FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ

MIRELLA VIRGÍNIA LIRA GOMES

OS AVANÇOS TECNOLÓGICOS E OS CRIMES CIBERNÉTICOS:
uma análise da conduta de cyberstalking na legislação penal brasileira

Recife

2021

MIRELLA VIRGÍNIA LIRA GOMES

OS AVANÇOS TECNOLÓGICOS E OS CRIMES CIBERNÉTICOS:
uma análise da conduta de cyberstalking na legislação penal brasileira

Trabalho de Conclusão de Curso apresentado ao curso de Direito da Faculdade Damas da Instrução Cristã, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Leonardo Henrique Gonçalves de Siqueira

Recife

2021

Catalogação na fonte
Bibliotecário Ricardo Luiz Lopes CRB-4/2116

Gomes, Mirella Virgínia Lira.
G633a Os avanços tecnológicos e os crimes cibernéticos: uma análise da conduta de Cyberstalking na legislação brasileira / Mirella Virgínia Lira Gomes. - Recife, 2021.
52 f.

Orientador: Prof. Dr. Leonardo Henrique Gonçalves de Siqueira.
Trabalho de Conclusão de Curso (Monografia - Direito) – Faculdade Damas da Instrução Cristã, 2021.
Inclui bibliografia.

1. Crimes cibernéticos. 2. Cyberstalking. 3. Stalking. 4. Legislação brasileira. I. Siqueira, Leonardo Henrique Gonçalves de. II. Faculdade Damas da Instrução Cristã. III. Título.

340 CDU (22. ed.) FADIC (2021.1-014)

MIRELLA VIRGÍNIA LIRA GOMES

OS AVANÇOS TECNOLÓGICOS E OS CRIMES CIBERNÉTICOS:
uma análise da conduta de cyberstalking na legislação penal brasileira

Trabalho de Conclusão de Curso apresentado ao curso de Direito da Faculdade Damas da Instrução Cristã, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Recife - PE, __ de _____ de ____

BANCA EXAMINADORA

_____

Presidente Prof. Dr. Leonardo Henrique Gonçalves de Siqueira

_____

Prof. Dr.

_____

Prof. Dr.

Dedico este trabalho ao meu pai Nilson Gomes (in memoriam), minha maior inspiração de vida, que sempre foi apoio em todos os meus sonhos e projetos. Para ele, minha gratidão e amor infinitos.

AGRADECIMENTOS

Agradeço, primeiramente à Deus, pela iluminação e proteção divina.

Aos meus familiares, em especial minha mãe, Maria Inez e meus irmãos, Márcia e Victor, os maiores e melhores incentivadores, com quem dividi minhas dificuldades, encontrei refúgio e amor sem medidas.

Ao meu maior incentivador, meu pai, à quem dedico toda minha graduação. A minha inspiração, de onde vem a minha força diária para enfrentar as adversidades da vida. Tenho o maior orgulho de dizer que é pra você e por você, por sempre acreditar em mim e me dizer que eu sou capaz. Meu amor e gratidão são infinitos.

As minhas amigas de graduação, Anna Carollina e Ylanna Araújo, que estiveram presentes na minha vida durante todo o curso, me apoiando em todos os dias difíceis com uma amizade sincera que levarei para sempre comigo. Sem elas, os cinco anos de curso não teriam passado com um toque de leveza e com um tom especial.

A Vinicius, pelo apoio, compreensão, cuidado e amor durante esse período de entrega do trabalho de conclusão. Com quem espero compartilhar não somente este, mas muitos outros momentos da minha vida que estão por vir.

Ao corpo docente e todos que fazem parte da Faculdade Damas, em especial ao professor Ricardo Silva, pela dedicação e persistência na disciplina de Orientação Monográfica, incentivando seus alunos a persistirem no caminho e sempre disponível para ajudar.

Por fim, agradeço, também, ao meu orientador e professor Leonardo Siqueira, quem também posso chamar de amigo, por seu acolhimento e disposição, bem como pela confiança e incansável dedicação durante o tempo de desenvolvimento deste trabalho de pesquisa. Seus ensinamentos e a paixão pelo Direito Penal - transmitida através de suas aulas - me motivaram a aprofundar os estudos e a escolher o tema aqui estudado. Meu muito obrigada!

"Não somos o que deveríamos ser; não somos o que queríamos ser; não somos o que iremos ser, mas graças a Deus, não somos o que éramos." (Martin Luther King)

RESUMO

Este trabalho tem por escopo analisar a conduta de *cyberstalking* e o tipo penal dentro do ordenamento jurídico brasileiro. O objetivo geral é analisar a conduta de *cyberstalking* e a atual legislação penal brasileira acerca do tema. Para tanto, apresenta uma retrospectiva da origem do computador e da internet e sua evolução recente com os avanços tecnológicos, passando brevemente pela criação das redes sociais que propiciaram a troca de informações rápidas entre os diversos atores e gradativamente conquistaram novos usuários que buscam informações, cultura, estudo, entretenimento. De outra feita, expõe o entendimento doutrinário pertinente aos crimes cibernéticos, sua definição e uma breve análise das principais classificações acerca desses crimes, como também, uma observação específica neste contexto da Lei nº 12.737 de 2012. Uma revisão geral acerca dos crimes cibernéticos é apresentada antes da análise da conduta específica de *cyberstalking*, a conceituação e o seu enquadramento na atual legislação brasileira.

Palavras-chave: Crimes cibernéticos*. Cyberstalking. Stalking*. Legislação Brasileira.

ABSTRACT

This work aims to analyze the conduct of cyberstalking and the criminal type within the Brazilian legal system. The general objective is to analyze the conduct of cyberstalking and the current Brazilian criminal legislation on the subject. To do so, it presents a retrospective of the origin of the computer and the internet and its recent evolution with technological advances, briefly passing through the creation of social networks that enabled the rapid exchange of information between the various actors and gradually conquered new users who seek information, culture , study, entertainment. On the other hand, it exposes the doctrinal understanding relevant to cyber crimes, its definition and a brief analysis of the main classifications about these crimes, as well as a specific observation in this context of Law No. 12737 of 2012. A general review about cyber crimes is presented before analyzing the specific conduct of cyberstalking, the concept and its framing in current Brazilian legislation.

Keywords: Cyber crimes. Cyberstalking. Stalking. Brazilian Legislation.

SUMÁRIO

1 **INTRODUÇÃO**

Com o passar dos anos a tecnologia dominou o mundo inteiro, de forma que, um simples *click* permite a acesso a inúmeros conteúdos e conexão com diversas pessoas em qualquer país. O meio digital, portanto, tornou-se a maior fonte de comunicação e informação de forma completamente instantânea, expandindo os horizontes de todas as pessoas do mundo e as conectando de forma nunca antes esperada.

O chamado espaço cibernético é o local onde ocorre as comunicações de redes de computação e não tem suas fronteiras claramente definidas o que impacta vigorosamente todos os seus usuários todos os dias.

Assim, o direito digital surgiu como uma nova vertente jurídica o qual busca trazer uma incidência de normas jurídicas que sejam aplicadas diretamente e especificamente ao ciberespaço, pois o direito não acompanha com tal velocidade e as mudanças vivenciadas pela sociedade da informação e o advento do mundo virtual e sua expansão desenfreada.

Entretanto, essa rápida expansão do meio digital (internet) e seu espaço infinito e amplo, trouxe um alerta: até que ponto há segurança no ciberespaço?

Bem como ocorre no âmbito das relações reais e concretas do mundo físico, o mundo virtual também se encontra sujeito à incidência de infrações e violações dos tipos penais, inclusive pela facilidade de acesso e rapidez dos sistemas, ante a ausência de barreiras ao anonimato, assim, os chamados crimes cibernéticos são aqueles que ocorrem dentro das fronteiras indefinidas do espaço cibernético.

Neste sentido, quanto à criminalidade cibernética, o sistema penal brasileiro ainda se encontra em desenvolvimento. Assim, torna-se um desafio para as ciências criminais os assuntos mais específicos e recentes relacionado às condutas cibernéticas, em específico uma conduta conhecida como perseguição virtual ou, também chamada, *cyberstalking* a qual tornou-se recentemente uma conduta típica no código penal brasileiro.

A reflexão acerca da conduta de *cyberstalking* no ordenamento penal brasileiro justifica-se pelo surgimento e avanço das novas tecnologias da era digital e os novos comportamentos humanos consequentes desse avanço, com o uso indiscriminado do sistema informático como um todo. Com isso, surge a necessidade

de aprofundarmos os estudos no Direito Penal Informático, buscando minimizar os efeitos negativos da expansão da tecnologia em relação aos seus usuários, desenvolvendo a visão crítica nesta área para a correta compreensão, com o intuito de proteger os bens jurídicos e os direitos básicos e extremamente fundamentais para a sociedade atual.

Além disso, busca-se atenuar a instabilidade jurídica frente ao desconhecimento e escassez doutrinária acerca do tema dessa pesquisa. Como também, contribuir no avanço da discussão dentro ordenamento jurídico brasileiro buscando a adequada repressão a tais condutas específicas, e assim, reduzindo a insegurança gerada na sociedade pelo número crescente de crimes cibernéticos que ocorrem diariamente.

Assim, a necessidade de aprofundamento se perfaz pelo desconhecimento da conduta por grande parte dos acadêmicos, possível notar que a análise da conduta de *cyberstalking* no ordenamento jurídico brasileiro pode impactar direta ou indiretamente todos os cidadãos que são usuários de tecnologias e estão sujeitos à serem vítimas da conduta, por isso a necessidade de uma maior repressão por parte do direito penal ou até mesmo um avanço na discussão do ordenamento penal brasileiro frente ao surgimento desta nova prática delitiva. Reconhecendo, assim, que a insegurança trazida pelas fronteiras infinitas do mundo virtual e suas trágicas consequências para o mundo real que podem ser amenizadas, ou até sanadas com a devida regulação e atenção acerca deste tema.

Diante desse cenário, o enfoque desse trabalho é propor uma resposta para o seguinte problema de pesquisa: Como se enquadra a conduta de *cyberstalking* na atual legislação penal brasileira tendo o ambiente informático como facilitador?

Portanto, o presente trabalho de pesquisa tem como objetivo geral analisar a conduta de *cyberstalking* na atual legislação penal brasileira, e definem-se os seguintes objetivos específicos: Apresentar os avanços tecnológicos da era digital no âmbito do direito; conceituar os crimes cibernéticos, apontando as principais classificações e fazendo uma breve análise do tipo penal específico constante na Lei nº 12.737 de 2012; e analisar a conduta de *cyberstalking* e seu enquadramento dentro do atual ordenamento jurídico brasileiro.

A metodologia para elaboração da pesquisa baseia-se no estudo de carácter descritivo, que apresenta enorme potencial teórico e prático para fazer progredir a

Ciência do Direito, através do método hipotético-dedutivo, onde será apresentada de forma qualitativa, a partir da coleta de informações de fontes secundárias, utilizando pesquisas bibliográficas já existentes, tais como: artigos científicos, livros, dissertações, teses e a pesquisa no campo da internet.

No primeiro capítulo, é abordado a relação entre tecnologia, internet e o Direito, entendendo as mudanças vivenciadas com o passar dos anos nos meios de comunicação dos seres humanos passando pela criação dos computadores e o surgimento da internet, buscou-se um entendimento resumido de como funcionava a internet e como ela surgiu também no Brasil. Considerando os avanços tecnológicos e a utilização em massa dos sistemas informáticos, continuou-se a discussão científica no entendimento do que seria o ciberespaço e sua definição, analisando neste contexto também, o surgimento das redes sociais - hoje os mais famosos meios de comunicação e interação no mundo.

