

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

**CIBERCRIMINALIDADE:**

ORIGEM E EVOLUÇÃO DOS CRIMES CIBERNÉTICOS.

ORIENTANDO (A): IGOR DUARTE SUGUIMOTO COSTA

ORIENTADOR (A): PROF. (A): JOSE HUMBERTO ABRÃO MEIRELES

GOIÂNIA-GO

2022

IGOR DUARTE SUGUIMOTO COSTA



**CIBERCRIMINALIDADE:**

ORIGEM E EVOLUÇÃO DOS CRIMES CIBERNÉTICOS

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).

Prof. Orientador: ME José Humberto Abrão Meireles.

GOIÂNIA-GO

2022

IGOR DUARTE SUGUIMOTO COSTA



**CIBERCRIMINALIDADE**

Data da Defesa: \_\_\_\_ de \_\_\_\_\_\_\_\_\_\_ de \_\_\_\_\_\_\_

BANCA EXAMINADORA

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Orientador: Prof. José Humberto Abrão Meireles Nota

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Examinador (a) Convidado (a): Prof. (a): ME Eufrosina Saraiva Silva



**CIBERCRIMINALIDADE**

IGOR DUARTE SUGUIMOTO COSTA

Neste trabalho serão abordados os aspectos históricos e conceituais dos crimes cibernéticos, bem como algumas noções gerais de cibercriminalidade e uma explanação das atuais leis brasileiras que tratam do tema. Não obstante, o enfoque da presente pesquisa é um estudo sobre a origem e evolução dos crimes cibernéticos, bem como as repercussões dos ataques à honra e à imagem de um indivíduo através desse meio de comunicação global e os desafios para punir os cibercriminosos. Os capítulos desta pesquisa trará uma análise de trabalhos correlatos ao tema de autores e doutrinadores renomados no meio acadêmico. Por fim, serão apresentadas possíveis soluções à indagação do trabalho, a qual se refere aos possíveis meios de coibir o ataque de cibercriminosos.

**Palavras-chave**: Cibercimes. Internet. Legislação. Espécie. Crimes cibernéticos.



**SUMÁRIO**

**INTRODUÇÃO**.............................................................................................................6

**1 ASPECTOS E EVOLUÇÃO HISTÓRICA**.................................................................7

1.1 NOÇÕES GERAIS DE CRIMES CIBERNÉTICOS................................................8

1.2 CRIMES PROPRIOS E IMPROPRIOS................................................................10

**2 ESPECIES DE CRIMES CIBERNÉTICOS**.............................................................11

2.1 CRIMES CONTRA HONRA.................................................................................12

2.2 CRIMES DE INVASÃO DE PRIVACIDADE E INTIMIDADE................................15

2.3 CRIMES CONTRA A INVIOLABILIDADE DO PATRIMONIO..............................16

2.4 CRIMES CONTRA A LIBERDADE SEXUAL ENVOLVENDO MENORES..........16

**3 CRIMES VIRTUAIS NA LEGISLAÇÃO**..................................................................18

3.1 LEGISLAÇÕES VIGENTES.................................................................................19

**CONSIDERAÇÕES FINAIS**.......................................................................................24

**ABSTRACT**................................................................................................................25

**REFERÊNCIAS**..........................................................................................................26

**INTRODUÇÃO**

Os crimes informáticos são realizados desde muito antes do advento da internet. Com a criação da internet, surgiram novos meios de interação social, e como tal, também está sujeito à marginalização e criminalidade.

Segundo informações da Pesquisa Nacional por Amostra de Domicílios Contínua (Pnad C), divulgada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), o Brasil fechou o ano de 2016 com 116 milhões de pessoas conectadas à internet, o que corresponde há 64,7% da população. É bem provável que esses dados apontados tenham aumentado, já que a tecnologia está evidentemente aumentando com o passar dos anos, como também o acesso a ela.

O presente trabalho se propõem a uma abordagem dos fatos históricos pertinentes à evolução da internet, desde sua concepção até sua disseminação na sociedade atual, através de pesquisas bibliográficas de conceitos históricos, bem como análises de casos de crimes cibernéticos no Brasil e como a legislação brasileira lida com esses delitos.

**1 ASPECTOS E EVOLUÇÃO HISTÓRICA**

A evolução da rede mundial de computadores é sistêmica e progressiva, em constante modernização e atualização frenética da tecnologia.

Há muito tempo antes de ser utilizada como ferramenta para a pratica de crimes, a tecnologia na era moderna era boicotada e rejeitada por muitas pessoas, que viviam de trabalho braçal durante a revolução industrial.

Em uma noção geral, os primeiros sinais de crimes informáticos seriam os primeiros atos de sabotagens, a novas tecnologias implantadas neste período histórico, como explicam Damásio de Jesus e José Milagres (2016, p. 22) que trazem exemplos de sabotagens em indústrias que possuíam inovações tecnológicas, pois em sua concepção, colocariam em risco seus empregos.

Obviamente o conceito de crimes informáticos somente ganharia contornos mais específicos algumas décadas depois. A Doutrina ainda se diverge sobre qual seria o primeiro registro de crime informático registrado no mundo, se dividindo em dois acontecimentos em universidades dos Estados Unidos, um que ocorreu em 1964 e outro em 1978 onde os estudantes invadiram os sistemas computadorizados de suas instituições de ensino.

Para começarmos a desenvolver o conceito de crimes informáticos é necessário compreender que esta diretamente ligada ao conceito de criptografia.

O conceito de criptografia se equipara a esconder ou mascarar dados ou informações através de uma linguagem codificada. Sendo esta uma pratica quase tão antiga quanto à humanidade, pois é conhecido que nos períodos de Guerra entre a pérsia e Grécia havia a necessidade de enviar informações de forma sigilosa, onde apenas o destinatário final da mensagem poderia decifrá-la.

