



**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS  
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO  
NÚCLEO DE PRÁTICA JURÍDICA  
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO  
PROJETO DE TRABALHO MONOGRAFIA JURÍDICA**

**CRIMES CIBERNÉTICOS  
BREVES CONSIDERAÇÕES**

**ORIENTANDO: AMANDA CARDOSO DA SILVA  
ORIENTADOR: PROF. DR. JOSÉ QUERINO TAVARES NETO**

**GOIÂNIA**

**2022**

**AMANDA CARDOSO DA SILVA**

**CRIMES CIBERNÉTICOS  
BREVES CONSIDERAÇÕES**

**Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito, Comunicação e Negócios, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS). Prof. Orientador: Dr. José Querino Tavares Neto.**

**GOIÂNIA**

**2022**

Dedico este trabalho a Deus pai que tanto iluminou os meus caminhos e os meus pensamentos fazendo com que chegasse até aqui; à minha família, em especial aos meus pais, e ao meu filho, Anthony Bernardo, que também foram de grande importância nesta minha caminhada.

## **AGRADECIMENTOS**

Agradeço a Deus por ter me dado a graça de estar com saúde e disposição para que eu pudesse galgar mais um degrau em minha vida pessoal e profissional através de um curso superior.

Aos meus pais por terem me orientado na vida de maneira a sempre buscar as coisas boas e fazer o bem aos meus semelhantes.

Ao meu filho que amo muito e a minha família por sempre acreditarem em mim, no meu esforço e no que eu poderia alcançar na vida. Aos meus amigos que sempre serviu de estímulo para estudar.

## Sumário

<b>RESUMO</b> .....	7
<b>ABSTRACT</b> .....	7
<b>INTRODUÇÃO</b> .....	8
<b>JUSTIFICATIVA</b> .....	9
<b>OBJETIVO</b> .....	10
<b>OBJETIVO GERAL</b> .....	10
<b>OBJETIVO ESPECÍFICO</b> .....	10
<b>PROBLEMA</b> .....	11
<b>METODOLOGIA</b> .....	11
<b>1 CRIMES CONTRA A HONRA</b> .....	11
<b>1.2 ESPIONAGEM ELETRÔNICA</b> .....	12
<b>1.3 CRIMES CIBERNÉTICO NO MUNDO</b> .....	12
<b>1.4 CRIMES CONTRA INDIVÍDUO</b> .....	13
<b>1.5 CRIMES CONTRA A SOCIEDADE</b> .....	13
<b>1.6 CRIMES POR MEIO ELETRÔNICO</b> .....	13
<b>2 COMO AGIR AO SER VÍTIMA DE UM CRIME</b> .....	13
<b>2.1 ESTELIONATO</b> .....	14
<b>2.2 INVASÃO DE PRIVACIDADE</b> .....	14
<b>2.3 CRIMES VIRTUAIS</b> .....	14
<b>2.4 DANO INFORMÁTICO</b> .....	15
<b>2.5 LIBERDADE DE EXPRESSÃO</b> .....	16
<b>2.6 ABUSO SEXUAL</b> .....	16
<b>2.7 RACISMO E INJÚRIA</b> .....	17
<b>3 AÇÃO PENAL</b> .....	18
<b>3.1 LEI 12.737/12. CAROLINA DIECKMANN</b> .....	19
<b>3.2 MARCO SILVA</b> .....	20
<b>4 DA CLASSIFICAÇÃO DOS CRIMES</b> .....	20
<b>4.1 CRIMES CIBERNÉTICOS PUROS</b> .....	20
<b>4.2 CRIMES CIBERNÉTICOS IMPUROS</b> .....	21
<b>4.3 PRINCÍPIO DA INOCÊNCIA</b> .....	21
<b>4.4 PRINCÍPIO DA LEGALIDADE</b> .....	21
<b>4.5 LAVAGEM DE DINHEIRO</b> .....	21
<b>4.6 ROUBO</b> .....	22
<b>4.7 PORNOGRAFIA INFANTIL</b> .....	22
<b>CONSIDERAÇÕES FINAIS</b> .....	26

