PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO , NEGÓCIOS E COMUNICAÇÃO

DANIEL BARBOSA DIAS

CONDUTAS CRIMINOSAS ATRAVÉS DO *CYBERESPAÇO*:
EVOLUÇÃO, CONSEQUÊNCIAS, IMPUNIDADE E ANÁLISE DE LEGISLAÇÃO VIGENTE

GOIÂNIA - GO
2022

DANIEL BARBOSA DIAS

CONDUTAS CRIMINOSAS ATRAVÉS DO *CYBERESPAÇO*:

EVOLUÇÃO, CONSEQUÊNCIAS, IMPUNIDADE E ANÁLISE DE LEGISLAÇÃO VIGENTE

Monografia Jurídica apresentada à Escola de Direito e Relações Internacionais da Pontifícia Universidade Católica de Goiás como requisito parcial para obtenção do título de graduação em direito.

Orientador: Prof. Dr. Gil César Costa de Paula.

GOIÂNIA - GO
2022

DANIEL BARBOSA DIAS

CONDUTAS CRIMINOSAS ATRAVÉS DO *CYBERESPAÇO*:
EVOLUÇÃO, CONSEQUÊNCIAS, IMPUNIDADE E ANÁLISE DE LEGISLAÇÃO VIGENTE

Data de defesa: 19/05/2022

BANCA EXAMINADORA

_____
Orientador: Prof. Dr. Gil César Costa de Paula.
Pontifícia Universidade Católica de Goiás

_____
Examinador Convidado: Prof. Dr. Marcelo Di Rezende
Pontifícia Universidade Católica de Goiás

GOIÂNIA – GO
2022

AGRADECIMENTOS

Mais um ciclo se encerra, e hoje olhando para trás vejo quantas pessoas me apoiaram desde o início desta trajetória. Quando tracei essa jornada me vi amparado por Deus, que de uma forma ou de outra me mostrava qual caminho seguir e me munia com muita força para que eu nunca desistisse. A ele, primeiramente, agradeço.

Devo inteiramente aos meus pais e irmãos que sempre me incentivaram, me apoiaram, e até mesmo se abdicaram de alguns sonhos seus para que eu pudesse vir a realizar o meu. Ensinaram-me que com fé, foco, disciplina e persistência, eu poderei alcançar objetivos inimagináveis.

A todos os professores do curso de Direito da Pontifícia Universidade Católica de Goiás, e em especial ao professor orientador Me. Gil César Costa de Paula por toda sabedoria, vivências e conhecimentos compartilhados que me permitiram um melhor desempenho em minha formação profissional.

Não poderia deixar de agradecer aos meus amigos que me encorajaram e que sempre falavam que eu seria capaz de conquistar tudo que venho conquistando. Estes estavam ao meu lado com muita lealdade, companheirismo e palavras de incentivos.

Obrigados à todos que participaram, direta ou indiretamente, durante todos esses anos de Graduação e fizeram com que eu crescesse não só como pessoa mas como formando e futuro operador do Direito: Matheus do Carmo, Mateus Borges, Renato Alexandre, Kássia Carvalho, Daniela Paim e Ricardo Freitas.

DEDICATÓRIA

Este trabalho é dedicado primeiramente ao papai do céu que sempre me abençoou, e às pessoas que sempre me deram apoio e base para persistir nesse caminho: aos meus pais socioafetivos Geraldo e Elizabeth, à minha mãe biológica Andréia, e aos meus irmãos Danillo, Iohanna, Kamilla e Ana Luiza.

RESUMO

O espaço virtual trouxe consigo mudança de paradigmas e de culturas, além de intensificar e impulsionar as relações humanas. Porém, os ataques à esfera de privacidade são cada vez mais recorrentes. O ciberespaço possibilitou novos tipos de ataques, que saem da esfera de violências físicas e passam agora para as violências psicológicas e patrimoniais. Dessa forma, este trabalho objetivou analisar como os crimes cibernéticos causam impactos sociais (financeiros e psíquicos), e quais medidas são e devem ser levantadas pela legislação. Para o alcance do objetivo geral, foram elencados os seguintes objetivos específicos: descrever acerca da evolução dos crimes virtuais, seus conceitos, modos operantes e seu histórico; apresentar as consequências geradas nas vítimas de ataques cibernéticos; e discorrer sobre as espécies, a legislação acerca dos crimes cibernéticos, como a Lei n° 12.737/12, e os principais problemas enfrentados para identificar e punir os criminosos. Trata-se de um estudo de abordagem dedutiva. Quanto ao método de procedimento utilizou-se o histórico e quanto aos objetivos a pesquisa é do tipo exploratória, realizada por meio da busca de artigos científicos, em inglês e em português. O presente estudo foi baseado na doutrina, na lei, em artigos e na interpretação do texto constitucional que assegura garantias e direitos fundamentais balizares do Estado Democrático de Direito. Em decorrência da evolução tecnológica e a crescente expansão da utilização da internet no Brasil e no mundo, tornou-se fundamental a criação de leis especificas que tratam da referida temática em pauta, vindo a tipificar novas condutas delitivas provenientes da fomentação da internet. A exemplo disso, a criação da Lei n° 12.737/12 (Lei Carolina Dieckmann), que modificou a norma penal trazendo várias inovações legislativas em relação a punibilidade mediante os crimes *cybernéticos.* O estabelecimento de direitos e deveres cibernéticos, ainda que tardio, é importante para o combate aos crimes virtuais, visto que é por meio dessas normas que pode ser visualizado com mais facilidade o que está sendo violado, estabelecendo assim as condutas ilícitas. O conhecimento dos fatos e das tendências é crítico para os esforços de prevenção do crime e da proteção de dados públicos e privados.

Palavras-chave: Crimes de ódio. Crimes virtuais. Lei Carolina Dieckmann. Marco Civil da Internet.

ABSTRACT

The virtual space has brought with it a change of paradigms and cultures, in addition to intensifying and boosting human relationships. However, attacks on the sphere of privacy are increasingly recurrent. Cyberspace has made possible new types of attacks, which leave the sphere of physical violence and now move to psychological and property violence. Thus, this work aimed to analyze how cyber crimes cause social impacts (financial and psychological), and what measures are and should be raised by legislation. In order to reach the general objective, the following specific objectives were listed: describe about the evolution of virtual crimes, their concepts, operating modes and their history; present the consequences generated in the victims of cyber attacks; and discuss the species, the legislation on cyber crimes, such as Law No. 12,737/12, and the main problems faced in identifying and punishing criminals. This is a deductive approach study. As for the method of procedure, the history was used and as for the objectives, the research is of the exploratory type, carried out through the search of scientific articles, in English and in Portuguese. The present study was based on doctrine, law, articles and the interpretation of the constitutional text that guarantees guarantees and fundamental rights that are the cornerstones of the Democratic State of Law. As a result of technological developments and the growing expansion of the use of the internet in Brazil and in the world, it has become essential to create specific laws that deal with the aforementioned theme in question, coming to typify new criminal behaviors arising from the promotion of the internet. As an example, the creation of Law No. 12,737/12 (Carolina Dieckmann Law), which modified the criminal law, bringing several legislative innovations in relation to punishment for cyber crimes. The establishment of cybernetic rights and duties, even if late, is important for the fight against cybercrimes, since it is through these rules that what is being violated can be more easily visualized, thus establishing unlawful conduct. Knowledge of facts and trends is critical to crime prevention efforts and the protection of public and private data.

***Keywords*:** Hate crimes. Virtual crimes. Carolina Dieckmann Law. Civil Rights Framework for the Internet.

SUMÁRIO

1 INTRODUÇÃO

A humanidade imerge em avanços tecnológicos e se inova cada vez mais nas formas de comunicação e de divulgação de informações. A internet, por exemplo, trouxe consigo várias facilitações e benefícios para a humanidade, como realizar compras virtuais no conforto de sua casa, conversar com pessoas que estão distantes geograficamente através de aplicativos como Facetime, WhatsApp, Instagram, dentre outros. Porém, os riscos dessas facilitades existem e podem causar grandes prejuízos aos envolvidos.

Os crimes cibernéticos são uma realidade e vem atacando a honra, a imagem, intimidade e a vida privada das pessoas, além de gerar consequências financeiras a particulares e ao Estado com suas políticas públicas. Com o dinamismo da tecnologia de informações, muitas dificuldades são enfrentadas pelos investigadores no processo de averiguação dos crimes cibernéticos. Desta forma, com os desafios enfrentados pela polícia investigativa, muitas soluções são procuradas, como por exemplo, a criação de leis específicas que poderão acompanhar de forma satisfatória o desenvolvimento da tecnologia, onde limitarão novas ameaças nos crimes virtuais.

Na atualidade, qualquer individuo com mínimo de conhecimento tecnológico pode ter a capacidade de cometer atos ilícitos por meio de computadores, *smartphones*, *tablets*, dentre outros aparelhos eletrônicos que podem ser utilizados para esse fim. Contudo, caso o individuo compreendesse que esses crimes podem gerar punição, possivelmente ocorreria a diminuição nos crimes cibernéticos.

