objetivo eficaz por ausência de empenho para resolução, de mais especificidade nas leis criadas, de instrumentos que viabilizem e da necessidade de longo tempo para resolução foi testada durante o trabalho e comprovada, visto que foram citados várias adversidades ao seu sucesso. Compreendeu-se que não há recursos tecnológicos suficientes para uso das autoridades policiais, e falta investimento e conhecimento tecnológico para solucionar os crimes cibernéticos.

Deste modo, o problema de pesquisa questionou se há celeridade e eficácia no procedimento de investigação dos crimes contra a honra cometidos em vias digitais, e obteve a resposta negativa.

A metodologia utilizada para este trabalho baseou-se em entendimentos firmados pela doutrina especialista em âmbito penal, cível e constitucional, assim como as previsões trazidas pela Legislação Brasileira, suas jurisprudências e artigos que discorrem sobre o assunto proposto.

Apesar do vasto conteúdo apresentado neste trabalho, encontraram-se limitações acerca do assunto no que tange especificamente aos crimes contra a honra, havendo, assim, escassez de fontes que norteiem de melhor forma os estudos sobre esta área.

Recomenda-se, portanto, que sejam realizadas novas pesquisas a respeito desse tema para que a sociedade em geral conheça os perigos que correm no "mundo digital", bem como seus direitos e deveres.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Maria Paula Castro de. **A evolução no combate aos crimes virtuais**. v. 2, n. 15, p. 17, 2015.

ARAS, Vladimir. **Crimes de Informática: uma nova criminalidade**. Disponível em: https://jus.com.br/artigos/2250/crimes-de-informatica. Acesso em: 18 set. 2020.

ARGACHOFF, Mauro. **A problemática da retorsão imediata no crime de injúria.** Disponível no site https://canalcienciascriminais.jusbrasil.com.br/artigos/328574858/a-problematica-da-retorsao-imediata-no-crime-de-injuria. Acesso em: 18 set. 2020.

BARRETO, Karolinne Brasil; BARRETO, Alesandro Gonçalves. **Investigação de crimes contra honra nas redes sociais e quebra de sigilo telemático para atribuição de autoria delitiva**. Disponível em: https://migalhas.uol.com.br/depeso/289280/investigacao-de-crimes-contra-honra-nas-redes-sociais-e-quebra-de-sigilo-telematico-para-atribuicao-de-autoria-delitiva. Acesso em: 04 out. 2020.

BRAGA, Diego Campos Salgado. **Métodos de investigações no âmbito cibernético**. Disponível em: https://jus.com.br/artigos/71463/metodos-de-investigacoes-no-ambito-cibernetico. Acesso em: 10 out. 2020.

BRANT, Cássio Augusto Barros. **A evolução da internet no Brasil e a dificuldade de sua regulamentação**. Disponível em: https://www.direitonet.com.br/artigos/exibir/1351/A-evolucao-da-internet-no-Brasil-e-a-dificuldade-de-sua-regulamentacao. Acesso em: 20 set. 2020.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Brasília, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 22 set. 2020.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da República Federativa do Brasil**, Brasília, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 21 set. 2020.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da República Federativa do Brasil**, Brasília, 23 abr. 2014. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 set. 2020.
CABETTE, Eduardo Luiz Santos. **O que é ação penal pública subsidiária da pública?**. Disponível em: https://eduardocabette.jusbrasil.com.br/artigos/121938044/o-que-e-acao-penal-publica-subsidiaria-da-publica. Acesso em: 16 out. 2020.

CAMPANHOLA, Nadine Finoti. **Crimes Virtuais Contra a Honra Conteúdo Jurídico**. Brasília, a. 2020. Disponível no site https://conteudojuridico.com.br/consulta/Artigos/51558/crimes-virtuais-contra-a-honra. Acesso em: 25 out. 2020.

CAROLINO, Anderson Zeferino dos Santos. **Inquérito Policial**. Disponível em: https://ambitojuridico.com.br/edicoes/revista-161/inquerito-policial/. Acesso em: 23 out. 2020.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais.** 2. ed. Rio de Janeiro, Lumen Juris, 2003.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. Disponível em: https://jus.com.br/artigos/1826/crimes-de-informatica/3. Acesso em: 15 out. 2020.
CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1. ed. São Paulo: Saraiva, 2011.

CAPEZ, Fernando. **Curso de Direito Penal - Volume 2 - parte especial arts. 121 a 212**. 20. ed. São Paulo: Saraiva Educação, 2020.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** São Paulo, a. 2012. Disponível no site https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 28 out. 2020.