**REFERÊNCIAS** .....27

## **RESUMO**

O objetivo do presente trabalho é estudar a prática do crime cibernético, seu impacto social e as soluções que nosso governo encontrou para prevenir e combater o crime correspondente. Para tanto, descreve brevemente o surgimento e o desenvolvimento da Internet global. Em seguida, lança luz sobre a história e a evolução legislativa do cibe crime, com foco no desenvolvimento da legislação brasileira. Por fim, analisa e discute as diversas seitas que definem os crimes fictícios, identifica os principais programas que servem como ferramentas para a prática ilícita e os principais autores desses crimes.

**Palavras-Chaves:** Crimes Cibernéticos. Internet.

## **ABSTRACT**

The objective of the present work is to study the practice of cyber crime, its social impact and the solutions that our government has found to prevent and combat the corresponding crime. To do so, it briefly describes the emergence and development of the global Internet. It then sheds light on the history and legislative evolution of cybercrime, focusing on the development of Brazilian legislation. Finally, it analyzes and discusses the various sects that define fictitious crimes, identifies the main programs that serve as tools for illicit practice and the main authors of these crimes.

**Key words:** Cybercrime.

## INTRODUÇÃO

“A justiça não consiste em ser neutro entre o certo e o errado, mas em descobrir o certo e sustentá-lo, onde quer que ele se encontre, contra o errado”.

Theodore Roosevelt

Vivemos em uma era tecnológica moderna e acessível, onde grandes populações utilizam inúmeros meios tecnológicos para diferentes formas de comunicação, muitas vezes tornando sua vida privada inimaginável. A comodidade que o mundo globalizado nos oferece, além de algumas vantagens, também nos coloca em uma posição um tanto quanto vulnerável. A um atendimento que o mundo globalizado nos oferece, além de algumas vantagens, também nos coloca em posição quanto ao mundo vulnerável. Ainda há um longo caminho a percorrer para coibir tal comportamento, mas uma forma prática de começar a combater esses crimes é educar esses usuários.

Por esse motivo, é muito importante entendermos os possíveis cenários que podem nos expor às ações de ciber criminosos que usam a tecnologia para cometer vários tipos de crimes e quão graves podem ser as consequências. A superexposição deliberada dessas vítimas. Além disso, é importante conhecer os crimes mais comuns cometidos por esses infratores e as leis que buscam dar proteção jurídica a quem sofre com esses crimes, como a Lei de Crimes Cibernéticos (12.737/12), a Lei Marco Civil (12.965/14) e a Lei Geral de Proteção de Dados (13.709/18).

Além disso, é importante conhecer os crimes mais comuns cometidos por esses infratores e as leis que buscam dar proteção jurídica a quem sofre com esses crimes, como a Lei de Crimes Cibernéticos (12.737/12), a Lei Marco Civil (12.965/14) e a Lei Geral de Proteção de Dados (13.709/18). Crimes de cunho pessoal são muito comuns em troca de dados sequestrados, como violação de sistemas de segurança.

Nesse mundo virtual onde o crime ganha novas formas, vale também explorar alguns dos direitos fundamentais garantidos pela Constituição Federal de 1988, incluindo a liberdade de expressão e suas restrições à livre expressão de ideias, opiniões e críticas, dentro e fora a Internet, e A proteção da dignidade humana, que sustenta a inviolabilidade dos direitos e valores individuais.

Considerando a importância de educar os usuários sobre formas de ter mais cautela em alguns programas cibernéticos perigosos, o presente trabalho visa explorar os

efeitos negativos da superexposição às redes sociais, onde os ciberdelinquentes encontram cada vez mais terreno fértil para operações mais complexas. Bem como uma introdução aos crimes cibernéticos mais comuns, as leis que tentam suprimi-los e as restrições à liberdade de expressão neste contexto.

O estudo, portanto, fez sentido pela necessidade de explorar o fenômeno da superexposição e como essa tendência está se tornando um problema crescente, comprometendo a vida dos expostos e daqueles ao seu redor. Essa situação exige maior cautela e atenção do povo e do país para que nosso ordenamento jurídico possa enfrentá-la nas novas circunstâncias.

