UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
DEPARTAMENTO DE DIREITO PÚBLICO

JÉSSICA JENIFER DE OLIVEIRA ALVES

CAMINHOS PARA RESPONSABILIZAÇÃO EFETIVA DOS AUTORES DE CRIMES CIBERNÉTICOS

FORTALEZA
2022

JÉSSICA JENIFER DE OLIVEIRA ALVES

CAMINHOS PARA RESPONSABILIZAÇÃO EFETIVA DOS AUTORES DE CRIMES CIBERNÉTICOS

Monografia submetida à Coordenação do Curso de Graduação em Direito, da Universidade Federal do Ceará, como requisito parcial para a aquisição do título de Bacharel em Direito. Área de concentração: Direito Penal.

Orientador: Prof. Dr. Sergio Bruno Araújo Rebouças.

FORTALEZA

2022

Dados Internacionais de Catalogação
na PublicaçãoUniversidade Federal do Ceará
Sistema de Bibliotecas

A1c Alves, Jéssica Jenifer De Oliveira.
Caminhos para responsabilização efetiva dos autores de crimes cibernéticos / Jéssica Jenifer de Oliveira Alves. – 2022.
69 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito,Curso de Direito, Fortaleza, 2022.
Orientação: Prof. Dr. Sergio Bruno Araújo Rebouças.

1. Crimes virtuais . 2. Alterações legislativas. 3. Responsabilização dos autores. 4. Procedimentosinvestigativos. I. Título.

CDD 340

JÉSSICA JENIFER DE OLIVEIRA ALVES

CAMINHOS PARA RESPONSABILIZAÇÃO EFETIVA DOS AUTORES DE CRIMES CIBERNÉTICOS

Monografia submetida à Coordenação do Curso de Graduação em Direito, da Universidade Federal do Ceará, como requisito parcial para a aquisição do título de Bacharel em Direito. Área de concentração: Direito Penal.

Orientador: Prof. Dr. Sergio Bruno Araújo Rebouças.

Aprovada em: __/__/____.

BANCA EXAMINADORA

_____
Prof. Dr. Sergio Bruno Araújo Rebouças (Orientador)
Universidade Federal do Ceará (UFC)

_____
Profa. Me. Vanessa de Lima Marques Santiago Sousa
Universidade Federal do Ceará (UFC)

_____
Prof. Me. Matheus Casirimo Gomes Serafim
Universidade Federal do Ceará (UFC)

Dedico este trabalho a Deus ea minha família, sanguínea e de coração, por todo apoio e torcida ao longo dos anos.

AGRADECIMENTOS

A Deus pelo dom da vida, por me fortalecer e iluminar em todos os momentos.

Aos meus pais que me proporcionaram o melhor estudo que podiam e que sempre acreditaram nessa conquista.

À minha mãe que espelhou o seu sonho na minha vida e hoje tenho a honra e o prazer de concretizá-lo.

Ao meu pai que trabalhou incansavelmente todos os dias para me prover conforto e ensino de qualidade.

À minha avó Nicinha que sempre sonhou comigo e foi um grande apoio e incentivo nessa trajetória.

A todos os meus familiares que sempre lançaram sobre a minha vida palavras de encorajamento.

Ao meu marido, Fábio Luiz, que foi fundamental durante a graduação e, com certeza, será durante toda minha vida. Ele me mostrou o real significado de amor e cumplicidade entre duas almas. Sem dúvidas, sua tranquilidade é meu ponto de equilíbrio.

À minha amiga, Maria do Socorro, que divide comigo as melhores piadas e em quem deposito uma confiança imensa. Sempre fiz questão de ouvir suas palavras, pois delas tive muitos direcionamentos. Agradeço pelas melhores memórias e conversas.

Aos meus filhos pets, Nina, Théo e Brucutu, que estiveram comigo no quarto do escritório durante as incontáveis horas de estudo para graduação, preparação para o Exame da Ordem e todo o processo de pesquisa e escrita deste trabalho.

Aos colegas da turma de graduação, pela troca de apoio e compreensão durante cinco anos de curso.

À Universidade Federal do Ceará, pelo acesso ao conhecimento que de fato contribuiu para formação de um ser humano mais completo e capacitado.

Ao Prof. Dr. Sérgio Bruno, pela aceitação do convite à orientação deste trabalho de conclusão de curso, cujo desempenhou com excelência.

Aos professores participantes da banca examinadora: Profa. Me. Vanessa de Lima Marques Santiago Sousa e Prof. Me. Matheus Casirimo Gomes Serafim, pelo tempo, pelas valiosas colaborações e sugestões.

RESUMO

Esse estudo tem como objetivo geral verificar quais são os caminhos para que os autores dos crimes cibernéticos sejam responsabilizados de forma efetiva. Nesse sentido, com o intuito de alcançar a finalidade principal, essa pesquisa traça objetivos específicos. Primeiramente, é feita a análise histórica da relação entre a internet e o direito, tendo como ponto de partida a Lei 12.965/2014, conhecida como Marco Civil da Internet e a conceituação dos crimes virtuais. Em seguida, estudam-se as principais alterações legislativas que trouxerem mudanças para o ordenamento jurídico e a responsabilização dos autores, com base na Lei 12.735/2012 – Azeredo, Lei 11.829/2008 – Pedofilia na Internet, Lei 12.737/2012 – Carolina Dieckmann, dentre outras. Em um terceiro momento, verifica-se a possibilidade de aplicação da responsabilidade civil aos autores dos crimes, bem como a viabilidade de indenização e afins. E por fim, faz-se um levantamento das mudanças ocorridas na organização e no método de procedimento investigativo do sistema jurídico nacional. A metodologia aplicada é uma análise qualitativa, de natureza bibliográfica, com resultado puro e objetivo descritivo. Conclui-se que os crimes virtuais têm mobilizado sobremaneira o legislador e a máquina judiciária, uma vez que importantes alterações legislativas foram sancionadas, além do aperfeiçoamento do aparato judicial nos procedimentos investigativos e da efetiva responsabilização dos autores em processos criminais e cíveis, com aplicação de pena e indenização por danos morais.

Palavras-chaves: crimes virtuais; alterações legislativas; responsabilização dos autores; procedimentos investigativos.

ABSTRACT

This study has the general objective of verifying which are the ways for the authors of cyber crimes to be effectively held accountable. In this sense, in order to achieve the main purpose, this research outlines specific objectives. First, a historical analysis of the relationship between the internet and the law is made, starting with Law 12.965/2014, known as Marco Civil da Internet and the conceptualization of virtual crimes. Then, the main legislative changes that bring changes to the legal system and the accountability of authors are studied, based on Law 12.735/2012 – Azeredo, Law 11.829/2008 – Pedophilia on the Internet, Law 12.737/2012 – Carolina Dieckmann, among others. In a third moment, there is the possibility of applying civil liability to the perpetrators of the crimes, as well as the feasibility of compensation and the like. Finally, a survey is made of the changes that have taken place in the organization and method of investigative procedure in the national legal system. The applied methodology is a qualitative analysis, of bibliographical nature, with pure result and descriptive objective. It is concluded that virtual crimes have greatly mobilized the legislator and the judiciary, since important legislative changes were sanctioned, in addition to the improvement of the judicial apparatus in investigative procedures and the effective accountability of perpetrators in criminal and civil proceedings, with the application of penalty and compensation for moral damages.

Keywords: virtual crimes; legislative changes; r/ accountability of authors; investigative procedures.

LISTA DE ABREVIATURAS E SIGLAS

CPC	Código de Processo Civil
CC	Código Civil
CPP	Código de Processo Penal
CP	Código Penal
ECA	Estatuto da Criança e do Adolescente
IP	Internet Protocol
OMS	Organização Mundial da Saúde
SINESP	Sistema Nacional de Informações de Segurança Pública
VPN	*Virtual Private Network* (Rede Privada Virtual)

SUMÁRIO

1 INTRODUÇÃO

A internet possui a capacidade de difundir rapidamente uma série de informações como nunca antes. É verdade que seus usuários possuem a facilidade de acessar qualquer conteúdo que tenham interesse em poucos segundos por diversos meios tecnológicos. Esta ferramenta desempenha um papel fundamental na vida humana. Com ela é possível estudar de forma mais eficiente, encontrar e falar com amigos e familiares, realizar transações bancárias, guardar documentos importantes, bem como fotos e recordações afetivas e tantas outras possibilidades.

Tal relevância foi ainda mais difundida com a chegada da pandemia do Coronavírus, em que foi possível "digitalizar" ainda mais as principais relações dos indivíduos. Nesse período, diversas empresas se viram obrigadas a manter seus funcionários trabalhando de casa, por meio da internet e concedendo acesso às VPNs (SANTANA JUNIOR; WOLKOF, 2021, s. p.; GANDRA, 2020, s. p.). Além disso, a população brasileira tornou-se ainda mais adepta às compras *online*, sejam elas de supermercado, farmácia, itens de vestuário, cosméticos, outros produtos de beleza e utilidades domésticas (LIN, 2021, s. p.; NASCIMENTO, 2022, s. p.).

Diante deste contexto pandêmico, as universidades também precisaram se adaptar ao *lockdown* e diversas outras restrições impostas pelo Governo sob recomendação da Organização Mundial de Saúde (OMS). Sendo assim, alunos e professores adequaram-se às aulas remotas com ajuda da internet e outros aplicativos (LUNARDI, 2021). Além disso, o *marketing* digital cresceu exponencialmente, sobretudo, durante o referido momento. Os usuários da internet, mais precisamente das redes sociais como *Instagram*, *Facebook* e *TikTok* consumiram demasiadamente cursos *online*, *e-books* e treinamentos diversos de acordo com os seus interesses. Todas essas oportunidades foram usufruídas pelos usuários sem sair de casa (ORLANDO, 2021).

Ora, ainda que tamanha praticidade seja um excelente bônus à comunidade humana, não seria estranho se um ônus também viesse atrelado. Segundo o Jornal G1, em 2020 as denúncias de crimes cometidos pela internet quase que dobraram em relação a 2019 (DENÚNCIAS..., 2021, s. p.). Os principais crimes apontados na matéria são

incitações ao neonazismo, racismo, discriminação, violência contra mulher e pornografia infantil.

O comportamento adotado pelos criminosos ao usar o meio digital para dar continuidade às suas práticas delituosas se dá pela sensação de que a internet é uma "terra sem lei" e que a impunidade é certa. Além disso, são pessoas que se escondem, muitas vezes, atrás de um perfil falso para incitarem ódio e violência, além de tirar proveito econômico de pessoas ingênuas ou sem instrução.

Contudo, em razão do princípio da inércia da jurisdição, que estabelece que o processo judicial deve ser promovido pela parte interessada, se faz necessário que as vítimas denunciem e busquem a responsabilização dos criminosos perante o Judiciário. Todavia, por se tratar de um problema relativamente novo, é temerário que a resposta dada pelo órgão competente não seja suficiente para reparar os danos sofridos pelas vítimas.

Por isso, é preciso a criação de novas leis que tipifiquem as condutas específicas como crimes, com penas inibitórias para que os atos criminosos provenientes do meio digital sejam freados de forma efetiva. Além disso, a possibilidade de recorrer ao judiciário por indenizações ao terem seus direitos de personalidade violados deve ser garantida como forma de tentar suprir o dano sofrido e servir de caráter pedagógico para o réu da demanda.

Diante desse cenário, essa pesquisa se propõe a responder o seguinte questionamento: quais são os caminhos para que os autores dos crimes cibernéticos sejam responsabilizados? Por isso, o principal objetivo dessa pesquisa é fazer uma análise de como o judiciário tem absolvido esta demanda e quais são as consequências previstas no ordenamento jurídico na seara cível e criminal para os autores de tais delitos. Sendo assim, com a finalidade de alcançar o intuito principal, esse estudo traçam-se alguns objetivos específicos divididos por capítulos.

O primeiro capítulo contém uma breve introdução sobre a relação da internet com o ordenamento jurídico brasileiro, bem como a relevância dos direitos e garantias dos usuários à luz da Lei14.965/2014, popularmente conhecida como Marco Civil da Internet, que trouxe uma regulamentação mínima para os servidores de internet e alterou o entendimento da jurisprudência pátria acerca da responsabilização (BRASIL, 2014), além da conceituação dos crimes virtuais sob a perspectiva de doutrinadores e juristas.

No segundo capítulo, verificam-se as inovações e alterações legislativas relevantes sobre a tipificação das condutas criminosas no âmbito virtual. Aborda-se uma análise descritiva sobre a construção de críticas acerca da Lei 11.829/2008 que abordou a pornografia infantil no meio virtual, as Leis 12.735/2012 e 12.737/2012, respectivamente conhecidas como, Azeredo e Carolina Dieckmann, e outras leis que estipularam penas e condutas específicas para os crimes contra a honra, ao patrimônio e à dignidade sexual praticados por meios informáticos e no contexto da internet.

No terceiro capítulo, aborda-se o conceito de responsabilidade civil e a sua aplicabilidade aos criminosos virtuais. Além disso, levantam-se nos principais Tribunais de Justiça dos estados do Brasil, quais sejam, Tribunal de Justiça do Estado de São Paulo (TJSP), Tribunal de Justiça do Estado de Minas Gerais (TJMG), Tribunal de Justiça do Estado de Tocantins (TJTO) e Tribunal de Justiça do Estado do Rio de Janeiro (TJRJ), além do Superior Tribunal de Justiça (STJ), decisões judiciais que estão relacionadas aos crimes cibernéticos para fins de verificar se as providências tomadas pelos operadores do judiciário foram satisfatórias no que diz respeito à responsabilização cível dos autores de crimes digitais.

No quarto capítulo, compreende-se a necessidade de aparatar os operadores do judiciário para que sejam capazes de entender quais são os trâmites necessários para trazer a resolução do conflito no âmbito digital de forma eficiente, resguardando todos os direitos da vítima e identificando os autores. Nesse momento, a verificação acerca dos procedimentos investigativos específicos é redigida de forma descritiva, pois considera-se uma inovação no trabalho da Policia Civil e Federal, além do Ministério Público. Ademais, a perspectiva do trabalho e atuação da defesa desempenhada por advogados e Defensoria Pública é também colacionada.

Destarte, para que tais objetivos sejam alcançados, adota-se uma abordagem ao problema de maneira qualitativa, utilizando-se fontes de conhecimento como maneira de descrever o conceito de crimes virtuais e observar o comportamento dos usuários de internet que estão mal-intencionados, além de verificar a responsabilização desses na seara cível e criminal.

Com relação ao procedimento técnico, a presente pesquisa é classificada como bibliográfica, uma vez que se utiliza do estudo de referências bibliográficas já publicadas sobre o tema dos crimes virtuais, como Sales (2013),Pinheiro (2021), Jesus (2022), Greco (2014), Nucci (2020), Tomasevicius Filho (2016), as jurisprudências

pátrias dos Tribunais de Justiça de São Paulo, Tocantins, Rio de Janeiro e Minas Gerais, além do Superior Tribunal de Justiça, além da legislação pátria como, por exemplo, as Leis nº 11.829/2008, nº 12.735/2012, nº12.737/2012, nº 12.965/2014 e nº 13.718/2018.

Ademais, a utilização dos resultados é de natureza pura, uma vez que busca contribuir de maneira teórica com o acúmulo de conhecimentos sobre crimes virtuais e os meios de responsabilização dos seus autores.

Por fim, o objetivo da pesquisa é de caráter descritivo, pois relata de maneira profunda o tema abordado, com levantamento bibliográfico denso que permite analisar de maneira segura o problema apontado.

2 A INTERNET E O DIREITO

Na pré-história, o homem tinha uma única preocupação: a sobrevivência. De forma simplória, o indivíduo ocupava-se em buscar alimento e proteção dos seus predadores. Todavia, ele tinha um diferencial com relação aos demais seres vivos: a sapiência. Logo descobriu que poderia fazer fogo para aquecer-se, produzir armas para facilitar a caça que proporcionaria além do alimento, vestes e adornos. (DEFLEUR; BALLROKEACH, 1993, p. 11)[1].

Ademais, o ser humano possui uma habilidade ímpar: a comunicação. (DIAS, 2013, p. 22).Os autores DeFleur e Ball-Rokeach (1993) aduzem que a comunicação humana possui uma evolução delineada. Nesse sentido, são delimitados por eras e idades que são: Era dos Símbolos e Sinais; Idade ou Era da Fala e da Linguagem; Era da Escrita; Idade ou Era da Imprensa; Idade ou Era da Comunicação de Massa; Era dos Computadores. É possível observar as primeiras tentativas de transmissão de mensagens ainda no período pré-histórico com as pinturas rupestres (BRAGANÇA, 2009, p. 1-5).

À medida que o indivíduo se organiza como uma sociedade, novas formas de comunicação são desenvolvidas. Bragança (2009) pontua ainda que na Mesopotâmia surge a escrita, no Egito os Correios, no Império Romano o Jornal. E assim cada cultura se desenvolve e constrói modalidades de comunicação, gerando mais tarde a invenção do telégrafo, depois do rádio, telefone, televisão, computador, e por fim, da internet, em meados de 1960, no contexto da Guerra Fria entre os Estados Unidos e a União Soviética (LIMA; MARCATO, 2022).