Devido ao fato de o crime informático ter a ausência física do agente criminoso, realizar a localização do agente se torna uma tarefa difícil, sendo necessário traçar algumas estratégicas com grupos de pessoas capacitadas para possam ajudar na identificação do criminoso. Nesse caso, geralmente as equipes se utilizam na fase investigativa de um sistema de “busca sistemática”. Trata-se de uma investigação preventiva, onde depende apenas da iniciativa da autoridade responsável pela condução do procedimento, no entanto, existe uma grande ocorrência de crimes cibernéticos, o que resulta numa lentidão dos processos investigativos.

Os crimes cibernéticos, envolvendo a honra da vítima, pode ocorrer por meio de danos psicológicos resultantes da divulgação de fotos íntimas, por exemplo, que faz parte da proposta do presente estudo, a qual resulta da necessidade de avaliar alguns direitos básicos da pessoa, para que esse tipo crime cybernético, e outros, não ocorram sem a devida punição do criminoso.

No primeiro capítulo partiu-se do cais velejando sobre os fatores históricos e culturais, fazendo nossa parada na era da globalização e pós-modernidade. Durante o percurso é analisado o ponto de vista de doutrinadores sobre a história da internet, o surgimento dos crimes virtuais, conceitos e etc. O capítulo 2 faz uma análise densa e específica sobre os crimes cibernéticos: classificação, tipos de crimes, programas utilizados na prática, autoria e competência para julgá-los. O terceiro capítulo é destinado às consequências geradas pelos criminosos virtuais. O quarto capítulo traz o aspecto jurídico como meio para fazer punir, com o intuito de cessar ou diminuir os crimes cometidos virtualmente.

Dessa forma, este trabalho objetiva estudar os principais tipos de crimes cybernéticos, analisando o seu desenvolvimento e como podem atingir a sociedade. Para o alcance do objetivo geral, foram elencados os seguintes objetivos específicos: descrever acerca da evolução dos crimes virtuais, seus conceitos, modos operantes e seu histórico; apresentar as consequências geradas nas vítimas de ataques cibernéticos; e discorrer sobre as espécies, a legislação acerca dos crimes cibernéticos, como a Lei n° 12.737/12, e os principais problemas enfrentados para identificar e punir os criminosos.

A metodologia a ser utilizada na elaboração desta pesquisa, envolveu o método dedutivo, bem como a pesquisa exploratória, realizada por meio da busca de artigos científicos, em inglês e em português. O método dedutivo é um julgamento empregado em distintas áreas e está relacionado com as diversas formas de discorrer sobre determinados assuntos. É um procedimento de exame de informações que induz a uma terminação e utiliza-se da dedução para descobrir sua implicação final. Neste sentido, aproxima-se de uma conclusão por meio das premissas.

2 HISTÓRIA DA INTERNET

A Internet não nasceu como uma rede pública de computadores projetada para atividades diárias das pessoas. Surgiu em 1959 como um projeto da Departamento de Defesa para Comunicações Militares dos Estados Unidos e acadêmicos daquele país. Seu objetivo era criar um meio de comunicação descentralizado que permitiria o fluxo constante de informações sobre aquele território. Com base nas técnicas de dispersão utilizadas pela guerrilha, a ideia era projetar um meio infalível de comunicação antes da hipótese de que uma bomba de energia nuclear colapsaria as telecomunicações em uma parte do território Norte-americano (ALMEIDA ,2005).

A história da Internet começa durante a fase de desenvolvimento da *Big Science* Americana dos anos 50, no marco da batalha tecnológica travada entre o governo dos Estados Unidos e da União Soviética durante a Guerra Fria. Após o lançamento do satélite Sputnik em 1957 pela administração União Soviética, o presidente americano Dwight Einsenhower ordenou que a criação do Departamento de Defesa de uma agência de investigação avançada realizar estudos sobre materiais de guerra e comunicações (LEINER et al., 1997).

Após a criação da ARPA (Agência de Projetos de Pesquisa Avançada, Agência de Pesquisa de Projetos Avançados), Jack Licklider, pesquisador do Instituto de Tecnologia de Massachusetts (MIT), foi colocado à frente do organismo com a missão para melhorar o uso da tecnologia do exército, criando uma rede de computadores militares. Publicando um trabalho sobre a *Galactic Rede* (Rede Galáctica), chamou a atenção das autoridades de defesa, que queriam ter um meio de comunicação flexível que permitisse o fluxo comunicações ininterruptas em todo o território norte-americano em face de um possível ataque nuclear soviético (LEINER et al., 1997).

Em 1965, outro cientista do MIT, Lawrence Roberts, conectou um computador em Massachusetts com outro na Califórnia por meio de uma linha telefônica comutada de baixa velocidade, dando origem à primeira rede de computadores de longa distância. Foi baseado em uma tecnologia de transmissão revolucionária de telecomunicações, tecnologia de comutação de pacotes, onde a troca de fluxos de dados foi realizada através de pacotes de informação em vez de circuitos. Em 1966, Roberts foi contratado pela ARPA e apresentou no ano seguinte o projeto de criação

da ARPANET - a rede ARPA-, às autoridades do Departamento de Defesa. Em 1969 começaram os primeiros testes para a conexão de computadores na rede militar (LEINER et al., 1997).

O primeiro nó ARPANET foi o computador central do Centro de Medições de Rede da Universidade da Califórnia. A ligação foi feita com o Instituto de Investigação de Stanford, de onde a primeira mensagem foi enviada para aquele destino. Em outubro de 1972, a rede militar foi apresentada no *International Computer Communicatios Conference* (Conferência Internacional de Computer Communications) desenvolvido nos Estados Unidos (GOETHALS; AGUIAR; ALMEIDA, 2000).

Um conceito-chave que motivou o desenvolvimento da rede foi o de *internetworking*. Para seus criadores, a arquitetura de rede aberta da ARPANET permitiria no futuro a fusão com outras redes - satélite e rádio, para exemplo- para a troca de recursos e informações. Através do conceito de *internetworking* (*networking*), redes individuais podem ser criadas e desenvolvido de forma independente para se tornar parte de uma rede mãe projetando um protocolo de comunicação padrão (LEINER et al., 1997).

Em julho de 1972, Lawrence Roberts expandiu sua utilidade ao escrever o primeiro programa utilitário de e-mail para listar, ler, arquivar, encaminhar e responder seletivamente às mensagens. A partir daí, o e-mail decolou como a maior rede aplicação há mais de uma década. Esse foi um prenúncio do tipo de atividade que vemos na *World Wide Web* hoje, ou seja, o enorme crescimento de todos os tipos de tráfego “pessoa a pessoa” (LEINER et al., 1997).

Contudo, mesmo com os benefícios que os computadores e o acesso à internet proporcional à sociedade, surgiram crimes com agentes detentores de conhecimentos tecnológicos por meio da internet. Tais crimes são denominados crimes virtuais, digitais, informáticos, cibernéticos, dentre outras nomenclaturas (ASSUNÇÃO, 2018).

2.1 CRIMES CIBERNÉTICOS

Para Assunção, as espécies de crimes cibernéticos ou crimes virtuais referem-se a:

> Crimes de ódio em geral (contra a honra, sentimento religioso, bullyng), crimes de invasão de privacidade e intimidade (que pode ou não incorrer em uma nova conduta lesiva contra a honra), crimes de estelionato, crimes de pedofilia, entre outros (ASSUNÇÃO, 2018, p. 11).

Como também relata a psicossocial do Safernet, Juliana Cunha, ter a intimidade exposta, por exemplo, é razão para inúmeros danos: “Geralmente as vítimas sofrem com muitos transtornos, mentais, físicos e psicológicos”, como depressão, medo, distúrbios e até mesmo pode ser levadas a cometerem suicídio. Portanto, é de suma importância a discussão acerca da temática proposta no presente estudo.

2.1.1 Conceitos

O tráfego diário na internet vem aumentando consideravelmente dia após dia, milheres de usários acessam vários sites para consumir algum serviço ou produto que as empresas digitais oferecem atualmente. Contudo, existem malefícios nessa rede e o ecossistema digital é altamente vulnerável a ataques de criminosos digitais que colocam em risco a segurança dos usuários que podem ser danificados em sua propriedade ou em sua pessoa.

Com isso, é importante que haja um sistema jurídico atualizado como forma de proteção efetiva aos usuários e contra qualquer comportamento criminoso típico desse ambiente tecnológico. Nesse sentido, Nucce (2010, p. 34) esclarece que:

> Estamos em um momento de transição em que as relações humanas se tornam cada vez mais interativas através dos dispositivos moveis de comunicação, porém, estamos nos tornando cada vez mais vulneráveis aos ataques a nossa esfera de privacidade.

Se tratando da ciência jurífica, o crime é um objeto de estudo importante no seu objetivo de gerar conhecimento para sua aplicação em prol do bem-estar da população no geral. A segurança da pessoa física ou jurídica é fundamental para manter a paz e a ordem que favoreçam o desenvolvimento comunitário.