Na continuação, ainda no primeiro capítulo, será abordado o surgimento de um ramo do Direito, chamado de Direito Digital, buscando um entendimento do contexto e a expansão do espaço cibernético e suas consequências relacionadas ao direito, como os avanços tecnológicos influenciaram no mundo jurídico e na vida da sociedade em geral, principalmente no Direito Penal.

No segundo capítulo, entra em foco os crimes cibernéticos, a nova denominação dos delitos que ocorrem no ciberespaço - também chamados de crimes digitais - que surgiram desde o surgimento da rede mundial de computadores, mas ganharam maiores destaques mais recentemente. Assim, o segundo capítulo traz uma conceituação do que seriam os crimes cibernéticos e uma breve passagem da legislação internacional acerca do tema.

Posteriormente, faz-se uma análise das principais classificações dos crimes cibernéticos em uma visão geral, definindo as suas características mais relevantes com ênfase no tipo penal da Lei nº 12.737 de 2012 - também chamada de Lei Carolina Dieckmann, a lei que tipifica o crime de invasão de dispositivo informático - traçando um paralelo do seu surgimento e fazendo uma breve análise de sua classificação.

E, por fim, no terceiro capítulo o principal ponto deste trabalho de pesquisa, o qual traz uma análise do crime cibernético específico que é o crime de *cyberstalking.* Inicialmente, busca-se a diferenciação entre o delito de *stalking* e *cyberstalking*,

posteriormente, a conceituação do delito de *cyberstalking* e todo o contexto que envolve o crime específico, de que forma ele ocorre e impacta o usuário que é a vítima.

Em continuação, após a definição e entendimento do delito é averiguado o tipo penal dentro do ordenamento jurídico brasileiro, na perspectiva de verificar como se enquadra o crime de *cyberstalking* na atual legislação penal brasileira capaz de assegurar a proteção ao bem jurídico violado no âmbito do mundo virtual.

2 **INTERNET, TECNOLOGIA E DIREITO**

2.1 O SURGIMENTO DO COMPUTADOR E DA INTERNET

Desde os primórdios da existência humana, a comunicação é imprescindível para o indivíduo, um dos fatores essenciais de sobrevivência humana. Os seres humanos, por serem cientificamente uma espécie que vive em grupos, e possuírem intenções cooperativas, criaram diversas formas de se comunicar e interagir entre si e com o mundo.

Assim, com o passar dos anos, o homem foi adquirindo formas mais claras e evoluídas de comunicação com a finalidade de interconectar povos e culturas. Inicialmente expressaram-se através de pinturas, símbolos, passando por gestos, grunhidos e posturas, até o desenvolvimento da escrita e da comunicação verbal, todas essas formas que se modificaram bastante durante os anos chegando as mais modernas tecnologias da comunicação.

A essencialidade e a necessidade da comunicação humana foi o que impulsionou a conexão entre povos de localidades e culturas diferentes, destacando cada povo e, deste modo, exaltando suas crenças, culturas e tradições individuais. Com o desenvolvimento humano e juntamente com os avanços da ciência e tecnologia, o homem criou novas interfaces de comunicação como maneiras mais eficazes e rápidas para conexão entre povos.

Assim, desde os tempos primitivos até os dias atuais, o homem passou pelas mais diversas formas de comunicação e atingiu as mais modernas tecnologias, tornando o ato de comunicar uma atividade essencial para a vida em sociedade.

Os meios de comunicação representam os veículos ou instrumentos que possibilitam o encaminhamento e o compartilhamento de informações utilizado para difundir a informação entre os homens. Hoje em dia, são instrumentos essenciais para a transmissão direta de conteúdos e conhecimentos pelo mundo, sendo o computador, o celular e a internet fortes exemplos desses meios de comunicação.

Observou-se duas transformações que foram extremamente relevantes no processo de comunicação da sociedade, dentre elas a primeira que foi a transformação tecnológica que houve com a ligação direta de computadores, a criação de softwares avançados e a conexão de redes sem fio, resultando na

digitalização da comunicação com a internet e a expansão da comunicação local-global. (CASTELLS, 2009, p. 99)

Apesar de dificuldade da especificação da data, sabe-se que durante o século XX foi criado o primeiro computador no molde similar ao que conhecemos atualmente. O desenvolvimento do computador, também chamado de máquina digital, pode ser entendido como uma máquina que é composta alguns elementos físicos de natureza eletrônica e com potência para praticar diversas tarefas com velocidade e precisão, e mostrou-se particularmente muito útil na segunda guerra mundial facilitando a interpretação de códigos para interceptação de sinais dos países em guerra.

Portanto, os primeiros computadores surgiram como um marco revolucionário no mundo inteiro, trazendo uma era de evolução da comunicação e das relações humanas em diversos aspectos, desde o início de seu surgimento e ainda, até os dias atuais, proporcionando grandes mudanças na sociedade e em toda história da humanidade.

Os computadores surgiram para facilitar nosso dia a dia, as tarefas que antes eram realizadas em espaços de tempo muito longos, passaram a ser realizadas quase de forma instantânea, o computador é uma máquina que armazena e transforma informações, sob o controle de instruções predeterminadas. (FRAGOMENI, 1987, p. 125)

O desenvolvimento da ciência e da tecnologia, juntamente com os meios de comunicação e a globalização, permitiram uma mudança significativa na sociedade contemporânea, propiciando uma enorme difusão do conhecimento e da comunicação no mundo inteiro, resultando na transformação digital. O mundo da tecnologia, a vida, o trabalho e as relações pessoais dos indivíduos sofreram mudanças gigantescas e que proporcionou a criação da internet, entendida atualmente, como o veículo de excelência e destaque na transmissão de informações.

Como uma forma de conexão entre computadores surgiu a internet que é sistema mundial público, de rede de computadores, ao qual qualquer pessoa ou computador, previamente autorizado, pode se conectar. Obtida a conexão o sistema permite a transferência de informação entre computadores, onde a infraestrutura utilizada pela internet é a rede mundial de telecomunicações.

A criação da internet não foi um processo rápido e nem simples, mas sabe-se que foi uma revolução à época, bem como nos dias atuais, e foi esse o intuito de sua criação. O primeiro passo do surgimento da internet foi dado nos Estados Unidos da América com fins exclusivamente militares no ano de 1969, exatamente durante a guerra fria. Com o intuito de revolucionar as invenções tecnológicas da época, e ainda destacar-se diante da União Soviética, foi desenvolvido o denominado *ARPANET*, um pequeno programa que interligou de uma rede de computadores montada pelo *Advanced Research Project Agency* (ARPA), uma agência de pesquisas do departamento de defesa dos EUA. (CASTELLS, 2003, p. 13)

Almejava-se atingir uma tecnologia que tinha como função principal a conexão de vários sistemas dos centros de pesquisas dos Estados Unidos, onde de maneira segura pudessem manter os canais de comunicação. Assim, facilitaria o cruzamento de informações e o planejamento das estratégias de defesa em caso de uma guerra nuclear.

A Internet, como se conhece e se utiliza hoje, se popularizou e foi disponibilizada ao público nos anos 1990, quando o engenheiro Tim Berners-Lee criou e concretizou um sistema no qual denominou de *World Wide Web* (www), com uma área de atuação gráfica e a possibilidade de desenvolvimento de sites mais modernos tecnologicamente. Foi o compartilhamento de informações gerada pelo *world wide web*que possibilitou o amplo alcance global da internet mediante a associação de fontes de informação através da computação interativa. (CASTELLS, 2003, p. 18)

É possível esclarecer, portanto, que a internet chamada de rede mundial de computadores, é uma rede mundial que interliga os computadores em escala global e, dessa forma, fornece aos usuários acesso a diversas informações compartilhadas, e correspondeu a um salto no desenvolvimento da humanidade, representando uma mudança de paradigmas no pensar e no agir da sociedade e um marco do mundo moderno.

Em termos de definição, a Internet foi conceituada como “um meio de comunicação que permite, pela primeira vez, a comunicação de muitos com muitos, num momento escolhido em escala global” (CASTELLS, 2003, p. 8). Assim, um conjunto de computadores interligados que tem em comum um conjunto de

protocolos e serviços, de uma forma que os usuários conectados possam usufruir de serviços de informação e comunicação de alcance mundial.

O processo de comunicação foi potencializado com a internet, que permitiu a interação e a socialização à distância, com a ausência do corpo físico mas sempre trazendo as experiências para seus usuários de interações reais dentro do mundo virtual.

O sistema de redes composto pela internet é complexo, em definições mais simplificadas a internet é a interligação de milhares de dispositivos através do chamado *Internet Protocol* (IP) com um mesmo padrão de dados, podendo ser por meio de cabos de fibra óptica, satélites, linhas telefônicas e outros. O que faz o usuário estar conectado e navegando é a utilização de um browser, o programa que é o meio de interpretação e acesso à vários websites e através desse programa que podemos ter acesso aos sons e imagens produzidos. São alguns exemplos de browsers: o *Internet Explorer* (*Microsoft*), o *Netscape Navigator* (*Netscape*), o *Mozila Firefox* (*The Mozila*). (PINHEIRO, 2013, p. 39)

Assim, o usuário acessa a internet fornecendo ao computador o endereço IP para que seja conectado à rede e, posteriormente, o usuário dispõe na rede os subendereços conectados com os provedores. O que conhecemos pelos endereços dos sites que acessamos, são nada mais do que informações do IP numéricos convertidos em palavras pelo protocolo chamado *Domain Name System* (DNS), os domínios dos *websites* que são seus endereços de conexão na rede. Já as terminações do endereço são feitas de acordo com os *Top Level Domains* (TLD), que são os caracteres após o último ponto no endereço do *website*que registram também o país de origem do usuário. (PINHEIRO, 2013, p. 39)

No Brasil a internet começou a ser utilizada na década de 1990, por iniciativa da Fundação de Amparo à Pesquisa do Estado de São Paulo, juntamente com a Universidade do Rio de Janeiro e do Laboratório Nacional de Computação Científica. Com isso, foi criada a Rede Nacional de Pesquisa pelo Ministério da Ciência e Tecnologia que teve o papel de iniciar e coordenar o acesso à internet no país, que foi disponibilizada apenas para centros de pesquisas e universidades.

A explosão da internet no Brasil foi gerada pela empresa de telecomunicação Embratel, quando em meados de 1994 através da exploração comercial, lançou um *backbone2*, que em definições simplificadas é uma rede constituída por cabos que

permite a transmissão de dados, voz e imagem, o que favoreceu a qualidade da internet disponibilizados à época pela Embratel.

Segundo as pesquisas mais atuais no Brasil apontam que a Internet era utilizada em 82,7% dos domicílios do País em 2019, um aumento de 3,6 pontos percentuais (p.p.) em relação a 2018. Sendo assim, podemos observar que está cada dia maior o número de brasileiros com acesso à internet e conectados ao mundo virtual[1].

Um fato indiscutível é que a internet uma das maiores sensações dos tempos modernos, tornou-se um símbolo da nossa engenhosidade tecnológica e oferece ao ser humano uma série de benefícios e um mundo novo no qual há infinitas possibilidades.

2.2 OS AVANÇOS DA TECNOLOGIA, O CIBERESPAÇO E O SURGIMENTO DAS REDES SOCIAIS

A expansão da comunicação em escalas mundiais e a eclosão dessa recente onda tecnológica gerada pela internet, trouxe muitas expressões novas para o nosso idioma, oriundas da era da tecnologia da informação, que foi se tornando natural e comum em todo país, expressões como era digital, mundo virtual e cibernética foram um dos exemplos disso.