Aos longos dos séculos, a criptografia foi evoluindo juntamente com a tecnologia despertando interesse em especialistas de diversas áreas. A criptografia é a ciência de esconder informações, as noções mais robustas de crimes cibernéticos se originam no intuito de obter informações sigilosas.

O mais popular de todos foi Alan Turing, indubitavelmente conhecido como pai da computação. Alan era britânico, graduado em matemática pela universidade de Cambridge e criptoanalista, prestou seus serviços à inteligência britânica na segunda guerra mundial, foi o responsável por criar uma série de códigos que quebrariam a criptografia alemã. Podemos dizer que Alan Turing foi um dos primeiros “Hackers” da história, pois expôs a fragilidade dos sistemas “*DOS”* à época.

Na década de 1950, houve maior relevância no contexto histórico da internet. Neste período, se deu o auge a decorrência de crimes informáticos, sendo somente possível com a criação do projeto militar ARPANET. Esse projeto foi o precursor da internet, pois foi criada a primeira rede operacional de computadores interagindo a base de computação de dados, (PEASANI, 2000).

Em sua dissertação de mestrado, Marcelo Sávio de Carvalho nos diz que a corrida armamentista na Guerra fria influenciou na caracterização e desenvolvimento desse invento, pois serviu de estimulo para a melhoria desta invenção, tornando algo mais sofisticado.

A internet começou a ter uma concepção mais próxima da atual, passando de uma arma militar para um produto lucrativo, a popularização da internet começou nos anos de 1990, quando os EUA tiveram interesses comerciais na abertura da rede.

Nos próximos anos, iniciou-se uma verdadeira revolução tecnológica o que gerou um ciclo de mudanças na internet, deixando de ser um sistema restrito a pequenos grupos para se tornar o meio de comunicação mais utilizado no mundo. O crime cibernético também se iniciou junto uma nova fase, já que a criptografia utilizada pelas corporações se tornou objeto de desejo dos cibercriminosos.

* 1. **NOÇÕES GERAIS DE CRIMES CIBERNETICOS**

No inicio do milênio, o mundo digital ainda era enigmático e obscuro para o homem comum. Com o amplo uso e a popularização da internet nas mais diversas atividades, começa a aparecer a preocupação em relação à segurança das informações compartilhadas em modo *online*.

Embora o termo cibercrime seja antigo, foi originado na década de 1990 em uma reunião do G-8 que discutia sobre a praticas ilícitas na internet de forma preventiva e punitiva. Desde então, este termo foi utilizado para as infrações penais que eram praticadas no âmbito virtual.(D’URSO,2017)

Com a progressão tecnológica, o combate contra os crimes cibernéticos se dificulta bastante. Com o uso ilimitado da internet, alguns indivíduos com conhecimentos mais aprofundados, passaram a roubar informações criptografadas por proveito econômico ou mera diversão.(JESUS e MILAGRES, 2016)

Foram esses indivíduos denominados “Hackers”, um designativo da era moderna, o termo é de origem da língua inglesa que se refere a pessoas com conhecimento muito avançado em computação, cujas habilidades têm enfoque em invadir sistemas e roubar, adulterar ou apenas olhar dados e informações de outras pessoas pelos mais variados motivos.

Desta forma, a quebra de códigos e invasão de sistemas deixou de ser um instrumento de guerra para virar oportunidade de lucro ou mero passatempo.

Os estelionatários, por exemplo, viram a oportunidade de aplicação de golpe via internet.

Existem inúmeras formas de condutas delituosas na internet, desde pedofilia, prostituição, tráfico, pirataria, até terrorismo. A digitalização dos meios de trabalhos economizam bilhões de reais as empresas anualmente, porém causa muitos problemas as pessoas em todo o mundo. Só neste ano foram registrados inúmeros casos de sequestros de dados e informações sigilosas no mundo inteiro.

Em 2017, o hospital do câncer de Barretos e outros administrado pela fundação Pio XII, foram alvo de hackers aonde sequestraram os dados e exigiram um resgate de US$: 300,00 (trezentos dólares) por maquina o que geraria ao hospital um custo de US$ 360 mil, o equivalente a cerca de 1,08 milhão de reais na cotação da época.

Além de causarem transtornos, alguns crimes geram enorme prejuízo ao país, a pirataria tem sido um problema cada vez mais difícil de enfrentar, seja ela nos filmes, livros, musicas, propriedade intelectual e artística, nunca estiveram tão vulnerável.

Alvir Reichert Junior era dono de um site chamado *MP3 Forever*, o qual disponibilizava ilegalmente centenas de músicas para *download*. O embasamento de sua prisão foi no artigo 184 do Código Penal (ESTADÃO, 2003), o qual dispõe:

“Art. 184. Violar direitos de autor e os que lhe são conexos:

(...)

§ 3o Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente”.

O dispositivo acima trata sobre a violação feita por meio da internet, e somente havia sido inserido no código penal há pouco menos de 1 mês da data do crime. É necessário ressaltar que o artigo não se refere a um crime informático, mas sim da violação dos direitos autorais, tratando o paragrafo 3º de tipificação da conduta pelo meio utilizado, havendo a majoração da pena tratando-se de uma qualificadora.

A internet não somente facilitou o acesso a informações como também criou uma realidade virtual, aonde os usuários desenvolveram uma linguagem e um meio de interação própria desta realidade, fazendo com que exista um submundo obscuro, aonde direitos básicos garantidos pela constituição federal como dignidade, privacidade, igualdade foram subjugados e violados uma vez que a mão da lei ainda não alcançava esses infratores.

