CENTRO UNIVERSITÁRIO TABOSA DE ALMEIDA – ASCES/UNITA

BACHARELADO EM DIREITO

GESUALDO MARQUES DE MELO NETO

A PROTEÇÃO JURÍDICA ÀS VÍTIMAS DOS CRIMES CIBERNÉTICOS

Caruaru

2022

GESUALDO MARQUES DE MELO NETO

A PROTEÇÃO JURÍDICA ÀS VÍTIMAS DOS CRIMES CIBERNÉTICOS

Artigo Científico apresentado à Coordenação do Núcleo de Trabalhos de Conclusão de Curso, do Centro Universitário Tabosa de Almeida (ASCES-UNITA), como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Professor Msc. Marupiraja Ramos Ribas

Caruaru

2022

BANCA EXAMINADORA

Aprovado em: ____/___/_____

_____

Presidente: Professor Msc. Marupiraja Ramos Ribas

_____

Primeiro (a) Avaliador (a): Prof. (a)

_____

Segundo (a) Avaliador (a): Prof. (a)

RESUMO

O presente artigo jurídico pretende discutir a criminalidade cibernética e quais as possibilidades de uma efetiva proteção para as vítimas destes crimes cibernéticos, que infelizmente cada vez mais, tem integrado a rotina do brasileiro, certo de que a tecnologia ocupa um espaço relevante na vida moderna, mas a utilização inadequada das ferramentas tecnológicas, pode ser uma arma perigosa para a convivência harmônica das pessoas com consequências desastrosas para a sociedade. Neste cenário, é indiscutível que o crescimento da criminalidade cibernética deve preocupar as autoridades públicas e ser merecedora sim, de um olhar preventivo, exatamente voltado para um efetivo acolhimento das vítimas das diversas e perversas práticas delituosas, as quais são reproduzidas simetricamente nas redes sociais, notadamente, observamos várias injúrias, calúnias e difamações que impregnam o mundo virtual, somando-se a *fake news* e campanhas difamatórias articuladas contra instituições e pessoas públicas, causando um caos cibernético, com riscos incalculáveis para a sobrevivência política e econômica de nosso país. Assim, para a construção de uma compreensão mais clara sobre este assunto, o artigo aqui apresentado apresenta, em um estudo desenvolvido a partir de extensa pesquisa bibliográfica, além de uma compreensão sobre o Direito e as ações contra os crimes cibernéticos, apoiados em casos concretos e nas observações da doutrina clássica e da jurisprudência dominante sobre a temática.

Palavras-chave: Novas tecnologias; Crimes cibernéticos; Criminalidade; Vítimas.

ABSTRACT

This legal article intends to discuss cybercrime and what are the possibilities of an effective protection for the victims of these cybercrimes, which unfortunately have increasingly integrated the Brazilian routine, certain that technology occupies a relevant space in modern life, but the inadequate use of technological tools can be a dangerous weapon for the harmonious coexistence of people with disastrous consequences for society. In this scenario, it is indisputable that the growth of cybercrime should concern public authorities and be deserving, yes, of a preventive look, precisely aimed at an effective reception of victims of the various and perverse criminal practices, which are reproduced symmetrically on social networks, notably, we observe various insults, slanders and defamations that permeate the virtual world, in addition to fake news and defamatory campaigns articulated against institutions and public persons, causing cyber chaos, with incalculable risks for the political and economic survival of our country. Thus, to build a clearer understanding of this subject, the article presented here presents, in a study developed from extensive bibliographic research, an understanding of the Law and actions against cybercrimes.

Keywords: New Technologies; Cyber Crimes; Criminality; Victims.

SUMÁRIO

	INTRODUÇÃO	**6**
1	**DA CRIMINALIDADE CIBERNÉTICA**	**7**
1.1	O DESENVOLVIMENTO JURÍDICO E AS AMEÇAS CIBERNÉTICAS	10
1.2	OS CRIMES COMETIDOS NO AMBIENTE CIBERNÉTICO	14
2	**A INCIDÊNCIA NORMATIVA PENAL E ADOÇÃO DAS NOVAS TECNOLOGIAS MALÉFICAS**	**16**
3	**A PROTEÇÃO JURÍDICA CONTRA CRIMES CIBERNÉTICOS**	**20**
	CONSIDERAÇÕES FINAIS	**24**
	REFERÊNCIAS	**25**

INTRODUÇÃO

O presente estudo, visa mostrar a notoriedade do avanço do uso das tecnologias, para fins de atividades pessoais, familiares, profissionais, empresariais e dos setores públicos e até mesmo no lazer das pessoas, entretanto, além do seu uso positivo para o desenvolvimento econômico e social do nosso país, deve ser observado cuidadosamente, o seu uso negativo e as terríveis consequências deixadas nas vidas das pessoas, notadamente, o mau uso das redes sociais. Assim, pode-se observar também, exponencialmente, um grande aumento dos crimes cibernéticos.

No entanto, quanto mais nos transportamos para a vida digital, constatamos que o universo virtual não possui uma entidade pública e/ou jurídica para a proteção das vítimas dos cibercrimes, podendo, assim, ser verificado que os infratores, não se amedrontam com as normas que lhes podem ser impostas, tornando-se reincidentes nos diversos crimes virtuais, o que torna isto um fator preocupante para o nosso ordenamento jurídico, portanto, merecedor de um olhar diferenciado e aprofundado.

Assim, pode-se considerar a relevância material sobre a relação entre o Direito Penal e os crimes cibernéticos, estabelecendo maior clareza sobre a influência deste ambiente jurídico, que surge como um meio para solução dos conflitos digitais e têm sido um dos assuntos mais debatidos atualmente em nossa sociedade, destacando-se a Lei (Carolina Dieckmann) de nº 12.737 de 30 de novembro de 2012, a Lei (do Marco Civil da Internet) de nº 12.965 de 2014 e por último a Lei (Geral de Proteção de Dados) de nº 13.709 de 2018, como sendo alguns relevantes pilares jurídicos previstos para a proteção das pessoas vítimas dos crimes digitais, com relevância para os fatos delituosos cometidos através das redes sociais.

Nota-se que a regulação de instrumentos normativos, seria um fator primordial no avanço para obter um ecossistema digital mais seguro, ademais, esses instrumentos normativos, seriam no sentido de não só punir o responsável por tamanha crueldade virtual, mas, também, prevenir os milhares de usuários a não cair ou serem vítimas dos crimes decorrentes da avançada tecnologia. Ao longo deste estudo, serão discutidos vários aspectos em relação aos crimes cibernéticos, suas implicações e proficuidades, e

sem dúvida, busca-se aqui, apontar soluções satisfatórias que promovam a proteção e prevenção jurídica as vítimas dos crimes alhures mencionados.