O que antes era conhecido como sociedade industrial, deu margem a um novo modelo de sociedade denominado de sociedade da informação e o marco principal de rompimento foram os avanços tecnológicos, em que todas as transformações foram acontecendo de forma célere no piscar de olhos, ou de *clicks*, e o cenário era completamente novo. O tempo e o espaço foram redefinidos dentro do ambiente virtual e as barreiras que antes eram bem delimitadas e conhecidas, foram derrubadas dando margem ao mundo cibernético com a ausência de fronteiras.

A internet propiciou o surgimento de um espaço próprio chamado de ciberespaço ou espaço cibernético. A expressão surgiu inicialmente na obra *neuromancer* do escritor William Gibson, no qual fez a expressão ser difundida

[1]IBGE – Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal 2019 PNAD contínua (ajeitar citação IBGE)

através de sua obra de ficção científica mesmo não tendo sido criada com esse intuito, foi incorporada pelo meio acadêmico para relacionar a ideia de um espaço de comunicação, conceituado como um ambiente virtual de comunicação livre. (GIBSON, 1984, p. 51)

O ciberespaço constitui um campo vasto e aberto, ainda parcialmente indeterminado, que não pode ser definido por apenas uma característica, pois ele tem vocação para se interconectar e se combinar com quaisquer dispositivos de criação, gravação, comunicação e simulação. Marcel Leonardi considera:

> "é importante frisar, como já fizemos anteriormente, que o ciberespaço não existe como realidade física: não é um Estado soberano, mas apenas uma representação audiovisual criada e mantida por sistemas informáticos e programas de computador, presente em quase todos os países do mundo." (LEONARDI, 2011, p. 129)

Ainda neste sentido, é errôneo classificar o espaço cibernético como um local de navegação onde se busca locais para a interação de usuários como se estivesse relacionando tal espaço ao território físico que é de fácil conhecimento e compreensão. A falsa impressão da internet como um lugar, inclusive dificulta o entendimento e o desenvolvimento de mecanismos eficazes de regulação e de tutela. (LEONARDI, 2011, p. 34)

Portanto, o ciberespaço seria um conceito do mundo virtual onde as conexões acontecem, mas não é um lugar e sim vários lugares, tudo acontece simultaneamente constitui-se um novo espaço de sociabilidade que é não-presencial e que possui impactos importantes na produção de valor, nos conceitos éticos e morais e nas relações humanas. A extensão do ciberespaço acompanha e acelera uma virtualização geral da economia e da sociedade.

Segundo Luís Martino:

> "Uma das características do ciberespaço é sua arquitetura aberta, isto é, a capacidade de crescer indefinidamente. É fluido, em constante movimento - dados são acrescentados e desaparecem, conexões são criadas e desfeitas em um fluxo constante. " (MARTINO, 2014, p. 29)

Todo o ambiente virtual é complexo e extremamente amplo como já apontado anteriormente, além de umas das suas características mais relevantes que é a fluidez. A cada ano veio se renovando e mostrando as inúmeras possibilidades de

exploração que há nesse meio. Assim o ano de 2006 representou um significativo marco para a Internet, quando surgiu um novo avanço das redes, com o advento de novas plataformas virtuais que ganharam espaço, como o *Orkut*, *Facebook*, *Twitter*, *Instagram* e afins, as chamadas redes sociais ou mídias sociais.

As redes sociais, foram assim denominadas por surgirem na rede como mais um meio de socialização e comunicação, estabelecendo relações, não só de trabalho, mas também de busca por inovação, de estudo ou mesmo de amizade, além de outros interesses que perpassam a sociedade como um todo.

Ressalta-se a importante conexão entre a comunicação humana e a internet e como toda a sociedade foi modificada a partir dela, o desenvolvimento de relações humanas pautadas na flexibilidade e dinamicidade da rede e de seus usuários é uma ideia de representação das redes sociais. Desse modo, as formas de organização social foi a parte determinante como elo de interação, onde foi fundada sob um tipo específico de vínculo que constrói a relação aí evidenciada. Ao longo da história vários tipos de organização social foram desenvolvidos, cada uma delas fundada sobre um tipo específico de vínculo ou laço, isto é, o elemento que forma a base da convivência nas mídias sociais e o fator determinante de interação. (MARTINO, 2014, p. 52)

A cada dia, novas formas de comunicação social são introduzidas na sociedade, com a participação de pessoas do mundo inteiro, com destaque para as redes sociais que, gradativamente conquistaram um maior número de usuários, despertando o interesse de estudiosos de relações sociais.

Com o surgimento da internet, das mídias sociais e toda a era digital que se desenvolveu com ela, fizeram surgir novos paradigmas e desafios para a sociedade, bem como provocou o debate sobre os avanços da tecnologia e o papel jurídico nesses contextos. O que exigiu muita atenção e para o direito em sua regulamentação e organização, permeando com a problematização da atuação do direito nesse meio.

Não há o que se discutir de todos os benefícios trazidos pela internet e os avanços do mundo digital, as facilidades de acesso juntamente com as evoluções de diversos segmentos foram e continuam sendo significativas. Porém, não podemos ignorar a dificuldade da sociedade em impor os limites em um espaço sem fronteiras definidas e a facilidade do anonimato que ocorre na internet.

2.3 O SURGIMENTO DO DIREITO DIGITAL: A RELAÇÃO DO DIREITO E AS MUDANÇAS CONTEMPLADAS PELA SOCIEDADE DIGITAL

O mundo passou por transformações significativas e hoje se vive a era digital, momento no qual a sociedade respira tecnologia e grande parte da interação de grupos se dá por meio de processos tecnológicos. Com as mudanças da sociedade surge o seguinte questionamento: De que maneira o direito é afetado com as mudanças da era digital na sociedade?

Pois bem. Essa pergunta não é facilmente respondida, pois há uma vastidão de influências da internet no mundo jurídico que atinge, inclusive, vários ramos do direito. Deixando nítido a conexão, até fortuitamente, do meio jurídico com tais mudanças. Porém, o que de fato tem acontecido é que o direito vem sendo influenciado e modificado pela internet desde seu surgimento.

Como conceituado por Hans Kelsen o Direito é uma ordem normativa da conduta humana, porém não é apenas uma norma e sim, um conjunto de normas. Ou seja, é um sistema de normas que regulam o comportamento humano. (KELSEN, 1999, p. 28)

Contudo não se pode deixar de observar que o direito ainda vai além. Esse conjunto de normas não é apenas quem regulamenta a conduta humana, mas é também quem é regulamentado pela conduta de toda uma sociedade e por ela modificado. Afinal, a realidade sociológica começou a fazer parte do direito e este como ciência social precisou estudar seus impactos nas relações humanas, que vem se modificando com o passar dos anos e necessita acompanhar o que acontece atualmente da sociedade moderna.

Sendo assim, ao se compreender o Direito como a ciência que rege e normaliza a vida no seio social, entende-se que com o advento da tecnologia e todas as mudanças trazidas por ela em caráter global, é necessário aprofundar os estudos que relacionam as duas ciências e os efeitos que a segunda tem sobre a primeira, com o intuito de alcançar o "ideal de justiça" e, se possível, de traçar as fronteiras do "ilegal e do obrigatório" a ser perseguido.

Destarte, o Direito e a tecnologia não são independentes entre si, não existem mais separadamente. Como o Direito sofreu diversas influências com a invenção de alguns elementos ao longo da história, também foi forçado a se reestruturar diante dos riscos e inovações que surgiram, compelindo todo o sistema jurídico a ser modificado normativamente. (LEONARDI, 2011, p. 27)

Um ramo do direito surge resultado da relação da tecnologia com a ciência do direito, tratando-se de um conjunto de normas, aplicações, conhecimentos e relações jurídicas, oriundas do universo digital. O direito digital, portanto, é o ramo jurídico que corresponde ao conjunto de normas que visam tutelar as relações humanas e as violações comportamentais em ambientes digitais.

Neste sentido, Patrícia Peck Pinheiro aponta que estamos equivocados ao pensar que o direito digital é completamente novo. Ao contrário do que pensamos ele tem sua base na maioria dos princípios das normas jurídicas atuais e aproveita-se da maior parte das legislações em vigor atualmente no país, a com exceção de pontos específicos, a diferenciação da aplicação das normas está, muitas vezes, na interpretação e aplicação. (PINHEIRO, 2013, p. 49)

Desse ponto sobrevém a importância de estudos nessa área do Direito com a finalidade de contribuir de modo original à ciência jurídica brasileira, propondo-se útil diante da dificuldade advinda das modificações rápidas que andam ocorrendo. O fato é que a nova realidade da sociedade digital não se adaptará as normas jurídicas atuais, mas o contrário parece mais adequado e eficiente.

O papel do Direito é a consecução da Justiça entre os homens, um agente essencial na convivência social, em que pese ser indiferente que as relações ocorram por meio de uma ferramenta tecnológica que pareça separada da realidade palpável. O principal é que as consequências prejudiciais são sentidas no mundo real e necessitam de um posicionamento adequado e eficiente. O que a ciência jurídica busca, na verdade, é a proteção aos direitos e bens jurídicos. (LEONARDI, 2011, p. 42)

A respeito do assunto considera:

> “O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral,

> Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.)" (PINHEIRO, 2013, p. 46)

O grande desafio da atualidade jurídica é a perpetuação de sua aptidão ao refletir as grandes modificações comportamentais e culturais vividas pela sociedade. Ou seja, a proposta é que o Direito siga sua vocação de refletir as grandes mudanças culturais e comportamentais vividas pela sociedade, porém com a cautela exigida, uma vez que o ritmo da evolução tecnológica será sempre mais veloz que as mudanças sofridas no ordenamento jurídico. Por isso, qualquer lei que venha a tratar dos novos institutos jurídicos deve ser genérica o suficiente para sobreviver ao tempo e flexível para atender aos diversos formatos que podem surgir de um único assunto.

O ciberespaço e todas as suas possibilidades nos trouxeram uma inquestionável vantagem, entretanto também malefícios neste meio tal qual a ausência de normatização das problemáticas jurídicas instaladas. As modificações nas relações humanas causadas pelo meio são significativas e o direito não pode permanecer inerte diante deste acontecimento. Assim, a inatividade legislativa resultaria no obsoletismo dos institutos jurídicos. Com a finalidade de, justamente, evitar a atrofia desses institutos é que surge o grande desafio do ajustamento das condutas aos sistemas jurídicos nacionais, uma maneira de adequar o direito à realidade a que se propõe tutelar. (REINALDO FILHO, 2011)

Sabe-se que a lógica jurídica não acompanha a sociedade no mesmo ritmo, porém, também é fato a necessidade de discussões e incentivos da manifestação jurídica nesse contexto digital. Esta coesão de pensamento possibilita efetivamente alcançar resultados e preencher lacunas nunca antes resolvidas no âmbito virtual, trazendo maior segurança jurídica bem como a efetividade da essência do direito à proteção dos bens jurídicos e dos direitos dos indivíduos no mundo digital.

3 **DOS CRIMES CIBERNÉTICOS**

3.1 DO CONCEITO DE CRIMES CIBERNÉTICOS

As ciências jurídicas como um todo têm sido ostensivamente impactadas pela era digital e suas evoluções, principalmente a esfera criminal com os chamados crimes cibernéticos. No entanto, não existe uma nomenclatura padronizada para os respectivos delitos, por isso esses são intitulados também de crimes virtuais, crimes informáticos, crimes de computador, *cybercrimes*, *computer crimes*, delito informático, crimes eletrônicos ou ainda crimes digitais, diversas denominações para classificações aparentemente semelhantes dentro do âmbito do direito penal. Essas condutas criminosas foram especificamente denominadas como cibernética ou virtuais por serem crimes que envolvem qualquer atividade ou prática ilícita na rede.