No Brasil, a internet chegou em meados dos anos 80 e o seu acesso era restrito apenas à comunidade acadêmica que tinha por finalidade conectar instituições de ensino do Brasil com os Estados Unidos. Somente no ano 1996 foi difundida e comercializada para os demais usuários, ou seja, para população. Todavia, era um

[1] A experiência inicial da espécie humana em nosso planeta é amiúde descrita por arqueólogos e outros eruditos em termos de eras e idades. Exemplos são as Idade da Pedra Antiga, Média e Nova, ou as Idades do Bronze e do Ferro. Estes nomes referem-se a períodos – alguns mais ou menos curtos e outros multisseculares – durante os quais os primitivos homens faziam ferramentas com diferentes materiais ou criavam diferentes tecnologias para resolver problemas na produção de comida ou construção de armas. Esses intervalos e suas numerosas subdivisões (Paleolítico, Mesolítico, Neolítico, etc.) são indiscutivelmente úteis para traçar a evolução da confecção de ferramentas e da tecnologia, mas falham totalmente sob o aspecto bem mais fundamental da existência humana – a capacidade de comunicar-se. (DEFLEUR;BALLROKEACH, 1993, p. 11).

serviço caro e somente pessoas com poder aquisitivo mais elevado poderiam fazer uso no primeiro momento (FERREIRA; PEDROSA, 2021, s. p.).

Ademais, um estudo mais recente realizado em janeiro de 2022 por Simon Kemp (2022), disponibilizado na plataforma Datareportal, levantou que cerca de 4,95 bilhões de pessoas possuem acesso à internet, ou seja, 62,5% da população mundial. Ora, percebe-se que o acesso à rede mundial dos computadores é crescente e cada vez mais está presente na vida do ser humano. Uma vez que o indivíduo tem acesso a essa ferramenta e percebe que ela facilita suas atividades básicas, estase torna inerente ao seu dia a dia.

Sendo assim, Inouye (2016) afirma que a massificação de usuários reunidos na internet a torna uma importante ferramenta de utilização dos direitos humanos, assim como uma potência na violação desses. Nesse sentido, cumpre salientar que as conquistas de direitos são feitas no decorrer da história e da importância dada pelo cidadão no momento em questão.

Foi assim com o sufrágio universal, abolição à escravatura e a jornada de trabalho reduzida, por exemplo. Bobbio (2004, p. 20) reforça que “os direitos do homem são direitos históricos, que emergem gradualmente das lutas que o homem trava por sua própria emancipação e das transformações das condições de vida que essas lutas produzem”.

Portanto, Inouye (2016) interpreta que o acesso à internet é, sobretudo, um meio que garante outros direitos humanos também importantes, quais sejam: liberdade de expressão, opinião e direito à educação. Sendo assim, o Estado que restringe o acesso dos cidadãos à internet sem qualquer justificativa não deve ser encorajado, devendo este promover políticas públicas para garantir o acesso universal deste meio às pessoas com o objetivo de difundir o direito à todas as classes.

Contudo, o advento da internet trouxe mais um desafio para o Direito, uma vez que verificou-se que o dinamismo da internet deve ser acompanhado por esta área do saber devido ao seu valor fundamental, além do que é necessário assegurar a previsibilidade das condutas e das estruturas econômicas (ROTUNDO, 2018).

Diante disto, o surgimento da internet trouxe questões ligadas a diversos ramos do Direito Público e Privado, tais como as novas modalidades de condutas criminosas, o direito à liberdade de expressão, à privacidade e o acesso à informação.

Sendo assim, no final de 2005 é fundada uma associação civil de direito privado chamada *SaferNet* Brasil visando a promoção e a defesa dos Direitos Humanos

na internet no país. A criação da instituição se deu pela urgência em resolver os problemas ocasionados por usuários mal-intencionados neste meio de comunicação, pois a violação contra os Direitos Humanos, bem como a ocorrência de crimes era latente na Rede Mundial de Computadores (SAFERNET, 2022).

Todavia, o Brasil não possuía políticas ou leis concretas que de fato fossem capazes de enfrentar o ônus ocasionado pelo uso da internet. Desse modo, a *SaferNet* tornou-se referência no combate à casuística e tem se fortalecido ainda de forma veemente, uma vez que possui cooperação firmada com órgãos judiciários, como por exemplo, o Ministério Público Federal (SAFERNET, 2022).

Ademais, a associação cuidou em criar a Central Nacional de Denúncias de Crimes Cibernéticos que é conduzida em parceria com os Ministérios Públicos e a Secretaria de Direitos Humanos da Presidência da República (SDH) para fortalecer as ações de combate aos *cybercrimes* contra os Direitos Humanos. Além disso, desempenha um importante papel instrutivo e educacional em seu site afim de promover o uso consciente da Internet (SAFERNET, 2022).

Destarte, ainda que o trabalho desenvolvido pela associação retro mencionada tenha destaque e apoio do sistema judiciário brasileiro, ainda não foi suficiente para atingir o objetivo principal da demanda, qual seja, a responsabilização específica e necessária com fim pedagógico e que trouxesse amparo efetivo à vítima, uma vez que não freou os crimes cibernéticos.

Entende-se que é preciso que a mobilização seja compreendida tanto pelo Poder Legislativo, formulando leis que regulem o serviço de internet e preveja consequências personalizadas àqueles que se utilizam da Rede Mundial de Computadores de maneira criminosa, quanto pelo sistema judiciário, que deverá investir na sua tecnologia e na capacitação dos seus servidores e membros, além das adequações precisas nos métodos investigativos desempenhados pela Policia Civil e Federal.

2.1 Lei 12.965/2014 – Marco Civil da Internet

Ainda que a urgência pela regulamentação da rede mundial de computadores tenha sido levantada pelos juristas, o Brasil foi retardatário na criação de leis que permitissem os direitos e garantias dos usuários e dos provedores de internet. Tal demora resta demonstrada uma vez que a chegada da rede mundial de computadores se deu em meados dos anos 80 e a primeira lei que instituiu a regulamentação de tal

tecnologia ocorreu em 2014 com a promulgação da Lei 12.965, que ficou conhecida como Marco Civil da Internet. Um atraso em torno de 30 anos.

Antes da Lei 12.965/2014, o judiciário brasileiro resolvia conflitos advindos do meio digital tomando como base a Constituição Federal de 1988, assim como o Código Civil e Penal, além do direito consuetudinário e precedentes jurisdicionais. Ora, uma vez que o ordenamento jurídico não faz previsões expressas punindo e responsabilizando as condutas abusivas dos usuários do meio digital surge a sensação de impunidade, pois o meio de operação passa a ser executado por uma máquina e não com as próprias mãos do agente.

Além disso, o usuário tinha a percepção de que nunca seria descoberto e que suas condutas não trariam nenhuma consequência jurídica. Todavia, uma crítica tecida ao Marco Civil da Internet é que a lei não "estabelece sanções penais e, sim, orientações acerca das condutas praticadas no âmbito digital" (MARRA, 2019, p.151).

Cumpre salientar que o principal objetivo da Lei nº 12.965/2014 é a garantia da privacidade dos usuários. Nesse sentindo, referida norma trouxe nos primeiros artigos a inserção dos direitos à privacidade, intimidade, liberdade de expressão e do acesso à internet, dentre outras tantas garantias já prevista na Constituição Federal de 1988 (BRASIL, 2014).

Nos artigos 7º e 8º da referida Lei, o legislador assegura que o acesso à internet é essencial para o exercício da cidadania e detém-se em garantir a inviolabilidade da intimidade e da vida privada, bem como o sigilo das comunicações tidas ou armazenadas pela internet, salvo por ordem judicial. Além disso, garantiu diversos direitos consumeristas, tais como a não suspensão da conexão à internet, salvo por débito existente, bem como a manutenção e a qualidade de conexão à rede conforme admissão e o direito a ter informações claras dos contratos de prestação de serviço com detalhamento (BRASIL, 2014).

Conseguinte, o legislador previu a necessidade de neutralidade de rede no artigo 9º, pois ao provedor é vedado bloquear ou monitorar o conteúdo dos pacotes de dados. Sendo assim, o responsável pela transmissão possui "o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação", nos termos da lei (BRASIL, 2014, s. p.).

Todavia, ainda que seja necessária a reafirmação dos direitos constitucionais já garantidos, a principal interferência do Marco Civil da internet se deu na responsabilização dos provedores, restando consignado que estes não serão

responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros (BRASIL, 2014).

Nesse sentido, o legislador preocupou-se em assegurar a liberdade de expressão e impedir a censura, uma vez que o provedor de internet somente será responsabilizado na esfera civil por danos de conteúdo gerado por terceiros caso negue tomar providências após ordem judicial. Por exemplo, após o juízo oficiar que a página e o conteúdo gerado em determinado meio digital sejam retirados da rede e o provedor não o fizer (BRASIL, 2014).

Ademais, a lei garantiu que nos casos em que o conteúdo tratar de violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado, o provedor de aplicações na internet responderá civilmente por danos quando não responder a solicitação de forma eficaz e diligente a indisponibilidade do conteúdo após a notificação do lesado ou seu representante legal que não autorizou a divulgação. Nesse cenário, não requer ordem judicial, basta a notificação da pessoa que sofreu o dano (BRASIL, 2014).

Consequentemente, o legislador garantiu o direito do usuário da rede a possibilidade de instalar em seus aparelhos de uso pessoal programas que façam o controle parental de conteúdo entendido como impróprio aos filhos menores, desde que respeitados os princípios desta lei e do Estatuto da Criança e do Adolescente, cabendo ao Poder Público, juntamente com os provedores de conexão e de aplicação de internet, a promoção da educação e fornecimento de informações sobre o uso desses programas e definição de boas práticas para inclusão digital de crianças e adolescentes (BRASIL, 2014).

Ademais, no tocante ao combate de ato ilícitos cíveis e criminais no âmbito virtual, vislumbra-se a possibilidade de identificação dos usuários autores de tais atos como uma resposta possível à vítima:

> Do ponto de vista social, a internet proporciona contatos interpessoais anônimos, do ponto de vista técnico, toda ação realizada pela internet é passível de registro pelos provedores de acesso e de conteúdo, o que torna possível a identificação dos usuários. (TOMASEVICIUS FILHO,2016, p. 274).

Desse modo, o art.13, *caput*, do Marco Civil da Internet determina que o administrador da provisão de conexão à internet mantenha sob sigilo os registros de conexão pelo prazo de 1 (um) ano e pelo art.15, *caput*, o registro de acesso a aplicações

da internet pelo prazo de seis meses, podendo ser guardado por período superior caso a autoridade policial ou o Ministério Publico requeira (BRASIL, 2014).

Por isso, a todos os registros somente são concedidos acesso mediante autorização judicial em razão do princípio da inviolabilidade à privacidade e das comunicações, nos termos dos artigos 7º, III; 10, §§1º e 2º; 13, §§3º e 5°; 15, §3ºda lei 12.965/2014 e art. 5º, XII da Constituição Federal de 1988 (BRASIL, 2014).

Sendo assim, a materialidade dos ilícitos cometidos no âmbito virtual pode ser fornecida por meio dos provedores de internet, uma vez que esses detêm dados imprescindíveis para que seja feita a identificação dos agentes responsáveis pelos danos causados à vítima na esfera cível e para o trabalho investigativo da polícia judiciária.

Contudo, é necessário ressaltar que a Lei do Marco Civil da Internet recebe diversas críticas quanto ao seu conteúdo, pois Tomasevicius Filho (2016) aduz que se trata de uma lei sem conteúdo normativo, uma vez que considera que não houve mudanças substanciais, pois o acréscimo à legislação vigente foi mínimo. Por isso, este infere que a tamanha expectativa criada pela Lei do Marco Civil se deu pelos juristas acreditarem que as orientações já contidas no ordenamento jurídico brasileiro não fossem aplicáveis nas relações jurídicas do âmbito digital.

Todavia, em sua crítica, Tomasevicius Filho (2016) levanta três aspectos positivos advindos pelo Marco Civil da Internet: i) vedação da imposição de mecanismos de censura, bloqueio, monitoramento, filtragem e análise de dados que trafegam pela infraestrutura da internet dentro do território brasileiro; ii) regulamentação dos procedimentos judiciais específicos para obtenção dos registros de navegação para fins de instrução processual civil e penal; e iii) a disciplina dos chamados *cookies*, arquivos instalados nos computadores ou telefones para registrar informações e preferências dos usuários quando acessam determinada página na internet, nos termos do artigo 7º, VIII da referida lei.

Em contrapartida, os pontos sugeridos pelo autor estão na redundância de direitos e garantias já dispostas na Constituição Federal, bem como normas e conceitos vazios instituídos pelo legislador, além de não trazer a definição do conceito de "provedor de internet", o que seria substancial no contexto, pois esses são os principais destinatários das obrigações e recomendações advindas do Marco Civil.

Por fim, cabe ressaltar um ponto controvertido que a referida lei trouxe a respeito da responsabilidade civil dos provedores de conexão à internet, qual seja, deliberação de que não há responsabilidade civil dos provedores por atos ilícitos

praticados por seus usuários, pois não há nexo de causalidade entre a atividade e os danos sofridos, uma vez que sua atividade consiste apenas na promoção da conexão entre os usuários e a internet (BRASL, 2014).

Todavia, antes dessa alteração, Tomasevicius Filho (2016) aduz que o provedor devia se manter vigilante, pois poderia ser acionado judicialmente por responsabilidade solidária com o agente que causou danos à terceiro. Dessa feita, a mobilização para oferecer canais de denúncia para retirada de conteúdo era maior.

Destarte, uma última crítica é trazida pelo autor. Com o Marco Civil da Internet, estabeleceu-se a responsabilidade civil dos provedores, e por isso a vigilância e a diligência desses foi reduzida, por isso poderá facilitar os agentes violadores. Nos moldes da alteração legislativa, o usuário que sofrer qualquer dano deverá acionar prioritariamente o usuário que causou danos, pois esse é o responsável principal. A única possibilidade em que o provedor possa responder civilmente por danos, será quando esse se recusar a cumprir ordem judicial para retirada do conteúdo violador dos direitos da personalidade (TOMASEVICIUS FILHO, 2016).

Logo, é necessário compreender que a Lei do Marco Civil da Internet se mostrou vaga e distante da realidade, pois deixou de apresentar conceitos importantes e não trouxe garantias inovadoras aos seus usuários, uma vez que praticamente fez uma cópia da Constituição Federal de 1988. Os anseios dos usuários não foram supridos, pois esses buscavam soluções, direcionamentos e definições concretas acerca dos ilícitos cometidos no ambiente virtual. No próximo tópico, remonta-se uma construção do conceito desses delitos.

2.2 Conceito de crimes virtuais

A internet trouxe avanços significativos em áreas do conhecimento das mais diversas especialidades. Contudo, todo bônus carrega consigo um ônus, e com o avanço da informática e tecnologia da informação não seria diferente. Surgiram também novas formas de cometer delitos, causando vítimas por meio da internet, criando os chamados crimes cibernéticos.

Neste sentido, Nucci (2020) atesta sobre conceito de crime de forma analítica como sendo uma conduta típica, antijurídica e culpável, dada por ação ou omissão de um comportamento que fora proibido, contrário às normas jurídicas e com reprovabilidade social sobre o autor e o fato, observadas ainda as hipóteses de não

aplicação da exclusão de ilicitude e a imputabilidade do agente.A Lei de Introdução ao Código Penal Brasileiro (Dec. Lei nº 3.914/41), no artigo 1º aduz que:

> [...] Considera-se crime a infração penal a que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com pena de multa, contravenção a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente (BRASIL, 1941, s. p.).

Sendo assim, com o advento da internet e outros meios eletrônicos, bem como a incidência e o aumento de práticas criminosas utilizando-se dessesmétodos, se fez necessária a conceituação de tais atos. Desse modo,a apresentação de especialistas a respeito do temaé fundamental para conceituar de forma mais precisa os crimes virtuais.

Pinheiro (2021) aponta que grande parte dos crimes cibernéticos são os mesmos praticados no mundo real, sendo o computador e a internet apenas o meio facilitador para tal conduta criminosa. Ressalta ainda que não se deve esquecer que a rede ainda assegura o anonimato para o autor do crime. Todavia, os conceitos que são aplicados pelo Código Penal (CP) e pelos doutrinadores ao direito penal tradicional também podem ser aplicados aos crimes digitais.

Teixeira (2020, p.214) prefere nomear como “crime de informática” por entender ser o mais apropriado para a definição, uma vez que abrange todos os tipos de meios de comunicação informáticos e não apenas a internet. Segundo o autor, crime de informática é aquele realizado por “meios informáticos como instrumento de alcance ao resultado pretendido, e também aquele praticado contra os sistemas e meios informáticos”.

Jesus e Oliveira (2016, p. 49-50) preferem conceituar como crime informático o fato típico e antijurídico realizado por intermédio ou em desfavor da tecnologia. Ademais, o autor assegura que “em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal”.

Crime virtual, nas palavras do autor Ferreira (2005) é conceituado como aqueles atos criminosos que ocorreram por meio de um sistema informático que lesaram o patrimônio, a liberdade individual e a propriedade imaterial. Ademais, Conte e Fiorillo (2016) trazem a definição da *Organização para Cooperação Econômica e Desenvolvimento da Organização das Nações Unidas*, em 1983, de crime informático como sendo “qualquer conduta ilegal, não ética, ou não autorizada que envolva

processamento automático de dados e/ou a transmissão de dados" (PALAZZI, 2000, p. 39).