Para tanto, nossa metodologia será lastreada em revisão bibliográfica, na catalogação sequencial da legislação pertinente a relação do Direito Penal com a criminalidade cibernética, trazendo também a contribuição da jurisprudência pátria e neste contexto, veremos a criminalidade cibernética, a relação entre o Direito Penal e as novas tecnologias, até referenciarmos a proteção jurídica das vítimas destes crimes.

1 DA CRIMINALIDADE CIBERNÉTICA

Inicialmente, deve ser registrado que o controle estatal sobre a criminalidade comum tem representado uma tarefa árdua e contínua, o que de logo, sinaliza as dificuldades de se fazer um controle efetivo sobre a criminalidade cibernética, que diferente da comum, se perfaz num ambiente específico e ainda em evolução e duvidoso, tendo a tecnologia como uma ferramenta em constante desenvolvimento, mas de domínio complexo para todos os integrantes da sociedade, sendo o desconhecimento, um verdadeiro facilitador para o crescimento incontrolável dos crimes cibernéticos e logicamente para o impedimento da impunidade gerada aos seus protagonistas.

Para Pereira e Oliveira (2019), antes de qualquer iniciativa sobre a relação entre a relação protética do Poder Jurídico diante dos diversos crimes realizados por meios virtuais, fazendo-se necessário conhecer o nível desses crimes em um processo histórico, bem como a forma de classificar, regular e estabelecer os meios para composição da relação adequada entre o Direito e o meio digital.

Indiscutivelmente tem-se no ambiente virtual uma ideia de certa nebulosidade, notadamente, quando utilizado indiscriminadamente para a prática de diversos delitos, daí que o seu combate, passou realmente a ser um interessante desafio para as autoridades de segurança pública de nosso país.

Numa visão histórica, as ameaças cibernéticas surgiram com a invenção da internet, onde na visão de Fabiane Marra (2019), a internet deve ser observada como uma das principais invenções humanas, já que remodelou drasticamente o modo de comunicação social, segundo o referido autor, é por meio desse ambiente que uma

quantidade nova e significativa de benefícios é oferecida às pessoas como meio de facilitar a troca de conhecimento e informações. Interessante observar que este espaço significativo para uma nova forma de comunicação universal, tenha também se transformado em solo fértil para o crescimento da criminalidade cibernética também de alcance mundial.

Para Lins (2013), a internet foi capaz de unificar o mundo, já que, por meio dela, qualquer pessoa, em qualquer lugar do mundo, pode ter qualquer tipo de informação. Este sentido de união e desenvolvimento da humanidade gerado pela internet, também restou refletido diretamente nas diversas ações criminosas praticadas com ardileza extrema neste gigante e indominável ambiente virtual.

Neste contexto, sustentou Fabiane Marra (2019), que a internet também se tornou um meio fácil para a realização de ações novas e prejudiciais às pessoas, defendendo ainda, que esta questão não é de exclusividade do meio digital, já que qualquer invenção humana pode ser utilizada para realização dos mais diversos crimes. Dessa forma, é necessário estabelecer um caminho histórico, como afirmou Decarli (2018), para conhecer como a evolução histórica foi capaz de proporcionar, também, a evolução dos crimes por meio da internet.

A internet surgiu em meio a Guerra Fria (1947 – 1991), período de disputa militar entre os EUA e a antiga União Soviética, e, naquela época havia a necessidade de trazer maior integração de computadores, principalmente para os dispositivos que estavam distantes entre si, e isto, foi executado para trazer melhor comunicação e troca de dados com maior velocidade, crucial em um ambiente instável, como o encontrando naquele período de guerra, assim, em 1969, foi registrada a criação da ARPANET, uma rede que foi capaz de interligar três universidades (Califórnia, *Stanford e Utah*), fornecendo a capacidade de interação entre essas entidades, mesmo em grandes distâncias (DECARLI, 2018), sendo seu registro histórico e importante para o nascimento da internet.

Segundo Alves (2018), no fim dos anos de 1970, cria-se o *Transmission Control Protocol/Internet Protocol* (TCP/IP), que é usado como o principal protocolo de rede até os dias atuais. Já nos anos de 1980, a rede começa a se expandir pelos EUA e começa a permitir maior troca de informações entre universidades, governo e os ambientes

militares, todavia, somente no ano de 1986, a ARPANET passou oficialmente a ser denominada de internet.

A partir de então a internet começou a ser promovida, esse avanço se inicia com a criação do *World Wide Web* (WWW) e do *Hypertext Markup Language* (HTML), protocolos que foram capazes de proporcionar uma expansão e popularização da internet, páginas *web* colocaram a internet dentro do ambiente global, transformando essa tecnologia no principal meio de comunicação em poucos anos de sua criação, tendo então um rápido alcance.

No mesmo ambiente construído para o desenvolvimento tecnológico e de comunicação, que se apresentou com o advento da internet, também surgiram ameaças aos recursos de rede. Surgiram os programas que utilizavam replicação de suas informações para invadir bases de dados e tomar informações. Atenta-se, porém, que o desenvolvimento primordial desses programas não tinha como objetivo o crime, mas tinha teor científico. Um dos exemplos, foi o desenvolvimento do jogo *Core Wars*, que foi desenvolvido de fato para colocar um código malicioso no computador que o executasse, o intuito dos programadores era desenvolver mecanismos de defesa, ou seja, uma verdadeira proteção, como o primeiro antivírus chamado *Reaper* (LINS, 2013).

O primeiro vírus para computador, o *Elk Cloner*, foi desenvolvido pelo pesquisador Richard Skrenta, em 1882. O código se espalhava em cópias de disquetes contaminados, método que posteriormente foi utilizado como método para causar danos reais em computadores (ASAAD, 2020). Em 1986, dois pesquisadores paquistaneses criaram o vírus *Brain,* que tinha como proposito causar lentidão nos sistemas operacionais e tinha, à época, técnicas robustas para impedir sua detecção. O primeiro antivírus contra o *Brain* só foi desenvolvido em 1988, e foi desse ano que o desenvolvimento de mecanismos de ataque (vírus) e de defesa (antivírus) passaram a compor o ambiente cibernético (ALVES, 2018), registre-se deste modo, a lentidão na proteção e punição para os invasores da internet, clamando-se à época por uma rápida e significativa evolução nos diversos mecanismos de proteção no uso da internet

O primeiro vírus a causar forte apelo midiático e social, foi o *Michelangelo*, que era utilizado para sobrecarregar o disco rígido das vítimas, e a data para essa sobrecarga era o do nascimento do pintor renascentista, 6 de março. Mas somente em 1994 o

primeiro autor de vírus sofreu punição jurídica. O crime foi registrado na Inglaterra e o autor do vírus *Pathogen* foi condenado a 18 meses de prisão (STUANI; FUCHS, 2021; AKGUL et al., 2021), uma punição festejada.