Em uma breve análise acerca das nomenclaturas utilizadas para a matéria, a falta de uma unificação das terminologias utilizadas traz consequências reais para o estudo doutrinário e acadêmico, bem como uma desorientação ao tratar do assunto pelas divergências em sua aplicação prática. Com a harmonia do *nomen juris* dado à matéria, toda pesquisa sobre o tema se embasaria em uma única e abrangente terminologia jurídica, com suas convenientes ramificações para as aplicações jurisdicionais. (BECKERT TRINKEL, 2010, p. 10)

Assim sendo, a nomenclatura "crimes cibernéticos" é considerada uma das mais adequada por abranger todos os delitos cometidos no classificado espaço-tempo cibernético ou por meio deste cometido, diferenciando-os das condutas cometidas no mundo real.

Pois bem. O cenário virtual tornou-se favorável para a prática de crimes, e apesar das vantagens oferecidas pela internet e dos sistemas informáticos, há a inquestionável fragilidade dos seus usuários e, com isso, cada vez mais pessoas se valem desse acesso à rede para a realização dos mais variados tipos de delitos. Com o surgimento da rede virtual, os delitos já tipificados pelo Código Penal passaram a ser praticados também online, bem como foram criadas novas modalidades que passaram a ser exercidas através da utilização deste meio.

No mundo atual, uma simples postagem nas redes sociais pode significar o início de um problema maior. E os mais variados crimes podem ser cometidos a

partir dos dados pessoais expostos na comunicação virtual, o que se concretiza, por exemplo na violação de fotos íntimas, ou na invasão de contas bancárias, na usurpação de dados pessoais para compras através do e-commerce, dentre outros.

Foram identificadas novas situações jurídicas que passaram a demandar reformulação de conceitos e a necessidade de buscar um maior conhecimento do tema, na expectativa de assegurar aos cidadãos a tutela jurídica, na medida em que a nova tecnologia trouxe em seu bojo uma vulnerabilidade que pode atingir a todos indiscriminadamente.

Em verdade, pode-se afirmar que nos crimes virtuais, o sistema digital pode ser o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal. Assim, crime cibernético não envolve apenas a internet, mas o sistema informático por completo, os crimes praticados via internet são apenas uma área, um ramo.

Por meio do conceito analítico de crime, pode-se chegar à conclusão de que crimes cibernéticos são todas as condutas “típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática” (SCHMIDT, 2014)

Ainda neste sentido, Augusto Rossini destaca:

> “O conceito de ‘delito informático’ poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.” (ROSSINI, 2004, p. 78)

É evidente que o aumento do número de acessos à internet e de usuários online no mundo todo, trouxe consigo uma insegurança pelo desconhecido que é vivenciado no ciberespaço. O acesso ao mundo virtual é feito com apenas um click ou um toque na tela, e despertou incerteza nos usuários tanto pela facilidade de acesso quanto pela possibilidade de anonimato, enaltecendo a vulnerabilidade destes, tornando-os vítimas de perigos reais.

Os crimes cibernéticos, portanto, consistem em delitos praticados por pessoas que, em geral, dispõem de conhecimento técnico de informática, utilizando-o com o objetivo de causar dano a terceiros. À luz do magistério de Sérgio Marcos Roque, crime cibernético é “toda conduta, definida em lei como crime, em que o

computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material" (ROQUE, 2007, p. 25)

Segundo dados da Norton, empresa especializada em segurança digital, quase 500 milhões de consumidores no mundo foram vítimas de crime cibernético, com quase 350 milhões só no último ano[2].

A preocupação diante do crescimento do número de delitos informáticos é uma questão mundial e não é apenas na atualidade, pois, já na década de 60 falava-se em crimes virtuais e suas consequências na vida real. Assim, foi criado em 23 de novembro de 2001, pelo Conselho da Europa, a Convenção Europeia dos Crimes Cibernéticos desenvolvida na cidade de Budapeste, na Hungria, por isso também conhecida como a Convenção de Budapeste.[3]

A convenção está em vigor desde 2004 e hoje possui mais de sessenta e dois Estados Membros, é considerado o mais importante e abrangente ato normativo de incriminação aos crimes cibernéticos e tem o objetivo de facilitar a cooperação internacional para o combate ao crime cibernético, apresentando uma tentativa de união geral de esforços sobre o que já se discutia há alguns anos e tipifica os principais crimes cometidos na Internet.

O Brasil ainda não é signatário da Convenção de Budapeste, tendo sido convidado em dezembro de 2019 a aderir[4] ao referido plano de cooperação internacional, podendo, desde já, participar como observador. Neste sentido, o Governo Brasileiro encaminhou ao Congresso Nacional para o processo de ratificação legislativa a adesão do Brasil como Estado Parte da Convenção.[5]

A pandemia enfrentada atualmente impulsionou ainda mais o uso da internet como ferramenta cotidiana, e se os delitos informáticos já viam em grande

---

[2]Relatório de Informações de Segurança Cibernética do NortonLifeLock. Empresa especializada em segurança cibernética. Disponível em: https://br.norton.com/nortonlifelock-cyber-safety-report

[3]É A Convenção Europeia que versa sobre os crimes cibernéticos, também chamada de Convenção de Budapeste. É um tratado internacional para definir de forma harmônica os crimes praticados por meio da Internet e as formas de persecução.

[4]Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública, 2019. Disponível em:https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publicaAcesso em: 9 mai.2021.

[5]Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética, 2020. Disponível em: https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-ciberneticaAcesso em: 10 mai.2021.

crescimento, neste período aumentou de forma exponencial. Com isso, favoreceu a rediscussão da necessidade de ampliação de legislações sobre crimes cibernéticos através da adesão à Convenção de Budapeste, de modo que poderia assegurar ao Brasil uma estruturação legal mais vigorosa para tratar o aumento da vulnerabilidade no espaço cibernético, alinhando-se aos outros países nas demandas globais acerca do assunto e cooperando no combate aos crimes virtuais.[6] (SENNA ; FERRARI, 2020).

Diante do cenário atual no Brasil, ainda há muito para avançar no que diz respeito aos estudos e pesquisas relacionados aos crimes virtuais no ordenamento jurídico brasileiro, bem como, a relação direito e tecnologia. Porém não se pode negar que o tema tem sido mais discutido atualmente e, inclusive, alcançando a sociedade os verdadeiros usuários e os mais atingidos pelas consequências do avanço desenfreado da internet.

Com isso, a adesão à convenção pelo Brasil resultaria no aperfeiçoamento da conjuntura jurídica acerca do tema, com a criação de tipos penais específicos, além de proporcionar a harmonização da legislação brasileiras com a legislação de outros países mais desenvolvidos, facilitando a cooperação internacional em investigações, e nas medidas de prevenção e repressão aos crimes cibernéticos, tornando mais efetiva a possibilidade de punição nos casos enfrentados. Além disso, contribuiria no aprofundamento e desenvolvimento de pesquisas, o que é um ponto de extrema importância na qual deve ser essencialmente considerado pelas autoridades brasileiras.

3.2 BREVE ANÁLISE DA CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS E A LEI Nº 12.737 DE 2012

Os crimes cibernéticos podem ser cometidos contra um sistema virtual ou, apenas, sendo utilizado como meio para a realização de outras condutas, algumas são as classificações desses delitos como veremos na sequência.

A importância da análise da classificação dos crimes cibernéticos no âmbito do Direito Penal justifica-se na ausência de quantidade significativa de estudos

[6]Convenção de Budapeste e crimes cibernéticos no Brasil, 2020. Disponível em:https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasilAcesso em: 18 mai.2021

realizados na área, bem como do pouco aprofundamento da temática no ordenamento jurídico brasileiro. É bem verdade, que nos dias atuais falamos bem mais dos delitos virtuais e todas as suas definições, características e classificações, porém os referidos delitos não são considerados assim uma novidade pelos especialistas na área, com isso estamos em grande desvantagem frente à velocidade do mundo digital e a impacto dos delitos na vida dos usuários da rede. Ainda, a relevância ganha destaque no avanço e aprofundamento da temática no âmbito nacional em detrimento aos outros países mais desenvolvidos.

Neste sentido, os Delitos de Informática Próprios ou Puros são aqueles em que a realização da conduta meio e fim pretendidos pelo infrator situa-se no próprio meio da informática. Ou seja, o transgressor utiliza-se do meio informático para atingir elementos do próprio ambiente, através da utilização de softwares, sistemas, programas podendo ser visando atingir um indivíduo ou vários, ou ainda, o sistema inteiro. (LIMA VIANNA, 2001, p. 13)

Especificamente nesta classificação o bem jurídico ofendido é a tecnologia da informática em si, na qual toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas, o bem jurídico pela norma penal dos delitos virtuais próprios é inviolabilidade das informações automatizadas os referidos dados.

Nesta linha da concepção classificatória, observa-se que o entendimento amplamente difundido pela mídia e parte considerável da doutrina sobre os delitos informáticos seriam o que o doutrinador denominada “crimes informáticos impróprios”, ou seja, delitos comuns em que, de acordo com o conceito analítico de crime, são as condutas típicas, antijurídicas e culpáveis, perpetrados por meio de mecanismos informáticos como ferramenta, contudo, poderiam adotar um outro meio para atingir seu fim. Enquanto os delitos informáticos próprios são as condutas típicas, antijurídicas e culpáveis que têm por fim violar um sistema informáticos ou seus dados, de forma precisa em sua confidencialidade, integridade e disponibilidade. (SYDOW; GOMES, 2015)

A complexidade que permeia os delitos virtuais próprios está diretamente relacionada à complexidade dos sistemas informáticos e ainda pela vasta diversidade dos crimes que se enquadram nessa classificação, dentre alguns deles

estão: delito de acesso não autorizado à sistemas computacionais, a interferência em sistemas e/ou dados computacionais e ainda a interceptação ilegal de sistemas. Esses delitos possuem suas especificidades e detalhamentos, mas em uma visão geral consistem na invasão e acesso às redes com o fito de impossibilitar a utilização de sistemas e/ou dados, ainda manipulá-los ou capturá-los.

Um outro delito virtual bem comum e conhecido pelos usuários de tecnologias informáticas é a criação e divulgação de programas de computadores destrutivos, com a utilização de vírus informáticos. Certamente qualquer indivíduo como usuário assíduo de tecnologias e computadores já ouviu sobre os nomes mais comuns de vírus, como cavalo de tróia (*trojan*), *Ransomware, autorun, majava*, dentre outros.

Uma outra classificação são os Delitos Informáticos Impróprios, em que o computador é utilizado como meio na prática de alguma conduta já existente e tipificada no ordenamento.

Conforme preceitua, Damásio de Jesus, são os delitos em que:

> “ a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais.” (JESUS; MILAGRE, 2016, p. 54)

As ocorrências mais comuns que se enquadram nas condutas virtuais impróprias são, por exemplo, os crimes contra a honra realizados através de redes sociais, tais como *instagram* e *facebook*, onde a pessoa utiliza-se do meio para difundir a sua ofensa mais rápida. Diferentemente da classificação vista anteriormente, esta não está diretamente relacionada ao sistema computacional, mas utilizando dele como meio para a realização de condutas anteriormente conhecidas.