O desenvolvimento deste trabalho está dividido em três capítulos principais, sendo que o primeiro abordará os perigos da superexposição nas redes sociais e o seu impacto na vida das pessoas. A segunda parte apresentará alguns dos crimes cibernéticos mais comuns, os procedimentos para buscar proteção da justiça e a legislação promulgada para coibir esses crimes e, por fim, a terceira parte propõe uma discussão sobre a trajetória do direito à liberdade de expressão e suas consequências. Restrito na salvaguarda da dignidade humana.

## **JUSTIFICATIVA**

O objetivo deste artigo é examinar os principais crimes cometidos por meio da Internet e mostrar a importância de estes terem um tipo específico, visto que a ausência desse tipo é encontrada no ordenamento jurídico \*brasileiro hoje, criando uma lacuna legislativa que incentiva a continuidade da Internet. Comportamento criminoso. Portanto, é difícil punir quem se aproveita da falta de previsão legal. É claro que a legislação vigente está desatualizada, por isso a importância deste estudo também é mostrar que embora a lei sempre tenha tentado acompanhar a evolução de toda a história social, muitas vezes foi encontrada em seu tempo e assim falhou muitas vezes. Os avanços tecnológicos interferem. Diretamente no comportamento humano, de que a Internet é um exemplo. As vantagens que a web nos oferece são infinitas, mas com elas também vêm os riscos de segurança digital que são suportados pelos usuários. Ciberataques contra honra, calúnia, difamação e intimidação são cada vez mais comuns, e um dos principais catalisadores é o desconhecimento do usuário.

É de fundamental importância que os usuários conheçam os riscos e, sobretudo, saibam identificá-los, só assim poderão ser mais eficazes no combate ao ciber

crime. Uma das maiores preocupações ao usar a Internet é que muitos usuários pensam que não têm chance, que seu dispositivo é apenas um entre milhares e dificilmente será alvo de hackers. Você deve saber que, mesmo navegando no mundo virtual, tudo o que acontece lá é real, a informação é real e os riscos também.

A pesquisa deste livro é comprovada porque o autor queria tornar mais fácil para os usuários identificarem os riscos que enfrentam, para que possam evitar ataques. Também será capaz de medir o nível atual de compreensão da população da área e, assim, indicar aos governos quais ações preventivas precisam ser tomadas para difundir a ideia de comportamento seguro pelo mundo. Internet.

### **OBJETIVO**

Demonstrar o conceito de boas práticas no uso da Internet e avaliar o nível de conhecimento das pessoas sobre os riscos de segurança associados ao uso da Internet.

O direito está diretamente relacionado à sociedade e sua evolução e, à medida que a sociedade se desenvolve, o direito é projetado para acompanhá-la. Portanto, com o avanço da tecnologia, é necessário proteger as vítimas de crimes que existem há muito tempo no ambiente virtual por meio de leis. Este artigo tentará verificar o método de análise do crime virtual, encontrar sua autoria, suas características e sua evolução histórica.

### **OBJETIVO GERAL**

O direito está diretamente relacionado à sociedade e sua evolução e, à medida que a sociedade se desenvolve, o direito é projetado para acompanhá-la. Portanto, com o avanço da tecnologia, é necessário proteger as vítimas de crimes que existem há muito tempo no ambiente virtual por meio de leis. Este artigo tentará verificar o método de análise do crime virtual, encontrar sua autoria, suas características e sua evolução histórica.

### **OBJETIVO ESPECÍFICO**

Este trabalho tem como objetivos específicos:

- a) Descrever os tipos de ataques da atualidade;
- b) Demonstrar formas de prevenção para esses ataques;
- c) Exemplificar quais as boas práticas de utilização da Internet;

## **PROBLEMA**

Implícito neste tema na ausência de uma classificação legal dos crimes cometidos por meio da telemática, trata-se de uma lacuna legislativa que favorece a continuidade da prática criminosa, pois não há punição correspondente ao crime cometido. Portanto, enquanto houver omissões na legislação penal, os atos criminosos praticados da forma acima não constituem crimes. Desta forma, o agente que praticar este tipo de crime terá o benefício\* da impunidade, uma vez que é válido no direito penal brasileiro, não há crime sem a definição legal anterior, e não há pena da lei anterior. Comissão, ou seja, não pode penalizar ou impor qualquer sanção a condutas não especificamente criminalizadas pela lei penal não o considerem explicitamente um criminoso.