Em 1999, a Coréia do Sul, China e Turquia sofreram grandes prejuízos financeiros por causa do vírus *Chernobill,* que causava danos severos aos discos rígidos dos usuários, deixando os dados inoperantes. Em 2000, o vírus *Love Letter* causa 9 milhões de dólares em prejuízos nos EUA e na Europa em apenas 6 dias (WILLEMS, 2019). O que colocou o mundo em crescente necessidade de ações mais assertivas de segurança para coibir e punir os desenvolvedores desses crimes, notadamente pelos prejuízos econômicos causadas às nações.

Os dispositivos móveis também não ficaram aquém aos ataques de códigos maliciosos, o primeiro vírus para celular foi desenvolvido em 2004. O *Cabir* tinha capacidade de se disseminar através do *Bluetooth* e era capaz de descarregar baterias dos celulares e as deixá-las inoperantes (QUISSANGA, 2019). Assim, com a polarização de códigos maliciosos e sua capacidade de lastro social, tornou-se necessário, ou seja, imperioso, portanto, peremptório, a melhoria na capacidade de coibição e nas políticas jurídicas de proteção.

A partir dessa perspectiva, faz-se necessário observar os meios e os mecanismos capazes de promover proteção para os usuários que se beneficiam de forma lícita do meio digital. Assim, com essa compreensão, o Direito passa a ter um papel essencial no desenvolvimento da estabilidade social tão necessária para a manutenção da civilidade. Segundo o que dita Alves (2018), é somente através do Direito que existe seguridade para que os relacionamentos desenvolvidos entre pessoas possam alcançar o progresso mútuo.

1.1 O desenvolvimento jurídico e as ameaças cibernéticas

Com esta compreensão, quando são apresentados cenários que não favoreçam o desenvolvimento desse progresso há o aumento da violência e da impunidade, o que acaba ocasionando a inseguridade jurídica, e a descaracterização do papel do Direito.

Segundo o que defende Fabiane Marra (2019), isto o ocorre quando as pessoas passam a não confiar na capacidade do Estado em responder assertivamente na solução dos conflitos em que estas pessoas estão envolvidas.

Dessa forma, como apresenta Azevedo e Cardoso (2021), existe a clara necessidade de colocar na balança a relação entre o Direito, e sua visão conservadora dos fatos, e o desenvolvimento progressivo social. O processo de observância dessa relação, como afirma o autor, é o que irá auxiliar o aperfeiçoamento do Direito diante das diversas e novas necessidades sociais. E isto pode (deve) ocorrer tanto por meios legislativos quanto por meio da jurisprudência.

Ao se deparar, portanto, com a nova realidade da comunicação e da informação, o Direito passa a necessitar entrar em consonância com este modelo. Isto pode ser observado quando Fabiane Marra (2019) afirma que não existem mais fronteiras e que o mundo vivência uma nova realidade de interligação social através do ciberespaço.

O autor abre, dessa forma, a compreensão de que, como o Direito não é um instrumento em si mesmo, mas se apresenta a partir de normas estabelecidas pela sociedade para responder a fenômenos sociais criados por esta coletividade, este mesmo Direito passa a ter a função de manter a ordem para que estes fenômenos não atentem contra a própria sociedade que o criou.

Com o surgimento da modalidade cibernética de interação entre pessoas, também foi possível perceber a criação de uma variedade inédita de bens, que podem ser um bem material ou imaterial. Este processo também promoveu a necessidade de reestabelecimento de um no Direito, o Direito cibernético. Este Direito se evidencia quando diante da necessidade protetiva de um ente, faz-se necessário garantir que sua segurança seja inviolada (AZEVEDO; CARDOSO, 2021).

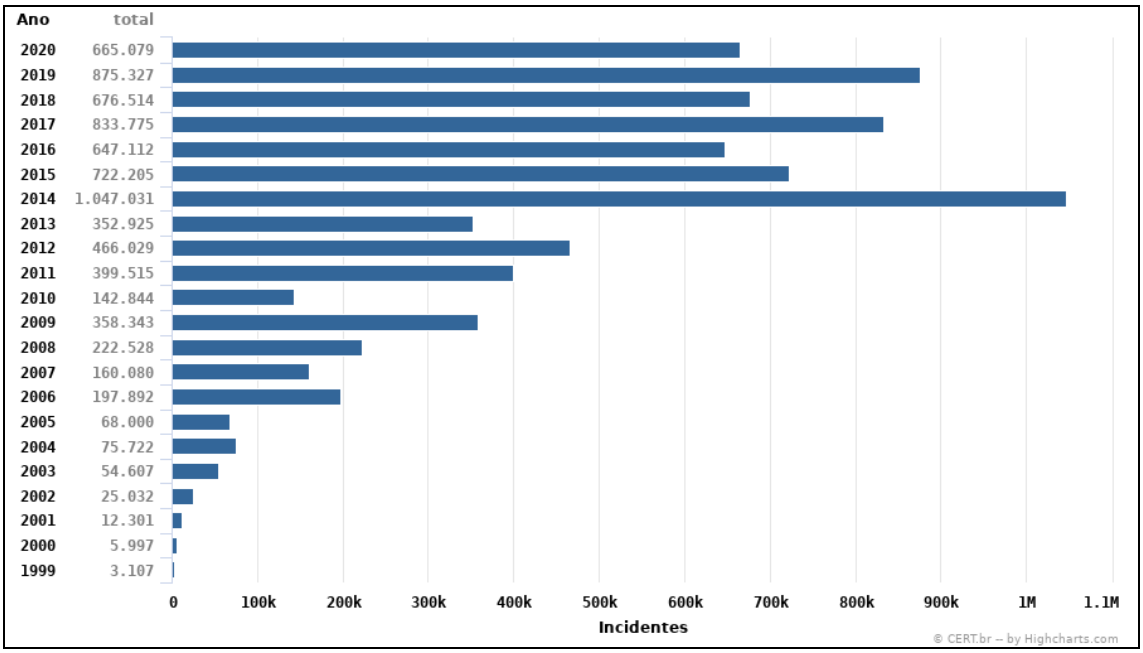
Porém, para se chegar em mecanismos legais que garantam a sustentação do Direito dentro do ambiente cibernético, é necessário compreender que não se pode estabelecer, como garantia Constitucional, qualquer ameaça contra um outro Direito. Dessa forma, a garantia da execução protetiva social dentro do ambiente digital, passa por uma evolução sistemática que requer o cuidado do próprio Direito para chegar tal questão.

Compreende-se que leis protetivas para ambientes digitais vem antes mesmo desses ambientes se tornarem perigosos, porém, o Direito pode chegar com certo atraso, já que depende de um processo elaborativo e executório que extrapole o controle e as linhas da Constituição Federal vigente.