No Brasil, temos varias leis que surgiram com essa nova modalidade de crimes, um exemplo é a LEI Nº 12.737 apelidada de "Lei Carolina Dieckmann". Ela altera o Código Penal para tipificar como infrações uma série de condutas no ambiente digital, principalmente em relação à invasão de computadores, além de estabelecer punições específicas.

Sua redação prevê os crimes que decorrerem do uso indevido de informações e materiais pessoais, que dizem respeito à privacidade de uma pessoa na internet, como fotos e vídeos.

* 1. **CRIMES PROPRIOS E IMPRORPIOS**

Os professores Damásio de Jesus e José Antônio Milagres (2016) acrescentam que o crime virtual é um fato típico e anti-jurídicos, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou redes de computadores.

Para os autores VIANA E MACHADO, os crimes informáticos são definidos como próprios e impróprios.

Os crimes de informática próprios são aqueles que o bem jurídico tutelado pela norma penal é a inviolabilidade das informações de dados, ou seja, uma invasão a um dispositivo informático violaria os dados de proteção, o qual seria caracterizado crime próprio, além de outras condutas tipificadas.

Já os crimes informáticos impróprios são aqueles que o computador é usado como instrumento para executar o crime, mas não há ofensa contra o bem jurídico da inviolabilidade da informação.

Os crimes informáticos impróprios em sua maioria não exigem conhecimentos técnicos do uso de computadores. Seria os delitos contra a honra que pode ser cometido com um simples envio de e-mail ou mensagens para que haja o ganho de alguma vantagem. Seja ela de cunho monetário ou não, um exemplo seria envio de mensagens para extorsão, coação, ameaça, e outros afins.

**2. ESPECIES DE CRIMES CIBERNÉTICOS**

O presente capítulo será abordado com mais ênfase nos crimes virtuais impróprios diante da regularidade de suas ocorrências. Isso ocorre pelo fato de que a internet tem se tornado uma ferramenta para o anonimato, o que, em tese, estimula o descumprimento de leis.

Dentre esses, destacam-se os crimes de ódio, crimes de invasão de privacidade e intimidade, crimes de estelionato, crimes de pedofilia entre outros.

A internet tem a possibilidade de criar uma realidade onde as pessoas encurtam a distancias físicas, conectando-as como se estivessem próximas. Para que haja a participação efetiva das pessoas no “ciberespaço”, é necessário que o Estado garanta a segurança de seus direitos e garantias fundamentais, impossibilitando de novas tecnologias violarem esses direitos (PANNAIN, PEZZELLA, 2015).

**2.1 Crimes contra honra**

A honra é constitucionalmente protegida, sendo um direito fundamental (art. 5º, x, da Constituição Federal). Os crimes contra a honra são bem conhecidos no meio jurídico, além de ser considerado um direito da personalidade, tendo a proteção da dignidade pessoal do individuo e sua reputação (BARROSO,2004).

Para a doutrina brasileira, a honra se divide em objetiva e subjetiva. A objetiva se relaciona com a reputação e a fama que o indivíduo desfruta no meio social em que vive, a subjetiva esta ligada a dignidade e o decoro pessoal, ou seja, o juízo que cada indivíduo tem de si mesmo (ASSUNÇÃO,2018).

A honra objetiva pode ser chamada de objeto jurídico, sendo a reputação ou a imagem que o individuo tem perante a sociedade, enquanto a subjetiva recebe o nome de objeto material. (NUCCI 2017).

No tópico dos crimes contra a honra, encontramos na legislação penal três tipos de crimes: calúnia, difamação e injúria. Na legislação o tipo penal e as penas distinguem-se conforme observemos:

**Calúnia**

Art. 138 Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa.

**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 (BRASIL, 1940, online).

O professor Rogério Sanches (2014) explica que na calúnia e na difamação tem a presença especifica de uma conduta, imputar a alguém fato concreto e ofensivo, necessariamente falso, e no caso da calúnia definido como crime. A injúria por sua vez, trata-se de uma imputação genérica, um defeito ou algo que menospreze a vítima. Nas duas primeiras, a sua ocorrência exige que a frase desonrosa chegue aos conhecimentos de terceiros, o que é desnecessário para o tipo penal da injúria (ASSUNÇÃO 2018).

O art. 141, do CP traz em seu segundo parágrafo aumento de pena. Essa majorante tem incidência nos crimes contra a honra, ou seja, na calúnia, na difamação e na injúria. “§ 2º Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena”. (Lei nº 2.848 de 07 de Dezembro de 1940).

Por outro lado, a difamação corresponderia ao ato de descredibilizar uma pessoa publicamente, imputando-lhe algo que venha a ferir sua honra e dignidade, ocorrendo no momento em que a acusação chegue ao conhecimentos de terceiros.

Na injúria, ao contrario dos delitos anteriores, o direito tutelado é a honra subjetiva do ofendido, sendo tipificado como ofender, determinada pessoa por ação ou omissão, ofendendo sua dignidade. Nesse caso, não há regra para a imputação de fatos específicos, mas sim a conceituação negativa da vítima (ASSUNÇÃO, 2018).

É um insulto que fere a honra subjetiva de alguém, atingindo sua dignidade maculando a sua autoimagem, por vontade específica (*animus diffamandi)*, sendo consumado no momento em que o insulto chega ao conhecimento do ofendido, não importando o conhecimento de terceiros.

O uso dos computadores e das ferramentas informáticas *online,* bem comoas múltiplas possibilidades de os usuários cometerem crimes levaram o Estado a constatar que este não estava preparado de fato para julgar e punir esses potenciais criminosos, cuja ações atingem a honra de terceiros (SILVA; BEZERRA, SANTOS, 2016).