Tal classificação não exige do agente infrator um conhecimento aprofundado em computação, outrossim a simplicidade e facilidade do acesso anônimo nas redes e websites torna-os responsável por uma expressiva quantidade de ações praticadas nesse sentido. A internet e os computadores são usados nesse caso como instrumentos para a prática da conduta típica na modalidade de publicar. (LIMA VIANNA, 2001, p. 38)

Portanto, constitui-se apenas mais um meio de execução de delitos, assim como ocorre nos crimes já tipificados pela lei penal a saber: o estelionato, a ameaça, os crimes contra a honra, crimes eleitorais, favorecimento à prostituição, a veiculação de pornográfica infantil, o crime de violação ao direito autoral, entre outros.

Já os Delitos Informáticos Mistos, tem essa denominação por corresponderem a mescla de delitos de naturezas diferentes. Possuem uma maior complexidade e gravidade, visto que são condutas que infringem mais de um bem jurídico, associando a violabilidade dos dados e/ou sistemas com outras condutas típicas.

São as condutas em que a utilização de meios informáticos corresponde a condição necessária para a efetivação da conduta, embora não seja o principal bem jurídico lesado na ação. Assim, conceitua como “crimes complexos em que, além da proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico” (JESUS; MILAGRE, 2016, p. 54)

Alguns exemplos de delitos informáticos mistos são: o crime de acesso não autorizado a sistemas computacionais eleitorais, a transferência ilícita de valores intitulada de *homebaking* e, ainda, o crime de *salemislacing*, caracterizado pela retirada diária de pequenas quantias do saldo inúmeras de contas bancárias.

Há, ainda, a classificação dos Delitos Informáticos Mediatos ou lndiretos, em que pese a utilização do computador como meio para a obtenção de um fim específico diverso do campo virtual. De forma simplificada “trata-se do delito informático praticado para a ocorrência de um delito não informático consumado ao final.” (JESUS; MILAGRE, 2016, p. 54)

Neste sentido, o jurista e mestre Túlio Viana defende que o delito informático mediato não se relaciona e não se confunde com a classificação do delito impróprio. Uma vez que nos crimes mediatos há a lesão ao bem jurídico da inviolabilidade dos sistemas computacionais ainda que tal ofensa não seja a finalidade do transgressor, porém a invasão foi realizada e só não será punida em detrimento da aplicação do princípio da consunção. (LIMA VIANNA, 2001, p. 52)

Exemplificando dentro do direito informático mediato, comumente uma conduta informática é cometido como meio para a prática de um delito-fim de ordem patrimonial, em que o agente captura dados bancários e utiliza-os para desfalcar a

conta corrente da vítima, este só será punido pelo delito-fim, à saber o crime de furto. Destarte, pelo princípio da consunção que, como bem classificado por Cezar Roberto, “há consunção quando o fato previsto em determinada norma é compreendido em outra, mais abrangente, aplicando-se, somente esta.” (BITENCOURT, 2016, p. 256)

É fundamental destacar que, segundo os princípios da anterioridade e da legalidade, previsto no artigo 5º, XXXIX da Constituição Federal[7], e no artigo 1º do Código Penal[8], não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Essa é uma garantia constitucional do cidadão frente ao poder punitivo do Estado. Assim, para que uma ação ou omissão seja tida como crime, inclusive de caráter informático, é preciso que a norma seja anterior ao fato e que esta esteja prevista na legislação, ou seja, tipificada.

Embora tenham sido observados em outros países anteriormente, os crimes cibernéticos ganharam visibilidade maior no Brasil a partir de 1997, quando foram detectados a pratica dos crimes de racismo, clonagem de cartões de crédito, pedofilia, assédio. Colares elenca alguns crimes que podem ser cometidos no meio cibernético, tais como: calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, preconceito, discriminação por raça, dentre outros. (COLARES, 2002)

Em uma visão breve e geral essas são as principais classificações e as mais comuns dos delitos informáticos, há ainda classificação quanto aos sujeitos, bem como uma lista extensa dos mais variados crimes relacionados ao meio digital o qual excede o objetivo deste trabalho, assim seguiremos a análise acerca de uma das classificações dos crimes cibernéticos.

Tendo em vista a vasta possibilidade de delitos cometidos neste meio, o objetivo deste trabalho de pesquisa neste capítulo, importa analisar, preferencialmente, a conduta de Invasão de dispositivo informático, que alterou o

[7]Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;

[8]Art. 1º - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal.

Decreto-Lei nº 2.848 - Código Penal, para incluir o artigo 154-A através da Lei 12. 737 de 2012[9].

A inovação tecnológica trazida pela Internet e pelas redes sociais cuja popularização acarretou novos riscos para os usuários, ensejou a tipificação de um novo crime denominado Invasão de Dispositivo de Informática, acarretando o acréscimo de um novo artigo ao Código Penal, o art. 154 A, com a seguinte redação:

> "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."
> (BRASIL)

É interessante comentar que a legislação em destaque foi intitulada de "Lei Carolina Dieckmann", teve essa denominação popular depois de uma atriz da Rede Globo de televisão ter sido vítima de invasão indevida do seu sistema informático de natureza privada, na qual teve suas imagens íntimas divulgadas. O episódio

[9]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.

acelerou o andamento de projetos que já tramitavam no Congresso Nacional com o fito de regulamentar essas práticas invasivas perpetradas em meios informáticos.

A modificação legislativa decorreu da percepção da prática de novos ilícitos propiciados pela evolução da informática, os quais resultaram na invasão da privacidade alheia. No referido artigo fora criada o novo delito informático, que pode ser definido como o ingresso não autorizado de um usuário no sistema alheio, mesmo que este não tenha intenção de obter nenhum tipo de vantagem, podendo ou não se valer do uso de meios violentos ou ardilosos neste caso.

O dispositivo apresenta o que foi denominado de “invasão de dispositivos informáticos” e foi criado com o objetivo de assegurar a inviolabilidade dos segredos, ou seja, a inviolabilidade dos dados e arquivos dos aparelhos eletrônicos, além de proteger a integridade dos dados e a sua disponibilidade. Nesse tipo de crime, consistem em bens juridicamente protegidos a liberdade individual e o direito à intimidade, consubstanciados na proteção da inviolabilidade dos dados presentes no dispositivo de informática. (GRECO, 2017, p. 538)

Na legislação a referida conduta encontra-se inserida no capítulo que regula os crimes contra a liberdade individual (dos artigos 146 – 154, CP), na Seção IV – Dos Crimes contra a inviolabilidade dos Segredos (artigos 153 a 154 – B, CP). Além disso, é objeto de tutela desta conduta específica a vida privada e a intimidade, sendo consideradas garantias fundamentais e expressamente protegidas pela Constituição Federal Brasileira de 1988 em seu artigo 5º, inciso X.[10]

O verbo utilizado no núcleo do tipo penal é o verbo “invadir”, que significa devassar, ingressar sem autorização, penetrar. O verbo em destaque possui a conotação do acesso não autorizado em sistema informático alheio, por violação de mecanismos de segurança para a obtenção de arquivos ou programas do dispositivo informático alheio. Uma outra característica é a finalidade do agente em obter, adulterar ou destruir dados ou informações, podendo ainda, na oportunidade, instalar vulnerabilidades no sistema, tais como vírus ou programas invasores.

[10] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: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;

O artigo em comento enquadra quatro tipos de condutas típicas diferentes a depender de sua finalidade: a) invasão com o fim de obter dados ou informações; b) invasão com o fim de adulterar dados ou informações; c) invasão com o fim de destruir dados ou informações; d) invasão com o fim de instalar vulnerabilidades para obter vantagem ilícita. Assim, para a adequação do delito é necessário para o caso das três primeiras condutas que estas sejam efetivadas sem autorização do titular do dispositivo. (SYDOW; GOMES, 2015)

Quanto à conduta típica praticada com a finalidade de instalar vulnerabilidade para obtenção de vantagem ilícita, faz-se necessária que haja a invasão do dispositivo alheio por parte do sujeito ativo, em que através da violação de algum mecanismo de segurança o agente consiga instalar vulnerabilidade informática.

É relevante destacar que não exige o tipo penal que o dispositivo informático esteja conectado à rede mundial de computadores, mesmo que o dispositivo não esteja conectado à internet, o tipo penal pode ser enquadrado, uma vez que não está diretamente relacionado ao uso da rede e sim ao sistema informático como um todo, em que o intuito é proteger os dados e informações constantes dos dispositivos de informática.

Em se tratando do sujeito ativo, o eventual partícipe do crime incorre na mesma penalidade definida para o autor, conforme o parágrafo 1º do art. 154 A, acima citado. Com relação ao parágrafo 3º[11], onde aparece a qualificação do crime de invasão de dispositivo de informática, há uma explícita proteção dos direitos fundamentais à vida privada e à intimidade, assim estabelecidos no inciso XII do art. 5º da Constituição Federal de 1988[12], a qual dispõe ser inviolável o sigilo de dados: "É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (...)".

[11]Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:§ 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

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

No parágrafo 4º[13] do mesmo artigo, divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas acarreta no aumento da pena de um a dois terços. É, portanto, diferente quando o agente pretende apenas obter os dados e/ou informações e guarda-las para si, caso resolva transmitir os dados a outrem amplia-se o dano à privacidade e enseja a reprimenda mais gravosa. Foi a maneira que o legislador encontrou de demonstrar a reprovabilidade ampliada na conduta como causa especial de aumento o que normalmente seria um *post factum* não punível ou mero exaurimento delitivo.

Observa-se, que a discussão quanto aos delitos cibernéticos tem se ampliado não só entre os legisladores e os juristas, mas também na sociedade brasileira. É de extrema importância o desenvolvimento e difusão do tema a fim de encontrar soluções adequadas para as demandas enfrentadas neste âmbito. Não se justifica, apenas, na criação de legislações e na adequação do ordenamento penal brasileiro, isto se faz sim necessário, porém a questão está para aquém da tipificação e abrange também o comportamento da Justiça e dos Órgãos correlatos frente as buscas por entendimento e soluções viáveis social e antropologicamente na atual realidade brasileira.

Neste sentido, em 2016, a Câmara dos Deputados optou por instalar uma Comissão Parlamentar de Inquérito (CPI) destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade do País, onde conclui-se:

> "Conforme apurado por esta Comissão Parlamentar de Inquérito, a legislação brasileira ainda é muito incipiente no que diz respeito aos crimes cibernéticos.
> De fato, um dos únicos crimes que pode ser chamado de "crime cibernético próprio" previstos em nosso ordenamento jurídico é aquele inserido no art. 154-A do Código Penal pela Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann), comumente chamado de "invasão de dispositivo informático".
> Todavia, tal dispositivo foi elaborado de tal forma que diversas condutas que deveriam ser penalizadas não se encontram abrangidas pelo tipo penal. Para se ter uma ideia do absurdo, conforme afirmou a Dra. Fernanda

[13]Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: § 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (Incluído pela Lei nº 12.737, de 2012)

> Teixeira Souza Domingos, Procuradora do Ministério Público Federal, perante esta CPI, “a lei chama-se Lei Carolina Dieckmann, mas não abarcou a própria situação que a atriz sofreu, que foi a obtenção e exposição de dados pessoais privados”
> Dessa forma, não há dúvida que a legislação precisa ser aprimorada neste particular.”

Os dispositivos previstos no ordenamento jurídico brasileiro acerca dos crimes cibernéticos não se mostraram capazes de assegurar uma proteção efetiva aos usuários da Internet, na medida em que as normas não foram suficientemente eficazes para coibir as práticas danosas difundidas no mundo virtual, impondo a necessidade de estabelecer uma legislação especial e maior aprofundamento da temática.