Logo, diversas são as nomenclaturas possíveis e adotadas: "crimes cibernéticos", "crimes virtuais", "crimes digitais", "cybercrimes", "crimes informáticos", dentre outros. Todavia, resume–se em uma definição básica: tipos penais praticados por intermédio de aparelhos informáticos podendo fazer uso da internet ou não. Portanto, são crimes virtuais aqueles atos ilícitos cometidos por meio de um dispositivo tecnológico. Tal meio de operação criminosa é muito eficaz e pode fazer vítimas em massa.

Em razão da forma de aplicabilidade e do alto poder propagador dos crimes virtuais, o legislativo brasileiro deve prever consequências razoáveis para esses delitos, com tipos penais bem delimitados e penas inibitórias específicas com o objetivo de frear a ação dos criminosos e garantir uma resposta do Estado às vítimas, conforme aborda-se no capítulo seguinte.

3 ALTERAÇÕES E INOVAÇÕES LEGISLATIVAS NO BRASIL

Souza e Pereira (2009) aduzem que o ordenamento jurídico precisava acompanhar as inovações tecnológicas e o poder legislativo necessitava desenvolver leis que assegurassem o direito dos usuários de internet. Nesse ínterim, surge a convenção de Budapeste, que engloba cerca de 20 países e tem o objetivo de tipificar os principais crimes cometidos por intermédio da internet. Todavia, o Brasil não foi signatário da convenção realizada em 2001 e que teve seus objetivos vigorados a partir de 2004.

Outrossim, ainda que o Brasil não fosse precursor de tal convenção, percebeu a necessidade de editar leis que responsabilizassem de forma específica aqueles que cometessem os conceituados, anteriormente, crimes digitais, pois a internet já era acessível desde os anos 90 no país. A urgência se dava em razão da movimentação da máquina do judiciário por vítimas de crimes virtuais que não obtinham a devida resposta e não visualizavam a criminalização de seus algozes de maneira específica.

A título de exemplificação, imagina-se que uma pessoa teve seu computador invadido por um terceiro e busca o indiciamento correto e particular desse autor, todavia, não se podia responsabilizar os criminosos, em observância ao princípio da legalidade, uma vez que não havia lei que punisse tal ato. O princípio da previsão legal anterior ao fato está disposto no Código Penal Brasileiro, nos termos do art. 1º e 2º, veja-se:

> Art. 1º - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal. Art. 2º - Ninguém pode ser punido por fato que lei posterior deixa de considerar crime, cessando em virtude dela a execução e os efeitos penais da sentença condenatória (BRASIL, 1941, s. p.).

Por isso, surgiu a necessidade de trazer a responsabilização cível e a tipificação criminal de tais atos praticados por usuários com más intenções, sobretudo porque o direito penal tem como princípio norteador a legalidade que coíbe excessos e analogias, ou seja, para que um ato ou omissão seja crime, ele precisa estar tipificado em uma lei de âmbito federal.

Segundo Carolina Borges Rocha (2013), a internet era isenta de qualquer regulamentação jurídica até o ano de 2012, feito que tornava difícil a punibilidade dos atos praticados por seu intermédio. Outrossim, ela desenvolve que a internet facilitava a execução dos crimes, pois não demonstrava ser um instrumento violento, bastando ter

um aparelho informático (computador, celular, *tablet*) e acesso ou não à rede. Além da facilidade, é um meio eficaz para pôr em prática condutas que prejudicam os usuários.

De todo modo, ainda que a internet estivesse presente desde os anos 90 no Brasil e toda a mobilização global acerca da necessidade de edição de leis e normas a respeito da sua utilização para fins criminais tenha sido ressaltada, como foi citada a Convenção de Budapeste em 2001, o Brasil esteve atrasado nessa corrida, pois somente em 2008 foi sancionada a primeira lei de matéria criminológica virtual, de nº 11.829/2008, que regulamenta a pedofilia na internet.

Ademais, somente em 2012outras duas leis brasileiras acerca dos crimes virtuais foram sancionadas, quais sejam: Lei 12.735/2012 – Azeredo e Lei 12.737/2012 – Carolina Dieckmann. Referidos textos normativos serão melhores explicitados em tópicos posteriores.

Apesar disto, o autor Tomasevicius Filho (2015, p. 272) critica que o Direito Penal tradicional é ineficaz no combate aos crimes virtuais, uma vez que a Internet não obedece aos limites territoriais e tão pouco a soberania nacional dos países que dela fazem uso. A responsabilidade criminal aos autores dos delitos tem se atualizado dia a dia de acordo com as "inovações" dos seus atos. Isso por que a legislação ainda não consegue prever todos os atos criminosos que podem resultar em vítimas do ambiente digital.

Ademais, ainda que nos dias atuais hajam previsões no ordenamento jurídico brasileiro acerca dos ilícitos cometidos no âmbito virtual, o que se vê na prática é a ineficiência de tais leis, uma vez que são espaças e vagas. Para Angelo e Sanches (2018), é indispensável que sejam instituídas penas específicas destinadas aos autores dos crimes que sejam proporcionais aos danos causados.

Segundo Bononi Fernando (2021), os crimes cibernéticos foram tipificados com novas modalidades nesse dispositivo, sendo diferentes as expectativas, pois penas mais graves foram impostas aos agentes que se utilizaram do ambiente virtual para cometer crimes. Nessa baila, a grande maioria dos tipos penais que se encontram no ordenamento jurídico brasileiro podem ser praticados por meio virtual e assim serem considerados crimes cibernéticos.

Nas próximas laudas o objetivo será analisar as leis específicas sancionadas no Brasil que versem sobre os crimes que têm como meio principal os dispositivos cibernéticos.

3.1 Lei 11.829/2008 – Alterações no ECA

A Lei 11.829/2008 sancionada pelo então Presidente Luiz Inácio Lula da Silva, tipifica os crimes de pornografia infantil virtual, alterando o Estatuto da Criança e do Adolescente (ECA).Teixeira (2020) interpreta a pedofilia como sendo uma anomalia em que seus portadores possuem atração por crianças, sendo a pornografia infantil um dos meios pelos quais o pedófilo obtém satisfação sexual.É valido ressaltar que essa foi a primeira lei a mencionar os meios informáticos para tipificação de um crime. Sem dúvidas, os crimes de pedofilia e pornografia infantil causam urgência na responsabilização dos seus autores, pois o clamor social é imenso.

O dispositivo legislativo introduziu ao Estatuto da Criança e do Adolescente os artigos 240 e 241, os quais versam sobre a produção, filmagem e fotografia de material pornográfico que envolve crianças e adolescentes, bem como a proibição da venda e comercialização de tal material. A pena prevista para tais crimes é de reclusão de 4 a 8 anos e multa. Trata-se de um delito informático, uma vez que previu a utilização de equipamentos tecnológicos como, por exemplo, câmeras, telefones, máquinas fotográficas, gravadores e tantos outros dispositivos (BRASIL, 2008).

A Lei 11.829/2008 ainda inseriu no ECA os artigos 241-A e 241-B. Tais dispositivos retratam a vedação da distribuição e do armazenamento de material pornográfico infantil por qualquer meio, incluindo o sistema informático ou telemático. A pena prevista é de reclusão, de 3 (três) a 6 (seis) anos, e multa. Na mesma pena incorre quem assegura o acesso do material por rede de computadores. Além disso, aquele que armazena material pornográfico infantil ou juvenil incorre em crime punível de reclusão de 1 (um) a 4 (quatro) anos, e multa (BRASIL, 2008).

Além disso, a lei incluiu ainda ao Estatuto da Criança e do Adolescente o artigo 241-C que torna crime a simulação da participação em ato sexual da criança ou adolescente quando feito por montagem de foto, vídeo ou outro meio visual. Nesse artigo, o legislador previu que o criminoso virtual ainda poderia usar a imagem de uma criança para adulterar cenas pornográficas e trazer grave dano ao menor. A pena prevista é de reclusão, de 1 (um) a 3 (três) anos, e multa (BRASIL, 2008).

Por fim, o art. 241-D tipifica como crime o aliciamento, por qualquer meio de comunicação, de criança com o fim de praticar atos libidinosos. A conduta tem pena de reclusão, de 1 (um) a 3 (três) anos, e multa. O legislador também pune aquele que

induz ou facilita o acesso de material pornográfico a criança para com ela praticar atos libidinosos (BRASIL, 2008).

Segundo Teixeira (2020), são três as principais formas da prática dos crimes de pornografia infantil. No primeiro momento, o dono do acervo pornográfico recebe um valor dos usuários que possuem o intuito de adquirir fotos de crianças ou adolescentes em situações sexuais. Ainda prevê a possibilidade da manutenção de sites e redes sociais que são livremente acessadas pelos pedófilos. E por fim, há a hipótese de distribuição do material pornográfico de maneira gratuita entre usuários criminosos por meio de e-mails e torpedos, por exemplo.

Destarte, como sendo uma lei pioneira na previsão dos crimes virtuais, recentemente o Senado avalia o Projeto de Lei (PL) nº 830/2022, de iniciativa do Senador Flávio Bolsonaro, que busca agravar as penas previstas primeiramente pela referida lei, pois segundo o representante do povo, os números de tais crimes não param de crescer e precisam de uma retaliação maior por parte da população (PROJETO..., 2022, s. p.). Segue abaixo as penas comparadas:

Tabela 1: PL 830/2022

Veja o que prevê o projeto		
Crime	**Pena atual**	**Pena proposta**
Registrar, vender ou expor pornografia infantil	4 a 8 anos	5 a 8 anos
Divulgar material pornográfico infantil	3 a 6 anos	4 a 6 anos
Armazenar registro pornográfico infantil	1 a 4 anos	2 a 5 anos
Assediar ou simular participação infantil em cena pornográfica	1 a 3 anos	2 a 4 anos

Fonte: PORTELA, 2022.

3.2 Lei 12.735/2012 - Azeredo

A Lei ordinária nº 12.735 teve origem no Projeto de Lei 84/1999, proposto pelo Deputado Federal Luiz Piauhylino. Todavia, houve um longo caminho até ser sancionada em 2012.A principal colaboração da referida lei foi a implementação de delegacias e outros órgãos judiciais especializados no combate e apuração dos crimes cibernéticos cometidos, bem como a cessação do compartilhamento de mensagens de teor racista.

Nas palavras de Sales (2013), o reforço da polícia judiciária para buscar formas de combate aos crimes virtuais foi de caráter político. Destarte, tal dispositivo legislativo não foi suficiente para responsabilizar os criminosos, pois não tipificou crime algum. Todavia, no Capítulo 4 desse trabalho serão analisados os desdobramentos da instituição de órgãos judiciários especializados no combate e apuração dos crimes cibernéticos.

3.3Lei 12.737/2012 - Carolina Dieckmann

A lei ordinária de nº 12.737/2012 possui um contexto relevante e merece ser exposto na atual monografia. A atriz Carolina Dieckmann teve seu computador invadido, sendo chantageada por criminosos que cobraram o valor de R$ 10.000,00 (dez mil reais) para que não vazassem as fotos obtidas, de acordo com as informações dadas pelo O Globo (GOULART, 2012, s. p.).

Entretanto, a atriz recusou-se a pagar o valor solicitado e 36 fotos íntimas foram divulgadas pelos invasores. Sem dúvidas tal exposição trouxe um profundo constrangimento à vítima. Contudo, não existia ainda no Código Penal brasileiro nenhum crime tipificado que punisse a invasão de computadores.

Insurgindo-se contra o fato, em novembro de 2012 foi sancionada a Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, que trouxe alterações ao Código Penal com a criminalização de crimes informáticos. Assim sendo, a lei inclui ao Código o art. 154-A que tipificou a conduta de invasão de dispositivos eletrônicos ou informáticos, sendo eles conectados ou não a internet, por meio de violação ilegal dos mecanismos de segurança com o objetivo de conhecer os dados do titular (BRASIL, 2012).

É importante frisar que a citada norma somente tipifica como crime a invasão quando há o rompimento de mecanismo de proteção, em atenção ao princípio da legalidade. Dessa feita, vale-se a necessidade de o usuário sempre proteger seus dados com senhas, antivírus e outros mecanismos existentes de segurança. (SALES, 2013).

Além disto, o parágrafo primeiro do art. 154-Atambém criminalizou aquele que fornece programas ou dispositivos com finalidade de obter vantagem ilícita sobre dados alheios. As condutas tipificadas acima tiveram a fixação de pena de detenção de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 2012).

O legislador preocupou-se em aumentar a pena fixada no *caput* de um sexto a um terço quando da invasão eletrônica resultar em prejuízo financeiro. Se do resultado da invasão o criminoso obter informações sigilosas, segredos comerciais ou industriais e mensagens privadas, a pena será de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. Ademais, caso haja divulgação ou propagação de tais conteúdos obtidos pela invasão, aumenta-se a pena de um a dois terços (BRASIL, 2012).

Ainda verifica-se o aumento de pena de um terço à metade se o crime for praticado contra algumas das autoridades do Poder Executivo, quais sejam: I) Presidente da República, governadores e prefeitos; II) Presidente do Supremo Tribunal Federal; III) Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV) dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (BRASIL, 2012).

O art. 154-B estabelece que o crime tipificado no art. 154-A é de ação penal condicionada à representação, salvo quando praticado contra a administração pública direta ou indireta (BRASIL, 2012). Contudo, recentes modificações foram implementadas aos artigos acima descritos, uma vez que a Lei nº 14.155/2021 agravou as penas antes impostas. Segue abaixo um quadro comparativo:

Tabela 2: Alterações na Lei 12.737/2012 pela Lei 14.155/2021**Alterações na Lei 12.737/2012 pela Lei 14.155/2021**

Crime	**Pena**	**Pena alterada**
Invadir dispositivo informático de uso alheio	Detenção, 3 meses a 1 ano.	Reclusão, 1 a 4 anos.
Se da invasão resultar prejuízo econômico	Aumento de um sexto a um terço	Aumento de um terço a dois terços
Se da invasão tiver obtenção de comunicações privadas, segredos comerciais ou industriais, informações sigilosas	Reclusão, seis meses a dois anos	Reclusão, dois a cinco anos.

Ademais, a Lei 14.155/2021 modificou o caput do art. 154-A não sendo mais necessária a invasão "mediante violação indevida de mecanismo de segurança" (BRASIL, 2021, s. p.). Além disso, a lei 12.737/2012 tipificou ainda como crime a interrupção de serviço telegráfico ou informático no art. 266 do CP. A pena atribuída ao delito é de detenção, de um a três anos, e multa (BRASIL, 2012).

Por fim, o legislador tipificou a conduta de falsificação de cartão, seja ele de débito ou crédito, ao acrescentar o parágrafo único ao art. 298 do Código Penal Brasileiro. Viu-se a necessidade de alteração, pois se equiparou a documento particular o cartão de crédito ou débito e tipificou como crime a clonagem de tal documento. A pena prevista para tal delito é de reclusão, de um a cinco anos, e multa. Ademais, no caso concreto é importante a análise de ocorrência de estelionato, furto ou extorsão para aquisição do cartão (BRASIL, 2012).

Segundo Teixeira (2020), diversos consumidores evitam comprar em sites com o cartão de crédito, pois temem que seus dados sejam vazados e seus cartões clonados, sendo utilizados por terceiros de má-fé. A principal conduta dos *crackers*, ou seja, aqueles que possuem *expertise* na área de tecnologia da informação, mas utilizam a sua habilidade apenas em benefício próprio ou até para prejudicar terceiros, é o ataque aos servidores de lojas *online* que armazenam os dados dos clientes dessa forma, pois possuem barreiras de segurança inferiores àquelas utilizadas pelos bancos ou entidades financeiras.

Destarte, Vasconcelos (2014) afirma que a lei em análise é merecedora das críticas levantadas pelos juristas e especialistas, uma vez que seus artigos possuem a capacidade de gerar dupla interpretação. Ainda aduz que as penas são brandas e passíveis de resolução em juizados especiais, não sendo possível uma contribuição expressiva no combate ao crime virtual.

3.4 Crimes contra a honra no âmbito digital

A Constituição Federal de 1988 assegura a inviolabilidade de direitos fundamentais aos brasileiros e estrangeiros residentes no Brasil. Segundo consta no art. 5º, inciso X: "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988, s. p.).

Ora, sendo a honra um direito inviolável, o Código Penal Brasileiro reuniu em um capítulo condutas típicas afim de responsabilizar criminalmente aqueles que violam tal garantia constitucional. São elas: calúnia, injúria e difamação, os chamados crimes contra a honra (BRASIL, 1940).

Os crimes contra a honra cresceram de forma assustadora desde o aumento do uso das redes sociais. De forma mais corriqueira, os usuários destilam ódio e comentários ácidos nos perfis de outros usuários. O termo *hate* é utilizado pelos perfis para denominar mensagens maldosas ou severos comentários a respeito do conteúdo publicado ou sobre a pessoa que publicou. Muitas vezes disfarçado de "crítica construtiva" ou até mesmo de forma explícita com o intuito de ofender diretamente o outro.