Mesmo com esse entendimento, os crimes dentro do ambiente cibernético podem aparecer há qualquer momento, basta o ambiente ser capaz de estabelecer troca de informações e relações entre pessoas. A internet não só trouxe esse fato de forma mais assertiva e generalizada, mas deu possibilidade para que as possam realizassem essas ações de forma anônima, o que foi capaz de atrair os mais diversos tipos de criminosos.

Segundo o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil – CERT.br (2022), entre os anos de 1999 há 2020, os crimes reportados ao centro de estudo ultrapassaram a casa dos milhões de casos. A Figura 1 apresenta a evolução crescente de crimes reportados e acompanhados pela entidade durante esse período.

Figura – Crimes reportados ao CERT.br até o ano de 2020



Fonte: Disponível em CERT.br (2022)

Como pode ser observado no acompanhamento da entidade, o ano de 2014 foi o período com maior índice de crimes cometidos em ambiente digitais, com mais de um milhão de casos. Este aumento forçou o desenvolvimento, durante as últimas décadas, de delegacias especializadas, processos investigativos mais informatizados, ambientes de repressão mais rápidos e assertivos, entre outros (MARRA, 2019).

Com esse número expressivo não é nada incomum o fato de existir uma diversidade de crimes possíveis que podem ser cometidos em ambientes. Dessa forma classificar e dividir esses crimes auxilia no processo de identificação do criminoso, bem como a motivação para a execução do ato de delito. Segundo as informações fornecidas por Huebner et al (2003), os crimes dentro do ambiente digital podem ser divididos em três categorias:

> Crimes direcionados ao computador – Para esta categoria se evidenciam os crimes que são direcionados aos sistemas de redes, computacionais ou dispositivos de armazenagem;
> Crimes auxiliados por computadores – Aqui podem ser caracterizados os crimes que podem ou não ser executados com o um computador, já que para esta tipologia o computador é utilizado como uma ferramenta para execução do crime;
> Crimes incidentais através de computadores – Aqui o computador é uma peça eventual ou incidental do crime. (HUEBNER ET AL, 2003).

Outro modo de classificar os crimes dentro do ambiente cibernético é através classificação de crimes próprios e impróprios. Para a primeira tipologia, crimes próprios, o objetivo do delito é atingir o sistema computacional em si, crimes contra sites se enquadram aqui; já para a segunda tipologia, crimes impróprios, são crimes que utilizam a internet ou meios digitais para executar o crime, crimes de falsificação de documentos e estelionatos se enquadram nesse tipo.

Segundo Marra (2019), os crimes cibernéticos fechados necessariamente precisam do meio computacional para existir, isto pode ser exemplificado pelos art. 154-A e art. 154-B, do Código Penal, sobre crimes de invasão de dispositivo informático. Já crimes mais abertos, podem ou não ser praticados pelo dispositivo digital.

Relacionado exclusivamente para crimes dentro do ambiente digital, existem uma variedade grande de ameaças que podem ser usadas como eventuais meios para se

cometer atos criminosos. A exemplo de uma das principais ameaças: são os códigos maliciosos, utilizados para invadir e sequestrar informações ou valores de uma pessoa.

Para estes, Alves (2018), afirmou que o trabalho do universo jurídico é ainda maior, já que essas ameaças exigem conhecimento mais apurado para a realização da investigação e supressão de um novo crime. Ainda segundo autor, faz-se necessário conhecer esses códigos, mesmo que de forma superficial, para se conduzir da melhor maneira possível a execução assertiva do Direito.

Os vírus de computadores ou códigos maliciosos, são capazes de propagar e sequestrar os mais variados tipos de informações ou mesmo valores. O vírus *boot,* usado como exemplo, tem capacidade de dificultar a inicialização de um computador. Já o vírus *Botnet,* tem capacidade de permitir que o computador de uma vítima seja manipulado a distância, assim, pode testar as vulnerabilidades dos softwares e a capacidade operacional, em geral as vítimas não têm ciência de que o código esteja em seu computador. Esse vírus também tem capacidade de sobrecarregar servidores conectados a uma variabilidade de computadores, o que pode ser usados como instrumento de crimes contra empresas, Empresas estas que também necessitam investir em ciber-segurança para garantir a integridade das informações (ARAGÃO, 2021).

Outro código que tem capacidade de acessar o computador de uma vítima a distância é o Cavalo de Troia. Este código tem capacidade extrair dados sigilosos, como senhas, dados pessoais ou mesmo, informações de segurança financeira de uma vítima. O Cavalo de Troia é instalado dentro do computador através de objetos que camuflam seus objetivos e se parecem atrativos ou uteis a possível vítima.

1.2 Os crimes cometidos no âmbito cibernético

A partir daqui é possível estabelecer um aparato, mesmo que superficial, dos principais crimes encontrados dentro do ambiente digital. Segundo Marra (2019), não só o número de pessoas aumentou, o nível de interação também passou para níveis mais elevados. Dessa forma, os crimes podem alcançar qualquer pessoa em qualquer lugar.

Uma das observações claras é a inserção massiva de crianças e adolescentes dentro do ambiente digital, principalmente pelo uso de mídias digitais, como o as redes sociais. Para Aragão (2021), é praticamente inviável separar as crianças ou adolescentes do ambiente digital, o que as tornam vulneráveis ao crime de pedofilia. Por isso, existe a necessidade de um maior poder interventivo do ambiente jurídico para estabelecer proteção às essas crianças e adolescentes.

Segundo Guragni (2019), o principal modo de atuação de crimes de pedofilia dentro do ambiente digital, é quando o criminoso se passa por outra pessoa, muitas vezes outra criança, conquistando a confiança da vítima para persuadi-la a compartilhar fotos, vídeos íntimos ou mesmo marcar encontros para persuadir a vítima a realizar o que o criminoso deseja.

As penas para este tipo de crime são estabelecidas no Estatuto da Criança e do Adolescente (ECA), no art. 241-A, ao afirmar que “quem exportar, comercializar, distribuir, divulgar etc.” conteúdo de pornografia infantil poderá ter pena prevista de 3 a 6 anos, além de multa. Para coibir esses tipos de crimes, os órgãos de controle costumam promover ações educativas para pais e crianças.

Outro crime comumente visto no ambiente cibernético são crimes de sites fraudulentos. Segundo Aragão (2021), esses sites se utilizam da grande movimentação de compra e venda via redes digitais para praticar a comercialização de produtos ou serviços inexistentes com o objetivo de roubar quantias financeiras ou mesmo dados fornecidos pelos clientes na hora da compra.