Não podemos nos esquecer de discorrer sobre a liberdade de expressão. O fundamento da liberdade de expressão está ligado diretamente a autonomia e dignidade humana, sendo necessário respeitar os direitos fundamentais da pessoa humana. As tecnologias informáticas colocam a liberdade de expressão em um novo olhar, devendo-se destacar, positivamente, o aumento de participação social, de interação cultural trazendo o acesso à uma verdadeira democracia. (PANNAIN; PEZZELLA, 2015).

A liberdade de expressão é uma ideia para a obtenção de respostas adequadas para os problemas da sociedade, por meio de um debate livre de ideias contrárias, onde prevalecem as melhores. (SARMENTO, 2018).

O conflito entre a liberdade de expressão do individuo e as condutas que ferem a honra (objetiva ou subjetiva) das vítimas. Sabe-se que a liberdade de expressão não pode ser exercida de forma totalmente livre e que é necessário estabelecer limites, ponderando o direito de se expressar com o direito de outros. Porém, nem sempre as condutas criminosas realizadas pela internet são punidas penalmente, seja pela dificuldade de se comprar o verdadeiro infrator ou pela falta de preparo do Estado para lidar com tal situação.

As condutas são motivadas pelo ódio puro e simples sem qualquer filtro social. Um caso bastante conhecido que chamou a atenção dos noticiários em 2015 foi o da Maria Júlia Coutinho, que em suas redes sociais, recebeu vários comentários racistas pelo simples fato de ter postado uma foto.

A jornalista [Maria Júlia Coutinho](http://g1.globo.com/tudo-sobre/maria-julia-coutinho) foi alvo de comentários racistas na página do [Jornal Nacional](http://g1.globo.com/jornal-nacional/index.html) no Facebook, em post publicado na noite de quinta-feira. Alguns internautas escreveram comentários racistas no post que tem uma foto de Maju, e várias pessoas saíram em defesa dela. No Twitter, ela respondeu um comentário agressivo de um internauta. Ela deu um reply e escreveu apenas: "Beijinho no ombro". [William Bonner e Renata Vasconcellos gravaram um vídeo postado no Facebook](https://www.facebook.com/JornalNacional/videos/vb.159354314154963/835593653197689/?type=2&theater) em que dão um recado, com a equipe do JN. Eles mostraram um cartaz e gritaram a "SomosTodosMaju". No Twitter, a hashtag #SomosTodosMajuCoutinho chegou ao topo dos tópicos mais comentados (G1.GLOBO.COM, 2015, *online).*

Outros crimes que são muitos conhecidos nos ambientes virtuais são os de ameaça e também os crimes contra a liberdade individual prevista no artigo 147 do Código Penal Brasileiro.

Deve-se levar em conta a individualidade da vítima ao analisar o crime de ameaça. Portanto, raça, idade, sexo, cor, opção sexual, entre outras características são levadas em consideração para se analisar se houve ou não a conduta de causar-lhe mal injusto. (CUNHA, 2014).

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.

(Código Penal Brasileiro, 1940)

Casos como esse ocorrem todos os dias, muitos por conta da homofobia, machismo, preconceitos inseridos na sociedade, etc. Após o advento da rede mundial de computadores, surgiu o *cyberbullyng,* situação que aspessoas se ofendem gratuitamente sem nenhum motivo em específico, simplesmente por acreditarem que estão em um “mundo” sem lei. No ambiente virtual, as pessoas se sentem confortáveis para se expressarem, e algumas acabam extrapolando e cometendo vários dos crimes estudados nesse tópico.

**2.2 CRIMES DE INVASÃO DE PRIVACIDADE E INTIMIDADE**

A privacidade e intimidade é um direito constitucional previsto no artigo 5º, X, da Constituição Federal.

A Lei nº 13.737 de 2012 conhecida popularmente como Lei Carolina Dickmann, foi inserida no código penal brasileiro em seu artigo 154-A, e discorre a respeito da invasão de dispositivos informáticos, *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. (CODIGO PENAL, 1940, online).

Os bens jurídicos tutelado são a intimidade, a vida privada e o direito ao sigilo de dados, sendo essencial à primeira parte do tipo penal o verbo invadir, ou seja, violar virtualmente sem autorização expressa ou tácita do titular do dispositivo, não tendo a necessidade de fazer adulterações, destruição ou obtenção de dados.

A atriz Carolina Dickman em 2011 foi vítima de um crime cibernético onde teve seu computador invadido e suas fotos intimas roubadas e expostas na rede mundial de computadores. O bem jurídico tipificado no artigo 154-A é a privacidade individual armazenada em dispositivos informáticos. A violação de seus mecanismos de segura ou instalação de dispositivo de vulnerabilidade caracteriza invasão de dispositivo informático alheio. (ASSUNÇÃO, 2018).

Pensando em uma forma mais efetiva de punição, o legislador previu em seu §3º, do artigo 154-A uma qualificadora importante, que se conecta diretamente, com a privacidade da vítima. Nessa situação, a invasão resulta em obtenção de informação sigilosa (segredos da vítima) entre outras coisas, aumentando a pena para dois a cinco anos e multa. (CAPEZ, 2016)

No mesmo sentido, o §4º aponta uma majorante do crime, que estabelece um aumento na pena “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” (CÓDIGO PENAL, 1940, *online).*

**2.3 CRIMES CONTRA A INVIOLABILIDADE DO PATRIMONIO**

Um crime que teve grande aumento nos últimos anos com a popularização dos dispositivos informáticos foi o de estelionato, o crime mais comum quando tratado o assunto de inviolabilidade patrimonial.

O artigo 171 do Código Penal prevê “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”.