CRIMINAIS, Canal Ciências. **As Leis nº 12.735/2012 e 12.737/2012 e os crimes digitais: acertos e equívocos legislativos**. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/artigos/201526971/as-leis-n-12735-2012-e-12737-2012-e-os-crimes-digitais-acertos-e-equivocos-legislativos. Acesso em: 22 set. 2020.

CUNHA, Rogério Sanches. **Teses do STJ sobre os crimes contra a honra (1ª parte).** Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2019/08/13/teses-stj-sobre-os-crimes-contra-honra-1a-parte/. Acesso em: 03 nov. 2020.

DELMANTO, Celso. **Crimes contra a honra**. Rio de Janeiro, a. 2002. Disponível em https://www.direitonet.com.br/resumos/exibir/107/Crimes-contra-a-honra. Acesso em: 15 nov. 2020.

DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade**. Disponível em: https://jus.com.br/artigos/63549/crimes-ciberneticos-

dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade/2. Acesso em: 06 nov. 2020.

FOGLIATTO, Juliana. **Os crimes cibernéticos e os meios que a polícia utiliza para a identificação dos criminosos**. Disponível em: https://jus.com.br/artigos/77225/os-crimes-ciberneticos-e-os-meios-que-a-policia-utiliza-para-a-identificacao-dos-criminosos. Acesso em: 08 nov. 2020.

FONTES, Edison. **Segurança da Informação: o Usuário Faz a Diferença.** 1. ed. São Paulo: Saraiva, 2006.

G1. **Lei 'Carolina Dieckmann', que pune invasão de PCs, entra em vigor**. Disponível em: http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html. Acesso em: 10 nov. 2020.

G1. **Cresce uso da internet durante a pandemia, e crimes virtuais aumentam quase 50% em MG**. Disponível em: https://g1.globo.com/mg/minas-gerais/noticia/2020/05/22/cresce-uso-da-internet-durante-a-pandemia-e-crimes-virtuais-aumentam-quase-50percent-em-mg.ghtml. Acesso em: 13 nov. 2020.

GRECO, Rogério. **Curso de direito penal: parte geral.** 17. ed. Niterói: Impetus, 2015.

HIGA, Paulo. **Juiz manda tirar WhatsApp do ar no Brasil**. Disponível em: https://tecnoblog.net/174326/juiz-bloqueio-whatsapp-brasil/. Acesso em: 10 nov. 2020.

JÚNIOR, Jose Mendes da Silva. **Características do inquérito policial**. Disponível em: https://ambitojuridico.com.br/edicoes/revista-140/caracteristicas-do-inquerito-policial/. Acesso em: 11 nov. 2020.

JUSTIFICANDO. **Crimes digitais: quais são, quais leis os definem e como denunciar**. Disponível no site https://www.justificando.com/2018/06/25/crimes-digitais-quais-sao-quais-leis-os-definem-e-como-denunciar/. Acesso em: 12 nov. 2020.

LAVADO, Thiago. **Uso da internet no brasil cresce e 70% da população está conectada.** Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/08/28/uso-da-internet-no-brasil-cresce-e-70percent-da-populacao-esta-conectada.ghtml. Acessado em: 17 nov. 2020.

LIBRELON, Rachel. **Proposta insere no Código Penal o crime de estelionato virtual.** Disponível no site https://www.camara.leg.br/noticias/680058-proposta-insere-no-codigo-penal-o-crime-de-estelionato-virtual/. Acesso em: 15 nov. 2020.

LIMA, Adriano Gouveia; DUARTE, Adrienne. **Crimes virtuais: conceito e formas de investigação**. Disponível em: https://www.boletimjuridico.com.br/artigos/direito-penal/10382/crimes-virtuais-conceito-formas-investigacao. Acesso em: 16 nov. 2020.

MARINS, André Rodrigues. **Aspectos Controvertidos dos Crimes Contra a Honra Praticados pela Rede Mundial de Computadores.** Disponível em: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/1semestre2010/trabalhos_12010/andremarins.pdf&ved=2ahUKEwilx4fG7Y_tAhXtCrkGHR-5BXYQFjAAegQIBRAB&usg=AOvVaw2t93OpOCn0lHz8HPcC5baR. Acesso em: 14 nov. 2020.

MARTINS, Patrícia Vieira. **Crimes Cibernéticos e a Correlação Ao Crime Contra Honra**. Disponível em: http://revistas.unifenas.br/index.php/BIC/article/download/192/146. Acesso em: 17 nov. 2020.

MINAS, Estado de. **Crimes cibernéticos disparam e expõem fragilidade tecnológica no Brasil**. Disponível em: https://www.em.com.br/app/noticia/politica/2019/08/04/interna_politica,1074689/crimes-ciberneticos-disparam-expoem-fragilidade-tecnologica-no-brasil.shtml. Acesso em: 13 nov. 2020.