Importante registrar que, considerando a exiguidade de tempo para a elaboração de um estudo mais aprofundado sobre os crimes cibernéticos, neste trabalho monográfico não se discorre com mais vagar sobre o tema, mesmo porque haveria o risco de ampliação excessiva do horizonte de pesquisa, podendo prejudicar a objetividade necessária.

4 **UMA ANÁLISE DA TIPICIDADE DO *CYBERSTALKING***

4.1 A DIFERENCIAÇÃO ENTRE A CONDUTA DE *STALKING* E *CYBERSTALKING* E A CONCEITUAÇÃO DA CONDUTA DE *CYBERSTALKING*

Inicialmente, é importante ressaltar que no presente trabalho de pesquisa optou-se por manter e utilizar o termo da conduta - objeto principal de estudo - em outro idioma, a língua inglesa, pois a sua tradução é complexa e exige uma dedicação especial. Não há no direito penal brasileiro uma equivalência adequada do termo, por ser uma conduta relativamente nova no contexto jurídico brasileiro, bem como uma tradução que retrate fielmente a palavra utilizada no idioma estrangeiro, pois ainda carece de estudos aprofundados sobre o tema e inclusive sobre a nomenclatura mais adequada para utilização no país.

Ao adentrarmos no foco da pesquisa é necessário que tenhamos um entendimento amplo da caracterização da conduta aqui em destaque, partindo do pressuposto de que o Direito Penal é guiado pelo princípio da taxatividade, é relevante o entendimento da conduta e sua conceituação clara para, posteriormente, nos debruçarmos sob a análise do tipo penal e suas características.

A relevância da definição do tipo penal está fundamentada em duas grandes vertentes, a primeira delas é a compreensão técnica da conduta no âmbito do Direito Penal, em que com uma definição adequada pautada no princípio da taxatividade podemos ampliar nossa compreensão de cada ponto abordado pela conduta. E a segunda justificativa guarda relação com a escassez de estudos sobre o tema, sendo ainda pouco abordado e explorado no país. O que resulta em uma ausência de definição concreta, possibilitando, de forma negativa, a interpretação e compreensão de formas diferentes dificultando ainda mais o amplo devido entendimento do tipo penal.

Em um primeiro olhar, há a correlação da conduta de *cyberstalking* à conduta de *stalking*, as nomenclaturas são similares e a associação é bem comum. Para que se entenda o *cyberstalking*, é interessante a busca da definição do *stalking* como base de entendimento e ponto de partida.

A definição do *stalking* ainda é bem divergente dentre os pesquisadores e especialistas na área, porém considera-se a forma de violência que ocorre mais comumente no âmbito de uma relação íntima.(FERREIRA, 2013, p. 18)

Uma das possíveis definições, considera o *stalking* como uma perseguição obsessiva, em que pode haver ou não um contato com a vítima, efetivada através de várias condutas de assédio e perseguição (telefonemas, envio de mensagens, monitoramento das atividades diárias, dentre outros).

O *stalking*trata-se de mais de um ato de perseguição não desejada dirigida à um indivíduo específico, é a ameaça ou assédio anormal que ocorre a longo prazo. É uma conduta complexa, difícil de investigar e identificar, e que envolve uma perseguição intencional, maliciosa e repetida, capaz de provocar medo na vítima. (MELOY, 1998, p. 23)

A expressão *"stalking"* deriva do verbo inglês *"to stalk"* que, numa tradução aproximada, significa perseguir algo ou alguém. Utilizada, inicialmente, para se referir ao predador que caça sua vítima de forma contínua e furtiva, sem ser visto ou ouvido. Outrora o conceito foi transposto para o mundo das relações humanas para traduzir a situação em que alguém (*stalker*), motivado por uma perturbação ou uma obsessão, observa e persegue outrem (vítima) de forma insistente e permanente. (LANÇA FERREIRA , 2016, p. 8)

Em uma tentativa branda de definição, é uma conduta que tem como característica a perturbação da vítima, em que através de qualquer meio de contato, vigia, persegue e assedia a vítima, fazendo-a sentir medo e insegurança, resultando na perda de sua tranquilidade, na violação da privacidade e temor de que um mal injusto ou grave ocorra.

Parte da doutrina entende como *stalking* a conduta *off-line* e o *cyberstalking* como sendo a conduta *online*. Desta forma, surge o questionamento acerca da natureza jurídica do tipo penal de *cyberstalking* - isto porque, muitos doutrinadores entendem que a conduta é uma mera espécie própria do delito de *stalking*, sendo dele derivado e diferenciando-se apenas pelo meio utilizado. Já uma outra parte dos juristas, entende que este é um delito autônomo, assim possui suas próprias características e sua definição específica.

Na compreensão do *cyberstalking* como um delito derivado tem-se os autores como: Marcelo Crespo, Alexandre Morais da Rosa, Damásio de Jesus, Luiz

Flávio Gomes. Já no entendimento da autonomia do tipo penal encontra-se os autores como Paul Bocij, Richard Jones e Spencer Toth Sydow.

Nesta linha de um delito autônomo, entende-se por *cyberstalking*:

> "um conjunto de comportamentos em que um indivíduo, grupo de indivíduos ou organização use de informação e tecnologia de comunicação para assediar outro indivíduo, grupo de indivíduos ou organização. Tal comportamento pode incluir, mas não está limitado a envio de ameaças e falsas acusações, usurpação de identidade, furto de dados, dano a dados ou equipamentos, monitoramento informático " (BOCIJ, 2004, p. 10)

A conduta de *cyberstalking* é extremamente complexa, pois ela é não é formada somente por uma ação isolada e específica. Pode ocorrer de diversas formas e atingir a vítima de maneiras diferentes. A figura do agente que pratica o *cyberstalking* - seja por vingança, admiração obsessiva, crença, interesse ou relação afetiva/íntima - busca conhecer todos os passos dados por sua vítima dentro do espaço virtual e a partir de tais informações agir para ameaçar, violar sua privacidade virtual, promover e disseminar o ódio contra sua vítima ou os familiares, destarte a possibilidade de condutas é infinita o que torna ainda mais difícil a identificação.

Enquanto o *stalker* – denominação dada àquele que realiza a conduta de *stalking* – encontra-se geograficamente próximo da sua vítima e a conhece, podendo assim, realizar as condutas de vigilância, perseguição, ameaça, amedrontamento, perturbação com envio de "presentes" e cartas, a pessoa que pratica o *cyberstalking* na grande maioria das vezes não conhece sua vítima e pode, inclusive, não se encontrar geograficamente próximo.

É possível que a conduta de *stalking* evolua para a de *cyberstalking*, utilizando-se do meio informático para ampliar suas ações, mas pode ser que isso nunca ocorra. Do mesmo modo, a pessoa que pratica a perseguição virtual passe a realiza-la, também, no ambiente da vida real observando e amedrontando sua vítima pessoalmente. (SYDOW; CASTRO, 2017, p. 122)

Para outros tipos de crimes, uma ação é suficiente para sua tipificação e reconhecimento. Entretanto, para que seja identificada a conduta de *stalking* e *cyberstalking*, a ações devem ser realizadas em repetição ou devem ocorrer em uma situação por um longo período de tempo. A ação - ou ações - realizada em repetição

é obrigatória para demonstrar o curso de conduta que envolve o agente e sua vítima. Desta forma, qualquer uma das ações, desde que sejam realizadas repetidas vezes e fizerem a vítima experienciar uma reação psicológica negativa à essas ações, constitui o crime. Com isso, a observância da repetição das ações é uma exigência para que seja configurado o crime e é um outro motivo pelo qual o *stalking* e o *cyberstalking* são tipos especiais de crime. (CHEYNE; GUGGISBERG, 2018, p. 5)

O jurista e especialista em Direito Penal Informático Spencer Sydow, defende a linha do *cyberstalking* como uma conduta autônoma e não derivada do delito de *stalking*, mesmo reconhecendo suas similaridades defende que a diferenciação não se encontra somente no meio pelo qual o agente realiza a conduta, pois há vários pontos de divergência entre eles. Os bem jurídicos tutelados, a questão da proximidade geográfica entre a vítima e seu agressor, a possibilidade de terceirização de ofensas e condutas, grau de prejuízo gerado e até a existência relacionamento entre os sujeitos. (SYDOW; CASTRO, 2017, p. 122)

O *cyberstalking* pode ser conceituado como a prática de várias ações - de forma reiterada - do agressor contra sua vítima utilizando-se dos meios informáticos com o intuito de monitorar e saber todas as informações da vítima, as movimentações e interações online de sua vítima, podendo assim, invadir seu sistema informático, ameaçar, usurpar sua identidade, promover o ódio contra outrem em nome vítima ou contra a própria vítima, difusão de falsas acusações e boatos, divulgar conteúdos pessoais da vítima, assediar, dentre outras várias condutas.

Enquanto dentro do crime *stalking* a vítima teme principalmente mais pela sua integridade física e sua liberdade de locomoção, dentro do *cyberstalking* o temor maior está direcionado a sua honra, imagem, confidencialidade dos seus dados e até a sua liberdade de manifestação livre de pensamento dentro do meio virtual, afetando perturbadoramente seu psicológico.

Até o ano de 2020, não havia um tipo penal específico para o *stalking* e *cyberstalking* dentro da realidade jurídica brasileira. Porém, neste ano de 2021 foi aprovado o Projeto de Lei que tratava do tema, sancionada para modificar o Código Penal e incluir o artigo tipificando o delito de *stalking*, bem como o de *cyberstalking* objeto desta pesquisa, em um próximo tópico analisaremos o tipo penal específico e sua classificação.

4.2 A LEI Nº 14.132 DE 2021 E A TIPIFICAÇÃO DA CONDUTA NO ORDENAMENTO JURÍDICO BRASILEIRO

Na doutrina brasileira tem-se poucas publicações que tratam do tema e o maior número está dedicado ao estudo da conduta de *stalking*, em que resulta numa sucinta abordagem do *cyberstalking*. Assim, o tema ainda é pouco explorado e o estudo direcionado especificamente o delito de *cyberstalking* com a análise e tentativa de definição do tipo é bem rara. Para o aprimoramento do tema de forma mais ampla e com boa base teórica as pesquisas predominantes são em línguas estrangeiras de países que há anos já estudam o delito, tais como: Estado Unidos, Austrália, Reino Unido, Portugal, entre outros. Esse é sem dúvidas, um fator limitante do acesso ao conteúdo e do incentivo aos novos pesquisadores das ciências criminais.

Destarte, há pontos positivos dentro do avanço, ainda que lento, das pesquisas acerca do tema na realidade jurídico-legal brasileira com a busca pela ampliação da discussão dos crimes cibernéticos e da espécie de *cyberstalking*. Com isso, surgiram movimentações e preocupações legislativas com o tema em questão, o que ensejou a criação de Projetos de Lei - PL, como a PL do Senado Federal n.º 236/2012[14], o qual traz uma mudança e um Novo Código Penal Brasileiro e, em destaque a PL n.º 1369/2019 que discutia a tipificação das condutas de *stalking* e *cyberstalking* - e que foi apensada àquele a PL n.º 5.419/2009. Assim, deu origem à Lei Ordinária 14.132/2021, na qual acrescenta o artigo 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal - para prever o crime de perseguição e, também, revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 - Lei das Contravenções Penais. Vejamos:

> "Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a

[14]Projeto de Lei do Senado n° 236, de 2012, de autoria do Senador José Sarney (MDB/AP) o qual institui a Reforma do Código Penal Brasileiro.

> capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.
> § 1º A pena é aumentada de metade se o crime é cometido:
> I – contra criança, adolescente ou idoso;
> II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código;
> III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.
> § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência.
> § 3º Somente se procede mediante representação."

A lei surge para modificar o Código Penal e acrescentar o artigo 147-A, tipificando, assim, a conduta de *stalking* e *cyberstalking* no Brasil, o qual foi intitulada de crime de perseguição. Conforme o tipo penal, os verbos trazidos foram "perseguir", "ameaçar", "restringir", "invadir" e "perturbar". Assim, o agente que ameaçar a integridade física ou psicológica da vítima; restringir-lhe a capacidade de locomoção; ou de qualquer forma, invadir ou perturbar sua esfera de liberdade ou privacidade - de forma reiterada - pratica o crime de perseguição, o *stalking*.

Nota-se que o artigo em destaque traz a expressão "por qualquer meio", na tentativa do legislador de associar o meio informático e telemático para a prática da conduta e assim, abarcar o crime de *cyberstalking*, tipificando-o também.

Todavia, ao analisar profundamente os termos utilizados no tipo penal verifica-se uma maior associação a ocorrência da conduta através do meio físico, isto porque, o verbo "perseguir" traz a ideia de ação presencial, bem como o emprego da expressão "restringindo-lhe a capacidade de locomoção", associando, deste modo, de forma mais clara à conduta de *stalking* e deixando dúbio o entendimento da aplicabilidade do referido artigo à conduta específica de *cyberstalking*.

Neste seguimento, defende: "o uso de palavras que podem gerar sentidos múltiplos pode servir como obstáculo à aplicação da norma para repressão de tais delitos. "(SYDOW; CASTRO, 2017, p. 148)

Um outro ponto significativo de verificação é quanto à expressão "ameaçando-lhe a integridade física ou psicológica". Pode-se dizer que a intenção do legislador foi a de trazer o grande impacto físico e psicológico que a conduta causa na vítima. A ideia de ameaça à integridade física parece cabível, entretanto,

quanto à existência de ameaça à integridade psicológica da vítima, revela uma fragilidade do tipo penal quanto ao seu entendimento. Uma vez que, quando há a ação de amedrontamento da vítima através da ameaça com terror e "jogos" psicológicos com o intuído de ameaçar-lhe a integridade psicológica, este já está de fato configurado – ou seja, a ameaça já configura o abalo psicológico resultando na dicotomia da expressão utilizada no tipo.

As legislações mundo afora têm combatido o fenómeno de várias formas. Alguns países optaram por criar leis que criminalizam autonomamente as condutas de *cyberstalking*. Outros preferem modificar a sua legislação *anti-stalking* de forma a abranger também o *stalking* online, integrando no conceito de perseguição o uso de qualquer forma de tecnologia. O legislador brasileiro optou por definir o conceito de *stalking* de forma ampla de modo a que possa abranger também o *cyberstalking*, entendendo que o primeiro deriva-se do segundo, com os mesmo bens jurídicos à serem tutelados diferenciando-se tão somente pelo meio praticado.

A lei sancionada revoga expressamente o artigo 65 da Lei das Contravenções Penais, o qual menciona: "Molestar alguém ou perturbar-lhe a tranquilidade, por acinte ou por motivo reprovável: Pena - prisão simples, de quinze dias a dois meses, ou multa, de duzentos mil réis a dois contos de réis". Tal artigo era utilizado como o tipo penal mais viável no ordenamento jurídico para suprir o vazio legal quando à perseguição/ assédio criminoso. Em outras circunstâncias, também poderia ser aplicado o crime de ameaça, previsto no artigo 147[15]., do Código Penal.

Nota-se, neste contexto, que a conduta de perseguição do *stalker* vai além de um simples molestar ou perturbar a tranquilidade da vítima, posto que sua conduta se perfaz de reiterados atos de perseguição e ameaça, o que denota a gravidade de sua ação.

O fenômeno jurídico penal que se relaciona ao artigo da contravenção penal acima descrita é a *novatio legis in pejus*, no qual refere-se como à lei nova – a Lei 14.132/2021 – sendo mais severa do que a anterior. Como no Direito Penal, admite-se a retroatividade da lei penal para benefício do réu – Princípio da Retroatividade da Lei Penal - as condutas anteriores à entrada em vigor da lei, que tipifica as

[15]Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:Pena - detenção, de um a seis meses, ou multa.

condutas de *stalking* e *cyberstalking*, ainda poderão caracterizar, a depender do caso concreto, a prática da Contravenção Penal prevista no artigo 65.

Uma parte dos doutrinadores defendiam a aplicação do referido artigo da Lei de Contravenções Penais para incriminar o delito de *stalking*, e este era utilizado para preencher a lacuna legislativa que havia. Porém, quanto ao delito de *cyberstalking* esse o artigo 65 da Lei de Contravenções Penais não se enquadrava, deixando a conduta sem um adequado enquadramento normativo.

Com a inclusão do artigo 147-A no Código Penal, há atualmente um enquadramento específico para os crimes de *stalking* e *cyberstalking*, em que o presente trabalho passa a analisar a sua classificação dentro do Direito Penal.

4.3 DA CLASSIFICAÇÃO DO TIPO PENAL

Inicialmente, é importante destacar que todo e qualquer indivíduo é titular de direitos e garantias fundamentais, que são resultado de uma constitucionalização dos direitos humanos positivados na Constituição da República Federativa do Brasil, no qual serve como objetivo e norte da ordem jurídica, devendo sendo respeitados por todos e, inclusive, pelo próprio Estado.

Cada tipo penal existente busca a proteção integral do bem jurídico violado pelo delito em espécie, uma garantia do Estado aos indivíduos que tiveram seus direitos e garantias lesados. O novo artigo encontra-se localizado no Código Penal dentro do Capítulo VI – dos crimes contra a liberdade individual, na Seção I – os crimes contra a liberdade pessoal. Portanto, o bem jurídico tutelado no delito em estudo é o da liberdade individual – que possui sentido amplo e extenso, mas é entendido como a o requisito essencial para se ter uma vida plenamente satisfatória, para que o indivíduo se desenvolva como pessoa e possa se expressar, pensar e agir livremente – entendida em sua completude pela natureza física e psíquica.

Registre-se, portanto, que a nova lei de incriminação do cyberstalking trouxe a pretensão do legislador de tutelar a esfera de liberdade individual da vítima. Pois, entendeu-se que “o ofendido, por passar a ter o seu modo de vida restringido por

atos alheios a sua vontade, provocados por outrem, fica mais disponível a sofrer o conhecido transtorno do pânico. ”[16]

Para que se entenda de fato qual bem jurídico é tutelado no delito aqui em discussão, é válida a observância da violação e consequências causadas à vítima. A habitualidade deste crime em espécie é uma de suas características mais fortes. Em que, o transgressor causa perturbação na vítima através das ações violadoras que decide tomar. Sejam elas, a comunicação através de e-mails, mensagens em aplicativos, envio de fotos, comentários em redes sociais, e tantas outras formas utilizando-se da tecnologia para atingir de várias maneiras a vítima.

O agente pode, portanto, querer atingir a vítima espalhando falsas afirmações sobre sua vida e/ou de seus familiares, incitando o ódio de outras pessoas, sejam elas conhecidas ou não, da vítima para que a atinjam. Divulgar fotos pessoais e tentar ridicularizar a vítima no cenário escolhido pelo agente, bem como perturbar, invadindo e monitorando seu espaço virtual e assim acessando a tudo que for pessoal da vítima. Como se observa as possibilidades de atingir a vítima são diversas.

O ciberespaço é caracterizado pela sua amplitude e infinidade, um mundo de possibilidade. Porém, com o crescente número de usuários nesse espaço, a mistura do mundo virtual com mundo real encorajou os usuários a usufruírem desse espaço e buscarem nele as semelhanças e as seguranças que buscam na realidade fora das telas. Assim, as ações tomadas pelas pessoas que utilizam do meio com consciência, se pautam na fidelidade e preservação dos seus direitos e garantias, onde buscam a segurança e a privacidade, por exemplo, que tanto valorizam em suas vidas e relações tangíveis.

Desta forma, como há a honra do indivíduo como um direito que não pode ser violado, há também a honra virtual deste indivíduo usuário da rede que também tem esse direito fundamental indisponível. O mesmo ocorre com a intimidade, a vida privada, a imagem e assim por diante, com todos os direitos e garantias fundamentais do homem. Neste sentido, a Constituição Federal prevê no seu artigo 5º, inciso X, a inviolabilidade da intimidade, da vida privada, da honra e da imagem dos indivíduos. Senão vejamos:

[16]Projeto de Lei n.º 5.419-A, DE 2009

> “Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> 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)

Além de proteção constitucional, a honra e a dignidade são protegidas pela Declaração Americana dos Direitos e Deveres do Homem – Pacto San José da Costa Rica – e pela Declaração Universal de Direitos Humanos, nos seus artigos 11 e 12, respectivamente:

> Artigo 11 - Proteção da honra e da dignidade
> 1. Toda pessoa tem direito ao respeito da sua honra e ao reconhecimento de sua dignidade.
> 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
> 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.
>
> Artigo 12
> Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

Neste escopo, não é razoável concluir que em uma conduta tão complexa como esta, marcada por um impacto significativo na integridade psíquica e física da vítima – quando se tratar de *stalking* – sejam associadas entre si e tratadas dentro do ordenamento jurídico como se violassem os mesmos bens jurídicos.

Ora, quando cometido tal delito este atinge a vítima de forma muito intensa e significativa, em que a pessoa violada passa a permanecer em estado de alerta constante e pavor. Posteriormente, a pessoa atingida deixa de se deslocar livremente, de se expressar publicamente, de se manifestar e utilizar as redes sociais e os recursos informáticos, rompe relacionamentos afetivos ou até relacionamentos num geral devido ao medo desenvolvido. (SYDOW; CASTRO, 2017, p. 136)

> “Diante disso tudo, é correto afirmar que o bem jurídico nos delitos de *stalking* e *cyberstalking* são da modalidade complexa e resultam da soma da violação de intimidade, privacidade, integridade psíquica, liberdade e honra, estendendo-se, por vezes, a ofensas ao patrimônio, à integridade física e à vida. Daí porque, em face da complexidade, são delitos de expressiva gravidade. ”(SYDOW; CASTRO, 2017, p. 140)

Quanto à autoria, trata-se de um delito comum, o que significa que pode ser praticado por qualquer pessoa, homem ou mulher. Por ser um crime cometido através da utilização de tecnologias e do sistema informático como um todo, resta uma grande dificuldade de investigação e identificação do transgressor, que muitas vezes nem conhece pessoalmente sua vítima, mas sabe cada passo dela e assim, utiliza-se de ferramentas para burlar sua identificação através da facilidade do anonimato do mundo virtual.

No Brasil, há a conhecida Lei Maria da Penha – Lei 11.340 de 2006[17]- a qual cria mecanismos para coibir a violência doméstica e familiar contra a mulher. Recentemente no país uma decisão do Tribunal de Justiça de Minas Gerais[18], através de decisão monocrática, reconheceu a aplicação por analogia da Lei Maria da Penha para o caso de adoção de medida protetiva para a mulher vítima da conduta de *cyberstalking*. Apesar de não ser o objeto de estudo deste trabalho debruçar-se sob a análise de ocorrência do crime de *cyberstalking* contra mulheres - entende-se que há uma grande possibilidade de ocorrência deste crime tendo como vítima as mulheres, em razão de grandes números de violência contra o gênero no país.