O crime consuma-se com a obtenção de vantagem ilícita indevida, em prejuízo alheio. Induzir ou manter a vítima em erro é crime doloso, pois mostra claramente a vontade livre e consciente manter ou induzir alguém em erro.

A discussão na doutrina a respeito da diferença entre a fraude penal e a fraude civil é algo negativo, pois, fraude é fraude considerado como ato ardiloso de má-fé, que visa a obtenção de vantagem indevida, trazendo prejuízo a outrem. O código penal visa punir a “astúcia”, a “esperteza” daqueles que despojam a vítima de seu patrimônio (CUNHA, 2014).

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

**2.4 CRIMES CONTRA A LIBERDADE SEXUAL ENVOLVENDO MENORES.**

O estatuto da criança e adolescente prevê diversas condutas criminosas que são constantemente praticadas no ambiente virtual, as principais tipificações são dos crimes contra a liberdade sexual da criança e adolescente (CAPEZ, 2016).

Ao contrário das condutas anteriormente descritas, estas acontecem em extremo sigilo na maioria das vezes. Alguns aplicativos de celular facilitam a troca de mensagens, instantaneamente o que faz com que vários usuários compartilhem a informação sem saber que estão incorrendo, necessariamente, em crime. (CUNHA, 2014).

O artigo 241 do ECA (estatuto da criança e adolescente) e seus artigos subsequentes discorrem as condutas ilícitas envolvendo menores.

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 (ECA, 1990, *online*).

As condutas mais comuns no âmbito virtual são as do artigo 241-A e 241-B. O artigo 241-A prevê as condutas ilícitas de: Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar material que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente por meio de sistema de informática, ou qualquer outro meio.

O artigo 241-B pune qualquer um que obter por qualquer meio imagens, vídeos, filmes, fotografias ou outras formas de registros, materiais que contenham sexo explicito ou pornografia envolvendo crianças e adolescentes.

**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) (ECA, 1990, *online).*

Com relação a prática desses crimes, ao serem consumados no ambiente virtual, a jurisprudência é dura na aplicação da pena, considerando até mesmo que os crimes cometidos na rede mundial de computadores tem caráter intercontinental (NUCCI, 2016).

Com a modernização de aplicativos de mensagem instantânea a conduta do artigo 241-B tornou-se mais frequente. Os tipos penais estabelecidos nesse artigo torna a punição do agente que possui, em seu poder, imagens, vídeos, ou fotos contendo pornografia infantil ou sexo explicito envolvendo crianças e adolescentes. (ASSUNÇÃO, 2018).

A *deep web* (rede profunda) é uma “plataforma” obscura e pouco conhecida por usuários comuns da internet. É um local que para ter acesso às pessoas precisam de certa maestria no mundo dos computadores, pois é uma rede extremamente difícil de ser acessada.

A *Deep Web* não pode ser acessada por meio convencionais de pesquisas em navegadores, como o [*google*](https://www.techtudo.com.br/tudo-sobre/google.html) ou [*bing*](https://www.techtudo.com.br/tudo-sobre/bing.html). Justamente pela dificuldade de acesso, é usada para o compartilhamento de conteúdo ilegal, como venda de drogas, contratação de assassinos profissionais, vendas ilegais de armas de fogo e pedofilia.

De acordo com um estudo conduzido pela britânica University of Portsmouth, 83% do tráfego na deep web tem relação com pornografia infantil. A web oculta requer outros meios de acesso diferentes de um navegador comum, isso porque seu conteúdo não é indexado pelos mecanismos de busca padrão, se tornando um local onde crimes e violações cibernéticas são cometidos com mais frequência (PAYÃO, 2015, online).

Em 2019, uma operação da Policia Federal em conjunto com o FBI (Departamento Federal de Investigação dos Estados Unidos), deflagraram uma operação conjunta para combater os crimes praticados na deep web.

O principal alvo da ação é um cidadão israelense que vive em Brasília e é responsável por administrar um site, na zona obscura da rede, para a prática de tráfico de drogas e armas, contrabando e lavagem de dinheiro [...] O homem, preso nessa segunda-feira (06/05/2019), também é suspeito de crime de pornografia infantil e foi alvo de mandado de busca e apreensão para investigar o delito, em outubro de 2018. Na ocasião, a PF apreendeu R$ 1 milhão em espécie na residência dele em [Brasília](https://www.metropoles.com/distrito-federal/seguranca-df/policia-investiga-participacao-de-brasilienses-em-grupos-extremistas), além de notebooks e smartphones (CAIXETA, PINHEIRO, 2019, *online).*

**3. CRIMES VIRTUAIS NA LEGISLAÇÃO**

Neste capitulo será analisada a legislação vigente acerca dos crimes virtuais, bem como projetos de lei e medidas legislativas presente no nosso ordenamento jurídico, que visam tipificar as condutas criminosas e punir quem as pratica.

O ambiente virtual é bem dinâmico e está em constante ampliação e inovações tecnológicas, o que leva o legislador um considerável desafio de contemplar as pratica delitivas do ambiente virtual.

**3.1 LEGISLAÇÕES VIGENTES**

Levando em consideração a quantidade de pessoas que possuem conexão com a internet e desfrutam diariamente deste mundo virtual, é compreensível que a legislação ainda esteja em processo de desenvolvimento e atualizações constantes.

Os órgãos judiciais e investigativos ainda possuem grandes desafios e dificuldades na identificação dos sujeitos que praticam crimes no ambiente virtual, que se devem as tecnologias cambiantes que facilitam a ocultação do individuo na rede mundial de computadores.

No Brasil, em 1998, tivemos a Lei 9.609 que dispôs sobre a proteção da propriedade intelectual de programa de computador. Tal lei substituiu a Lei 7.646/87 e teve considerações inovadoras a respeito da tecnologia.