Primeiramente, é necessário realizar uma sepração entre as condutas ilícitas realizadas no espaço físico e as do mundo virtual. Dessa forma, Inellas (2004, p. 3) diz que:

> A internet é uma rede de computadores, integrada por outras redes menores, comunicando entre si, os computadores se comunicam através de

> um endereço lógico, chamado de endereço IP, onde uma gama de informações são trocadas, surgindo ai o problema, existe uma quantidade enorme de informações pessoais disponíveis na rede, ficando a disposição de milhares de pessoas que possuem acesso à internet, e quando não disponíveis pelo próprio usuário, são procuradas por outros usuários que buscam na rede o cometimento de crimes, os denominados Crimes Virtuais.

Em relação aos crimes, existem os crimes cibernéticos e são realizados no ambiente virtual. Pode-se definir os crimes cibernéticos como aquelas condutas criminosas que são perpetradas através do uso das diversas Tecnologias da Informação e Comunicação, como computadores, *smartphones* e da internet, consideradas prejudiciais e que violam os direitos das pessoas no ciberespaço. Nesse sentido, cumpre frisar as lições dos autores Lima e Rossino (2004, p. 110):

> O conceito de delito informático poderia ser descrito 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 a confidencialidade.

A principal diferença entre a delinquência tradicional e o crime digital reside na natureza do computador, estrutura da rede e alcance global. Além disso, o crime cibernético é uma realidade indesejável em todo o mundo, visto que a tecnologia é amplamente difundida, seja em maior ou menor grau. Espera-se que ele continue aumentando devido ao aumento considerável no uso das tecnologias disponíveis no mercado (GORDON; FORD, 2006).

Assim como o crime tradicional, o crime cibernético possui diferentes facetas e ocorre em uma ampla variedade de cenários e ambientes. As definições atuais de cibercrime evoluíram experimentalmente. Eles diferem dependendo da percepção do observador/protetor e da vítima, e são parcialmente uma função da evolução geográfica dos crimes relacionados a computadores (GORDON; FORD, 2006).

Por exemplo, o Tratado de Cibercrime do Conselho da Europa usa o termo “Cybercrime” ao qual referem-se a delitos que vão desde atividades criminosas contra dados até violação de conteúdo e direitos autorais (GORDON; FORD, 2006). No entanto, Zeviar-Geese (1997) sugere que a definição seja mais ampla, incluindo atividades como fraude, acesso, pornografia infantil e *cyberstalking*.

O Manual das Nações Unidas sobre Prevenção e Controle de Crimes Relacionados a Computadores inclui fraude, falsificação e acesso não autorizado (UNITED NATIONS, 1995) em sua definição de crime cibernético.

Infelizmente, modelar a definição de crimes cibernéticos em categorias existentes em trabalhos como Parker (1998) é problemático, pois o trabalho existente tende a ser descritivo e não baseado em uma estrutura teórica. Com isso em mente, define-se o Cibercrime como: “qualquer crime que seja facilitado ou cometido por meio de um computador, rede ou dispositivo de hardware”. Dessa forma, o computador ou dispositivo pode ser o agente do crime, o facilitador do crime, ou o alvo do crime; na verdade, o crime pode ocorrer apenas no computador ou em outros locais não virtuais.

2.1.2 Cybercrime

Dada a amplitude desta definição, é benéfico subdividir o cibercrime em dois tipos distintos; assim Gordon e Ford (2006) definem operacionalmente para o Crime Cibernético em Tipo I e Tipo II. O objetivo dos autores não é definir legalmente o Cibercrime, mas sim tentar criar uma estrutura conceitual que os legisladores possam usar para criar definições legais que sejam significativas do ponto de vista técnico e social.

Atualmente, as atuais definições legais de cibercrime variam drasticamente entre as jurisdições; no entanto, se os técnicos da área em todo o mundo puderem compreender adequadamente as nuances do crime eletrônico, poderão resultar definições legais mais coesas. De acordo com o esquema proposto por Gordon e Ford (2006), o crime cibernético Tipo I tem as seguintes características:

1. Geralmente é um evento singular ou discreto do ponto de vista da vítima.

2. Muitas vezes é facilitado pela introdução de programas de *crimeware* como *keystroke loggers*, vírus, *rootkits* ou cavalos de Tróia no sistema de computador do usuário

3. As introduções podem, mas não necessariamente serem facilitadas por vulnerabilidades. Além disso, um único evento ou instância discreta, da perspectiva do usuário, pode ser algo assim:

1. O usuário fica online para realizar uma tarefa, ou seja, acessar alguma página web ou ler/responder a um e-mail.

2. O usuário toma uma ação que permite o acesso do criminoso às informações (inserir informações pessoais no site parecido, (ou) clicar em algum objeto resultando no *download* de um Trojan ou *keystroke logger*.

3. Essas informações são usadas pelo invasor.

4. O usuário toma conhecimento do crime – este é o único evento da perspectiva do usuário. Isso geralmente ocorre muito mais tarde no ciclo de vida do Cibercrime.

5. O crime é investigado e resolvido.

O cibercrime tipo II, na outra extremidade do espectro, mas não se limita a atividades como *cyberstalking* e assédio, predação infantil, extorsão, chantagem, manipulação do mercado de ações, espionagem corporativa complexa e planejamento ou realização de atividades terroristas online.

Uma série de eventos no ciclo de vida de um Crime Cibernético Tipo II, podendo ocorrer da seguinte forma:

1. O usuário(a) acessa a internet para ver o que pode descobrir sobre a criação de lhamas.

2. O usuário(a) decide participar de um fórum on-line sobre criação de lhamas.

3. Usuário(b) vê o usuário(a), observa sua participação no fórum por vários dias, responde a alguns de seus comentários.

4. O usuário(b) então envia uma solicitação para bate-papos privados usando um cliente comum de mensagens instantâneas.

5. O usuário(a), estando familiarizado com o usuário(b) através do fórum on-line, responde positivamente e começa a conversar diariamente, bem como a participar do fórum. Este é um período conhecido como incutir confiança.

6. Após várias interações, o usuário(a) revela que é solteiro, gosta de lhamas, tem um quarto de milhão de dólares disponível para iniciar uma fazenda de lhamas e que gosta de ir a shows. Ela diz a ele que seu nome verdadeiro é Jenny.

7. O Usuário(b) pede ao usuário(a) para se encontrar pessoalmente e ir a um show.

8. O usuário(a) fica desconfiado quando o usuário(b) não fornece suas informações de contato além das informações on-line, e ela se recusa.

9. A usuária(b) torna-se irracional e começa a postar falsas alegações contra a usuária(a) no fórum on-line, acusando-a de fraude, dentre outros. Ele posta o

número da casa dela. Ele também entra em outros fóruns se passando por usuário(a), e deixa mensagens pedindo datas – deixando seu número de telefone e nome verdadeiros.

10. Usuário(a) tenta se defender no Fórum e pede ao usuário(b) privadamente para parar. Ela começa a receber inúmeros e-mails sobre as datas que pediu e percebe então que alguém está se passando por ela online. Ela confronta o Usuário(b) com suas suspeitas.

11. O Usuário(b) torna-se mais irracional e começa a desligar o telefone e assediar o usuário(a). O usuário(a) teme por sua segurança.

12. A companhia telefônica e a polícia local se envolvem.

13. O usuário(a) apresenta queixa contra o usuário(b), que é, mais tarde, um ex-pornógrafo infantil com ligações ao crime organizado, sob investigação pelo desaparecimento de três mulheres que ele supostamente conheceu na Internet.

Embora essa troca possa parecer absurda, o *cyberstalking* é um problema muito real na comunidade online de hoje. Como tal, são diferentes dos Crimes Cibernéticos Tipo I que são mais técnicos em sua natureza.

Além disso, existem outros tipos de crimes cibernéticos, ao qual inclui: fraude por e-mail e pela internet, fraudade de identidades por meio de roubo e uso, roubo de dados financeiros, roubo e venda de dados corporativos, extorsão cibernética (como apresentado no Tipo II acima), roubo de criptomoedas, espionagem de dados do governo ou de empresas, dentre outros. A maior parte dos crimes ciberbnéticos se enquadra em duas categorias principais: atividade criminosa que visa computadores e atividade criminosa que usa computadores para cometer outros crimes.

3 PRÁTICAS DOS CRIMES NA INTERNET

Se tratando da origem e do surgimento dos ciberataques e, posteriormente, do ciberterrorismo, Barrientos-Gutiérrez (2012) considera que “o advento da Web 2.0 revoluciona conceito de rede”, onde todos compartilham informações que são constantemente atualizadas. O ataque pode ser realizado de qualquer lugar o mundo, o que oferece ao cibercriminoso várias vantagens. Ao analisar essas vantagens pode-se observar o seguinte: o criminoso se sente seguro, pois não está exposto fisicamente para sua vítima, muito menos para a possível intervenção das forças de segurança, tendo em vista que a sua ação criminosa é realizada à distância e isso o faz ter o sentimento de confortável impunidade, mesmo sabendo que existem lacunas legislativas a nível internacional, razão pela qual muitos dos crimes cometidos não são punidos.