De fato, os *haters*, como são chamados aqueles que produzem esse comportamento agressivo nas redes sociais, têm confundindo a liberdade de expressão com as condutas reprováveis pelo Código Penal Brasileiro e pela Constituição Federal de 1988, conforme será apresentado a seguir. Ademais, crimes contra a honra praticados pela internet não exigem que se estabeleça a relação causa e resultado, pois é notado no instante em que a mensagem agressiva foi disponibilizada nas redes. Assim, recentes decisões do Superior Tribunal de Justiça (STJ) têm entendido que:

> 'Crimes contra a honra praticados pela internet são formais, consumando-se no momento da disponibilização do conteúdo ofensivo no espaço virtual, por força da imediata potencialidade de visualização por terceiros' (CC 173.458/SC, Rel. Ministro João Otávio de Noronha, Terceira Seção, DJe 27/11/2020).HC 591.218/SC, Rel. Ministro Joel Ilan Paciornik, Quinta Turma, julgado em 09/02/2021, DJe 12/02/2021 (BRASIL, 2021, s. p.).

Portanto, para Nelson Hungria (1980) os crimes contra a honra podem assumir diversos meios de execução. Como, por exemplo, a linguagem falada, escrita, mímica ou figurativa. Outrossim, tais condutas são de ação penal privada, ou seja, somente são processadas por meio de queixa-crime e mediante representação da vítima, nos termos do art. 38 do Código de Processo Penal. Portanto, o CPP estabelece ainda no art. 38 o prazo de 6 meses a partir do dia da ciência da autoria para que o ofendido represente pela denúncia (BRASIL, 1941).

Ademais, o órgão competente, em regra é o Juizado Especial Criminal, formalizado pela lei 9.099/1995que institui a competência dessa unidade judiciária para julgar as infrações penais de menor potencial ofensivo, ou seja, as contravenções penais e os crimes que possuem a pena máxima não superior a 2 (dois) anos, nos termos do art. 61, sendo assim não resultam em prisão, mas por vezes em composição civil dos danos ou pena não privativa de liberdade, nos termos do art. 72 da mesma lei (BRASIL, 1995).

3.4.1 Calúnia

A doutrina, nas palavras de Nucci (2020), compreendeu como calúnia o ato de acusar alguém falsamente de um crime com o intuito de tirar a credibilidade social do caluniado. Não obstante, o Código Penal tipifica no art. 138 o crime como “caluniar alguém, imputando-lhe falsamente fato definido como crime”. A pena prevista para essa conduta é de detenção, de 6(seis) meses a 2 (dois) anos, e multa (BRASIL, 1940).

Ademais, “vislumbra-se, pois, que a calúnia nada mais é do que uma difamação qualificada, ou seja, uma espécie de difamação” (NUCCI, 2020, p. 936). Sendo assim, afeta a honra subjetivada vítima, ou seja, aquele conceito que o próprio indivíduo tem de si mesmo, bem com seus valores e seus princípios (GRECO, 2015), pois atribui a sua conduta um factoide definido como crime pelo ordenamento brasileiro.

Cumpre salientar que, em razão do princípio da formalidade, o artigo que tipifica a conduta detém apenas fatos constituídos como crimes, ou seja, caso uma pessoa seja relacionada como autora de uma contravenção penal que não ocorreu, o seu acusador não comete calúnia, mas difamação.

3.4.2 Injúria

A injúria é uma ofensa que atinge a dignidade ou a reputação de alguém. Sendo assim, Aníbal Bruno (1979), busca distinguir dignidade de decoro, pois o Código Penal aduz ser crime a injúria contra as duas possibilidades. Em suas palavras, a dignidade é como a pessoa se sente perante a sociedade, ou seja, como ela é vista. Já o decoro se refere às qualidades físicas e habilidades desenvolvidas pela pessoa.

Sendo assim, "Dizer de um sujeito que ele é trapaceiro seria ofender sua dignidade. Chamá-lo de burro, ou de coxo seria atingir seu decoro" (BRUNO, 1979, p. 300). Nessa ocasião o dolo do agente é atribuir adjetivos pejorativos ao outro. O código penal prevê a pena de detenção, de 1 (um) a 6 (seis) meses, ou multa (BRASIL, 1940).

3.4.3 Difamação

Greco (2015) exprime que para que haja difamação é necessário que o agente impute fatos que ofendam a reputação da vítima. Ademais, compreende que a difamação é um delito de menor gravidade e está diretamente ligado a honra objetiva do ofendido. Perceba-se que o fato atribuído não precisa ser falso, mas basta que ofenda a boa fama do difamado. Em outras palavras:

> Isso significa que, mesmo sendo verdadeiro o fato, o que se quer impedir com a previsão típica da difamação é que a reputação da vítima seja maculada no seu meio social, uma vez que o que se protege, aqui, é a sua honra considerada objetivamente, ou seja, como já frisamos, o conceito que o agente presume que goza perante a sociedade. (GRECO, 2015, p. 443).

Conclui-se que o dolo do agente é prejudicar o outro perante a sociedade, denegrindo a sua fama. O Código Penal Brasileiro pune tal conduta com a pena de detenção, de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 1940).

3.4.4 Pena especial para os crimes contra a honra praticados no âmbito digital

A internet possibilitou a ligação entre pessoas de uma forma nunca antes experimentada. Para Soares (2016), o usuário deve ter consciência sobre suas expressões e opiniões ao serem publicadas nas redes, pois deve ser coibida toda e qualquer forma de crime, limitando-se tão somente a liberdade de expressão. Uma vez que os usuários possuem o direito de expor suas opiniões,desde que não sejam criminosos. Este aduz que é necessário diferenciar a publicação que afirma que não se agrada de uma pessoa, da publicação que ridiculariza e discrimina o outro, resultando em crime.

Ainda, os crimes virtuais mais comuns são os contra a honra e podem causar uma desaprovação da pessoa no convívio social, contribuindo ainda para que a sua autoestima seja diminuída (SOARES, 2016). Além disso, com advento de *blogs* e redes sociais o compartilhamento das mensagens e ou informações a respeito do indivíduo que teve sua honra maculada tomou proporções escalonáveis.

Por isso, o legislador institui na Lei 13.964/2019, que trata a respeito de quando o crime contra a honra for praticado ou divulgado por qualquer meio de rede social na internet. Referido instituto prevê aplicação do triplo da pena prevista. Tal redação busca trazer consequências mais graves àqueles que praticam crimes contra a honra na internet.

Portanto, caso seja um caso de injúria, a pena será de 3 (três) a 18 (dezoito) meses, e multa. Sendo um crime de difamação, a pena imposta é de 9 (nove) meses a 3 (três) anos, e multa. Na ocasião de uma calúnia a pena imposta será de 18 (dezoito) meses a 6 (seis) anos, e multa (BRASIL, 2019).

3.5 Lei 14.155/2021- Crimes contra o patrimônio no âmbito digital

Percebe-se que a realidade das movimentações bancárias e fechamentos de negócios, como compra e venda de produtos e prestação de serviços, muitas vezes se dão por transações *online*, por meio de um aplicativo de banco que as partes interessadas possuem, em decorrência da praticidade e agilidade característica.

Entretanto, negócios fajutos estavam sendo realizados e golpes estavam sendo aplicados corriqueiramente naqueles menos atenciosos ou com pouca instrução. Desse modo, as alterações legislativas advindas do dispositivo legal nº

14.155/2021trouxeram novos tipos penais no contexto de crimes contra o patrimônio praticados pela internet. A previsão das condutas criminosas se deu pela necessidade de punir de forma específica aqueles que foram autores de furto mediante fraude e de estelionato por meio digitais.

3.5.1 Furto mediante fraude virtual

O furto está tipificado no Código Penal Brasileiro no art. 155 como "subtrair, para si ou para outrem, coisa alheia móvel – pena: reclusão de 1 a 4 anos, e multa" (*caput*). Além disso, admite a qualificadora de furto mediante fraude (BRASIL, 1940). Nessa modalidade o agente busca inverter a posse do objeto aplicando um meio para ludibriar a vítima, sem aplicar qualquer violência ou grave ameaça.

A Lei nº 14.155 tipificou uma nova qualificadora do furto no art. 155, § 4º-B no Código Penal que prevê o furto mediante fraude quando "cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo". A pena cominada ao tipo penal é mais grave que as demais qualificadoras e consiste em reclusão, de (quatro) a 8 (oito) anos, e multa (BRASIL, 2021).

A inovação legislativa se deu em razão do aumento do número de casos e denúncias durante o período pandêmico e tem a finalidade punir mais gravemente aquele que se utiliza de meios eletrônicos para cometer furtos mediante fraude. Ademais, o legislador ainda previu duas causas de aumento ao crime em questão. O aumento de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional e o aumento de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável (BRASIL, 2021).

Necessário destacar que o dispositivo eletrônico deve ser utilizado como meio para praticar o crime, ou seja, é um instrumento que possibilita o agente cometer o delito. Como exemplo de tal crime, pode-se citar as fraudes bancárias cometidas em detrimento dos titulares das contas. Em suma, são transferidos valores e empréstimos realizados sem o consentimento do possuidor dos valores de forma fraudulenta. Nesse sentido, a Jurisprudência pátria tem entendido que a tipificação aplicada é a do art. 155 § 4º-B do CP.

No Tribunal de Justiça do Distrito Federal, no processo nº 07179219020228070000 1437715, a Câmara Criminal considerou a incidência da tipificação do art. 155, § 4º-B, do Código Penal, pois entendeu que a vítima não tinha conhecimento e nem consentimento dos valores subtraídos de sua conta bancária. Outrossim, entendeu ainda que não deve incorrer o crime de estelionato por fraude eletrônica, pois o autor do delito não obteve proveito em relação a vítima por indução ao erro. Na verdade, o valor retirado de sua conta bancária foi por meio de fraude para retirar a vigilância da vítima (BRASIL, 2022).

No mesmo sentido e com a mesma fundamentação teórica, o Superior Tribunal de Justiça julgou o conflito de competência n. 181.538/SPe determinou que, com base da narração fática, o delito cometido deve ser tipificado no artigo 155, § 4º-B, do Código Penal, qual seja furto qualificado por fraude eletrônica, e considerou que a competência é o local da consumação do fato, quando o autor do delito detém a posse do bem, ou seja, onde ocorreu a contratação de empréstimos fraudulentos vinculados à conta corrente da vítima na agência bancária na cidade de Santa Helena/MA, bem como a transferência dos valores a contas situadas no Estado de São Paulo, nas cidades de Campinas, Itaim Paulista e São Paulo, por meio de fraude eletrônica (BRASIL, 2021).

Assim, o entendimento de que não se deve confundir o furto mediante fraude com dispositivo eletrônico do estelionato é o que prevalece, uma vez que as vítimas se quer tinham o conhecimento que transações estavam sendo feitas de suas contas bancárias.

3.5.2 Estelionato virtual

O estelionato está tipificado no art. 171, *caput*, do Código Penal e prevê como crime: “Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento”. A pena prevista é de reclusão, de 1 (um) a 5 (cinco) anos, e multa (BRASIL, 1940).

Não obstante, o legislador previu na lei 14.155/2021 a qualificadora do estelionato cometido por meio digital acrescentando assim o § 2º-A que comina a pena de reclusão de 4 (quatro) a 8 (oito) anos e multa se o estelionato é cometido por indumento ao erro por meios das redes sociais ou meios análogos. A pena imposta nessa qualificadora pode sofrer ainda o aumento de 1/3 (um terço) a 2/3 (dois terços) caso o

crime seja praticado com uso de servidor mentido fora do Brasil. Tal agravo se dá pela dificuldade de investigação com esse cenário (BRASIL, 2021).

Ademais, se o crime de estelionato virtual é cometido contra idoso ou pessoa vulnerável, a lei prevê o aumento de pena de 1/3 (um terço) ao dobro. Diferentemente do furto, a vítima entrega vantagem solicitada pelo autor do crime de maneira equivocada, uma vez que está sendo ludibriada, acreditando em uma contraprestação ou estar ajudando terceiros. Além disso, trata-se de uma entrega voluntária da vítima que está em condição adversa (BRASIL, 2021). Ademais, o Superior Tribunal de Justiça possui entendimento pacífico:

> O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente. (STJ, CC 67.343/GO, Terceira Seção, Rel. Min. Laurita Vaz, j. 28/03/2007, DJ 11/12/2007, p. 170). (BRASIL, 2007, s. p.).

Por fim, segue recente decisão do Tribunal de Justiça de Amazonas que condena o réu pelo estelionato qualificado pela fraude eletrônica por aplicar golpes em terceiros. Trata-se de um recurso de Apelação que buscou a absolvição do acusado e subsidiariamente ao Acordo de não persecução penal, instituído no art. 28-A do CPP (BRASIL, 1941).

Ademais, o Relator decidiu que restavam comprovadas a autoria e a materialidade por meio da declaração da vítima, relatório de investigação, boletim de ocorrência, *prints* das conversas por meio do *WhatsApp* e o comprovante de pagamento de PIX no valor de R$ 1000,00 (mil reais). Ademais, o golpe aplicado consistia em anunciar celulares em sua rede social com preços atrativos.

A vítima, interessada em fazer esse tipo de negócio, entrou em contato por mensagem e após a negociação efetuou o pagamento do PIX no valor de R$ 1000,00 (mil reais) na conta do acusado, todavia, após a transação o perfil responsável por anunciar a venda não respondeu as mensagens e tampouco cumpriu com a obrigação de entregar o produto divulgado e pago pela vítima. Outrossim, a Polícia Civil identificou por meio da SINESP que a chave pix pertencia ao Apelante, além de conte outros boletins de ocorrência relatando fatos criminosos similares ao caso (BRASIL, s. d.).

Portanto, o acusado contribuiu para o crime, uma vez que disponibilizou sua conta bancária para que o golpe fosse aplicado e por isso deve responder criminalmente. Outrossim, a colenda câmara criminal do Tribunal de Justiça do Amazonas confirmou a condenação do réu pelo crime de estelionato majorado por fraude eletrônica, nos termos do art. 171, § 2.º-A, do Código Penal. A pena cominada é de 4 (quatro) anos em regime aberto e 10 dias-multa (BRASIL, 1941).

Por fim, o Tribunal indeferiu o pedido de acordo de não persecução penal, pois a pena aplicada ao delito não é inferior a 4 (quatro) anos. Desse modo, tantos outros delitos são cometidos com o *modus operandi* similar, fazendo vítimas e causando além do dano material, o dano psicológico, uma vez que o lesado se sente culpado por ter caído em tamanha "armadilha". Sem falar no sentimento de medo que consumidores portam em realizar novas compras ou fazer negócios por intermédio da internet, temendo ser vítima de outro golpe estelionatário (BRASIL, s. d.).

Portanto, superada a questão da diferenciação entre furto e estelionato, pode-se analisar que o crime de contra o patrimônio no âmbito digital tem feito diversas vítimas no Brasil, sobretudo no período pandêmico. A situação mundial, como antes relatada, foi uma grande alavanca para que os criminosos utilizassem o meio cibernético para cometerem crimes.

3.6 Dos crimes contra a dignidade sexual no âmbito digital

A dignidade da pessoa humana é garantida constitucionalmente como fundamento, nos termos do art. 1º, inciso III, da CF (BRASIL, 1988). Ademais, os autores Costa da Silva e Lima (2020) aduzem que a dignidade sexual é um dos aspectos da dignidade da pessoa humana, pois consideram ser intrínseca ao ser humano a sua sexualidade e merece ser tutelado pelo âmbito penal. Por sua vez, Nucci (2014, p. 31) implica que "a dignidade sexual liga-se à sexualidade humana, ou seja, o conjunto dos fatos, ocorrências e aparências da vida sexual de cada um".

Por isso, é importante que seja observado pelo Código Penal todas as condutas que minam esse direito fundamental. Dessa maneira, com o advento da internet, criminosos encontraram mais um meio de cometer seus delitos, maculando o direito íntimo da vítima, causando transtorno e vergonha. Outrossim, com o meio empregado, qual seja a internet, o poder da disseminação da informação e da violação

da intimidade da vítima é exponencialmente maior. Por essa razão se dá a urgência de formular dispositivos capazes que coibir tais condutas de maneira veemente e eficaz.

Em atenção à urgência insurgida o legislador produziu duas leis importantes que trouxeram novos tipos penais que visam punir àqueles que ferem o direito à dignidade sexual, são elas: Lei 13.718/2018 e Lei 13.772/2018.No dispositivo 13.718/2018 restou tipificada a conduta criminosa de divulgação de fotos ou vídeos com conteúdo pornográfico sem o consentimento da vítima e ainda qualquer material audiovisual que remeta a cena de estupro ou estupro de vulnerável, tipificado no art. 218-C do Código Penal(BRASIL, 2018).

A pena cominada é de reclusão, de 1 (um) a 5 (cinco) anos, e multa. Ademais, ainda previu um aumento de pena de 1/3 (um terço) a 2/3 (dois terços), caso o agente que possibilitou a divulgação do material tenha mantido relação intima com a vítima e ou possuía o dolo de causar humilhação ou por vingança (BRASIL, 2018).