A Lei 9.609/1998 apresenta conceituação de programa de computador nos seguintes termos:

Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados. (LEI Nº 9.609, 1998, online)

A Lei ainda discorre sobre a proteção aos direitos de autoria e também sobre o registro de programas virtuais, de contratos de licença de uso, garantias aos usuários de programas de computador, comercialização e transferência de tecnologia.

O tipo penal previsto pela Lei 9.609/1998 apresenta a seguinte redação:

Art. 12. Violar direitos de autor de programa de computador:

Pena - Detenção de seis meses a dois anos ou multa.

§ 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:

Pena - Reclusão de um a quatro anos e multa.

§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.

A Lei 9.610/1998 é complementar à Lei 9.609/1998 ao discorrer à questão dos direitos autorais, porém, a primeira se aplica à tudo que for omisso, a segunda, trata-se de questão envolta à tecnologia. (SIQUEIRA, 2017).

Em razão da necessidade eminente do aprimoramento da legislação em relação aos crimes cibernéticos, o Congresso Nacional aprovou no ano de 2012, a Lei 12.737, conhecida como Lei Carolina Dieckmann que dispôs acerca da tipificação criminal de delitos informáticos e alterou o Código Penal. (BARBOSA et al, 2014).

Na época foi uma inovação legislativa, onde introduziu no Código Penal o tipo nominado “invasão de dispositivo informático”, descrita assim pela conduta:

[**Art. 154-A**.](http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm#art154a) 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 (LEI 12.737, 2012, *online)*.

Uma qualificadora muito bem colocada foi o paragrafo 2º “Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.”, hoje em dia infelizmente é muito comum ver noticias nos jornais onde empresas tiveram seu banco de dados invadido por *hackers*, e todo o seu sistema informático comprometido.

Semana passada, a Americanas S.A., detentora dos e-commerce Americanas, Shoptime, Submarino, Sou Barato e carteira digital AME, além de atuações em logística e crédito, passou pelo maior temor de todas as empresas e indústrias no mundo: ser invadida e bloqueada por hacker. Pelo número de negócios on-line, é praticamente como ser invadida no mundo real por um batalhão armado, segurando como refém o negócio por três dias. “Qualquer paralisação traz prejuízos imediatos e de longo prazo, seja na perda de receita direta, seja com imagem, reputação, processos e outros. Isso é válido para qualquer tipo de empresa, não é exclusividade da Americanas”, disse Geraldo Guazzelli, diretor-geral no Brasil da multinacional americana Netscout, uma das maiores no setor de cibersegurança, com clientes como Banco Votorantim, IBM e Nestlé. No caso da Americanas, até sua volta ao ar, a empresa perdeu 12% em valor de mercado — os papéis oscilaram de R$ 33,72 (sexta-feira, 18, véspera do ataque) para R$ 29,69 (quarta-feira, 23) e fecharam uma semana depois a R$ 32,45 (quarta-feira, 2). Os números da companhia são gigantescos, como 398,3 milhões de transações e 49,8 milhões de clientes no acumulado de 12 meses. (IVANOV, 2022, *online).*

Houve também atualizações no artigo 266 do Código Penal, pela Lei 12.737/2012, que diz sobre a “interrupção ou perturbação de serviços telegráficos, telefônicos, informáticos, telemáticos ou de informação de utilidade pública”. Pois já se previa o que poderia acontecer mais tarde.

Em novembro de 2020, o [**Superior Tribunal de Justiça**](https://pt.wikipedia.org/wiki/Superior_Tribunal_de_Justi%C3%A7a) (STJ) foi alvo de um [**ataque cibernético**](https://pt.wikipedia.org/wiki/Ataque_cibern%C3%A9tico), do tipo [*ransomware*](https://pt.wikipedia.org/wiki/Ransomware), por meio do [programa malicioso](https://pt.wikipedia.org/wiki/Malware) (*malware*) "[RansomExx](https://pt.wikipedia.org/w/index.php?title=RansomExx&action=edit&redlink=1)". Como resultado do ataque, todo o acervo de processos da Corte foi [criptografado](https://pt.wikipedia.org/wiki/Criptografia), impedindo seu acesso sem o pagamento do resgate exigido pelo criminoso. [...]  O presidente do [Supremo Tribunal Federal](https://pt.wikipedia.org/wiki/Supremo_Tribunal_Federal) e do [Conselho Nacional de Justiça](https://pt.wikipedia.org/wiki/Conselho_Nacional_de_Justi%C3%A7a), [Luiz Fux](https://pt.wikipedia.org/wiki/Luiz_Fux), determinou a criação de um comitê para elaborar soluções para proteger a Justiça de novos ataques. O ataque foi considerado como um dos mais graves já efetuados contra uma [instituição de Estado](https://pt.wikipedia.org/wiki/Poder_P%C3%BAblico) do Brasil. Em 28 de abril de 2021, o [Tribunal de Justiça do Rio Grande do Sul](https://pt.wikipedia.org/wiki/Tribunal_de_Justi%C3%A7a_do_Estado_do_Rio_Grande_do_Sul), sofreu um [ataque](https://pt.wikipedia.org/w/index.php?title=Ataque_cibern%C3%A9tico_ao_Tribunal_de_Justi%C3%A7a_do_Rio_Grande_do_Sul&action=edit&redlink=1) similar, do mesmo tipo [*ransomware*](https://pt.wikipedia.org/wiki/Ransomware), afetando cerca de 12 mil computadores e deixando vários processos inacessíveis. Investigações estão sendo conduzidas sobre o ataque (ESTADÃO, 2021, *online).*

Em 2014 foi oficialmente aprovada a Lei nº 12.956, mais conhecida como “marco civil da internet”. Trata-se de norma legal que disciplina o uso da internet no Brasil, por meio da previsão de princípios, garantias, direitos e deveres para quem faz uso da rede, bem como da determinação de diretrizes para a atuação do Estado.