Além disso, o infrator tira vantagem do anonimato de suas ações cibernéticas, pois é difícil identificar o atacante, sendo ele: qualquer usuário que tenha um equipamento informático e ligação à Internet, com conhecimento técnico e com um investimento econômico não alto. Qualquer ataque cibernético envolve um efeito da vulnerabilidade e falta de proteção individual (FURLANETO; SANTOS; GIMENES, 2018).

Entre os crimes classificados como crimes cibernéticos encontra-se: fraude, roubo, chantagem, falsificação e apropriação indébita de dinheiro público. Com as últimas alterações legislativas, foram introduzidos outros crimes que utilizam tecnologias de informação e comunicação, como o assédio eletrónico contra a liberdade das pessoas, fenômeno também conhecido como *Shitstorm*, além da descoberta e divulgação de segredos, a interferência ilegal de informação ou dados, crimes contra a propriedade intelectual e abusos para fins sexuais através da Internet ou outro meio de telecomunicação a menores (COURI, 2011).

3.1 DOS CRIMES

No Brasil, observa-se um crescimento de 265% no ano de 2020 em relação aos crimes cibernéticos (SSP, 2021). Dentre os crimes cibernéticos mais comuns, estão o crime de ódio em geral (contra a honra, sentimento religioso, *bullyng)*, crimes de invasão de privacidade e intimidade (que pode ou não incorrer em uma

nova conduta lesiva contra a honra), crimes de estelionato, crimes de pedofilia, entre outros.

3.1.1 Crimes contra a honra

O art. 5º, X, da Constituição Federal de 1988 dispõe que a honda é protegida e tem *status* de Direito Fundamental “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”. A honra é um direito da personalidade previsto constitucionalmente, portanto, é necessária a proteção da dignidade do indivíduo e de sua reputação (BARROSO, 2004).

Para a doutrina brasileira, a honra é dividida em objetiva e subjetiva. A primeira trata da reputação e a boa fama que a pessoa desfruta em seu meio social. A segunda diz respeito a dignidade e decoro pessoal da vítima e do juízo que cada um tem de si próprio (CUNHA, 2014).

Em relação ao tópico dos crimes contra a honra, segundo a legislação penal específica existem três tipos de crimes distintos: calúnia, difamação e injúria. Distinguem-se na legislação e tipo e as penas correspondentes a cada um, *in verbis:*

> **Calúnia:**
> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos.
>
> **Difamação:**
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
>
> **Injúria:**
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena:
> I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II - no caso de retorsão imediata, que consista em outra injúria.
> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.
> § 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência: (Redação dada pela Lei nº 10.741, de 2003)
> Pena - reclusão de um a três anos e multa. (Incluído pela Lei nº 9.459, de 1997) (BRASIL, 1988).

Tais insultos podem atingir a honra das vítimas, podendo atingir também a sua dignidade e autoimagem (*aninus diffamandi*), ocorrendo no momento em que o insulto chega ao conhecimento do ofendido (NUCCI, 2017). Além disso, existem múltiplas possibilidades do uso de computadores e das ferramentas *online* que levam o Estado a constatar que não há preparo para julgar ou punir os criminosos, cujas ações podem atingir a honra, o decoro e a dignidade de terceiros (SILVA; BEZERRA; SANTOS, 2016).

Adentrando ao tema “liberdade de expressão”, esta se funda no respeito à autonomia e dignidade humana, sendo necessário um respeito dos direitos fundamentais de outrem. A liberdade de expressão é colocada à uma nova luz adjunta das tecnologias digitais e, portanto, vale destacar, positivamente, o aumento das oportunidades de participação social, interação e divulgação cultural e, consequentemente, do acesso à uma verdadeira democracia (PANNIN, PEZZELLA, 2015).

Contudo, pode ocorrer conflitos em decorrência da liberdade de expressão das pessoas, o que não pode ser exercida livremente. É necessário ponderar o direito de expressão com o direito dos demais, devendo os agressores responder judicialmente por seus excessos. Contudo, nem sempre as condutas realizadas pela internet são punidas penalmente.

Tais condutas são, na maior parte dos casos, motivadas por ódio puro e simples, sem filtro social. Um caso que chamou a atenção da mídia foi o racismo sofrido pela jornalista Maria Júlia Coutinho, conhecida como Majú Coutinho, em 2015, que recebeu vários comentários racistas pelo fato de ter postado uma foto de si mesmo em sua rede social.

Um outro tipo de crime que surge, por consequência, é o crime de ameaça, crime contra a liberdade individual previsto no art. 147 do Código Penal Brasileiro, *in verbis:*

> **Ameaça:**
> 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.
> Parágrafo único - Somente se procede mediante representação (BRASIL, 1940).

Ao analisar o crime de ameaça, deve-se considerar a individualidade da vítima. Com isso, a ideia de sexo, raça, cor, idade, opção sexual, entre outras, são fatores que devem ser avaliados no caso para que analise se houve ou não a conduta de causar dando injusto a outrém (CUNHA, 2014).

Acerda dos fatores de desigualdades, como, por exemplo, as desigualdades na forma de estereótipos e sobre a raça, onde um grupo se sente no poder de colocar outro grupo em situação de inferioridade, reforça-se ainda mais a desigualdade material entre os indivíduos. Dessa forma, pode-se notar a relevância do Direito proteger e amparar as relações sociais, visando a proteção da igualdade e dignidade humana.

Diante disso, o artigo 2º da Declaração sobre a raça e os preconceitos raciais da UNESCO, de 1978, prevê:

> §1. Toda teoria que invoque uma superioridade ou uma inferioridade intrínseca de grupos raciais ou étnicos que dê a uns o direito de dominar ou de eliminar os demais, presumidamente inferiores, ou que faça juízos de valor baseados na diferença racial, carece de fundamento científico e é contrária aos princípios morais étnicos da humanidade.
>
> §2. O racismo engloba as ideologias racistas, as atitudes fundadas nos preconceitos raciais, os comportamentos discriminatórios, as disposições estruturais e as práticas institucionalizadas que provocam a desigualdade racial, assim como a falsa ideia de que as relações discriminatórias entre grupos são moral e cientificamente justificáveis; manifesta-se por meio de disposições legislativas ou regulamentárias e práticas discriminatórias, assim como por meio de crenças e atos anti-sociais; cria obstáculos ao desenvolvimento de suas vítimas, perverte a quem o põe em prática, divide as nações em seu próprio seio, constitui um obstáculo para a cooperação internacional e cria tensões políticas entre os povos; é contrário aos princípios fundamentais ao direito internacional e, por conseguinte, perturba gravemente a paz e a segurança internacionais.
>
> §3. O preconceito racial historicamente vinculado às desigualdades de poder, que tende a se fortalecer por causa das diferenças econômicas e sociais entre os indivíduos e os grupos humanos e a justificar, ainda hoje, essas desigualdades, está solenemente desprovido de fundamento.

A discriminação não é sobre, exclusivamente, um certo indivíduo, podendo ocorrer também sob todo um grupo e a ideia nasce do preceito de que a humanidade é separada em seres superiores e inferiores (BOBBIO, 2002).

3.1.2 Crimes de invasão de privacidade e intimidade

O art. 5º, X, da Constituição Federal de 1988 dispõe acerca da proteção constitucional à privacidade e à intimidade, sendo inseridos no roll de direitos

fundamentais: ”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”.

Acerca dos crimes de invasão de privacidade e intimidade, a Lei nº 12.737 de 2021 (Lei Carolina Dieckmann), tem-se a disposição legal do art. 154-A do Código Penal Brasileiro sobre a invasão de dispositivo informático, *in verbis:*

> 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 (BRASIL, 1940).

A Lei referida recebeu o nome da atriz Carolina Dieckmann, que foi vítima de invasão de seu computador e consequente distribuição de arquivos pessoais, como suas fotos íntimas, a qual foram disseminadas na internet (CUNHA, 2014). Os objetos jurídicos tutelados, nesse caso, são a intimidade, a vida privada e o direito ao sigilo de dados constantes em dispositivo informático (CAPEZ, 2016).

3.1.3 Crimes contra a inviolabilidade do patrimônio (estelionato)

Um outro crime que teve um aumento da incidência, com o advento da internet, foi o crime de estelionato. Trata-se do crime mais ocorrido quanto se trata do assunto de inviolabilidade de patrimônio e ganhou grande visibilidade com os chamados golpes virtuais.

O art. 171 do Código Penal Brasileiro, dispõe sobre o crime de estelionato como sendo:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.

O crime decorre da obtenção de vantagem ilícita indevida, em prejuízo alheio, ao induzir ou manter a vítima em erro. Trata-se de um crime doloso, apresentado pela vontade livre e consciente de induzir ou manter alguém em erro (CAPEZ, 2016).