Para Paulo Roberto Aguiar de Lima Filho (2021), os criminosos copiam sites de grandes empresas e colocam produtos bem abaixo do preço de mercado, a fim de maravilhar a vítima, que acaba por comprar e pagar pelo produto ou serviço que, na realidade, não existe. Segundo Serviço de Proteção ao Crédito (SPC), entre os anos de 2018 e 2019 este tipo de crime foi o que teve maior número de vítimas no Brasil.

Em continuidade, outro já relatado é o sequestro de dados pessoais de uma vítima através de códigos maliciosos. Para este tipo de crime, as vítimas, muitas vezes não tem conhecimento que estão sendo monitoradas, e tem seus dados pessoais, bancários ou mesmo familiares sequestrados por criminosos que costumam pedir quantias para não divulgar tais dados.

Não só pessoas comuns estão diante da possibilidade de serem vítimas de crimes cibernéticos, empresas e até órgãos públicos estão sujeitos a esses possíveis crimes. Um dos eventos mais recentes que pode ser usado como exemplo para esses crimes, foi o ataque cibernético ao órgão da Justiça Federal em Pernambuco (JFPE), que teve seus sistemas desligados por horas devido a este ataque.

Segundo o Site G1 (2022), o ataque derrubou diversos sistemas de recursos, além, também, da telefonia do prédio. Ainda segundo o site, muitas outras tentativas de ataques foram relatadas por diferentes órgãos judiciários no Brasil, o que coloca maior atenção a esta realidade de ataques cibernéticos dentro dos sistemas jurídicos do país.

2 A INCIDÊNCIA NORMATIVA PENAL E ADOÇÃO DAS NOVAS TECNOLOGIAS MALÉFICAS

Atualmente, não existe mais diferença entre a vida comum e social dentro do ambiente cibernético, principalmente com o advento e a polarização da internet. As pessoas passaram a não somente trocar mensagens ou informações comuns, mas ditaram seus trabalhos, suas vidas amorosas e até as suas transações financeiras através da internet e de suas tecnologias (PADOVEZ; PRADO, 2019), isso reflete a importância do mundo digital na vida moderna.

Desse modo, segundo as contribuições de Lima (2021), o meio cibernético formulou um novo ambiente para troca de informações e comunicações, mas também promoveu a possibilidade do surgimento de práticas ilícitas com o uso da *web.* O *cibercrime*, termo utilizado para se referir a atos ilícitos organizados pelo uso da internet ou tecnologias relacionadas, pode não ser um crime observado de forma tangível (como os crimes físicos), mas tem o mesmo impacto devastador para a vida da vítima e de seus entes queridos.

Segundo os relatos de Lima (2021) e Tebet, Pereira e Jorge (2016), os crimes cibernéticos têm características a eficiência do uso da tecnologia, a velocidade no acesso e a disseminação da informação que traz peculiaridades não comuns para estes tipos de atividades ilícitas. Ainda segundo os citados autores, a novidade que esses crimes promovem fomentam a necessidade de maior conhecimento sobre o assunto para que

se possa materializar a infração e caracterizá-la em uma tipologia penal, isso se apresenta como fundamental, ou seja, essencial para a relação entre o Direito Penal e as novas tecnologias.

Segundo o que afirma Rocha (2013), o Direito é um dos instrumentos reguladores e organizadores do tecido social, e dentro dessa perspectiva, fica de responsabilidade do Direito não somente estabelecer os meios para regular as mudanças sociais, mas também evoluir junto com essas mudanças. O referido autor ainda afirmou que é através dessa adaptação que o Direito promove a seguridade para que as verdadeiras mudanças possam acontecer.

Dessa forma, tem-se a necessidade de estabelecer medidas que protejam os direitos fundamentais, até mesmo dentro do ambiente cibernético. Com esse intuito a jurisprudência atual se debruça na composição de regulamentos e leis que premissem regular os crimes cometidos dentro dos ambientes digitais, na tentativa de moldar o Direito Penal às necessidades sociais e tecnológicas atuais (MARRA, 2019; HERNANDEZ; TOLEDO, 2021).

Por essas questões, torna-se de suma importância compor entendimento sobre como estes mecanismos ilícitos podem ocorrer dentro dos ambientes digitais, além de impor conhecimento sobre qual o papel do Direito Penal para identificar, nivelar a gravidade, coibir e punir de forma a proteger tal ambiente das ações criminosas, evitando a danosa sensação de impunidade na internet.

Crimes como injuria, calúnia, ameaça, difamação, divulgação de material confidencial, estupro virtual, pedofilia, golpes financeiros e de falsa identidade são alguns que podem ser descritos como crimes cibernéticos e que estão expostos dentro de leis no âmbito penal. Boa parte desses delitos são cometidos por profissionais (*hackers*) que se utilizam de mecanismos bem estruturados (como os vírus) para invadir e sequestrar informações de usuários a fim de tomar algo da vítima de forma ilícita (PADOVEZ; PRADO, 2019; ROCHA, 2013).

Nota-se que os autores dos crimes virtuais são criminosos específicos, treinados, com profundo conhecimento das redes virtuais e além de preparos nas ferramentas digitais, estão prontos para agir de modo muito violento.

Dessa forma, importa-se estabelecer o conhecimento sobre as mais diversas tipologias de crimes que podem ser cometidos dentro do ambiente cibernético e quais leis protetivas existem para manter as pessoas salvas da exposição de crimes e delitos dentro do ambiente digital, tendo como exemplos legislativos interessantes e existentes em nossa realidade jurídica, Lei nº 12.737 de 2012 (para Crimes Cibernéticos), Lei nº 12.965 de 2014 (do Marco Civil da Internet) e finalmente a Lei nº 13.709 de 2018 (Geral de Proteção de Dados).

Para Silvano Flumignan e Wérvertton Flumignan (2017, p. 249): “o Marco civil da Internet é referência mundial de garantia básica dos usuários”, fazendo estes, uma expressa e relevante referência aos princípios, garantias, direitos e deveres insertos no citado instrumento normativo, tido como revolucionário para assegurar uma proteção jurídica às pessoas que utilizam a internet e preparando o cenário jurídico para a forte e necessária incidência do Direito Penal, quando verificada a prática de delitos cibernéticos, com o marco, deixamos aquele vazio legislativo que incomodavam a todos os gerenciadores e usuários da internet.

Preocupados com a regulamentação e proteção dos dados no uso da internet, Pimentel e Cardoso (2015) abordaram a problemática do direito ao esquecimento, isso, partindo da indispensável verificação do direito comparado e, após a vigência e os efeitos da lei do marco civil da Internet, instrumento normativo que para além de estabelecer uma proteção do direito ao esquecimento, fez a previsão de uma interessante fragmentação normativa específica sobre o alcance real da responsabilidade civil dos provedores.