Ademais, na Lei 13.772/2018, restou consignado como crime no art. 216-B do Código Penal, o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. A pena prevista é de detenção, de 6 (seis) meses a 1 (um) ano, e multa. Outrossim, o agente que produz montagem de foto, vídeo ou áudio com o intuito de associar a imagem de outra pessoa em cena de sexo ou ato libidinoso intimo também incorre em crime (BRASIL, 2018).

Nesse tipo penal, basta que o agente produza material audiovisual pornográfico sem o consentimento do parceiro, não importando se fará a divulgação do conteúdo. Ora, o dolo do autor é obter cenas ou áudio de um momento intimo sem o consentimento do outro. Destaca-se que a pena imposta no art. 218-C antes exposto é mais grave que a do art. 216-B, pois o dolo do agente é divulgar sem o consentimento da vítima as cenas captadas no momento íntimo (BRASIL, 2018).

Ainda que a Constituição Federal traga a possibilidade de reparação de danos por meio de ação indenizatória, nos termos do seu art. 5º, inciso X, o abalo sofrido pela exposição de um momento íntimo da vítima é irrecuperável e se faz necessário a responsabilização criminal perante o fato.

Ante o exposto, as recentes modificações legislativas foram capazes de punir a violação da intimidade da mulher, uma vez que são as mais atingidas. O fato de divulgar ou obter cenas pornográficas sem o consentimento do parceiro, tipificados nos artigos 216-B e 218-C do Código Penal Brasileiro, buscou coibir e desencorajar a

conduta, que antes era tratada apenas como um crime contra honra e não era suficiente para reduzir os danos causados. (SOUZA, 2020).

Diante do exposto nesse capítulo, resta consignado que o legislador tem se preocupado em prever penas mais duras aos tipos penais já existem e que podem ser aplicados aos delitos praticados no ambiente digital, bem como a promulgação de leis que tragam novos tipos penais de acordo com as inovações criminosas no âmbito virtual. Sendo assim, ainda que a passos curtos, o legislativo mostrou-se atento às mudanças provocadas pela inovação da internet.

4 RESPONSABILIDADE CIVIL E O DEVER DE INDENIZAR

A responsabilidade jurídica pode ser de natureza cível ou penal. O presente trabalho, nos capítulos introdutórios trouxe a responsabilidade penal dos crimes praticados na internet colacionados com as suas respectivas penas e aplicabilidades. Por isso, agora aborda-se o conceito e a aplicação da responsabilidade civil aos autores dos crimes virtuais.

Nesse sentido, Tartuce (2015) traz que o ato ilícito pode ser de natureza civil, penal ou administrativo. Além disso, destaca que alguns atos podem causar dano tanto ao particular, caracterizando o ilícito civil, quanto a sociedade, causando o ilícito penal.

O Código Civil de 2002, no art. 186 preceitua a definição de ato ilícito que consiste em violar direito ou causar dano a outro (material ou moral), por meio de ação ou omissão voluntária, negligência ou imprudência. Ademais, nos termos do art. 187 da mesma lei, o ato ilícito é cometido quando há o abuso de direito por parte do titular (BRASIL, 2002). Portanto, no presente capítulo, serão levantadas as hipóteses de ilícito civil e as causas de responsabilidade, bem como o dever de indenizar.

Diante disto, a responsabilidade civil é o caminho para aquele que comete algum ilícito civil venha ser responsabilizado por tal ato e possa “recompensar” o lesado de forma proporcional ao seu dano. Por isso, nos termos do artigo 935 do Código Civil, a responsabilidade civil independe da criminal (BRASIL, 2002). Para Tartuce (2015) são elementos da responsabilidade civil: conduta humana, culpa, nexo de causalidade, dano ou prejuízo.

A conduta consiste no comportamento humano, na ação humana negligente, omissa ou imprudente que causa o dano. Quando se fala em culpa, tem-se dolo e culpa em sentido estrito. O dolo é a intenção de praticar o ato. E a culpa é o resultado não pretendido. Trata-se da ação ou omissão voluntaria com intuito de praticar o ato ilícito (TARTUCE, 2015).

Por fim, o artigo 927 do Código Civil aduz que a ocorrência de ato ilícito traz a consequência do dever de indenizar, ou seja, reparar o dano. Ademais, a indenização é fixada conforme a gravidade do ato (BRASIL, 2002).

4.1 Aplicação do dever de indenizar aos autores dos crimes virtuais

O Código Penal prevê o ressarcimento à vítima de um ilícito penal, seja contravenção ou crime. Ademais, nos termos do artigo 91, inciso I, há a obrigação de reparar o dano como sendo um efeito da condenação penal (BRASIL, 1940).

Além disso, há a possibilidade de diminuição da pena, quando é oferecida a reparação do dano de forma voluntária pelo agente que cometeu crime sem violência ou grave ameaça, nos termos do artigo 16 do Código Penal, bem como a previsão de uma atenuante da pena quando o agente, antes do julgamento busca reparar o dano sofrido, com fulcro no artigo 65, inciso III, alínea "b" da mesma lei (BRASIL, 1940).

Além disso, o Código de Processo Penal estabelece no artigo 387, inciso IV, que o juiz deve proferir na sentença condenatória o "valor mínimo para reparação dos danos causados pela infração, considerando os prejuízos sofridos pelo ofendido". (BRASIL, 1941). Nesse caso, a sentença penal condenatória torna-se um título executivo judicial no juízo cível, sendo dispensada a ação de conhecimento e possível a ação cível *exdelicto*. Cumpre salientar que a indenização fixada pelo juiz penal pode ser de valor mínimo e poderá ser revisada pelo juiz cível.

Outrossim, há a possibilidade de propor a ação civil que busca reparar os danos causados por um ilícito penal, podendo ser ajuizada a qualquer momento, ou seja, antes, durante ou depois do curso da ação penal. Nesse sentido, o artigo 64 do Código de Processo Penal aduz que: "Art. 64. Sem prejuízo do disposto no artigo anterior, a ação para ressarcimento do dano poderá ser proposta no juízo cível, contra o autor do crime e, se for o caso, contra o responsável civil". (BRASIL, 1941).

Ora, o Código de Processo Penal prevê no seu conteúdo a possibilidade de execução após a sentença condenatória e o trânsito em julgado do processo, como, também, a propositura da ação que busca a reparação do dano de forma independente no juízo cível. Ademais, a segunda opção é viável desde que haja provas suficientes do delito, bem como o nexo de causalidade confirmados. Sendo assim, há a independência das jurisdições, podendo haver a duplicidade de ações, desde que sejam observadas as decisões e que essas não estejam em contradição.

Cumpre salientar ainda que fica facultado ao juiz civil a suspensão do processo cível até que esteja confirmada a autoria e a ocorrência do fato criminoso, nos termos do artigo 64, parágrafo único, do Código de Processo Penal (BRASIL, 1941). Assim, sendo uma faculdade do juiz, tal dispositivo não vincula sua decisão.

Nesse sentindo, os Tribunais Pátrios têm entendido que é possível a condenação cível antes da sentença transitada em julgado na esfera criminal. Ora, o Superior Tribunal de Justiça julgou no REsp: 1829682 SP 2019/0100719-8:

> RECURSO ESPECIAL. RESPONSABILIDADE CIVIL. AÇÃO DE INDENIZAÇÃO POR DANOS. AÇÃO CIVIL EX DELICTO. CONDENAÇÃO NA ESFERA PENAL. HOMICÍDIO. FILHO DA AUTORA. AUTORIA. INCONTROVERSA. REPARAÇÃO. EXAME DAS CIRCUNSTÂNCIAS. 1. Recurso especial interposto contra acórdão publicado na vigência do Código de Processo Civil de 2015 (Enunciados Administrativos nºs 2 e 3/STJ). 2. Cinge-se a controvérsia a discutir se o reconhecimento da existência de um crime e do seu autor na esfera penal ensejam o dever de indenizar na esfera cível. 3. O artigo 935 do Código Civil adotou o sistema da independência entre as esferas cível e criminal, sendo possível a propositura de suas ações de forma separada. Tal independência é relativa, pois uma vez reconhecida a existência do fato e da autoria no juízo criminal, estas questões não poderão mais ser analisadas pelo juízo cível. 4. A partir da doutrina e da jurisprudência do Superior Tribunal de Justiça acerca do tema, é possível concluir que a) em caso de sentença condenatória com trânsito em julgado, há incontornável dever de indenizar, e b) em caso de sentença absolutória em virtude do reconhecimento de inexistência do fato, da negativa de autoria, não haverá dever de indenizar. 5. Não havendo sentença condenatória com trânsito em julgado, deve-se avaliar os elementos de prova para aferir a responsabilidade do réu pela reparação do dano. 6. No caso, ainda que ausente a condenação criminal definitiva, não se pode negar a existência incontroversa do dano sofrido pela autora com a morte de seu filho e a autoria do crime que gerou esse dano. A acentuada reprovabilidade da conduta do réu, ainda que a vítima apresentasse comportamento agressivo e que tenha havido "luta corporal" entre vítima e o réu, não afasta o dever do causador do dano de indenizar. 7. Considerando as circunstâncias fáticas do caso, arbitra-se o valor de R$ 50.000,00 (cinquenta mil reais) a título de indenização por danos morais. 8. Recurso especial conhecido e provido.(STJ - REsp: 1829682 SP 2019/0100719-8, Relator: Ministro RICARDO VILLAS BÔAS CUEVA, Data de Julgamento: 02/06/2020, T3 - TERCEIRA TURMA, Data de Publicação: DJe 09/06/2020) (BRASIL, 2020, s. p.).

Por fim, vale salientar a disposição do Código Civil acerca da discussão. No teor do artigo 1.525 do dispositivo, prevalece o entendimento da possibilidade da independência entre as jurisdições, “não se poderá, porém, questionar mais sobre a existência do fato, ou quem seja o seu autor, quando estas questões se acharem decididas no crime” (BRASIL, 2002). Não obstante, quando um ato ilícito é cometido no âmbito digital se faz necessário que o lesado seja reparado de forma justa e compensatória. Assim, a autora Helena França (2020, p. 483) aduz que:

> Nesta perspectiva, a responsabilidade civil pode ser entendida como toda atividade humana que deve ser feita com responsabilidade; tal instituto integra o direito das obrigações e acarreta para o infrator o dever de reparar patrimonialmente o dano causado, ou seja, trata-se de uma obrigação pessoal que acarretará em perdas e danos se houver o nexo de causalidade entre o ato praticado pelo infrator e o dano sofrido pela vítima.

O exemplo mais simplório que se pode dar nessa tela de responsabilidade civil seria a responsabilização dos autores nos casos de *cyberbullying*, pois além de ser considerado um crime, causa um dano moral e psicológico à vítima, uma vez que é exposta na rede de internet sendo julgada por sua aparência e/ou postura. Portanto, cumpre salientar que a responsabilidade civil adota a teoria do risco e a teoria da culpa, onde Patrícia Pinheiro (2021) implica que a diferença entre elas está na presença obrigatória da culpa para que possa gerar o dever de indenizar.

Pinheiro (2021) segue aduzindo que consequentemente, no âmbito virtual a teoria do risco possui maior adequação, visto que se faz necessário atender aos interesses e as necessidades dos usuários. Cumpre apontar o fato do risco potencial de dano que a internet proporciona aos seus usuários. Por esse motivo, "a teoria do risco atende às questões virtuais e a soluciona de modo mais adequado" (PINHEIRO, 2021, p. 181). Observando ainda o conhecimento do provedor e do usuário, em caso de culpa concorrente. Portanto, se faz necessário estabelecer que:

> Os limites de responsabilidade dos provedores, dos donos de websites, das produtoras de conteúdo, dos usuários de e-mail e de todos os que tenham de algum modo participação, seja em sua produção, seja em sua publicação ou compartilhamento (PINHEIRO, 2021, p.960).

Todavia, a responsabilidade civil dos provedores foi tratada pela lei do Marco Civil da Internet e determinou que somente respondem civilmente por danos quando se mantém inerte após ordem de judicial que, por exemplo, determinou a remoção de um conteúdo ou que não informou o usuário responsável pela produção do conteúdo, incorrendo os provedores apenas em responsabilidade quando esses se mantiverem omissos.

Por isso, entende-se que a intenção do legislador foi equivocada e trouxe prejuízo à sociedade, pois como a vítima de um crime poderá responsabilizar aquele que não tem conhecimento da autoria? Ademais, os provedores tiveram algum proveito com o conteúdo publicado e deveriam ser responsabilizados por concorrerem em culpa, além do risco de atividade assumido. Em atenção ao disposto pelo art. 14 do Código de Defesa do Consumidor, o provedor na qualidade de fornecedor de serviços, deveria responder de forma objetiva pela reparação dos danos causados por defeitos advindos da prestação de serviços.

Por derradeiro, o entendimento do Superior Tribunal de Justiça diverge de Patrícia Pinheiro (2021) e aplica o entendimento do legislador do Marco Civil no que se refere a responsabilidade civil dos provedores. A quarta Turma do STJ julgou um Agravo interno no Agravo em Recurso Especial de n.685720 SP 2015/0066263-2, que tratava acerca da responsabilidade objetiva dos provedores de conteúdo. No julgado, reiterou-se o entendimento compreendido na Lei do Marco Civil que estabelece a responsabilidade do provedor apenas quando este remover o conteúdo exposto que causou lesão a terceiros após ordem judicial ou ao tomar conhecimento da queixa, em casos de crimes contra a dignidade sexual.

4.2 Análise Jurisprudencial

Nesse sentindo, estão colacionados no presente tópico jurisprudências dos Tribunais pátrios que condenaram o autor do crime virtual por dano moral, pois restou configurado o abalo sofrido pela vítima. Nesse sentido, foram selecionados 3 (três) principais crimes cometidos no âmbito digital para fim de pesquisa e amostragem.

4.2.1 Divulgação de cena pornográfica

No Recurso de Apelação Cível nº 0000838-41.2010.8.19.0210 (RIO DE JANEIRO, 2010), julgado na décima nona câmara cível do Tribunal de Justiça do Rio de Janeiro, a desembargadora relatora Lucia Regina Esteves de Magalhães condenou o réu, ex companheiro da vítima, por dano moral no valor R$ 20.000,00 (vinte mil reais), pois divulgou fotos íntimas da mulher e do casal mantendo relações sexuais em uma rede social sem o seu consentimento.

Tal ato, além de ser tipificado como crime, gera dano moral *in reipsa*, pois segundo a Relatora, a mera exposição de imagem que o indivíduo não autorizou, caracteriza ofensa ao direito da personalidade garantido pela Constituição Federal de 1988.Além disso, a magistrada destacou a gravidade da pornografia de vingança e o dano moral presumido no caso em questão.

Por fim, negou a redução do valor antes arbitrado pelo juiz.de primeiro grau. Vale ressaltar que a confirmação da condenação em danos morais e do valor arbitrado em questão se deu na esfera cível. A câmara cível incluiu em suas razões que o réu

apresentou defesa genérica e não impugnou de forma específica os fundamentos da sentença, ou seja, nenhum “contraprova” fora produzida.

Outrossim, no Recurso de Apelação Criminal Nº 0003281-13.2019.8.13.0243(MINAS GERAIS, 2022), julgado pela primeira câmara criminal do Tribunal de Justiça de Minas Gerais, o desembargador relator Wanderley Paiva condenou o autor pelo crime tipificado no art. 218-C,§ 1º, do Código Penal, pois restou comprovado a autoria e a materialidade do delito, uma vez que o agente divulgou cenas de pornografia sem o consentimento da outra parte. Além disso, teve a pena aumentada em razão de ter mantido uma relação intima afetiva com a vítima, caracterizando a vingança pornográfica.

Por fim, houve divergência entre o desembargador relator e revisor no tocante ao valor estabelecido pelo juízo de origem, a título de danos morais provocados à vítima. O relator entendeu que era necessário diminuir o valor de R$15.000,00 (quinze mil reais) estipulado pelo juiz criminal de origem, pois seria necessário avaliar o binômio necessidade/possibilidade das partes envolvidas, quais sejam o autor e a vítima.

Nesse sentindo, a análise da extensão dos danos e do enriquecimento ilícito também deviam ser questionadas pelo juízo. Por isso, arbitrou o valor mínimo de 1 (um) salário mínimo vigente a época dos fatos. Todavia, ainda ressaltou que caso a vítima entendesse que o valor merece análise, assim poderia ser feito na seara cível.

Contudo o Desembargador Revisor Edison Feital Leite divergiu do relator, pois entendeu que o dano causado à vítima e o valor fixado pelo juiz de origem é razoável e não merecia redução. Ademais, destacou ainda que desde a denúncia, o Ministério Público pleiteou pela condenação em danos morais e, portanto, o direito ao contraditório e a ampla defesa foram observados no decurso do processo criminal no que diz respeito à fixação da indenização cível. Sendo assim, todas as provas de dano já foram produzidas no processo criminal e desse modo o valor de R$ 15.000,00 (quinze mil reais) não deveria ser reduzido. Por fim, o Des. Alberto Deodato Neto, acompanhou a o voto divergente do Revisor, mantendo assim o valor fixado na sentença do juízo de origem e o relator restou vencido.