A Polícia Civil do Brasil orienta a população sobre como não se tornar uma vítima dos cibercriminosos. Segundo o site da Secretaria de Estado da Segurança Pública (SSP), 2021), os golpistas utilizam assuntos em evidência na mídia para atrair as pessoas e conseguir os seus dados pessoais e aplicar golpes.

> Por isso, faz-se o alerta para sempre ficar atento às informações que são divulgadas na internet, além de ter o cuidado com os próprios dados nas redes sociais. Nesse sentido, não se deve fornecer códigos que chegam por mensagens a terceiros, pois é através dessa numeração que os cibercriminosos clonam os aplicativos das vítimas.
>
> Mantenha as redes sociais fechadas, não forneça senhas e códigos recebidos por mensagem de texto (SMS), instale um antivírus nos dispositivos e verifique a autenticidade da informação antes de fazer depósitos ou transferências. Verifique a agência e entre em contato com a pessoa que estiver solicitando o dinheiro. São medidas simples para evitar cair no golpe", orientou.

O estelionato praticado por meio de meio eletrônico encaixa-se no tipo penal estabelecido pelo artigo 171 do Código Penal, sendo possível sua aplicação sem maiores ressalvas (CAPEZ, 2016).

3.1.4 Crimes contra a liberdade sexual envolvendo menores

Distinto das demais condutas supracitadas, esse tipo de crime ocorre em sigilo, na maioria dos casos. Existem alguns aplicativos celulares que facilitam a troca de informações e mensagens, de forma instantânea, o que leva diversos usuários a compartilharem informações sem notar que estão incorrendo, necessariamente, em crime (CUNHA, 2014).

O Estatuto da Criança e do Adolescente (ECA) apresenta a principal tipificação dos crimes contra crianças e adolescentes, buscando a prevenção de diversas condutas que podem ser praticadas contra eles (CAPEZ, 2016).

O artigo 241 do ECA, e seus artigos subsequentes, descrevem as condutas ilícitas envolvendo criança e adolescente, *in verbis*:

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa (BRASIL, 1990).

Se tratando da prática do crime em meio virtual, a jurisprudência brasileira é dura na aplicação da pena, considerando que os crimes comentidos em ambiente virtual mundial de computadores têm caráter transcional/internacional.

Com a popularização de aplicativos de comunicaçao, como o WhatsApp, a conduta do artigo 241-b se tornou mais frequente, *in verbis:*

> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
> § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por: (Incluído pela Lei nº 11.829, de 2008)
> I – agente público no exercício de suas funções; (Incluído pela Lei nº 11.829, de 2008)
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo; (Incluído pela Lei nº 11.829, de 2008)
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. (Incluído pela Lei nº 11.829, de 2008)
> § 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido. (Incluído pela Lei nº 11.829, de 2008)

Com a inclusão dos dois tipos penais estabelecidos no art, 241-B do ECA, tornou-se mais fácil a punição do criminoso que mantém, em seu poder, as imagens de menores de 18 anos envolvidos em pornografia.

Nas palavras de Nucci (2016, p. 785):

> A maneira pela qual o autor do crime adquire, possui ou armazena o material é livre, valendo-se o tipo da e pressão “por qualquer meio” Comumente, com o avanço da tecnologia e da difusão dos computadores pessoais, dá-se a obtenção de extenso número de fotos e vídeos pela Internet, guardando-se o material no disco rígido do computador, em disquetes, DVDs, CDs, pen drives, entre outros.

Além disso, segundo Nucci (2016), o objeto material do caso é a foto, vídeo, ou imagem contendo pornografia ou sexo explícito envolvendo criança ou adolescente, enquanto o objeto jurídico é a proteção à formação moral da criança e do adolescente.

A internet vem evoluindo rapidamente com o passar dos anos e essa velocidade traz consigo inúmeras consequências, na qual uma delas é a

disseminação dos crimes cibernéticos, em especial a do crime de pedofilia e pornografia infantil, sendo de extrema relevância para a sociedade. Nesse contexto, um outro tipo de crime virtual que atualmente é recorrente, são os crimes de ódio, do inglês *hate crime*, ao qual podem ser motivados por preconceito. São cometidos quando o criminoso seleciona intencionalmente a sua vítima em função de esta pertencer a algum grupo.

3.1.5 Cibercrimes de ódio

Com o advento da internet e das redes sociais a comunicação passou por uma revolução. Aplicativos como *Instagram, Facebook, WhatsApp, Skype,* entre tantos outros, são as ferramentas de comunicação muito utilizadas atualmente. Essas mudanças na comunicação vêm sendo estudadas por profissionais de diversas áreas, numa dinâmica que envolve a criação de neologismos próprios e a difusão de opiniões sobre diversos assuntos instantaneamente (PEREIRA et al., 2017). Entre esses neologismos criados pela comunicação *online* está o *shitstorm.*

Realizando uma tradução livre para a língua portuguesa o termo *shitstorm* significa ‘’tempestade de fezes’’, e tem por significado uma desenfreada comunicação na internet baseada em ofensas e julgamentos discriminativos. Em outras palavras, *shitstorm* é uma ‘’tempestade de indignação em um meio de comunicação da *Internet*, acompanhada, em parte, por comentários ofensivos (CALDAS; CALDAS, 2019).

Cabe destacar que tal vocábulo não tem por objetivo criticar esse modelo de comunicação, mas somente retratar um fenômeno observado onde há um verdadeiro escárnio em massa, com surtos de ofensas e insultos na internet (PEREIRA, 2017). Essa tempestade de manifestações ofensivas, aliada à instantaneidade da transmissão de informações na rede, se mostra um verdadeiro palco para discussões políticos virtuais e violação de Direitos Humanos amparada frequente anonimato (GARCIA, 2015).

Com relação a isso, fatores como o distanciamento entre o ofensor e a vítima fazem dos ambientes digitais um ambiente propício para o *shitstorm*. A ausência da vítima fisicamente faz com que o agressor se posicione de forma mais anárquica, já que o sistema punitivo estatal ou moral parece não atingir o *cyberespaço.* Diante disso, a frequente impunidade e a distância que os instrumentos de controle social adquirem frente à rápida comunicação na internet, esse comportamento ofensivo em

massa pode gerar mais discriminação e intolerância às diversidades em diversos contextos da vida (PEREIRA, 2017).

Atualmente a comunicação através da internet vem sendo discutida no âmbito das ciências jurídicas. Questões como o direito à privacidade, propriedade intelectual e as violações de bens jurídicos relevantes em meio virtual, trazem o foco da doutrina para a aplicação das normas jurídicas aos crimes de ódio cometidos em ambiente *online* (CALDAS; CALDAS, 2019).

Dentro desses debates surgem posições antagônicas: há os que defendem uma maior regulamentação estatal da internet, no sentido de uma aplicação eficaz das leis penais aos crimes que acontecem na rede; em contraposição, há a corrente que defende que a regulamentação da internet violaria a liberdade de expressão (CALDAS; CALDAS, 2019).

Como visto, os ambientes virtuais de comunicação se mostraram propício para a prática de crimes, tendo como escudo a distância entre a vítima e o agressor e a carência de mecanismos coercitivos para a defesa dos direitos ofendidos. Sobretudo, os crimes de ódio, motivados em razão por razões discriminatórias e preconceituosas, em que a vítima pertence a um determinado grupo social. Esses crimes são praticados pela manifestação de palavras tendentes a insultar, intimidar ou assediar a vítima, utilizando apontamentos referentes à sua raça, cor, etnia, origem, sexo, religião, idade, etc., (CALDAS; CALDAS, 2019).

Convém transcrever a definição de crime de ódio proposta por Perry (2001):

> Crime de ódio... envolve atos de violência e intimidação e com frequência são direcionados a grupos que já são estigmatizados e marginalizados. Como tal, é um mecanismo de poder e de opressão, cuja intenção é reafirmar as hierarquias precárias que caracterizam uma ordem social dada. Ele tenta reproduzir, ao mesmo tempo, a hegemonia ameaçada (real ou imaginária) do grupo do autor e a identidade subordinada “adequada” do grupo da vítima. É uma forma de marcar tanto o Eu quanto o Outro de tal forma a restabelecer suas posições relativas “adequadas”, conforme são dadas e reproduzidas por ideologias e padrões mais abrangentes de desigualdade social e política.

O sentimento de ódio é de ordem privada e, portanto, protegido dentre os direitos fundamentais. Ou seja, odiar é permitido e é um direito protegido quanto à liberdade de expressão. No entanto, como não existe direito absoluto, a liberdade de expressão encontra limite nos crimes quanto à honra, previstos no Código Penal brasileiro: calúnia, injúria e difamação. Portanto, nada impede que um indivíduo

manifeste a seguinte expressão: ‘’eu odeio o Presidente da República’’, porém se a expressão imputa uma situação criminosa a alguém, estaremos diante do crime de calúnia, *v.g.,* ‘’esse Presidente é um ladrão!’’ (PEREIRA, 2017).