Interessante anotar que o marco civil da internet estabelecido na Lei nº 12.965/2014, trouxe a neutralidade de rede, o que na visão de Silvano Flumignan e Wérvertton Flumignan (2017) transformou-se realmente como uma de suas colunas fundamentais, assegurando com isso, a todos os usuários da rede, uma isonomia de tratamento quanto às informações trafegadas na rede, impedindo assim interferências, desvios ou diferenciações neste envio e acesso online.

Assim, em consideração da relevância material sobre a relação entre o Direito Penal e os crimes cibernéticos, além de estabelecer maior claridade sobre a influência desse ambiente jurídico para as novas tecnologias, o presente trabalho toma por objetivo

avaliar como o Direito Penal se adapta para alcançar os meios cibernéticos e quais mecanismos legais podem ser (e são) utilizados. Para alcançar tal objetivo, o trabalho em questão se institui em: a) apresentar a evolução do Direito Penal para alcançar as novas tecnologias; b) mostrar o nível atual de capacidade protetiva do Direito Penal dentro do ambiente cibernético; e, c) apresentar os crimes comuns dentro do ambiente cibernético.

No poder público, não é diferente, existindo uma imperiosa necessidade de estabelecer uma frutífera e eficaz relação entre o Direito Penal e as novas tecnologias, notoriamente após o avanço da justiça 100% digital, de iniciativa do Conselho Nacional de Justiça (CNJ) e replicada no âmbito dos tribunais estaduais, federais e superiores tribunais brasileiros. (BRASIL, 2022).

O crescimento do uso do processo judicial eletrônico (PJe), bem como os efeitos da pandemia motivados pelo vírus Sars-CoV-2 (COVID-19), aceleraram o crescimento da prática de diversos atos processuais pelas redes sociais, tendo inclusive sido registrado um aumento turbinado do uso da internet, da videoconferência e da vídeo chamada pelos celulares dos servidores da justiça, com a ampliação do trabalho remoto e do atendimento digital pelo balcão virtual e por outras ferramentas digitais, também provocou a inexorável preocupação de estabelecer uma rígida proteção diante da ação dos criminosos virtuais, bem como na proteção dos dados das partes, dos advogados, servidores e das suas intimidades, tanto que na sua dissertação de mestrado, defendeu Marupiraja Ribas (2021) a existência de uma estratégia permanente pelos tribunais no resguardo das informações eletrônicas, visando principalmente proteger o acesso pelas partes e à proteção da imagem de todo os envolvidos na relação processual.

O Direito Penal indiscutivelmente é convocado a intervir com maior intensidade nos efeitos causados pela utilização das novas tecnologias, havendo uma cobrança de intervenção imediata para refrear o uso inadequado de todas estas ferramentas postas à disposição das pessoas físicas e jurídicas, e estas últimas de cunho privado e público e com consequências desastrosas para a sociedade quando ignorada esta relação, atualmente exigida de modo contínuo.

A compreensão específica da dogmática penalista e sua real relação com as novas tecnologias, clama pela sua intervenção severa na variedade do cardápio

criminoso cibernético ora constatado no mundo digital mundial, sendo assim, um evento sinalizador, de que ainda é muito precária a fiscalização, intervenção do Direito e a efetiva punição dos malfeitores/vilões digitais.

3 A PROTEÇÃO JURÍDICA ÀS VÍTIMAS DOS CRIMES CIBERNÉTICOS

Segundo Beppler (2019), no ano de 2017 o Brasil apresentou o segundo maior índice de crimes cibernéticos em uma comparação com todos os países do mundo. A pesquisa realizada pela *Norton Cyber Security,* apontou que 62 milhões de pessoas foram vítimas de crimes cometidos pela internet naquele ano, com prejuízo de 22 bilhões de reais.

Já no ano de 2016, o Brasil se encontrava em quarto lugar no *ranking* de países com maiores índices de criminalidade dentro do ambiente cibernético. Para Corrêa *et al.* (2021), boa parte dos crimes cibernéticos dos últimos anos, principalmente em período pandêmico, foram crimes virtuais contra mulheres, pedofilia, apologia a crimes, calúnia, difamação e golpes financeiros.

Um dos meios para o cometimento de crimes são as redes sociais. Segundo afirma Corrêa *et al.* (2021), tanto o WhatsApp quanto o Instagram são redes que apresentam maior vulnerabilidade para se cometer crimes. O autor afirma que são 44 milhões de vítimas somente entre 2017 e 2018.

Para Vieira (2020), o aumento expressivo no número de crimes cometidos dentro do ambiente digital, põe em xeque a capacidade do aparato jurídico para manter a proteção desses locais. Porém, como salienta Corrêa *et al.* (2021), o aparato jurídico é abrangente suficiente para garantir a proteção das pessoas, o que há nesses aumentos é a maior inserção de pessoas no mundo digital.

Isto é defendido ao se pensar que nos últimos anos se desenvolveu um aparato jurídico grande na tentativa de estabelecer ação contra os crimes cibernéticos. Uma das leis dentro do nosso ordenamento jurídico existente contra os crimes cibernéticos é a Lei de nº 12.737/2012, bastante conhecida como: “Lei Carolina Dieckman”, sendo a mesma nascida, ou seja, criada após o caso de divulgação de fotos intimas vazadas da atriz Carolina Dieckman, isso ocorrido no ano de 2011, quando a referida atriz teve seu

computador invadido por hackers e suas informações sigilosas divulgadas indiscriminadamente na internet, inclusive em diversas redes sociais.

Assim, a partir do fato ocorrido e acima descrito, o qual teve enorme repercussão, se alastrando rapidamente, foi elaborada a norma que puniria ações cometidas por prática de invasão a dispositivos eletrônicos, com tipificação estabelecida na Lei nº 12.737/2012, com acrescimentos de decreto-lei nº 2848, nos artigos 154-A, 154-B do Código Penal, afirmando ser crime “Invadir dispositivo informático alheio, conectado ou não à rede de computadores, ” com de 3 meses a 1 ano, multa e possibilidade de aumento da pena, sendo assim, nos termos do artigo 63 da Lei nº 9.099/1995, considerado um crime de menor potencial ofensivo e de competência do juizado criminal.

Outra lei do mesmo ano que a anterior, a Lei nº 12.735/2012, proposta pelo Deputado Federal Eduardo Azeredo (PSDB), promoveu a obrigação de suspensão imediata de mensagens com teor racista, como também o impedimento do uso de qualquer meio de comunicação, além da criação das delegacias virtuais.

Pode-se observar que dentro desta última lei, em seu artigo quarto, fora afirmado que caberia aos órgãos de polícia judiciária a estrutura e regulação de equipes e setores especializados no combate as ações criminosas dentro de computadores ou qualquer outro dispositivo de comunicação informatizada.

Além disso, também se observa, no artigo quinto da lei supracitada, um acréscimo no artigo 20 da Lei nº 7.716/1989 (Lei de Combate ao Racismo), em seu inciso II do § 3° que afirma “a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio” (BRASIL, 1989).