4.2.2 Crime contra a honra

No Recurso de Apelação cível nº 10000212751200001 (MINAS GERAIS, 2022), julgado na décima câmara cível do Tribunal de Justiça de Minhas Gerais, o desembargador relator Cavalcante Motta reconheceu que a apelada cometeu ofensas a honra da apelante, injuriando-a por meio do *WhatsApp* com o envio de áudios que a acusava de prostituição e de um relacionamento incestuoso com o próprio pai.

Nesse sentido, o relator condenou a ré por danos morais no *quantum* indenizatório de R$ 5.000,00 (cinco mil reais), uma vez que a honra subjetiva da apelante foi abalada sobre maneira. Além disso, destacou que a responsabilidade civil independe de condenação criminal, em observância a aplicação do artigo 1.525 do Código de Processo Civil que garante a independência das jurisdições.

No Recurso de Apelação Criminal nº 00171855320218272729 (TOCANTINS, 2022), julgado pela turma das câmaras criminais do Tribunal de Justiça de Tocantins, a desembargadora relatora Jacqueline Adorno de La Cruz Barbosa, julgou conhecido e improvido o recurso que buscava além do reconhecimento de extinção de punibilidade pelo crime de difamação em redes sociais, a minoração do valor indenizatório fixado pelo juiz sentenciante. Sendo assim, a câmara criminal julgou que as palavras proferidas contra a apelada, Prefeita de Palmas/TO, ultrapassaram os limites de liberdade de expressão e tinham o *animus injuriandi*, pois foram feitas em uma rede social onde não se tem limites de propagação.

Outrossim, as ofensas divulgadas não tinham o objetivo de criticar a gestão da então gestora municipal, mas sim atingir sua honra. Por esse motivo, resta configurado o dano moral decorrente de ato ilícito civil caracterizado pelo dolo, ânimo de ofender a pessoa. Por fim, a fixação do quantum indenizatório merece ser mantido no valor de R$ 5.000,00 (cinco mil reais) conforme o juiz de origem havia sentenciado.

4.2.3 Invasão de dispositivo e ou redes sociais

O delito de invasão das redes sociais possui uma particularidade no tocante à responsabilidade civil. É certo que o autor do crime de invasão de dispositivo eletrônico, previsto no artigo 154-A do Código Penal, deve responder tanto pelo processo criminal como também pelo possível dano moral gerado à vítima.

Todavia, há uma discussão jurisprudencial acerca da responsabilidade civil da plataforma onde o perfil está hospedado, pois existem diversas falhas de segurança que facilitam a ação do *hacker*. Sendo assim, pode o órgão julgador entender que há falha na prestação de serviço, devendo ser reconhecida a responsabilidade objetiva, nos termos do artigo 14 do Código de Defesa do Consumidor.

Na Apelação Civil Criminal nº 1031213-56.2021.8.26.0071 (SÃO PAULO, 2022), julgada pela trigésima câmara de direito privado do Tribunal de Justiça de São Paulo, o desembargador relator Lino Machado, julgou procedente a responsabilidade objetiva do provedor da rede social *Instagram*, pois restou comprovada nos autos do processo judicial a falha na prestação de serviços resultada da invasão da conta da autora por *hackers*. Ademais, a apelante não concorreu para que os criminosos obtivessem sucesso na empreitada, sendo assim foi afastada a teoria de culpa exclusiva da vítima. Por fim, o magistrado manteve a condenação em danos morais arbitrada pelo juízo *a quo* no valor de R$ 5.000,00 (cinco mil reais).

Todavia, não sendo caso de falha de segurança, no Recurso de Apelação civil de Nº 1008656-56.2018.8.26.0564 (SÃO PAULO, 2019), julgado pela 2ª câmara de direito privado do Tribunal de Justiça de São Paulo, a desembargadora relatora Marcia Dalla Déa Barone afastou a responsabilidade civil do Facebook, pois esse cumpriu com os ofícios expedidos pelo juízo *a quo*, apresentando dados do responsável como endereço IP, qual seja a corré “Alessandra” por invadir a conta da vítima e divulgar conversas privadas. Ademais, a responsabilidade indenizatória por dano moral recaiu apenas sobre essa no valor de R$ 3.000,00 (três mil reais).

Destarte, resta demonstrado que a responsabilidade civil advinda do cometimento de crime virtual se mostra aplicável aos mais diversos casos. Ainda que haja alguma divergência no tocante à valoração da quantia quando aplicada ainda no juízo criminal, percebe-se que quando há identificação do autor e são colacionadas provas acerca do ocorrido, os julgadores aplicam o valor indenizatório com a finalidade pedagógica para reparar o dano causado à vítima.

5 ATUAÇÃO DO SISTEMA JURÍDICO NACIONAL

Após amplo debate acerca das inovações legislativas pertinentes aos crimes virtuais, é chegado momento de verificar a atuação do sistema jurídico nacional acerca da persecução penal dos agentes. Nesse momento aborda-se a resposta dada pela atividade jurisdicional aos crimes virtuais, bem como as principais mudanças sofridas na sua organização e nos seus métodos de trabalho, quais sejam, investigativos e assistenciais.

Portanto, é necessário compreender que o sistema jurídico nacional é composto pelo Poder Judiciário, quais sejam juízes, desembargadores e ministros, e também pelo o Ministério Público, a Advocacia Pública e Privada e a Defensoria Pública que fazem parte das Funções Essenciais à Justiça, com fulcro nos arts. 127 a 135, da Constituição Federal (BRASIL, 1988).

Além disso, é necessário destacar ainda a importância das instituições do Poder Executivo, relacionadas à segurança pública, em especial às polícias civis que exercem a função de polícia judiciária e são responsáveis por fazer o trabalho investigativo de infrações cometidas, nos termos do art. 144, parágrafo 4º da Constituição Federal (BRASIL, 1988).

5.1 Mudanças e aprimoramentos do sistema jurídico nacional para o combate aos crimes virtuais

Deve-se considerar todas as particularidades existentes na investigação dos crimes cibernéticos e dessa maneira o Ministério Público Federal em atenção à demanda criou o Grupo de Apoio sobre Criminalidade Cibernética (GACC) da 2ª Câmara de Coordenação e Revisão - 2ª CCR coordenado por Fernanda Teixeira Souza Domingos e Neide Mara Cavalcanti Cardoso de Oliveira (GRUPO..., s. d., s. p.).

O referido grupo tem o objetivo: i) capacitar membros e servidores do MPF para o enfrentamento efetivo dos crimes cibernéticos; ii) instituir núcleos regionais para auxílio à investigação dos crimes cibernéticos; iii) implementar base de dados nacional para suporte na persecução dos crimes cibernéticos; iv) averiguar as dificuldades encontradas na persecução dos crimes cibernéticos; v) elaborar ou aperfeiçoar roteiros de atuação para persecução dos crimes cibernéticos (GRUPO..., s. d., s. p.).

Destaca-se o trabalho efetivo do grupo especializado ao oportunizar treinamento e capacitação àqueles que investigam e buscam responsabilizar os autores dos crimes cibernéticos. Nesse sentido, fica disponível o acesso a materiais de apoio e notas técnicas (GOÉS; OLIVEIRA, s. d., s. p.) acerca dos principais passos a serem tomados durante o trabalho investigativo.

Outrossim, em atenção a recomendação dada pela Lei Azeredo, a Policia Civil de diversos estados do Brasil instituiu delegacias especializadas na investigação e combate dos crimes cibernéticos. Por isso, a associação *SaferNet*, anteriormente citada nesse trabalho, levantou delegacias especializadas em combate e investigação de crimes cibernéticos presentes no território brasileiro, conforme tabela a seguir:

Tabela 3: Delegacias Especializadas na Lei 12.737/2012 pela Lei 14.155/2021

Delegaciasespecializadasem crimes virtuais no Brasil
Bahia - Grupo Especializado de Repressão aos Crimes por Meio Eletrônicos
Espírito Santo - Delegacia de Repressão a Crimes Eletrônicos
Maranhão - Departamento de Combate aos crimes tecnológicos
Mato Grosso - Gerência Especializada de Crime de Alta Tecnologia (GECAT)
Minas Gerais-DEICC-Delegacia Especializada de Investigações de Crimes Cibernéticos
Pará - Divisão de Prevenção e Repressão a Crimes Tecnológicos (DRCT)
Paraná - Núcleo de Combate aos Cibercrimes (NUCIBER)
Pernambuco - Delegacia de Polícia de Repressão aos Crimes Cibernéticos
Piauí - Delegacia Especializada de Repressão aos Crimes de Alta Tecnologia - DERCAT
Rio Grande do Sul – Delegacia de Repressão aos Crimes Informáticos (DRCI) – Departamento Estadual de Investigações Criminais (DEIC)
São Paulo- 4ª Delegacia de Delitos Cometidos por Meios Eletrônicos (DIG/DEIC)
São Paulo - Departamento de Homicídios e de Proteção à Pessoa – DHPP (4ª Delegacia de Polícia de Repressão à Pedofilia)
Sergipe - Delegacia de Repressão a Crimes Cibernéticos (DRCC)
Rio de Janeiro - Delegacia de Repressão aos Crimes de Informática (DRCI)
Tocantins - Divisão de Repressão a Crimes Cibernéticos – DRCC
Distrito Federal - Delegacia Especial de Repressão ao Crime Cibernético - DRCC

Goiás - Delegacia Estadual de Repressão a Crimes Cibernéticos (DERCC)
Santa Catarina - Polícia Civil

Fonte: *SaferNet.*

Nesse sentido, ao fazer um recorte no estado do Ceará, percebe-se que o Governador Camilo Santana sancionou em 2020 a criação da Delegacia de Repressão aos Crimes Cibernéticos (DRCC), todavia essa ainda foi implementada de forma efetiva. (CARDOSO, 2020)

Ora, a investigação de crimes ocorridos no ambiente digital, ou através dele, exige profissionais com conhecimento mais especializado e técnico na área, além de ferramentas mais específicas para possibilitar a apuração dos fatos, e as delegacias comuns não vinham atendendo de maneira eficaz esses requisitos, fazendo com que surgisse assim, a necessidade de delegacias especializadas.

Todavia, a sensação de desamparo ainda é elevada, uma vez que são poucas as polícias especializadas na investigação de tais crimes e muitas vezes, encontrar o autor do crime é uma tarefa muito difícil. Portanto, Emeline (2018) discute que é necessário que os profissionais envolvidos na apuração dos crimes sejam especializados na demanda, além de adquirir equipamentos capazes de analisar as condutas, pois entende-se que a impunidade atrelada aos crimes cibernéticos se dá em razão da fragilidade das informações rastreadas do que de alguma lacuna legislativa, uma vez que o dinamismo da internet dificulta a sua fiscalização.

Ademais, Pinheiro (2021) destaca ainda que a problemática presente nos crimes virtuais é a circunstância de que os criminosos estão um passo à frente e estabelece a também a importância do investimento na capacitação e no preparo das polícias aprimorando técnicas e ferramentas para designar perícias forenses, além dos métodos educativos a serem compartilhados com a população para que estejam atentos às modalidades de golpes e outros crimes.

Outrossim, a Defensoria Pública e os advogados, enquanto função essencial à justiça, encontraram uma demanda de atuação demasiadamente forte, em que pese a imensa procura de vítimas, além da possibilidade desses entes buscarem especialização no direito digital. Não obstante, o papel da defesa nos procedimentos é considerável, e Quintiliano, Filho e Plentz (2019) interpreta a imagem do advogado especialista em Direito Cibernético como um apoio à polícia no trabalho investigativo, atuando com

uma defesa investigativa e em colaboração com a Polícia para se chegar em uma resposta às vítimas, além de impulsionar a persecução criminal.

5.2 Autoria e materialidade do delito virtual: da identificação dos autores e outros procedimentos investigativos

Sendo assim, o procedimento investigativo de competência da polícia judiciária deve sempre buscar a autoria e a materialidade do delito, nos termos do art. 4º do Código de Processo Penal (BRASIL, 1941). Portanto, a legislação brasileira busca garantir a condução da investigação de forma transparente e séria, afim de evitar nulidades dos atos investigativos e a quebra da cadeia de custódia das provas.

Por essa razão, após o recebimento da *notitia criminis* deverá a polícia judiciária seguir uma espécie de "passo a passo" com o fito de garantir a ordem do inquérito policial, como por exemplo: dirigir-se ao local para garantir a conservação da cena do crime até a chegada dos peritos criminais, apreender objetos com relação ao fato, colher provas que esclareçam os fatos delituosos, ouvir o ofendido, bem como o indiciado, realizar o procedimento de pessoas e coisas, se for o caso, determinar examesde corpo de delito e outras perícias técnicas, conforme determina o art. 6º do Código de Processo Penal(BRASIL, 1941).

Conseguinte, a autoridade policial terá o prazo de 10 dias para concluir as investigações caso o indiciado esteja preso, ou 30 dias se estiver solto, e redigir relatório minucioso para o juiz, apontando todos os indícios de autoria e materialidade encontradas pelo trabalho da sua equipe de polícia. Nesse momento, o Ministério Público poderá fazer a denúncia, solicitar novas diligências para elucidação de dúvidas, requerer o arquivamento ao juiz ou propor acordo de não persecução penal, desde que os requisitos do art. 28-A do CPP estejam preenchidos, quais sejam: pena mínima menor que 4 anos, confissão deliberada, não ser caso de arquivamento e o crime não ser com violência ou grave ameaça (BRASIL, 1941).

Sendo caso de denúncia, o Ministério Público deve se atentar aos requisitos do artigo 41 do CPP que estabelece os requisitos para que a denúncia seja feita, quais sejam: a exposição dos fatos em detalhes, qualificação do acusado (aqui está sendo indicado o suspeito pela autoria), a tipificação do crime e, se possível, rol de testemunhas (BRASIL, 1941). Ora, caso não sejam observados a recomendação de

redação da denúncia ou queixa determinada por lei, o juiz poderá rejeitá-la, pois são consideradas ineptas nos termos do art. 395, inciso I, do CPP.

Além disso, o juiz ainda deve analisar a condição do exercício da ação, ou seja, se o Ministério Público ou o querelante possui capacidade de estar no polo ativo da demanda. E por fim, o magistrado ainda deve observar se há justa causa para o prosseguimento da ação penal, ou seja, se os indícios de autoria e materialidade são suficientes para que haja uma instrução criminal (BRASIL, 1941).

Portanto, é importante salientar que com a ocorrência de um crime virtual os mesmos requisitos devem ser observados. Ainda que alguns procedimentos não sejam possíveis ou estritamente necessários, os indícios de autoria e materialidade são inegociáveis e sem esses não há processo penal e nem caminho para responsabilizar o agente do delito.

Sendo assim, dentre os principais questionamentos feitos pelos usuários de internet quanto à responsabilização dos autores dos delitos está na identificação desses, ou seja, reconhecimento da autoria criminal, uma vez que muitos são os meios utilizados para que suas identidades sejam preservadas. Tal pergunta é relevante, pois é possível criar perfis falsos com muita facilidade.

Nesse sentido, o anonimato infere a sensação de impunidade, pois os atos dos usuários são, na verdade, praticados por uma máquina que não possui identidade real. Além disso, a possibilidade de criar novos perfis para o mesmo indivíduo é ilimitada.Entretanto, a máquina conectada à rede mundial de computadores é identificada por uma numeração chamada IP.

Portanto, é de conhecimento do Direito Digital que a forma mais eficiente para localizar uma máquina que acessou a rede é por meio do seu endereço IP, sendo este definido no art. 4º, inciso III: “endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais”. (BRASIL, 2014, s. p.) Ou seja, o IP é o endereço da máquina que acessou a internet.

Entretanto, esse endereço numérico poderá ser destinado para computadores diferentes, ainda que não simultaneamente, mas ocorrendo em um espaço de tempo curto. Por isso, é de extrema relevância que seja sempre resguardada pelas vítimas a data e o fuso horário do delito cometido, pois o trabalho dos órgãos responsáveis pela investigação em relacionar o endereço IP à máquina e posteriormente a máquina ao

sujeito que delinquiu será uma problemática a ser resolvida mais facilmente. (AGUIAR, 2015 *apud* COLLI, 2010, p. 89-91).

No tocante ao assunto, Pinheiro (2021, p. 693) entende que o IP é o sinônimo de identificação virtual e o anonimato é relativo, pois esses podem não possuir uma identidade real atrelada. Um caso análogo à realidade virtual, quando da existência de contas bancárias e empresas "fantasmas" vinculadas às identidades físicas falsas. Em consonância, a Procuradoria da República no Estado de São Paulo (2006) expõe que:

> [...] a identificação de um criminoso cibernético depende, em grande medida, da identificação do endereço IP do computador por ele utilizado. Um provedor de acesso normalmente controla uma gama de centenas ou milhares de endereços de IP, os quais são atribuídos aos assinantes, durante o período de conexão. Os números de IP são normalmente dinâmicos, ou seja, cada vez que um usuário faz a conexão à rede por meio de um provedor de acesso, seu computador é aleatoriamente vinculado a um endereço de IP, disponibilizado pelo provedor. O computador do usuário retém o endereço de IP pela duração da conexão, impedindo que o mesmo protocolo seja atribuído a outro assinante, no mesmo período. Quando, porém, o usuário encerra a conexão, o protocolo torna-se novamente disponível para ser atribuído a outro assinante. Assim, um endereço de IP de dado usuário normalmente difere a cada vez que ele se conecta por meio de algum provedor, e um dado endereço de IP poder estar associado a centenas ou milhares de diferentes usuários por um período de semanas ou meses.Para que seja possível identificar qual usuário estava ligado a determinado endereço de IP, num determinado dia e hora, os provedores de acesso e também de hospedagem devem manter um banco de dados eletrônico, uma lista de cada endereço de IP utilizado, juntamente com a correspondente data, horário e região de conexão [...] (BRASIL, 2006, s. p.).