NETO, Mário Furlaneto; GUIMARÃES, José Augusto Chaves. Crimes na Internet: elementos para uma reflexão sobre a ética informacional. **R. CEJ**. Brasília, v. 1, n. 20, p. 67-73, 2003.

NETO, Pedro Américo de Souza. **Crimes De Informática.** 2009. 92 f. Monografia (Graduação em Direito) - Universidade do Vale do Itajaí – UNIVALI, Itajaí.

PAESANI, Liliana Minardi. **Direito e Internet - Liberdade de Informação, Privacidade e Responsabilidade Civil.** 7. ed. São Paulo: Atlas, 2014.

PLANALTO. **Código Civil**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 07 nov. 2020.

PLANALTO. **Código de Processo Penal**. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm>. Acesso em: 30 out. 2020.

PLANALTO. **Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em 03 nov. 2020.

PLANALTO. **Constituição Federal de 1988**. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 30 out. 2020.

RIBEIRO, Fellype. **Breve relato da história dos crimes cibernéticos**. Disponível em: < https://idireitodigital.wordpress.com/2015/04/14/breve-relato-da-historia-dos-crimes-ciberneticos/>. Acesso em: 17 nov. 2020.

ROCHA, Carolina Borges. **A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012.** Disponível em: https://jus.com.br/artigos/25120/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-ciberneticos-e-a-lei-12-737-2012. Acesso em: 19 nov. 2020.

ROCHA, Josemary M. Freire Rodrigues de Carvalho. et al. A tutela Jurídica Sobre Os Crimes Cibernéticos. **Revista Campo do Saber**, v. 1, n. 1, p. 41-57, 2015.

ROMANO, Raquel Alexandra. **Documento eletrônico pode ser utilizado como prova**. Disponível em: https://www.conjur.com.br/2011-fev-23/possivel-verificar-autenticidade-prova-documental-eletronica. Acesso em: 18 nov. 2020.

SCHAUN, Guilherme. **Uma lista com 24 crimes virtuais**. Disponível em: https://guilhermebsschaun.jusbrasil.com.br/artigos/686948017/uma-lista-com-24-crimes-virtuais. Acesso em: 16 nov. 2020.

SCHMIDT, Guilherme. **Crimes Cibernéticos**. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em: 18 nov. 2020.

SILVA, Camila Requião Fentanes da. **Análise das Leis nº 12.735/2012 e 12.737/2012 e a (des)necessidade de uma legislação específica sobre crimes cibernéticos**. Disponível em: https://jus.com.br/artigos/32265/analise-das-leis-n-12-735-2012-e-12-737-2012-e-a-des-necessidade-de-uma-legislacao-especifica-sobre-crimes-ciberneticos. Acesso em: 16 nov. 2020.

SILVA, Guilherme Pereira da; DINIZ, Hemilly Maciel. **HACKER e CRACKER: Um estudo sobre suas diferenças e os crimes virtuais.** 2017. 16 f. Monografia (Graduação Técnico em Informática) - Instituto FederEducação em Ciência Tecnologia do Triângulo Mineiro, Paracatu.

SILVEIRA, Neil. et al. **Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann**. Disponível em: https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz-da-lei-carolina-dieckmann. Acesso em: 14 nov. 2020.

SOARES, Samuel Silva Basilio. **Os crimes contra honra na perspectiva do ambiente virtual.** Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/os-crimes-contra-honra-na-perspectiva-do-ambiente-virtual/amp/. Acesso em: 17 nov. 2020.

TAVARES, Adriano Lopes; REIS, Rafael Rocha dos. **Crimes De Informática.** Anápolis, a. 2014. Disponível no site https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiCgODbp8jsAhVFHLkGHQCKDesQFjAAegQIAhAC&url=http%3A%2F%2Fperiodicos.unievangelica.edu.br%2Findex.php%2Frevistajuridica%2Farticle%2Fdownload%2F1070%2F1012%2F&usg=AOvVaw2bSsi1J-6JMHqp5OlSeIDP. Acesso em: 16 nov. 2020.

TATEOKI, Victor Augusto. **Classificação dos Crimes Digitais**. Disponível em: https://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais. Acesso em: 18 nov. 2020.
VARGAS, Joana Domingues; RODRIGUES, Juliana Neves Lopes. Controle e cerimônia: o inquérito policial em um sistema de justiça criminal frouxamente ajustado. **Revista Sociedade e Estado**. v. 26, n. 1, p. 77-96, 2011.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. 2. ed. Rio de Janeiro: Brasport, 2013.

YOUTUBE. **Características do Inquérito Policial | Processo Penal | Quer entender Direito ? | Mapa Mental**. Master Juris. Disponível em: https://www.youtube.com/watch?v=QL79zliFdrg. Acesso em: 19 nov. 2020.