3.2 CONSEQUÊNCIAS DOS CRIMES VIRTUAIS

Os crimes virtuais têm sido um problema que impacta a vida de muitas pessoas ao redor do mundo. O crime cibernético é um crime que, é direcionado a computadores ou outros dispositivos como, por exemplo, invasão de computadores, e onde computadores ou outros dispositivos são parte integrante do crime, como, por exemplo, roubo de identidade, fraude online e distribuição de material de exploração infantil. Alguns dos tipos mais comuns de crimes cibernéticos incluem golpes e fraudes online, *hackers*, roubo de identidade, ataques a sistemas de computador, bem como conteúdo online proibido e ilegal (LUCCHESI; HERNANDEZ, 2018).

Tais atos são ilegais pois seus efeitos podem ser extremamente perturbadores para as vítimas e podem ir muito além de serem meramente por razões financeiras. O crime pode fazer com que suas vítimas se vejam impotentes como resultado da violação de sua privacidade e à medida que cresce a dependência econômica moderna da tecnologia, espera-se que o custo e a incidência do crime cibernético aumentem em muitas partes do mundo (MOREIRA et al., 2019).

Na falta de uma única definição universal, a aplicação da lei geralmente faz uma distinção entre dois tipos principais de crimes cibernéticos. Primeiro, o *cibercrime* avançado, que consiste em ataques sofisticados contra *hardware* e *software* de computador; e segundo, os crimes cibernéticos, em que muitos crimes tradicionais, como crimes financeiros, crimes contra crianças e até crimes de rua, tem tomado um novo rumo com o advento da Internet (LUCCHESI; HERNANDEZ, 2018).

As últimas décadas vêem novas tendências em crimes cibernéticos surgindo o tempo todo, resultando em um custo estimado de bilhões de *ringgits* para a economia global. Ao contrário do passado, onde o cibercrime era cometido principalmente por indivíduos ou pequenos grupos, hoje as economias enfrentam redes cibercriminosas altamente complexas que reúnem indivíduos de todo o mundo em tempo real para cometer crimes em uma escala sem precedentes (INTERPOL, 2016).

Tal situação convida as organizações criminosas a recorrerem cada vez mais à internet para acomodar suas atividades criminosas e, assim, maximizar seu lucro

ilegal no menor tempo possível. Os crimes em si não são necessariamente novos, eles podem ser do tipo fraude, jogo ilegal, roubo ou venda de medicamentos falsos, etc., mas estão evoluindo junto com as oportunidades crescentes e facilitadas pela internet e, por essas razões, estão se tornando cada vez mais difundidas e prejudiciais à sociedade.

Segundo a *Stop Think Connect* (2019), existem três dicas simples sobre como evitar ser uma vítima de crimes cibernéticos:

- Mantenha uma máquina limpa atualizando sempre o *software* e o sistema operacional em computadores e dispositivos móveis;
- Na dúvida sobre um anexo ou link, pare e pense antes de agir. Links no e-mail, mensagens instantâneas e publicações online são formas comuns para os cibercriminosos atacarem computadores;
- Use uma autenticação mais forte, especialmente para contas com informações confidenciais, como e-mails ou contas bancárias.

Dentre os mais variados tipos de crimes virtuais estão as fraldes por e-mail usando a internet, interceptação de informações pessoais de terceiros ou dados sigilosos de organizações e empresas, roubo de dados financeiros ou credenciais bancárias, invasão de computadores pessoais, dentre outros.

O *Cybercrime* descreve uma série de circunstâncias em que a tecnologia está envolvida na prática do crime e apresenta vários desafios em constante evolução para o governo e para a aplicação da lei.

4 EVOLUÇÃO LEGISLATIVA E PUNIBILIDADE CIBERNÉTICA

Comumente a sociedade utiliza a internet como um meio para facilitar a educação e interação social, abrindo as portas de suas casas, sem quaisquer restrições, por meio das redes sociais e aplicativos, onde se registram toda a sua rotina, podendo, segundo Martins (2017), expor sentimentos, experiências, conquistas, vida financeira por meio de *status,* alegrias e tristezas. Tais ações podem promover, facilmente, a ação de pedófilos, sequestradores e criminosos do mundo virtual.

Os crimes cibernéticos crescem à medida em que a tecnologia evolui, contudo, a legislação especifica não acompanha tantas mudanças. O ambiente virtual é um local que comumente consagra violações às garantias individuais, com gritante degradação social, visto que os crimes praticados em meio virtual se alastram descoordenada e permanentemente, cujo controle se torna inviável, em decorrência da ausência ou escassez de leis que tutelem adequadamente as atitudes ilegais dos usuários da internet.

De acordo com Mecabô e Colucci (2015, p. 6):

> “Os meios online impõem o desafio de conciliação entre os valores humanos consagrados na Constituição e os desvios comportamentais perpetrados em uma sociedade doente e individualista (...)” que os torna “(...) escravos da tecnologia criada”.

Atualmente, por um lado, a tecnologia da informação e suas aplicações industriais estão florescendo como nunca. Por outro lado, as questões de segurança da informação estão se tornando cada vez mais proeminentes. Ações hostis como ataques de *hackers*, invasões de *software* malicioso, crimes de computador e violações de privacidade constituem grandes ameaças à segurança da informação. Além disso, os desenvolvimentos na ciência e na tecnologia colocaram novos desafios à segurança da informação.

4.1 O PAPEL DO ESTADO NO COMBATE CRIMES CIBERNÉTICOS

Verifica-se o compromisso assumido pelos Estados internacionalmente, com relação à aplicação dos Direitos Humanos em seus respectivos ordenamentos jurídicos. A necessidade de tratamento igualitário, que garantam o próprio exercício

da dignidade da pessoa humana, e dos demais direitos fundamentais individuais e coletivos direitos sociais, é papel do Estado e está previsto na própria Carta Magna. Para a garantia desses direitos, cabe ao Estado implementar a repressão e punição aos crimes discriminatórios na internet bem como desenvolver um sistema de fiscalização eficiente para apuração dos crimes de ódio (MELO, 2020).

A Constituição Federal de 1988 deu especial destaque à não discriminação, colocando o combate às formas de preconceitos como um objetivo da República Federativa do Brasil sem seu artigo 3º, inciso IV: ‘’promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.’’ No artigo 4º, a Carta Magna ainda estabelece o repúdio ao racismo, inclusive classificando-o como um crime inafiançável e imprescritível, nos temos do Art. 5º, XLII (BRASIL, 1988).

Nesse contexto, o Brasil se mostra adepto às orientações internacionais sobre Direitos Humanos, e repudia expressamente as formas de discriminação social como o racismo. Ou seja, pelo menos formalmente o Estado cumpre o compromisso de garantir a igualdade e a não-discriminação, incriminando as condutas que causem tais prejuízos, principalmente à dignidade da pessoa humana (MELO, 2020).

Considerando-se todo o conteúdo exposto até o momento, percebe-se que as novas formas de discriminação decorrentes da comunicação no *cyberespaço* tem gerado a chamada *shitstorm,* difundindo discursos que pregam a intolerância e incentivam práticas discriminatórias e preconceituosas de segregação social. Essa prática se prolifera de forma generalizada, dada as características de anonimato e distanciamento entre autor e vítima propiciados pelo relacionamento virtual (CASTELLS, 1999).

Diante desse fenômeno social, há uma corrente filosófica que pede maior intervenção estatal e aplicação das leis penais no combate à discriminação na internet, e aos crimes cibernéticos. De outro modo, uma corrente sustenta que a internet é uma ferramenta que democratizou a informação e a comunicação, e limitar a liberdade de expressão na rede configuraria um retrocesso à disseminação de pensamentos.

Tendo em vista o combate às discriminações como sugere a própria Constituição Federal, o Estado brasileiro tem adotado medidas penais infraconstitucionais para incriminar condutas discriminatórias, como por exemplo a elaboração da Lei a Lei nº 12.737, voltada para crimes virtuais e delitos informáticos.

4.2 MARCO CIVIL DA INTERNET (LEI N° 12.695/2014)

A Lei nº 12.965, de 23 de abril de 2014, promulgou o denominado Marco Civil da Internet, com o intuito de estabelecer princípios, garantias, direitos e deveres para os usuários de internet no Brasil. A Lei foi sancionada em 23 de abril de 2014 e estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, ao qual estabelece alguns fundamentos e princípios acerca do uso da internet:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
>
> I - o reconhecimento da escala mundial da rede;
>
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
>
> III - a pluralidade e a diversidade;
>
> IV - a abertura e a colaboração;
>
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VI - a finalidade social da rede.
>
> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II - proteção da privacidade;
>
> III - proteção dos dados pessoais, na forma da lei;
>
> IV - preservação e garantia da neutralidade de rede;
>
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII - preservação da natureza participativa da rede;
>
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
>
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

As transformações resultantes do uso livre da internet geram perplexidade nas pessoas, que ainda não sabem como se portar civilmente nesse ciberespaço. A internet não é mais uma “terra sem lei” onde tudo é permitido pela aparente impossibilidade de descoberta de verdadeira identidade da pessoa.