Contudo, além da complexidade levantada para obtenção do endereço IP, ainda deve-se levar em consideração as manobras utilizadas pelos criminosos com o intuito de "camuflar" seu código IP, além de ataques remotos. Sendo assim, os peritos e investigadores devem ter conhecimento acerca desse comportamento, pois podem pôr em risco o resultado da apuração. (MAIA, 2017).

Portanto, demonstra-se que o rastreio para obtenção de um endereço IP é complexo e requer agilidade das autoridades e resguardo de informações complementares por parte da vítima.

Insta salientar que a Lei do Marco Civil determina que os provedores de internet resguardem pelo prazo de 1 ano os registros de conexão, sob sigilo, em ambiente controlado e de segurança, nos termos do art. 13 da referida lei, sob pena de responder por todos os danos resultantes. Outrossim, é importante ressaltar que todos os atos cometidos na rede são protegidos sua confidencialidade, por parte da Constituição Federal e da Lei do Marco Civil, não sendo permitido a quebra do sigilo sem ordem

judicial (BRASIL, 1988; 2014). Nesse sentindo, segundo os autores Quintiliano, Filho e Plentz (2019, p.25):

> A investigação cibernética é muito dependente dos provedores de serviços de internet, visto que as informações que poderão permitir a comprovação da materialidade, dinâmica e autoria dos crimes estão em seu poder e estão protegidas por sigilo.

Portanto, o Manual de Investigação disponibilizado pela Procuradoria da República no Estado de São Paulo (2006, p.15) acerca das investigações de crime cibernético convalesce a ideia de que após o recebimento da notícia do crime virtual, a principal ação a ser tomada é o conhecimento do meio utilizado para cometer o crime.

> Quando recebemos a notícia de um crime cibernético, a primeira providência a tomar é a identificação do meio usado: trata-se de a) um website?; b) um e-mail?; c) programas de troca de arquivos eletrônicos (do tipo Kazaa)?; d) arquivos ou mensagens ofensivas trocados em programas de mensagem instantânea (do tipo MSN Messenger ou ICQ)?; e) arquivos ou mensagens ofensivas trocados em salas de bate-papo (chats)?; f) grupos de discussão (como yahoogroups)?; ou g) comunidades virtuais como o Orkut? As características de cada um desses meios são diferentes e, por isso, as medidas a serem tomadas são igualmente distintas.

Ora, observa-se que o depoimento da vítima deve ser o mais transparente possível, pois somente com os detalhes esclarecidos a polícia poderá trilhar um caminho até o agente do crime. Por isso, o investigador deve filtrar as informações mais relevantes para o caso.

Entretanto, em razão do constrangimento causado pelo delito, a vítima tende a tentar se desfazer de objetos e *softwares* o qual o crime foi cometido, pondo em risco a confiabilidade e a análise dos materiais por parte dos peritos criminais, pois muitas vezes tentam apagar o conteúdo ou até mesmo formatar o aparelho (*desktop*, celular, tablete) (MAIA, 2017). Por isso, a instrução às vítimas é fundamental, sobretudo acerca dos procedimentos necessários para manter o rastro do agente delinquente, mediante políticas públicas e programas de acesso ao conhecimento, bem como projetos que debatem sobre o assunto. A Procuradoria da República no Estado de São Paulo (2006, p. 15) relata ainda:

> De modo geral, podemos dizer que as evidências dos crimes cibernéticos apresentam as seguintes características: a) possuem formato complexo (arquivos, fotos, dados digitalizados etc.); b) são voláteis, i.e., podem ser apagadas, alteradas ou perdidas facilmente; c) costumam estar misturadas auma grande quantidade de dados legítimos, demandando, por isso, uma análise apurada pelos técnicos e peritos que participam da persecução penal.

Além da busca pela autoria, requer que seja levantada meios probatórios acerca do crime, estabelecendo assim a materialidade do delito. A depender do tipo penal, a vítima poderá, por exemplo, registrar o fato criminoso por meio de um *PrintScreen*do dispositivo eletrônico, guardar o e-mail, domínio e registros de acessos também. Entretanto, o questionamento a acerca da veracidade dessas provas é levantado no processo criminal, tanto pelo magistrado quanto pela parte contrária.

Nesse sentido, o STJ reafirmou que há nulidade de provas baseadas pura e simplesmente por meio de *printscreen*, pois não há como verificar sua autenticidade havendo ainda quebra da cadeia de custódia.

A sexta turma do referido Tribunal Superior invalidou as provas obtidas por *printscreen*, pois a Ministra Laurita Vaz entendeu que há precedente considerando inválida a prova obtida pelo espelhamento de conversas via *WhatsApp Web*, porque a ferramenta permite o envio de novas mensagens e a exclusão de mensagens antigas ou recentes, tenham elas sido enviadas pelo usuário ou recebidas de algum contato, sendo que eventual exclusão não deixa vestígio no aplicativo ou no computador (RHC 99.735).

Por essa razão, determinou que as provas dessa natureza fossem desentranhadas do processo por serem consideradas provas ilícitas. Em razão do segredo judicial o número do processo original não foi divulgado (SEXTA..., 2021, s. p.). Insta salientar que a invalidade das provas poderia ser evitada caso alguns procedimentos especiais fossem feitos. Destaca-se, portanto, a importância da ata notarial levantada pelos autores Quintiliano, Filho e Plentz (2019, p.27) ao exemplificar um dos procedimentos a serem tomados em caso de crime virtual:

> Em caso de ocorrência de conduta criminosa, praticada por meio da internet, deve-se imediatamente promover a coleta e a preservação das evidências digitais que poderão comprovar a materialidade do fato, por meio da emissão de Ata Notarial, em Cartório. A Ata Notarial, por ter fé pública, é um meio de prova extremamente forte e que deve ser sempre utilizado nas investigações cibernéticas não-oficiais.

Ademais, aduz o art. 405 do Código de Processo Civil que: “O documento público faz prova não só da sua formação, mas também dos fatos que o escrivão, o tabelião, ou o funcionário declarar que ocorreram em sua presença” (BRASIL, 2015, s. p.).

Todavia, a busca por tal medida muitas vezes não é viável, pois demanda custo financeiro superior, além de não ser um meio ágil. Outrossim, a prova a ser

analisada por meio de ata notarial é feita por uma pessoa leiga, que testemunhará sem qualquer perícia técnica, sobretudo quando se trata de uma prova advinda de um meio dinâmico como o ambiente virtual.

Nesse contexto, urge a necessidade de desenvolver uma plataforma que pudesse fazer a verificação de autenticidade de forma rápida e com baixo custo. Por essa razão, a solução dada pela ferramenta *online* chamada *Verifact* é a coleta de provas digitais auditáveis e com validade jurídica de que o registro corresponde ao fato original na internet. No site da ferramenta encontra-se uma explicação acerca do serviço realizado:

> Nesse método é produzido um relatório técnico certificado com as telas registradas, dados e metadados técnicos auditáveis para uma eventual perícia técnica, além de um vídeo de registro da navegação, com áudio, além de arquivos baixados durante a sessão .O relatório técnico leva a assinatura certificada da Verifact e carimbo de tempo ICP-Brasil. O carimbo de tempo ICP-Brasil, ou timestamp utilizado no relatório gera imutabilidade dos dados, registrando o exato dia e horário que o conteúdo foi acessado na internet e impedindo que os dados sejam apagados ou alterados após o registro. Até mesmo se o conteúdo original desaparecer da Internet, com os dados e metadados coletados é possível realizar ampla perícia técnica das informações, para comprovar que o material é aquilo que diz ser e vem de onde diz ter vindo.

A ferramenta já consta como meio seguro e amplamente aceito como prova autenticada no meio judicial. Em que pese, segundo o Acórdão n. º 060024946-A do TRE do Piauí:

> Embora os Representados tenham mencionado a ocorrência de manipulação no material apresentado pela Representante, observo que as imagens foram extraídas do próprio perfil das redes sociais dos mesmos, verificada sua autenticidade por meio do serviço Verifact, como bem destacou o Procurador Regional Eleitoral. Ademais, para análise da irregularidade no presente caso faz-se necessário a utilização de tão somente uma simples régua para aferir a exata dimensão das fontes empregadas nos nomes dos candidatos (BRASIL, 2020, s. p.).

Ademais, o Ministério Público Federal firmou parceria para utilização da tecnologia da ferramenta *Verifact* para coleta de provas digitais, corroborando para validar a qualidade e efetividade do serviço prestado pela plataforma (NAVEGAÇÃO..., s. d., s. p.).Além disso, diversos outros órgãos também estabeleceram convênio com a empresa, quais sejam ABRACRIM Nacional (Associação Brasileira dos Advogados Criminalistas), Caixa de Assistência dos Advogados de Alagoas, da OAB e a APECOF (Associação Nacional dos Peritos em Computação Forense).

Visando a organização de um procedimento básico a ser constituído na investigação, o Ministério Público Federal facilitou o entendimento produziu uma

“linha do tempo” concatenando os meios para obtenção de provas a acerca da autoria e da materialidade do delito.

O primeiro passo é a identificação do crime e do meio empregado, qual seja e-mail, redes sociais ou site na web. Além disso, verificar o responsável do provedor de aplicações de internet e a consulta é feita nos sites do www.registro.br ou *whois* (informa se provedor está no exterior).

Posteriormente, é fundamental que a vítima tome as iniciativas iniciais acerca da materialidade do crime. Ou seja, deve-se notificar o provedor de internet ou do aplicativo identificado anteriormente para que esses preservem os registros e *logs* referente à questão. Esses devem atuar com colaboração, sob pena de sofrer responsabilizações cíveis mais tarde. Ressalta-se que o pedido deve ser feito o mais breve possível, uma vez que os agentes podem sorrateiramente tirar as páginas de circulação e prejudicar a persecução penal.

Em outras palavras, deve-se assegurar a integralidade dos dados. Nesse momento, também entra a possibilidade de tirar *printscreen* da tela onde constam as provas dos delitos e formalizar mediante Ata notarial ou por meio de aplicativos como o *Verifact*, conforme citado anteriormente.

Em seguida, é cabível o pedido judicial da quebra de sigilo de dados telemáticos com a finalidade de obter-se o endereço IP da máquina perante o provedor de aplicação à Internet, bem como dados que possibilitem a comprovação material do ato delituoso, quais sejam fotos, textos ou vídeos postados no provedor. Esse pedido tem fundamentação jurídica, nos termos do artigo 10, §§ 1º e 2º, do Marco Civil da Internet.

Com o endereço IP em mãos, deve-se buscar o provedor de conexão de dados, ou seja, as operadoras de telefonia ou telecomunicações, que ofereçam banda larga. A consulta pode ser feita nos sites do www.registro.br ou *whois* (informa se provedor está no exterior), conforme informado anteriormente. Ora, há a possibilidade de requerer ao provedor de conexão os dados do usuário indiciado, nos termos do artigo10, § 3º, do Marco Civil da Internet. Todavia, pode haver a recusa por parte desses, pois podem requerer a apresentação de ordem judicial.

Ultrapassado o conflito, o provedor de conexão disponibilizará os dados do titular daquele endereço IP, como nome e o endereço do terminal de conexão, que poderá ser um computador, celular, dentre outros dispositivos.

Por fim, a autoridade judicial deverá expedir um mandado de busca e apreensão do dispositivo eletrônico para que seja submetido à perícia e os demais procedimentos atinentes à conclusão do inquérito como, por exemplo, depoimento do indiciado.

Ressalta-se que esse é um procedimento básico e que pode ter outras intercorrências ou mecanismos especiais a depender do meio utilizado para a concretização do crime.

Destarte, a busca pela autoria e a materialidade dos crimes virtuais requer que a vítima, a polícia investigativa e o Ministério Publico estejam alinhadas e sem nenhuma reserva. Além disso, o conhecimento técnico é imprescindível assim como o conhecimento dos procedimentos necessário para validação dos elementos probatórios.

6 CONSIDERAÇÕES FINAIS

Diante o exposto no presente trabalho, algumas considerações finais merecem ser apontadas. Entende-se que é preciso que a mobilização seja compreendida tanto pelo Poder Legislativo, formulando leis que regulem o serviço de internet e preveja consequências personalizadas àqueles que se utilizam da Rede Mundial de Computadores de maneira criminosa, quanto pelo sistema judiciário, que deverá investir na sua tecnologia e na capacitação dos seus servidores e membros, além das adequações precisas nos métodos investigativos desempenhados pelos órgãos de segurança pública.

No primeiro capítulo, aborda-se o advento da internet e urgênciada necessidade de alguma forma de regulação legislativa com o fim de garantir os direitos e deveres dos usuários, uma espécie de "regras da boa convivência". A hipótese levantada no capítulo é o desafio para o direito em face da dinâmica da internet, no sentindo de possibilitar previsões de condutas, bem como garantias específicas.

Ainda que a internet tenha entrado no cotidiano do brasileiro em meados dos anos 90, nenhuma regulação especial foi feita para encarar o ônus da internet, qual seja, o potencial poder de cometer crimes e infringir a privacidade do outro.

Surge então, a associação *Safernet* que mais tarde obteve destaque e apoio do sistema judiciário brasileiro. Todavia, ainda não foi suficiente o trabalho desenvolvido por tal instituição, pois os delitos ainda ocorriam sem freios e a responsabilização específica e necessária com fim pedagógico e que trouxesse amparo efetivo à vítima não foi garantida.

Somente em 2014, o legislativo conseguiu sancionar a Lei do Marco Civil que foi considerada vaga e espaça, uma vez que não previa qualquer criminalização de condutas e tão pouco trouxe qualquer mudança significativa para a resolução de conflitos. Considera-se um compilado dos direitos fundamentais advindos da Constituição Federal. Ademais, o clamor dos usuários não fora atendido, pois esses buscavam direcionamentos e definições concretas acerca dos ilícitos cometidos no ambiente virtual.

No segundo capítulo, apontam-se as inovações legislativas no ordenamento jurídico brasileiro que era pressionado pela alta demanda advinda da movimentação do judiciário por parte das vítimas dos crimes virtuais. Nesse sentido, a capítulo deteve-se em trazer as principais leis que trouxessem novos tipos penais para o código penal, como também agravamentos de penas em ilícitos já tipificados que fossem praticados

no âmbito virtual. Demonstra-se que a preocupação do legislador em trazer uma resposta aos usuários e tem buscado acompanhar o ritmo frenético da Era Digital. Entende-se que o legislativo buscou trazer penas inibitórias e específicas com o objetivo de frear a ação dos criminosos e saciar o anseio dos usuários, além de mostrar-se atento às mudanças provocadas pela inovação da internet.

No terceiro capitulo, demonstra-se que a responsabilidade civil é um meio de impor limites àqueles que cometem ilícitos na internet, uma vez que a indenização por danos morais é cabível em casos de crimes e tem o caráter pedagógico afim de reparar o dano causado à vítima. Outrossim, a hipótese de mover duas ações em jurisdições distintas é cabível, desde de que haja elementos comprobatórios e que essas estejam em consonância.

No quarto capítulo, levanta-se a hipótese da necessidade de especialização dos profissionais que compõe o sistema jurídico nacional, quais sejam Ministério Público, órgãos de segurança pública, Defensoria Pública e escritórios de advocacia. Tal hipótese é confirmada ao percebe-se a mobilização desses na estruturação de suas equipes, na promoção de treinamentos capacitivos, preparo das polícias aprimorando técnicas e ferramentas para designar perícias forenses.

Outrossim, a busca pela autoria e a materialidade dos crimes virtuais requer um método investigativo eficaz e que a vítima, a polícia investigativa e o Ministério Publico estejam alinhados e sem nenhuma reserva. Além disso, o conhecimento técnico é imprescindível assim como o conhecimento dos procedimentos necessário para validação dos elementos probatórios e o sucesso da persecução penal.

Destarte, essa pesquisa se propôs a responder a indagação: quais são os caminhos para que os autores dos crimes cibernéticos sejam responsabilizados? O resultado se dá em três principais aspectos: i) a previsão legislativa específica para relações e condutas ilícitas produzidas no âmbito virtual; ii) o caráter pedagógico da reparação por danos, sejam esses morais ou materiais, uma vez que o impacto financeiro pode trazer uma certa inibição para as condutas ilícitas; iii) uma persecução penal bem-sucedida com métodos investigativos eficazes e específicos para a garantir os elementos que asseguram a autoria e a materialidade do delito.

REFERÊNCIAS

AGUIAR, Poliana Policarpo de Magalhães *et al*. **Gestão jurídico-estratégica do cibercrime no contexto da ciberdemocracia.** 2015. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/14244. Acesso em: 08 Nov. 2022.

BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro: Elsevier, 2004.