A lei do Marco Civil foi criada para suprir as lacunas no sistema jurídico em relação aos crimes virtuais, num primeiro momento tratando dos fundamentos, conceitos para sua interpretação e objetivos que o norteiam, além de enumerar os direitos dos usuários, tratar de assuntos polêmicos como por exemplo a solicitação de histórico de registros, a atuação do poder público perante os crimes virtuais e por último garante o exercício do direito do cidadão de usufruir da internet de modo individual e coletivo estando devidamente protegido. (SIQUEIRA, 2017, p. 126)

Segundo SOUZA (2021) O Marco Civil da Internet tem como intenção proteger a privacidade dos usuários, buscando assegurar o sigilo e a inviolabilidade das comunicações, conforme estabelece a Constituição Federal.

A lei impõe que os provedores de internet não podem violar a intimidade dos indivíduos e a privacidade dos usuários a quem fornece acesso à rede, vedando a divulgação dos dados bem como monitorar os dados compartilhados pela rede.

No que diz respeito à intimidade do usuário, a Lei procura proteger os dados junto aos provedores, assegurando aos usuários que cancelarem os serviços de *internet* a exclusão dos dados de navegação, conforme:

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Art. 11º Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. (...)

§ 3o Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. (LEI 12.965, 2014).

A questão da privacidade é levada tão a serio que em casos excepcionais, apenas com ordem judicial, possa haver quebra do sigilo dos dados (LISBOA, LOPES, 2016).

A aprovação do Marco Civil na internet é algo de extrema relevância, pois, houve respaldo legal aos direitos fundamentais na internet, como a intimidade, dignidade e honra (SOUZA, 2021).

A LGPD (Lei Geral de Proteção de Dados) foi sancionada em 2018, entrando em vigor apenas em 2020. Inspirada na DGPR (*General Data Protection Regulation*) da União Europeia tem como objetivo proteger os dados dos usuários.

Após a vigência da LGPD, o Brasil passou a integrar a parte dos países que contam com uma legislação específica para a proteção de dados.

A lei cria um conjunto de novos conceitos jurídicos, onde gera obrigações para os provedores de dados, estabelece condições nas quais os dados pessoais devem ser tratados, define os direitos para os titulares dos dados. A lei se aplica a toda informação que tratem de dados íntimos e sensíveis, tais como saúde, religião, questões raciais ou étnicas, pensamento politico e filosófico etc...

A lei estabelece uma segurança jurídica através de regulamentação e condutas que protegem os dados pessoais dos usuários em território brasileiro. Ela define o que são dados pessoais e estabelecem quais são os de maior proteção e os mais sensíveis, entre estes os que se referem ás crianças e adolescentes.

A LGPD cria uma regulamentação para o uso, proteção e transferência de dados pessoais no Brasil, nos âmbitos privado e público, e estabelece de modo claro quem são as figuras envolvidas e quais são suas atribuições, responsabilidades e penalidades no âmbito civil – que podem chegar a multa de 50 milhões de reais por incidente. (SOMADOSSI, 2018, online).

**CONSIDERAÇÕES FINAIS**

O Presente trabalho buscou analisar o surgimento dos crimes cibernéticos e a evolução tecnológica por trás de tudo, mostrando como o Brasil vem lidando com tal situação ao longo dos anos. Faz necessário abordar as tipicidades das principais condutas ilícitas praticadas no âmbito virtual. Bem como as principais medidas no combate aos crimes cibernéticos.

Verifica-se que a legislação brasileira não consegue acompanhar a evolução dos crimes cometidos na rede mundial de computadores, sendo necessário cada vez mais legislações específica e eficaz.

Diante das análises feitas ao longo do trabalho, percebe-se a extrema relevância do estudo à temática dos crimes virtuais. O cibercrime vem aumentando demasiadamente à medida que a tecnologia e internet vai se expandindo e se tornando cada vez mais popular.

Com a constante evolução no mundo virtual o ordenamento jurídico Brasileiro deve estar sempre em constante evolução para que assim contemple todas as condutas criminosas no ambiente virtual.

**CYBERCRIME**

**ABSTRACT**

In this work, the historical and conceptual aspects of cyber crimes will be addressed, as well as some general notions of cybercrime and an explanation of the current Brazilian laws that deal with the subject. Nevertheless, the focus of the present research is a study on the origin and evolution of cyber crimes, as well as the repercussions of attacks on the honor and image of an individual through this global means of communication and the challenges to punish cybercriminals. The chapters of this research will bring an analysis of works related to the theme of renowned authors and scholars in the academic environment. Finally, possible solutions will be presented to the question of the work, which refers to possible ways to curb the attack of cybercriminals.

**Keywords:** cybercrime. Internet. Legislation. Species. Cyber ​​crimes.

**REFERÊNCIAS**

ASSUNÇÃO, Ana Paula Souza. **CRIMES VIRTUAIS**. Disponível em: <repositorio.aee.edu.br/bitstream/aee/538/1/Monografia>. Acesso em 12 out. 2021.

CAIXEITA, Fernando, PINHEIRO, Mirelle. **Ação da PF com FBI prende morador do DF que usava dark web para crimes.** Disponível em: <https://www.metropoles.com/distrito-federal/seguranca-df/acao-da-pf-com-fbi-prende-morador-do-df-que-usava-dark-web-para-crimes>. Acesso em: 20 fev. 2022.