Além dessas ações que possibilitaram maior controle, mesmo diante das diversas controvérsias e discussões sobre o tema, foi elaborado em 2014 a Lei nº 12.936, denominado de Marco Civil da Internet, considerada a maior ação legislativa para as atividades do meio digital, a lei promoveu o surgimento de princípios e direitos para o uso dos meios digitais dentro do território nacional.

Segundo Padovez e Prado (2019), a referida lei forneceu orientação aos usuários sobre como se deve estabelecer o modo relacional entre a rede e as pessoas inseridas nela, e no contexto do seu artigo 5º, inciso I, tem-se a compreensão sobre o que seria a internet:

> I – Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes (PADOVEZ; PRADO apud BRASIL, 2019).

Para Marcacini (2016), o marco civil é um incremento largo para garantir princípios, garantias, direitos e deveres para se utilizar o ambiente cibernético por todas as pessoas dentro do Estado brasileiro. Dessa forma, como afirma o autor, o principal objetivo do Marco Civil da internet foi o de garantir o bom uso do ambiente digital pelos diversos usuários.

Segundo Marcacini (2016, p. 31), tem-se o encontro e a regulação de:

> [...] alguns fatos sociais que são fruto exclusivo da Internet – como é o caso das disposições que estabelecem a neutralidade da rede ou a responsabilidade dos provedores de Internet – mas resvalou também, e pretendeu regular, situações jurídicas que não são uma exclusividade do ciberespaço – como a privacidade, a proteção a dados pessoais ou a liberdade de expressão – embora essas possam encontrar na rede uma larga amplitude de casos concretos e, consequentemente, obter maior visibilidade midiática quando ligadas a fatos ocorridos online. Mas é difícil restringir tais situações apenas ao universo da Internet, no que o Marco Civil deixa uma sensação de incompletude, ou de um encaixe imperfeito, no trato dessas matérias. (MARCACINI, p. 31, 2016).

O autor ainda sustentou que os princípios que regem o Marco Civil da internet visam garantir a proteção das pessoas que ali estão em vários aspectos. A própria lei, nesse ponto, deixou claro quais são os pontos principais desses princípios. Vejamos o artigo terceiro da Lei nº 12.936/2014, que apresenta a seguinte normatização:

> I – Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II – Proteção da privacidade;
> III – proteção dos dados pessoais, na forma da lei;
> IV – Preservação e garantia da neutralidade de rede;
> V – Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI – Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII – preservação da natureza participativa da rede;
> VIII – liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos

> tratados internacionais em que a República Federativa do Brasil seja parte. (BRASIL, 2014).

A partir dessa afirmação tornou-se possível pautar o modo de uso seguro e com qualidade do ambiente digital. Somado a isso, a lei também promove a garantia do uso universal da internet. Outro ponto de importância estabelecido pelo Marco Civil é a regência sobre a liberdade de expressão. Para este, o Marco Civil da Internet seguiu o raciocínio estabelecido pela Constituição Federal, a necessidade de respeito as diferenças e o resguardo aos direitos individuais.

Porém, como afirma Padovez e Prado (2019), apesar dos avanços estabelecidos pelo ordenamento jurídico, ainda há uma discrepância entre as ações efetivas e a velocidade do aumento das condutas ilícitas dentro dos ambientes virtuais. Muitas vezes, as vítimas ficam à mercê da inercia jurídica diante do ineditismo dos fatos.

Mas, como apresenta Guaragni (2019) e Filho (2021), o âmbito jurídico se promove em legislar normas que possam garantir a proteção dessas vítimas. Isso pode ser observado nas mudanças observadas no Código Penal, que estabelece penas aos crimes ocorridos no meio digital. Outro é o uso das extensões da lei para o ambiente digital, crimes semelhantes são tratados de igual forma a fim de garantir respaldo e alcance da proteção da vítima.

Outro ponto sustentado por Corrêa *et al.* (2021), é que existe não somente a necessidade de estabelecer aparato protetivo, mas cabe aos órgãos responsáveis por essa proteção estabelecer políticas educacionais para que as pessoas possam identificar e se proteger de possíveis criminosos cibernéticos.

Segundo Marcacini (2016), embora seja difícil identificar perfis que podem vir causar danos as pessoas, existem certas formas de estabelecer meios para proteção. Já houve muitas características utilizadas “para identificar um criminoso. Hoje nem sequer podemos vê-lo, é uma ameaça invisível que vem atormentando os usuários da rede mundial de computadores. (BRITO, 2013, p. 83).

Dessa forma, boa parte dos órgãos de segurança fomentam que é necessário que os usuários estejam atentos a qualquer contato com pessoas que não sejam do seu vínculo social. Para além disso, crimes financeiros também podem ser cometidos com a utilização de clonagem de números de contato da agenda de possíveis vítimas

Por isso, como afirma, é necessário que a pessoa sempre use fator de segurança em duas etapas: como a ligação de vídeo, além da solicitação da confirmação dos dados mais pessoais de quem se está conversando, são maneiras de assegurar que a conversa está sendo realizada pela pessoa conhecida e evitar que o golpe seja realizado.

Para golpes mais complexos, cujo conhecimento cibernético é mais profundo, autores como Viera (2020), sugerem que sempre entre em contato com órgãos de segurança ao desconfiar de possíveis ataques com seus sistemas cibernéticos.

CONSIDERAÇÕES FINAIS

Em avanços tecnológicos colocaram a sociedade em um novo *status* com relação a capacidade de estabelecer comunicação. Porém, essa evolução não só trouxe benefícios, mas apresentou um meio real para que criminosos pudessem cometer delitos com a sensação de maior impunidade.

Os cibercrimes se instituíram no ambiente social de forma rápida. Tão logo houve o desenvolvimento da internet e de suas tecnologias, sugiram sistemas nocivos capazes de trazer altos prejuízos para pessoas, empresas ou órgãos governamentais. Prejuízos esses, que podem não ser nem financeiros, mas psicológicos também.

Sobre essa perspectiva, o trabalho aqui desenvolvido estabeleceu uma compreensão da responsabilidade jurídica sobre crimes cometidos dentro do ambiente cibernético. Além disso, o trabalho montou uma discussão sobre a velocidade que o sistema jurídico brasileiro apresenta para garantir resposta rápida as diversas novidades de crimes cometidos dentro do ambiente digital.

Observou-se, portanto, uma certa demora de resposta para alcançar um nível de organização jurídica protetiva aos usuários das redes sociais, além de estabelecer meios de controle dessas redes para garantir o respeito aos fundamentos constitucionais.

Outro ponto de interesse, foi a observância das diversas leis que se fomentam para reger o ambiente cibernético. Porém, o que se ver é uma ineficiência de sua aplicabilidade dentro desses ambientes. Dessa forma, como se apresentou no texto, faz-se necessário apresentar sistemas de controle, prevenção e punição mais assertivos.