BONONI, Fernando. Crimes cibernéticos: Avanço legislativo no Brasil. **Portal Migalhas,** 2021. Disponível em: https://www.migalhas.com.br/depeso/347513/crimes-ciberneticos--avanco-legislativo-no-brasil. Acessado em: 08 nov de 2022.

BRAGANÇA, Isabela. **Evolução da comunicação**. 2009. Disponível em: https://pt.scribd.com/doc/16088693/Evolucao-da-comunicacao-humana-Podemos-explicar-a-historia-da-existencia-humana-atraves-das-etapas-do-desenvolvimento-da-comunicacaoÇ

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 07 nov. 2022.

BRASIL. **Conflito de Competência Nº 67.343 - GO (2006/0166153-0)**. Conflito Negativo De Competência. Penal E Processo Penal. Fraude Eletrônica Na Internet. Transferência De Numerário De Conta Da Caixa Econômica Federal. Furto Mediante Fraude Que Não Se Confunde Com Estelionato. Consumação. Subtração Do Bem. Aplicação Do Art. 70 Do Cpp. Competência Da Justiça Federal Paranaense. Autor: Justiça Pública. Réu: Em Apuração. Suscitante: Juízo Federal Da 11a Vara Da Seção Judiciária Do Estado De Goiás. Suscitado: Juízo Federal Do Juizado Especial De Campo Mourão - SJ/PR. Relatora: Ministra Laurita Vaz, 25 de agosto de 2021. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202102439278&dt_publicacao=01/09/2021. Acesso em: 22 nov. 2022.

BRASIL. Decreto-**Lei nº 2.848, de 07 de dezembro de 1940.** Código Penal. Rio de Janeiro, RJ: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 28 nov. 2021.

BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**.Código de Processo Penal. Rio de Janeiro, RJ: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm. Acesso em: 07 nov. 2022.

BRASIL. **Decreto-lei nº 3.914, de 9 de dezembro de 1941**. Lei de Introdução ao Código Penal [...]. Rio de Janeiro, RJ: Presidência da República, [1941]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm. Acesso em: 07 nov. 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília,

DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 07 nov. 2022.

BRASIL. **Lei nº 11.829, de 25 de novembro de 2008**. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Brasília, DF: Presidência da República, [2008]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso em: 07 nov. 2022.

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. Brasília, DF: Presidência da República, [2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 07 nov. 2022.

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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 28 maio 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2014]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 nov. 2022.

BRASIL. **Lei nº 13.105, de 16 de Março De 2015**. Código de Processo Civil. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 07 nov. 2022.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável[...]. Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm. Acesso em: 07 nov. 2022.

BRASIL. **Lei nº 13.772, de 19 de dezembro de 2018**. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) [...]. Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13772.htm. Acesso em: 07 nov. 2022.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, [2019]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 07 nov. 2022.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático [...]. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 07 nov. 2022.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**.Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 07 nov. 2022.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 07 nov. 2022.

BRASIL. **Lei nº 9.099, de 26 de setembro de 1995**. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Brasília, DF: Presidência da República, [1995]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9099.htm. Acesso em: 07 nov. 2022.

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

BRASIL. Superior Tribunal de Justiça (3. Seção). **Conflito de Competência nº 181.538 - Sp (2021/0243927-8)**.Conflito De Competência. Processual Penal. Contratação De Empréstimo Bancário E Transferência De Valores. Fraude Eletrônica. Ausência De Entrega Voluntária Do Bem Pela Vítima. Estelionato. Não Configuração [...]. Suscitante: Juízo de Direito da 5a Vara Criminal de Campinas – SP. Suscitado: Juízo de Direito da 1a Vara de Santa Helena – MA. Relatora: Ministra Laurita Vaz, 25 de agosto de 2021. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202102439278&dt_publicacao=01/09/2021. Acesso em: 22 nov. 2022.

BRASIL. Tribunal de Justiça do Estado do Amazonas (1. Câmara Criminal). **Apelação Criminal n.º 0679630-36.2021.8.04.0001**. Penal E Processo Penal. Apelação Criminal. Estelionato Majorado. Fraude Eletrônica. Art. 171, § 2.º-A, Do Código Penal [...]. Apelante: Lucas Alfredo de Moraes. Apelado: Ministério Público do Estado do Amazonas. Relator: Des. José Hamilton Saraiva Dos Santos, [s. d.]. Disponível em: https://consultasaj.tjam.jus.br/cjsg/getArquivo.do?conversationId=&cdAcordao=3024011&cdForo=0&uuidCaptcha=sajcaptcha_. Acesso em: 22 nov. 2022.

BRASIL. Tribunal de Justiça do Estado do Distrito Federal e Territórios (Câmara). **Recurso Eleitoral 0600249465825**. Eleições 2020. Embargos de declaração. Recurso eleitoral. Representação [...]. Embargante: Nestor Renato Pinheiro Elvas. Embargado: Coligação Pra Bom Jesus Continuar Avançando. Relator: Des. Erivan José da Silva Lopes. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tre-pi/1273429621/inteiro-teor-1273429641. Acesso em: 07 nov. 2022.

BRASIL. Tribunal de Justiça do Estado do Piauí (Vice-Presidência). **Nome do Recurso07179219020228067000**0. Conflito negativo de jurisdição. Juízo da 2ª Vara Criminal [...].Relator: Des. Silvanio Barbosa dos Santos. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-df/1586369726/inteiro-teor-1586369727. Acesso em: 07 nov. 2022.

BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro (19. Câmara). **Apelação 00008384120108190210**. Apelação cível. Responsabilidade civil subjetiva. Ação indenizatória por danos morais ajuizada em face de ex-conjuge, com fundamento na criação de uma página na já extinta rede social denominada Orkut [...].Relatora: Desa. Lucia Regina Esteves de Magalhães. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-rj/1169880514. Acesso em: 07 nov. 2022.

BRUNO, Aníbal. **Crimes contra a pessoa**. 5. ed. rev. Rio de Janeiro: Rio. 1979. p. 300.

CARDOSO, Antônio. Governo do Ceará cria Delegacia exclusiva para combater crimes cibernéticos. **Ceará GOV.** Disponível em: https://www.ceara.gov.br/2020/09/25/governo-do-ceara-cria-delegacia-exclusiva-para-combater-crimes-ciberneticos/ . Acesso em: 05 dez. 2022

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

CONTE, Christiany Pegorari; FIORILLO; Celso Antonio Pacheco. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2016. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788547204198/. Acesso em: 07 nov. 2022.

DATASAFER. **Indicadores helpline** [s. d.]. Disponível em: https://indicadores.safernet.org.br/helpline/helplineviz/pt/. Acesso em: 07 nov. 2022.

DEFLEUR, Melvin L. **Teorias da Comunicação em Massa**. Tradução: Octavio Alves Velho. 5 ed. Editora Zahar: Rio de Janeiro, 1993.

DENÚNCIAS de Crimes Cometidos Pela Internet Mais Que Dobram Em 2020. **G1,** São Paulo, 09 fev. 2021. Disponível em: g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml. Acesso em: 17 ago. 2022.

DIAS, Carlos Antônio. **Tecnologias e novos modos de comunicação**. A (re)invenção do conhecimento no ciberespaço na percepção dos docentes imigrantes digitais de uma universidade pública. 2013. (Dissertação)– Mestrado em Cognição e Linguagem. Universidade Estadual do Norte Fluminense Darcy Ribeiro – Uenf, Campos Dos Goytacazes – Rj, 2013.

FERREIRA, Ivette Senise. **A criminalidade informática**: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2005.

FERREIRA, Luiz Cláudio; PEDROSA, Leyberson. Como era a internet no Brasil antes da comercialização. **Agência Brasil**, 04 maio 2021. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-04/como-era-internet-no-brasil-antes-da-comercializacao. Acesso em: 07 nov. 2022.

FRANÇA, Marlene Helena. A responsabilidade civil e criminal na internet: o papel do judiciário brasileiro. **Revista Quaestio Iuris**, v. 13, n. 01, p. 480-507, 2020. Disponível em: https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/41943 Acesso em: 08 Nov. 2022

GANDRA, Alana. Empresas adotam home-office por conta do coronavírus. BNDES recomenda aos funcionários quarentena após viagem. **Agência Brasil**, Rio de Janeiro, 07 março 2020. Disponível em: https://agenciabrasil.ebc.com.br/saude/noticia/2020-03/empresas-adotam-home-office-por-conta-do-coronavirus. Acesso em: 22 nov. 2022.

Greco, Rogério. **Curso de Direito Penal:** parte especial. 11. ed. Niterói, RJ: lmpetus, 2015.

GRUPO de Apoio sobre Criminalidade Cibernética – GACC. **Ministério Público Federal**, [s. l.], [s. d.], [s. p.]. Disponível em: https://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/comissoes-e-grupos-de-trabalho/combate-crimes-cirberneticos. Acesso em: 07 nov. 2022.

HUNGRIA, Nélson. **Comentários ao Código Penal**. São Paulo: Saraiva, 1980.

INOUYE, Giselle Ashitani *et al*. **Direito Digital Global: o Tribunal Penal Internacional como mecanismo de apuração da responsabilidade individual nos crimes cibernéticos.** 2016. Disponível em: https://repositorio.pucsp.br/jspui/handle/handle/7090. Acesso em: 08 nov. 2022.

JESUS, Damásio de. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

JESUS, Damásio de; OLIVEIRA, José Antonio Milagre de. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. E-book. 9788502627246. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627246/. Acesso em: 07 nov. 2022.

KEMP, Simon. Digital 2022: Global Overview Report. **Data Reportal**, 26 de janeiro de 2022. Disponível em: https://datareportal.com/reports/digital-2022-global-overview-report. Acesso em: 07 nov. 2022.

LIMA; Murilo Siolari de; MARCATO, Gisele Caversan Beltrami. *In*: **ETIC - Encontro De Iniciação Científica**, v. 18, n. 18, 2022. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/9414/67651301. Acesso em: 07 nov. 2022.

LIN, Nelson. Pesquisa aponta que o Brasil ampliou compras online na pandemia. **Radio Agência Nacional**, 21 julho 2021. Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/economia/audio/2021-

07/pesquisa-aponta-que-o-brasil-ampliou-compras-online-na-pandemia. Acesso em: 22 nov. 2022.

LUNARDI, Nataly Moretzsohn Silveira Simões et al. Aulas Remotas Durante a Pandemia: dificuldades e estratégias utilizadas por pais. **Educação & Realidade**[online]. 2021, v. 46, n. 2 [Acessado 17 Agosto 2022], e106662. Disponível em: https://doi.org/10.1590/2175-6236106662. Epub 09 Jun 2021. ISSN 2175-6236. https://doi.org/10.1590/2175-6236106662.

MAIA, Teymisso Sebastian Fernandes. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro.** 2017. Disponível em:https://repositorio.ufc.br/handle/riufc/31996. Acesso em: 08 Nov 2022

MARRA, Fabiane Barbosa. Desafios do direito na era da internet: uma breve análise sobre os crimes cibernéticos. **Journal of Law and Sustainable Development**, v. 7, n. 2, p. 145-167, 2019.

MINISTÉRIO PÚBLICO FEDERAL**. A atuação do Ministério Público Federal no combate aos crimes cibernéticos.** 2018. Disponível em: https://www.cnmp.mp.br/portal/images/Palestras/Atua%C3%A7%C3%A3o_do_MP_no_combate_aos_crimes_cibern%C3%A9ticosINFANCIA_E_JUVENTUDE.pdf. Acesso em: 07 nov. 2022.

MINISTÉRIO PÚBLICO FEDERAL. Procuradoria da República no Estado de SP. Crimes Cibernéticos. **Manual Prático de Investigação.** 2006, p. 15. Disponível em: http://tmp.mpce.mp.br/orgaos/CAOCRIM/pcriminal/ManualdeCrimesdeInform%C3%A1tica-versaofinal.pdf . Acesso em: 08 Nov 2022.

NASCIMENTO, Luciano. Pesquisa mostra aumento de compras online pelas mulheres na pandemia. Cerca de 70% das entrevistadas não devem modificar os hábitos. **Agência Brasil**, 08 março 2022. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2022-03/pesquisa-mostra-aumento-de-compras-online-pelas-mulheres-na-pandemia. Acesso em: 22 nov. 2022.

NUCCI, Guilherme de Souza. **Crimes Contra Dignidade Sexual.** Rio De Janeiro: Forense, 2014.

NUCCI, Guilherme de Souza. **Manual de direito penal**. 16. ed. Rio de Janeiro: Forense, 2020.

PALAZZI, Pablo Andrés. **Delitos informáticos**. Buenos Aires: Ad Hoc, 2000.

PINHEIRO, Emeline Piva. Crimes virtuais: uma análise da criminalidade informática e da resposta estatal. **Porto Alegre: PUCRS**, 2006. Disponível em: https://egov.ufsc.br/portal/conteudo/crimes-virtuais-uma-an%C3%A1lise-da-criminalidade-inform%C3%A1tica-e-da-resposta-estatal-0 Acesso em: 09 Nov. 2022

PINHEIRO, Patricia Peck. **Direito digital**. 7. ed. São Paulo Saraiva, 2021. *E-book*.

PORTELA, Raíssa. Projeto aumenta pena para registro, venda e exposição de pornografia infantil. **Agência Senado**, 06 junho 2022. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/06/06/projeto-aumenta-pena-para-

registro-venda-e-exposicao-de-pornografia-infantil. Acesso em: 07 nov. 2022.

QUINTILIANO, Paulo; FILHO, Dirceu Freitas; PLENTZ, Jefferson. **Investigação cibernética no ordenamento jurídico brasileiro.** 2019. Disponível em: http://icofcs.org/2019/ICoFCS2019-003.pdf . Acesso em: 08 nov. 2022.

ROCHA, Carolina Borges. A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. **Jus Navigandi,** Teresina, v. 18, 2013. Disponível em: https://amab.websiteseguro.com/wp/wp-content/uploads/2020/01/A_evolucao_criminologica_do_Direito_Penal.pdf Acesso em: 08 nov. 2022.

ROTUNDO, Rafael Pinheiro *et al.***A fenomenologia da sociedade da informação e a responsabilidade civil à luz da Lei n. 12.965/14–Marco Civil da Internet**. 2018. Disponível em: https://amab.websiteseguro.com/wp/wp-content/uploads/2020/01/A_evolucao_criminologica_do_Direito_Penal.pdf Acesso em: 08 nov. 2022.

SALES, Marcos Levy Gondim. **A comprovação da materialidade e da autoria nos crimes virtuais. 2013**. Disponível em: https://repositorio.ufc.br/handle/riufc/27345. Acesso em: 08 Nov 2022.

SANCHES, A. G.; ANGELO, A. E. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** 2018. Disponível em:https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil. Acesso em: 03 nov. 2022.

SANTANA JUNIOR, João Ubirajara; WOLKOFF, Igor Sa Gille. As implicações do home office no pós-Covid-19. **Conjur,** 8 março 2021. Disponível em: https://www.conjur.com.br/2021-mar-08/opiniao-implicacoes-home-office-pos-covid-19. Acesso em: 22 nov. 2022.

SEXTA Turma reafirma invalidade de prova obtida pelo espelhamento de conversas via WhatsApp Web. **STJ**, 09 março 2021. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/09032021-Sexta-Turma-reafirma-invalidade-de-prova-obtida-pelo-espelhamento-de-conversas-via-WhatsApp-Web.aspx. Acesso em: 07 nov. 2022.

SILVA, Taís Flávia Ferreira Costa da. **A dignidade sexual como bem jurídico penalmente tutelado**. 2020. Monografia (Bacharelado em Direito) – UniEVANGÉLICA, Anápolis, 2020. Disponível em: http://repositorio.aee.edu.br/jspui/handle/aee/16853. Acesso em: 07 nov. 2022

SILVA; Robéria Coelho; SOUZA, Luiza Catarina Sobreira de. "Pornografia De Vingança": Uma Análise Acerca Das Consequências Da Violência Psicológica Para A Intimidade Da Mulher. **Interfaces Científicas**, v. 8, n. 2, 2020. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/IF-dir_v.08_n.02.pdf. Acesso em: 07 nov. 2022.

SOARES, SAMUEL SILVA BASILIO. Os crimes contra honra nas perpectiva do

ambiente virtual. **Âmbito Jurídico**, v. 1, 2016.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as leis brasileiras. *In*: **1º Seminário Cibercrime e Cooperação Penal Internacional**, João Pessoa, 2009. Disponível em: https://www.charlieoscartango.com.br/Images/A%20convencao%20de%20Budapeste%20e%20as%20leis%20brasileiras.pdf. Acesso em: 07 nov. 2022.

TARTUCE, Flávio. **Manual de direito civil**: volume único. 5. ed. rev., atual. e ampl. São Paulo: Método, 2015.

TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico**. São Paulo: Saraiva, 2020. *E-book*. ISBN 9786555591484. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555591484/. Acesso em: 08 nov. 2022.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, n. 86, p. 269-285, 2016. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?format=pdf&lang=pt. Acesso em: 07 nov. 2022.

VASCONCELOS, Fernando Antônio de. A prática de crimes na rede internet e suas conseq6uentes implicações na apuração da responsabilidade civil. **Revista Jurídica do Ministério Público-Eletrônica**, n. 8, p. 199-214, 2014.