CAMPOREZ, Patrik. PIRES, Breno. **Ataque hacker trava 12 mil julgamentos e paralisa atividades no STJ.** Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/stj-diz-ter-sofrido-ataque-hacker-durante-julgamentos-e-manda-pf-investigar/>. Acesso em : 15 jan. 2022.

CAPEZ, Fernando Prado. **Código Penal Comentado**. São Paulo: Saraiva, 2016.

**DECRETO-LEI No**[**2.848, DE 7 DE DEZEMBRO DE 1940**](http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/DEL%202.848-1940?OpenDocument). Código Penal Brasileiro. Disponível em: <http://www.planalto.gov.br/ccivil\_03/decreto-lei/del2848.htm>. Acesso em 02 mar. 2022.

D’URSO, Luiz Augusto Filizzola. **Cibercrime: perigo na internet**. Disponível em: < https://politica.estadao.com.br/blogs/fausto-macedo/cibercrime-perigo-na-internet/>. Acesso em 15 nov. 2022.

FILHO, Eduardo Tomasevicius. **Marco Civil da Internet: uma lei sem conteúdo normativo**. Estud. av., São Paulo , v. 30, n. 86, p. 269- 285, Abr. 2016. Disponível em <https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?lang=pt.> Acesso em: 01 fev. 2022.

GOMES, Helton Simões. **Brasil tem 116 milhões de pessoas conectadas à internet, diz IBGE**. Disponível em <https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml> . Acesso em: 13 nov. 2021.

GUIMARÃES, Keila. **Os crimes dos hackers que interrompem até quimioterapia em sequestros virtuais de hospitais.** Dispoível em: <https://www.bbc.com/portuguese/brasil-40870377> . Acesso em 20 nov. 2021.

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

[**LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.**](http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2012.737-2012?OpenDocument) Código Penal Brasileiro. Disponível em: <http://www.planalto.gov.br/ccivil\_03/\_ato2011-2014/2012/lei/l12737.htm>. Acesso em 24 nov. 2021.

[**LEI Nº 12.965, DE 23 DE ABRIL DE 2014**](http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2012.965-2014?OpenDocument). Marco Civil da Internet. Disponível em: <http://www.planalto.gov.br/ccivil\_03/\_ato2011-2014/2014/lei/l12965.htm>. Acesso em 08 mar. 2022.

**LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.** Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil\_03/\_ato2015-2018/2018/lei/l13709.htm>. Acesso em 08 de mar. 2022.

MILAGRE, José Antônio. **Lei Azeredo, AI-5 digital e a cultura do contra**. Disponível em: <https://jus.com.br/artigos/13211/lei-azeredo-ai-5-digital-e-a-cultura-do-contra>. Acesso em: 15 jan. 2022.

NUCCI, Guilherme de Souza. **Manual de direito penal**. Rio de Janeiro: Forense, 2014.

PANNAIN, Camila Nunes; PEZELLA, Maria Cristina. **Liberdade de expressão e *Hate Speech* na Sociedade da Informação.** Disponível em: <https://periodicos.ufsm.br/REDESG/article/view/19432/pdf>. Acesso em: 14 jan. 2022.

PAYÃO, Felipe. **Estudo: mais de 80% da navegação na deep web é relacionada à pedofilia.** Disponível em: <https://www.tecmundo.com.br/internet/70985-estudo-80-navegacao-deep-web-relacionada-pedofilia.htm> . Acesso em 14/ nov. 2021.

PAESANI, Liliana Minardi. **DIREITO E INTERNET - LIBERDADE DE INFORMAÇÃO, PRIVACIDADE E RESPONSABILIDADE CIVIL.** São Paulo. EDITORA ATLAS S.A. 2000.

RUBINSTEINN, Gabriel. **Criminosos roubam R$6,3 bilhões em criptomoedas; Ethereum é principal alvo.** Disponível em: <https://exame.com/future-of-money/criminosos-roubam-r63-bilhoes-em-criptomoedas-ethereum-e-principal-alvo/>. Acesso em: 13 dez. 2021.

ROCHA, Adriano Aparecido. **CIBERCRIMINALIDADE OS CRIMES CIBERNÉTICOS E OS LIMITES DA LIBERDADE DE EXPRESSÃO NA INTERNET.** Disponível em < https://www.faef.br/userfiles/files/23%20-%20CIBERCRIMINALIDADE%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20NA%20INTERNET.pdf>. Acesso em 09 dez. 2021.

SARMENTO, Daniel. **A Liberdade de Expressão e o Problema do *Hate Speech.*** S/D. Disponível em < http://www.dsarmento.adv.br/content/3-publicacoes/19-a-liberdade-de-expressao-e-o-problema-do-hate-speech/a-liberdade-de-expressao-e-o-problema-do-hate-speech-daniel-sarmento.pdf> Acesso em 11 dez. 2021.

SOUZA. Mykaelly. **CIBERCRIMES E OS REFLEXOS NO DIREITO BRASILEIRO.** Disponível em: < https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/2659/1/TCC%20-%20MYKAELLY%20SOUZA%20.pdf>. Acesso em: 13 mar. 2022.

SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallaz Tomaz. **Relações Jurídicas Virtuais: Análise de Crimes Cometidos com o Uso da Internet.** Disponível em: < https://periodicos.unicesumar.edu.br/index.php/revcesumar/article/view/3952/2787>. Acesso em: 28 dez. 2021.

SILVA*,* Leonardo Werner*.***Internet foi criada em 1969 com o nome de “Arpanet” nos EUA*.*** Disponível em:*<*https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml.>. Acesso em: 14 nov. 2021.

VIANA, Túlio. MACHADO, Felipe. **CRIMES INFORMÁTICOS CONFORME A LEI Nº 12.737/2012.** Belo Horizonte. Editora Fórum. 2013.