## **METODOLOGIA**

A metodologia de pesquisa que será utilizada no desenvolvimento desta pesquisa será dedutiva, partindo de uma análise histórica do surgimento dos crimes virtuais, sua conceituação e os crimes que ocorrem no meio cibernético. Ressalta-se que o método dedutivo tem como objetivo de explicar o conteúdo das premissas, através de uma cadeia de estudo em ordem descendente, partindo-se dos conceitos gerais aos particulares, no intuito de alcançar uma conclusão final. Este estudo se desenvolverá a partir de uma pesquisa teórica acerca do assunto, levantamentos bibliográficos, revistas, revistas eletrônicas, artigos, entre outros recursos que serão amplamente explorando.

Uma abordagem comparativa também será aplicada, pois as diferenças entre a legislação nacional e internacional serão analisadas para comparar as linhas de raciocínio existentes descritas acima, levando o leitor técnico ou leigo a uma melhor compreensão do pânico que pretendemos aprofundar.

## **1 CRIMES CONTRA A HONRA**

Qualidades físicas, morais e intelectuais de um indivíduo são sua honra. A honra deve ser protegida pois é um patrimônio que a pessoa possui.

A honra do indivíduo é subjetiva, construída por sentimentos próprios de respeito, de moral de atributos intelectuais e por alguns outros elementos.

Crimes contra a honra estão previsto no código penal brasileiro e estes são os crimes mais comuns cometidos através da internet.

O crime de difamação é um dos crimes contra a honra, este está definido no artigo 139 do código penal: Difamar alguém, imputando-lhe fato ofensivo á sua reputação:

Pena- Detenção, de 3 meses a 1 ano e multa.

### **1.1 ESPIONAGEM ELETRÔNICA**

Atualmente, a utilização de tecnologias da informática por pessoas é acrescenta, com isso também cresce a dependência das empresas, o que eleva o tempo de conexão de ambas as situações a rede mundial de computadores, ocasionados o lançamento elevado de informação estratégias e pessoas nos servidores empresária. Essa prática aumenta a necessidade de prevenção e monitoramento da segurança da indenização.

O código penal não típico de forma específica o crime de espionagem eletrônica. Sendo que a conduta este definida no código penal em seus artigos 154 e 154.

### **1.2 CRIMES CIBERNÉTICO NO MUNDO**

No âmbito internacional, por meio de múltiplos organizamos multilaterais, buscou- se definir e delimitar os crimes cibernéticos, onde a primeira legislação conhecida sobre o assunto foi a realização pela OCDE (Organização para cooperação e desenvolvimento Econômico) em 1983, intimada crimes informáticos análise dos regulamentos legais.

A referida carta delineou a legislação existente naquela época e fez algumas recomendações para os estados membros seguirem, as quais foram refletidas em umas listas contento exemplos de uso indevido de tecnologia. Tais como falsificações e fraudes eletrônico, produção de programas eletrônico, espionagem de computadores, uso autorizado de computadores, entre outros, que devem ser proibidos e sancionados na legislação penal interna de cada país.

### **1.3 CRIMES CONTRA INDIVÍDUO**

Os crimes cibernéticos cometidos contra pessoas físicas incluem crimes como transmissão de pornografia infantil, assédio de qualquer pessoa com o uso de computador, como e-mail, difamação cibernética, posição indecente, extorsão de rede, código maliciosos, tráfico, distribuição, publicação, fraude no cartão de crédito, disseminação de material obsceno, pirataria.