4.2.1 Caso Concreto Carolina Dieckmamm

Em 07 de novembro de 2012 foi aprovado o Projeto de Lei, nº 2.793 de 2011. Apelidada de “Lei Carolina Dieckmann”, a Lei nº 12.737 de 30 de novembro de 2012, teve seu pleno vigor no dia 02 de abril de 2013.

À exemplo de crimes motivados por ações hostis, um caso ocorrido com a atriz Carolina Dieckmann, em maio de 2011, promoveu uma grande repercusão. Um hacker (criminoso virtual) invadiu o computador da atriz e teve acesso a 36 fotos pessoais de cunho íntimo. De acordo com a denúncia, o criminoso exigiu uma quantia de 10 mil reais para não publicar as fotos na internet (EGEWARTH, 2019).

A atriz recusou a exigência e acabou tendo as suas fotos vazadas na internet, o que criou grande discussão popular acerca da criminalização desse tipo de conduta, que ainda foi excessivamente fomentada pela mídia. Com isso, a atriz abraçou a causa e cedeu seu nome à lei. Ressalta-se que, antes do surgimento da lei, o ato de invadir um ambiente virtual e subtrair dados pessoais já era crime, mas não havia nenhuma norma que tratava especificamente sobre o assunto (EGEWARTH, 2019).

4.2.1.1 Aplicabilidade Lei Carolina Dieckmamm n° 12.737/2012

A lei é fruto do projeto apresentado pelos Deputados Federais Paulo Teixeira, Luiza Erundina, Manuela D’Ávila, João Arruda, Brizola Neto e Emiliano José em 29 de novembro de 2011 na Câmara dos Deputado.

> São inegáveis os avanços para a sociedade decorrente do uso da Internet e das novas tecnologias. Estes avanços trazem a necessidade da regulamentação de aspectos relativos à sociedade da informação, com o intuito de assegurar os direitos dos cidadãos e garantir que a utilização destas tecnologias possa ser potencializada em seus efeitos positivos e minimizada em seus impactos negativos. (BRASIL, 2011).

Eles viram a necessidade da criação de uma legislação que regulamentasse de forma mais especifica o uso “criminoso” dos meios cibernéticos devido ao impulso tecnológico do século XXI.

A Lei referida alterou o Código Penal Brasileiro, acrescentando-lhe os artigos 154-A, e 154-B. Além disso, ainda alterou o texto dos artigos 266 e 298, inserindo os crimes praticados via meios informáticos na legislação penal:

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o DecretoLei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1o Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2o O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B: “Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4o Na hipótese do § 3o , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.”

“Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.”

Art. 3o Os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação: “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266.

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR) “Falsificação de documento particular

> Art. 298. .....
>
> Falsificação de cartão
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)
>
> Art. 4o Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial. Brasília, 30 de novembro de 2012; 191o da Independência e 124o da República.
>
> DILMA ROUSSEFF
>
> José Eduardo Cardozo (BRASIL, 2012, F).

A lei não exige nenhuma qualidade ou condição especial do agente, portanto, o sujeito ativo pode ser qualquer pessoa que praticar a conduta descrita pelo tipo penal. Ou seja, não necessita ser um hacker o invasor. O sujeito passivo pode ser qualquer pessoa que seja titular do bem jurídico protegido pelo tipo penal incriminador que foi violado (NUCCI, 2014), podendo o mesmo ser o proprietário ou detentor do dispositivo, nos casos que o equipamento é fornecido pela empresa ao funcionário para utilização profissional (PRADO, 2013).

Para que haja a caracterização das condutas do tipo penal é fundamental haver o dolo e o especial fim de agir, que é a obtenção, a adulteração ou a destruição de dados ou informações, também a obtenção de vantagem ilícita (REIS, 2014). Dessa forma, admite-se a forma tentada quanto à violação do dispositivo informático, porém não se aceita no tocante a figura §1º, pois trata da preparação do previsto no *caput* e não se pune a tentativa da preparação, pois já é uma exceção em matéria de criminalização (NUCCI, 2014).

Quando a invasão resultar na obtenção de conteúdo de comunicação eletrônica privada, segredos comerciais ou industriais, informes sigilosos, definidos em lei, ou o controle ou acesso remoto sem autorização ao dispositivo, a qualificadora será pena será de reclusão, de 6 meses a 2 anos, e multa, se não constituir crime mais grave – prevista no art.154-A parágrafo terceiro –.

A referida Lei promove o aumento da pena de um a dois terços se os criminosos realizar a divulgação, comercialização ou transmissão dos dados e informações obtidas à terceiros. Além disso, aumenta-se a pena conforme o parágrafo quinto do art.154-A, de 1/3 (um terço) até 1/2 (a metade) se o delito for praticado contra Presidente da República, governadores e prefeitos, Presidente do STF, Presidente da Câmara dos Deputados, do Senado, de Assembleia Legislativa, da Câmara Legislativa do DF ou Câmara Municipal e de dirigente máximo da

administração direta ou indireta, estadual, municipal ou do Distrito Federal (NUCCI, 2014).

Em tais casos, a ação penal é pública condicionada à representação da vítima. Ou seja, a vítimida precisa autorizar e oferecer representação para que haja a investigação da Polícia e o processamento pelo Ministério Público, salvo quando o delito é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos, pois, nesses casos o Ministério Público pode processar diretamente (NUCCI, 2014).

Importante a informação da Nota Técnica Ministério Público de São Paulo (2013).

> Se a conduta for mais grave que a simples invasão com a finalidade de obtenção, adulteração ou destruição dos dados ou informações, ou a instalação de vulnerabilidades, como por exemplo, fraudes em netbanking (furto qualificado), estelionato ou extorsão, interceptação de comunicação telemática, o crime de invasão de dispositivo informático será desconsiderado, porque constituirá somente um meio para o cometimento daquelas condutas.

O principal objetivo dessa Lei é proteger a privacidade dos usuários da internet com relação a seus dados e informações pessoais, profissionais e que estejam armazenados em dispositivos eletrônicos e que tiveram a sua segurança violada sem autorização. Contudo, o estabelecimento de direitos e deveres cibernéticos, no geral, ainda que tardio, é importante para o combate aos crimes virtuais, visto que é por meio dessas normas que pode ser visualizado com mais facilidade o que está sendo violado, estabelecendo assim as condutas ilícitas.

Ante o exposto, observa-que com o advento da tecnologia, surgem impactos nas formas de comunicação, sociabilidade e acesso à informação. Dessa forma, os crimes cibernéticos, ao qual incluem as menifestações de ódio, preconceito e intolerância, fazem parte desse novo universo. O cibercrime é uma realidade que se faz presente no meio digital e que pode impactar negativamente a vida dos atingidos e que, portanto, deve-se ser pauta de discussão. Além disso, é possível conter esses crimes virtuais aplicando-lhes a cada caso a legislação pertinente ao qual lhe reprime.

Além disso, com base nestas informações, é possível observar que a informação, prevenção e conscientização formam o pilar mestre para que se reduza

o número de cibercrimes. Isto decorrerá essencialmente de impulsos governamentais, que disponibilizem informações e façam campanhas, utilizando-se da mídia para proteger os usuários que utilizam a internet como um todo.

5 CONSIDERAÇÕES FINAIS

O presente estudo foi baseado na doutrina, na lei, em artigos e na interpretação do texto constitucional que assegura garantias e direitos fundamentais balizares do Estado Democrático de Direito. O objetivo foi alcançado com sucesso. Por meio da pesquisa bibliográfica foi possível estudar sobre os principais crimes *cybernéticos*, compreender melhor sobre a evolução desses crimes, seus conceitos, modos operantes, seu histórico, bem como as consequências às vítimas e compreender melhor sobre as legislações existentes para punir tais criminosos.

A sociedade utiliza a internet como um meio para facilitar a educação e interação social, o que faz com que as pessoas abram as portas de suas casas, sem quaisquer restrições, por meio das redes sociais e aplicativos, onde podem registrar toda a sua rotina pessoal. O ambiente virtual é um local que comumente consagra violações às garantias individuais, com gritante degradação social, visto que os crimes praticados em meio virtual se alastram descoordenada e permanentemente, cujo controle se torna inviável em decorrência da ausência ou escassez de leis que tutelem adequadamente as atitudes ilegais dos usuários da internet.

Em decorrência da evolução tecnológica e a crescente expansão da utilização da internet no Brasil e no mundo, tornou-se fundamental a criação de leis especificas que tratam da referida temática em pauta, vindo a tipificar novas condutas delitivas provenientes da fomentação da internet. A exemplo disso, a criação da Lei n° 12.737/12 (Lei Carolina Dieckmann), que modificou a norma penal trazendo várias inovações legislativas em relação a punibilidade mediante os crimes *cybernéticos.* Contudo, o estabelecimento de direitos e deveres cibernéticos, ainda que tardio, é importante para o combate aos crimes virtuais, visto que é por meio dessas normas que pode ser visualizado com mais facilidade o que está sendo violado, estabelecendo assim as condutas ilícitas.