Uma das características de maior relevância do crime em estudo é a reiteração de condutas, quanto à consumação trata-se de crime habitual e não admite a forma tentada. Com isso, a habitualidade de ações do agente contra sua vítima é o que vai caracterizar a consumação do delito, pois quanto aos crimes habituais, não se admite a tentativa porque a consumação exige reiteração de atos. Uma ação isolada do transgressor, não irá configurar o crime aqui estudado, uma

[17]LEI Nº 11.340, DE 7 DE AGOSTO DE 2006. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher, nos termos do § 8º do art. 226 da Constituição Federal, da Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres e da Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher.

[18]Agravo de instrumento. 14ª Câmara Cível do TJMG. O caso, que tramita sob segredo de justiça, ocorreu em Pato de Minas, em Minas Gerais (MG). Decisão disponível em: https://bernardodeazevedo.com/conteudos/decisao-judicial-concede-medida-protetiva-a-mulher-vitima-de-cyberstalking/. Acesso em: 5.jun.2021

vez que necessita um conjunto de ações. Assim, ou ocorre reiteração e o crime se consuma, ou fato será atípico.

Outro ponto que merece relevância quanto esta conduta é a classificação do delito admitido na sua forma como crime comissivo ou comissivo por omissão. Na classificação do crime comissivo o transgressor pratica direta ou indiretamente a conduta, como por exemplo a ação de envio de mensagem, de publicação difamatória, de assédio, entre outras. Quanto à classificação como delito comissivo por omissão, entende-se quando o usuário permite de forma irresponsável a publicação da informação indevida na sua rede. No caso, quando um usuário permite a publicação de informações da vítima no site de seu domínio.

É válido reiterar que o delito é classificado pela sua habitualidade, com a junção de ações pelo transgressor contra sua vítima o que necessita de uma análise em um contexto de análise amplificada com relação as violações causadas, assim defende: “É preciso, assim, a análise do contexto, vez que tais práticas constituem comportamento reiterado que tem sua maior reprovabilidade exatamente por conta da repetição inerente e pelo dano gerado em tais circunstâncias. ” (SYDOW; CASTRO, 2017, p. 160)

Como visto anteriormente, a conduta objeto de estudo pode ser apenas um crime-meio, ou seja, o crime no qual o transgressor comete para obter as informações sobre a sua vítima e atingir sua integridade psíquica, sua privacidade e outros, para posteriormente, agir para realizar uma outra conduta como a de lesão corporal, estupro ou homicídio.

5 **CONCLUSÃO**

O desenvolvimento deste estudo teve por escopo os avanços tecnológicos e a sua relação com o Direito, com destaque para o crime de *cyberstalking*, considerando os estudos doutrinários acerca do tema para a adequada definição da conduta e sua classificação no Direito Penal, com a análise da legislação brasileira atual. Com efeito, inúmeras são as notícias veiculadas hoje em dia o qual impacta grandemente a sociedade atual, causando a violação de privacidade, divulgação de fatos da intimidade alheia, ofensa à honra, à dignidade das pessoas, acarretando dano, constrangimento, dor e sofrimento por vezes insuportáveis.

Nasceu dessa constatação o interesse em conhecer mais profundamente a relação da tecnologia, internet e Direito e, assim, o surgimento, definição e classificação dos crimes cibernéticos, com breve vista ao crime de invasão a dispositivo informático. E, posteriormente, como objeto principal de estudo a análise do crime cibernético específico – o *cyberstalking*. Dessa perspectiva buscou-se perquirir a legislação em vigor no Brasil que dispõe desse delito específico analisando se houve um adequado enquadramento da conduta na referida legislação.

Para tanto se fez necessário um estudo do surgimento da Internet com o intuito de aprofundar o conhecimento da moderna tecnologia da informação, desde sua origem até os dias atuais, considerando a dinâmica inerente às técnicas de comunicação virtual decorrentes.

Nessa evolução continuada, a Internet possibilitou a construção dos fundamentos tecnológicos para o que hoje se conhece Era da Informação, cuja forma organizacional se concretiza na rede, ferramenta que se instalou e cresceu em todos os campos da sociedade. Assim, de uma maneira generalizada, as atividades humanas, quer econômicas, quer políticas, quer sociais, ou culturais, passaram a se estruturar em redes de computadores, no “espaço” denominado de ciberespaço.

Uma das consequências mais relevantes da Internet vai ser identificada na oportunidade de criação das redes sociais, dentre as quais se destacaram o Orkut, o *Facebook*, *Instagram,* o *Twiter*, possibilitando o compartilhamento de informações as mais variadas, além de vídeos, imagens e arquivo de áudio. No entanto, o que se

constatou foi que a mesma tecnologia que permitia a divulgação de informações de interesse para a sociedade, também foi eventualmente utilizada para difamar, promover apologia a crimes, violar a intimidade de terceiros, agredir direitos humanos.

Os direitos e garantias fundamentais devem ser protegidos e valorizados, também, no ciberespaço. Desta maneira, o Direito Penal visa a proteção dos bens jurídicos contemplados pela Carta Magna, o qual deve propiciar a sociedade a proteção tanto na vida real quanto na virtual.

Com efeito, este conjunto de normas e diretrizes, relacionados aos crimes cibernéticos, cuja essência tem como finalidade a tutela do uso seguro e saudável da internet, permite a conclusão de que os poderes constituídos têm voltado maior atenção ao ambiente virtual de comunicação e interação social no Brasil, seus avanços e consequências dentro do ordenamento jurídico mesmo ante o crescente número de episódios envolvendo o mau uso da ferramenta. Se é fato que o ambiente virtual de comunicação e interação social é vulnerável e frágil, face a multiplicidade de possibilidades de seu uso, também não se pode ignorar os esforços de ampliar a discussão nacional acerca do tema, mesmo que ainda em passos lentos. Com isso busca-se uma harmonia com a sociedade civil, provedores, plataformas e redes sociais no sentido de tornar o uso da internet seguro, eficaz e útil ao cotidiano das pessoas, à feição do quanto explorado ao longo dos capítulos que compõem a presente pesquisa.

Neste sentido, considerando toda a análise desenvolvida no decorrer deste trabalho, considera-se que a legislação referente à conduta de *cyberstalking* carece de elementos mais precisos para que haja uma melhor definição e entendimento do tipo penal. Bem como, uma distinção do crime o qual normalmente é associado: o crime de *stalking*. Assim, um tipo penal mais consistente e sem aberturas para dubiedades pode ser eficientemente interpretada e posta em prática de maneira adequada, assegurando, com isso a proteção jurídica no ambiente virtual das vítimas desse crime específico. Adota-se, assim, o posicionamento de estudiosos do tema que entendem que não houve um enquadramento e definição adequados da conduta podendo haver dubiedade de interpretação e espaço para insegurança jurídico-penal. Considera-se que a criação da referida norma já é um avanço frente à proteção dos bens jurídicos que são violados, porém ainda necessita da utilização

de elementos e termos mais adequados para trazer uma interpretação mais consistente.

REFERÊNCIAS

BECKERT TRINKEL, Gustavo. **Crimes Cibernéticos**: Confinando uma Conduta de Repercussões Globais. Curitiba, 2010. Monografia (Direito) - Universidade Federal do Paraná, Curitiba.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal - Parte Geral**. 22ª. ed. São Paulo: Saraiva Educação S.A., v. 1, 2016.

BOCIJ, Paul. **Cyberstalking**: Harassment in the Internet Age and how to Protect Your Family. Londres: PRAEGER, 2004.

BRASIL. **Constituição**. República Federativa do Brasil de 1988. Brasília: Senado Federal, 1988.

BRASIL. Código Penal Brasileiro.

CASTELLS, Manuel. **A Galáxia da Internet**. Oxford: Oxford University Press, 2003.

CASTELLS, Manuel. **O Poder da Comunicação**. São Paulo: Paz e Terra, 2009.

CHEYNE, Nicola ; GUGGISBERG, Marika. **STALKING**: an age old problem with new expressions in the digital age. Hauppage, NY, 2018. Disponível em: <https://www.researchgate.net/publication/324246586_Stalking_An_age_old_problem_with_new_expressions_in_the_digital_age>. Acesso em: 25 mai. 2021.

COLARES, Rodrigo Guimarães. **Cybercrimes**: os crimes na era da informática. 2002. Disponível em: BuscaLegis.ccj.ufcs.Br. Acesso em: 23 mai. 2021.

FERREIRA, Joana . **Stalking como forma de violência nas relações de namoro**. 2013. Dissertação (de mestrado) - Instituto Superior de Ciência da Saúde Egas Moniz.

FILHO, Adalberto Simão; LUCCA, Newton de. **Direito & internet**: aspectos jurídicos relevantes. Quartier Latin, 2016.

FRAGOMENI, Ana Helena. **Dicionário enciclopédico de informática**. Rio de Janeiro: Campus, 1987.

GIBSON, William. **Neuromancer**. Nova Iorque: Ace Books, v. 2, 1984.

GOVERNO FEDERAL, Secretaria-Geral. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**. **Gov.br**. Disponível em: <https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica>. Acesso em: 10 mai. 2021.

GRECO, Rogério. **Código Penal Comentado**. Niterói: Impetus, 2017.

JESUS, Damásio de; MILAGRE, José Antônio M. . **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

KELSEN, Hans. **Teoria pura do Direito**. 6ª. ed. São Paulo: Martins Fontes, 1999. Tradução de: João Baptista Machado.

LANÇA FERREIRA , Bruno Filipe Dias. **Stalking**: Um novo crime para um velho comportamento. Lisboa, 2016. Tese (Faculdade de Direito) - Universidade Católica Portuguesa.

LEONARDI, Marcel. **Fundamentos De Direito Digital**. São Paulo : Revista dos Tribunais, 2019.

LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2011.

LIMA VIANNA, Túlio. **Do Acesso Não Autorizado à Sistemas Computacionais**: Fundamentos de Direito Penal Informático. Belo Horizonte, 2001. Dissertação (Faculdade de Direito) - Universidade Federal de Minas Gerais.

MARTINO, LUIS MAURO SA. **Teoria das Mídias Digitais**: Linguagens, ambientes e redes. Petrópolis: Vozes, 2014.

MELOY, J. Reid. **The Psychology of Stalking**: Clinical and Forensic Perspectives. San Diego: Academic Press, 1998.

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

REINALDO FILHO, Demócrito Reinaldo. **A Internet e o Obsoletismo das Leis**. **E-gov**. 2011. Disponível em: <https://egov.ufsc.br/portal/conteudo/internet-e-o-obsoletismo-das-leis>. Acesso em: 3 mai. 2021.

ROQUE, Sérgio Marcos. **Criminalidade informática**: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007.

ROSA, Fabrízio. **Crimes de informática**. 2005.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SCHMIDT, Guilherme. **Crimes cibernéticos**. **Jusbrasil**. 2014. Disponível em: <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em: 7 mai. 2021.

SENNA , Felipe; FERRARI, Daniella. **Convenção de Budapeste e crimes cibernéticos no Brasil**. **Migalhas**. 2020. Disponível em: <https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil>. Acesso em: 18 mai. 2021.

SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo de. **Stalking e cyberstalking**: obsessão, internet, amedrontamento. Belo Horizonte: Editora D'Plácido, 2017.

SYDOW, Spencer Toth; GOMES, LUIZ FLAVIO. **Crimes informáticos e suas vítimas**. 2ª. ed. 2015.