O presente trabalho, portanto, completou-se em estabelecer uma compreensão sobre os novos ditames sobre as questões relacionadas aos crimes cibernéticos, bem como observações sobre o aparato legal constituído para reger as redes digitais, com a colocação de uma necessária intervenção mais rápida e assertiva do sistema judiciário para garantir um ambiente cibernético longe de crimes.

Sugestiona-se, para trabalhos futuros, uma análise mais apurada sobre o desenvolvimento das leis que regem o ambiente cibernético, bem como apresentar um *status* sobre a existência de capacidade protetiva dessas leis para esses ambientes e quais caminhos podem ser trilhados para estabelecer melhorias nessas questões.

REFERÊNCIAS

AKGÜL, Ali et al. *A fractal fractional model for computer virus dynamics.* ***Chaos, Solitons & Fractals****,* v. 147, p. 110947, 2021.

ALVES, Flaviano de Souza. A criminalidade na Deep Web. **Revista da Escola Superior de Guerra**, v. 33, n. 67, p. 123-141, 2018.

ARAGÃO, Jackson José Lima. Crimes cibernéticos: a prevalência do direito à dignidade da pessoa humana sobre o direito da livre expressão do pensamento. **Revista Processus Multidisciplinar**, v. 2, n. 4, p. 541-566, 2021.

ASAAD, Renas Rajab. *Implementation of a Virus with Treatment and Protection Methods*. **Icontech International Journal**, v. 4, n. 2, p. 28-34, 2020.

AZEVEDO, Letícia; CARDOSO, Thais. **Crimes Cibernéticos.** 2021.

BEPPLER, Tamy et al. Notícias Falsas, Dano Real: Levantamento, Análise e Discussão de Phishing, Malware e Fake News sobre COVID-19. **Anais do Computer on the Beach**, v. 12, p. 080-087, 2021.

BRASIL. Conselho Nacional de Justiça – **CNJ. Portal do CNJ** – PJe. Disponível em: <https://www.cnj.jus.br-portal do CNJ/PJe>. Acesso em: 13/03/2022.

CORRÊA, Luciana et al. Balanço dos principais crimes cibernéticos ocorridos no município de Belém/PA no período de 2018 a 2020. **Research, Society and Development**, v. 11, n. 1, p. e43411125214-e43411125214, 2022.

DECARLI, Gian Carlo. **História e evolução da internet**. Tendências do marketing digital, p. 7, 2018.

FILHO, Paulo Roberto Aguiar de Lima. O direito penal na quarta revolução industrial: A expansão razoável frente aos crimes cibernéticos. **Delictae Revista de Estudos Interdisciplinares sobre o Delito**, v. 6, n. 10, 2021.

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN Wérvertton Gabriel Gomes. Direito e Ciência Política: Estudos em homenagem ao Professor Doutor Raymundo Juliano do Rego Feitosa. In: Fernando Gomes de Andrade (Org); Roberta Cruz da Silva (Org). **O Processo Judicial Eletrônico (PJE) e a Violação à Neutralidade de Rede**. Belo Horizonte: Arraes Editores. 2017.

GUARAGNI, Fábio André et al. Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea. **Revista de Estudos Criminais**, v. 18, n. 73, p. 167-196, 2019.

HERNANDEZ, Erika Fernanda Tangerino; TOLEDO, Nathália Karina Abucci. Crimes cibernéticos: seus efeitos revolucionários diante de uma legislação em constante evolução. **Revista Jurídica da UniFil**, v. 17, n. 17, p. 72-84, 2021.

LINS, Bernardo Felipe Estellita**.** A evolução da Internet: uma perspectiva histórica. **Cadernos Aslegis**, v. 48, p. 11-45, 2013.

MARCACINI, Augusto. **Aspectos Fundamentais do Marco Civil da Internet:** Lei 12.965/2014. São Paulo: Edição do autor, 2016.

MARRA, Fabiane Barbosa. Desafios do direito na era da internet: uma breve análise sobre os crimes cibernéticos. **Campo Jurídico**, v. 7, n. 2, p. 145-167, 2019.

PADOVEZ, Rafael Silva; PRADO, Florestan Rodrigo. O direito penal brasileiro no contexto dos crimes cibernéticos. **Etic-encontro de iniciação científica-ISSN 21-76-8498**, v. 15, n. 15, 2019.

PEREIRA, Kamille da Silva; OLIVEIRA, Fabio Machado. Perícia forense computacional e crimes cibernéticos. **Revista Interdisciplinar Pensamento Científico**, v. 5, n. 2, 2019.

PIMENTEL, Alexandre Freire; CARDOSO, Mateus Queiroz. A Regulamentação do direito ao esquecimento na lei do marco civil da internet e a problemática da responsabilidade civil dos provedores. **Revista da AJURIS**, Porto Alegre, v. 42, n. 137, p. 45-62, mar. 2015.

QUISSANGA, Fernando Cassinda. Caracterização de sistemas operacionais móveis celulares: Android, Symbian, iphone e Windows phone**. Project Design and Management**, v. 1, n. 2, 2019.

RIBAS, Marupiraja Ramos. **Juizado do forró de Caruaru**: **instrumento de garantia do acesso à justiça apoiado nas inovações tecnológicas**. Dissertação (Pós-graduação stricto sensu em Direito) – UNICAP- Asces-Unita, Caruaru, 2021.

ROCHA, Carolina Borges. A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. **Jus Navigandi**, Teresina, ano, v. 18, 2013.

SITE G1. Justiça Federal em Pernambuco sofre ataque cibernético e sistemas ficam fora do ar. **g1.com.br [site].** 2022. Disponível em: <https://g1.globo.com/pe/pernambuco/noticia/2022/04/06/justica-federal-em-pernambuco-ataque-sistema-fora-do-ar.ghtml>. Acesso em: 15/04/2022.

STUANI, Willian; FUCHS, Pedro. Crimes cibernéticos e a legislação brasileira. **Anuário Pesquisa e Extensão Unoesc**, São Miguel do Oeste, v. 6, p. e27927-e27927, 2021.

TABET, Arthur Gomes; PEREIRA, Luiza Barbosa; JORGE, Ricardo Clemente. **Uma análise da ineficácia do direito penal brasileiro em relação à internet**. Jornal Eletrônico Faculdade Vianna Júnior, v. 8, n. 2, p. 23-23, 2016.

VIEIRA, Edinilson Santos. **Prevenção Em Crimes Cibernéticos**. Clube de Autores, 2020.

WILLEMS, Eddy. ***Thirty years of malware: A short outline. In**: **Cyberdanger**. **Springer**, **Cham***. p. 1-12, 2019.