O conhecimento dos fatos e das tendências é crítico para os esforços de prevenção do crime e da proteção de dados públicos e privados. Além disso, também auxilia na criação de ferramentas e estratégias para o combate aos crimes *cybernéticos*. Em decorrência das ferramentas digitais utilizadas atualmente para cometer tais crimes, os criminosos se tornam mais anônimos e, consequentemente, mais difíceis de serem identificados.

REFERÊNCIAS

ALMEIDA, José Maria Fernandes. Breve história da Internet. 2005.

ASSUNÇÃO, Ana Paula Souza. CRIMES VIRTUAIS. 2018.

BARRIENTOS-GUTIÉRREZ, Tonatiuh et al. Aiming for the adolescent market: internet and video games, the new strategies of the tobacco industry. **Salud publica de Mexico**, v. 54, n. 3, p. 303-314, 2012.

BARROSO, Carolina Rodrigues de Carvalho et al. Meios de investigação e produção de provas nos crimes cibernéticos.

BOBBIO, Norberto; VIROLI, Maurizio. **Diálogo en torno a la república**. Tusquets, 2002.

BRASIL. Código Penal. **DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 02 dez. 2021.

BRASIL. Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988.4. ed. Brasília, DF: Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 07 nov. 2021.

BRASIL. Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988.4. ed. Brasília, DF: Disponível em: http://www.planalto.gov.br/ccivil03/constituicao/constituicao.htm. Acesso em 07 nov. 2021.

BRASIL. Estatuto da Criança e do Adolescente. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 03 dez. 2021.

CALDAS, Camilo Onoda Luiz; CALDAS, Pedro Neris Luiz. Estado, democracia e tecnologia: conflitos políticos e vulnerabilidade no contexto do big-data, das fake news e das shitstorms. **Perspectivas em Ciência da Informação**, v. 24, p. 196-220, 2019.

CAPEZ, Fernando. **Código penal comentado**. Saraiva Educação SA, 2016.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

COURI, Gustavo Fuscaldo. Crimes pela internet. **Disponıvel em: http://tinyurl. com/6khbmqx. Acesso em: maio de**, 2011.

CUNHA, Teresa. O insuportável ruído dos crimes de honra na Palestina. Maria's Grotto no coração dilacerado da nação. **e-cadernos CES**, n. 22, 2014.

DE INELLAS, Gabriel Cesar Zaccaria. Como advogar no crime: guia de atuação do advogado criminalista: orientações básicas introdutórias, orientação doutrinária, jurisprudência, modelos, legislação especial (código penal, código de processo penal, lei de execução penal, lei das contravenções penais, estatuto da advocacia ea OAB, lei de tóxicos, lei dos crimes hediondos, porte de arma.), glossário, bibliografia básica. **J. de Oliveira**, 2004.

EGEWARTH, Arthur Bernardo. Os crimes cibernéticos e a ineficácia da lei “Carolina Dieckmann”. 2019.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron. Veríssimo. Crimes na Internet e inquérito policial eletrônico. São Paulo: **Edipro**. 2018.

GARCIA, José Luís. **Uma crítica da economia da informação na era das mídias digitais**. Revista Novos Olhares. USP: São Paulo, v.4, n.1, 2015. Disponível em: <http://dx.doi.org/10.11606/issn.2238-7714.no.2015.102233>. Acesso em: 07 nov. 2021.

GOETHALS, Karen; AGUIAR, Antónia; ALMEIDA, Eugénia. História da Internet. **Faculdade de Engenharia da Universidade do Porto, Mestrado em Gestão da Informação**, 2000.
International criminal police investigation (Interpol) (2016). Cybercrime. Retrieved June 26, 2016. Disponível em: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime. Acesso em: 17 mar. 2022.

GORDON, Sarah; FORD, Richard. On the definition and classification of cybercrime. **Journal in computer virology**, v. 2, n. 1, p. 13-20, 2006.

LEINER, Barry M. et al. Una breve historia de Internet. **Novática**, v. 130, 1997.

LIMA, Maria de La Luz; ROSSINI, Augusto. Informática, Telemática e Direito Penal. **São Paulo: Memória Jurídica Editora**, p. 105, 2004.

LUCCHESI, Ângela Tereza; HERNANDEZ, Erika Fernanda Tangerino. CRIMES VIRTUAIS: ciberbullying, revenge porn, sextortion, estupro virtual. **Revista Officium: estudos de direito**, v. 1, n. 1, p. 2, 2018.

MARTINS, Patrícia. CRIMES CIBERNÉTICOS E A CORRELAÇÃO AO CRIME CONTRA HONRA. 2017.

MECABÔ, Alex; DA GLÓRIA COLUCCI, Maria. Revenge Porn: diálogo ético-jurídico à luz do Direito brasileiro. **Percurso**, v. 2, n. 17, p. 33-54, 2015.

MELO, Mateus Ramos. DIREITO DIGITAL: CRIMES CIBERNÉTICOS E MARCO CIVL DA INTERNET. 2020.

MOREIRA, Rodrigo Pereira et al. Prevenção de crimes virtuais contra crianças e adolescentes. **Interfaces-Revista de Extensão da UFMG**, v. 7, n. 2, 2019.

NUCCI, Guilherme de Souza. Curso de direito penal: parte especial. **Rio de Janeiro: Forense**, 2017.

NUCCI, Guilherme de Souza. Manual de direito penal/Guilherme de Souza Nucci.– 12. Ed. rev., atual. e ampl. **Rio de Janeiro: Forense**, p. 218, 2016.

NUCCI, Guilherme de Souza. Manual de Direito Processual Penal e Execução Penal. 2010.

NUCCI, Larry P.; NARVAEZ, Darcia; KRETTENAUER, Tobias (Ed.). **Handbook of moral and character education**. New York: Routledge, 2014.

PARKER, Donn B. **Fighting computer crime: A new framework for protecting information**. John Wiley & Sons, Inc., 1998.

PEREIRA, Luiz Ismael et al. O fenômeno Shitstorm: Internet, intolerância e violação de direitos humanos. **Interfaces Científicas-Humanas e Sociais**, v. 6, n. 1, p. 123-134, 2017.

PERRY, B. **In the Name of Hate: Understanding Hate Crimes**, London: Routledge, 2001.

PEZZELLA, Maria Cristina Cereser; PANNAIN, Camila Nunes. Novas Tecnologias e Tutela dos Direitos Fundamentais: O Discurso de Ódio nas Redes Sociais. **Revista de Direito, Inovação, Propriedade Intelectual e Concorrência**, v. 1, n. 1, p. 88-103, 2015.

PRADO, Fabiano Simão. CRIMES INFORMÁTICOS: A NOVA LEI 'CAROLINA DICKEMANN" E SUAS FALHAS. In: **Anais Eletrônicos do Congresso Acadêmico Científico da UEG de Porangatu**. 2013.

SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA. Golpes na internet crescem 265%. Disponível em: https://www.ssp.se.gov.br/Noticias/Detalhes?idNoticia=17634. Acesso em: 01 dez. 2021.

SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallas Tomaz. Relações Jurídicas Virtuais: Análise de Crimes Cometidos por meio do uso da Internet. **Revista Cesumar–Ciências Humanas e Sociais Aplicadas**, v. 21, n. 1, p. 7-28, 2016.

STOP THINK CONNECT (2019). How to recognize & prevent cybercrime. Retrieved October 15, 2019. Disponível em: https://www.dhs.gov/sites/default/files/publications/Week3TipCard-%20508%20compliant_0.pdf. Acesso em: 18 mar. 2022.

UNITED NATIONS: The united Nations manual on the prevention and control of computer related crime, 1995, supra note 41, paragraphs 20 to 73 in International Review of Criminal Policy, pp. 43–44 (1995).

UNESCO. Declaração sobre a raça e os preconceitos raciais. Disponível em: https://www.oas.org/dil/port/1978%20Declara%C3%A7%C3%A3o%20sobre%20Ra%C3%A7a%20e%20Preconceitos%20Raciais.pdf. Acesso em: 01 dez. 2021.

ZEVIAR-GEESE, Gabriole. The State of the Law on Cyberjursidiction and Cybercrime on the Internet. **Gonz. J. Int'l L.**, v. 1, p. 119, 1997.

PUC GOIÁS

TERMO DE AUTORIZAÇÃO DE PUBLICAÇÃO DE PRODUÇÃO ACADÊMICA

O(A) estudante Daniel Barbosa Dias
do Curso de Direito, matrícula 2017100010403O,
telefone: (62) 99854-8904, e-mail danielbarbosa366@hotmail.com na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Condutas criminosas através do ciberespaço: indução, consequências, impunidade e análise legislativa vigente, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JEPG): Som (WAVE, MPEG, AIFF, SNS); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 21 de Fevereiro de 2022.

Assinatura do(s): autor(es): Daniel B. Dias

Nome completo do autor: Daniel Barbosa Dias

Assinatura do professor- orientador:

Nome completo do professor-orientador: M/ Cesar Costa de Paula