### **1.4 CRIMES CONTRA A SOCIEDADE**

O quarto tipo de crimes cibernéticos está relacionado aos crimes contra a sociedade. Incluem-se nesta categoria falsificação, terrorismo cibernético, pornografia infantil, crimes financeiros, venda de artigos ilegais, extorsão na rede, contrabando cibernético, manipulação de dados, bombas lógicas, estelionato, notas de moedas falsificadas, selos de receita, folhas de marcação etc. Podem ser falsificação usando computadores e impressora de alta qualidade. Os hackers da web obtêm acesso e controle sobre o site de outra pessoa, mesmo que alterem o conteúdo do site para cumprir objetivos ou por dinheiro.

### **1.5 CRIMES POR MEIO ELETRÔNICO**

Verificar condutas criminosas que se propagam pela internet é uma tarefa delicada, pois é difícil localizar onde o agente que efetuou o crime se encontra, pois, a prática destes delitos não encontra barreiras pela internet e circulam livres pelo sistema Global de comunicação mundial.

A maioria destas ações delituosas ocorrem tanto pela rede quando pelo mundo real, porém alguns crimes têm certas peculiaridades o que torna necessário uma Adequação quanto ao seu tipo penal.

## **2. COMO AGIR AO SER VÍTIMA DE UM CRIME**

Cada tipo de crime tem uma maneira de agir ao ser uma vítima, mas basicamente todas compreendem coletar o máximo de evidências possíveis relacionadas ao crime praticado em questão, e ser dirigido imediatamente a uma delegacia especializada, para que seja registrado um boletim de ocorrência caso não haja, procure a delegacia mais próxima. Ressalta-se que, caso o crime se trate de divulgação de imagens íntimas ou

ofensas no Google, a vítimas deve evitar um pedido de remoção de pesquisas para o Google e aguardar para que estas sejam retiradas do ar.

## **2.1 ESTELIONATO**

Uma vez que o criminoso se utiliza na internet para obter vantagens e realizar golpes contra um usuário. Este criminoso almeja primeiramente a confiança do usuário, para obter dados pessoais e delicado do mesmo, com o intuito de desviar seus recursos, ou fazer com que ele confie nele a ponto de transferi-lo determinado valor em espécies ou crédito.

Estes golpes são bastante praticados no mundo virtual, sendo que a qualquer momento podemos ser vítimas de tal crime sendo que um dos exemplos praticados em nosso dia- a – dia, que pode estar acontecendo em nossa frente, São a venda de veículos no meio virtual e os sites de relacionamento.

## **2.2 INVASÃO DE PRIVACIDADE**

O crime de invasão pode ser classificado como: delito comum, pois pode ser praticado por qualquer pessoa; plurissubsistente, uma vez que se consome através de vários atos, comissivo, pois decorre da atividade de “instalar”, “invadir”, formal, pois a consumação independe de resultado, instantâneo, pois ocorre no momento da violação do dispositivo.

O bem jurídico tutelado pela norma é a liberdade individual e a privacidade que engloba o sigilo, a intimidade e a vida privada, consistente na proteção de dados e informações armazenadas em dispositivo informático.

Invasão de Privacidade acontece por Exemplo: Celulares, computadores, discos externos, smartphones, pen-drives etc.

## **2.3 CRIMES VIRTUAIS**

Comprar, vender, jogar, se relacionar, trabalhar, a internet moderna proporciona aos seus usuários a interação em tempo real, ferramentas com e-mail e chat que são constantemente utilizados de forma prática e rápida por todos usuário da rede. Da mesma forma, a navegação web e os games podem proporcionar lazer e acesso à educação

de forma interativa. Em crimes definidos como Fraude Virtual, a conduta aplicada é a de invasão, modificação ou alteração, adulteração em sistema de processamento de dados ou supressão de dados eletrônicos ou programas. O CERT-BR (Centro de estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil) diz que fraude eletrônica se dá por: Mensagem não solicitada afim de se passar por instituição conhecida ou ainda a mensagens que induzem o usuário a instalar de códigos de origem duvidosa. Fraudes virtuais possuem duas modalidades: As fraudes externas, onde quem comete a fraude não tem vínculo direto com o local a ser fraudado e a fraude interna que é cometida por aquele infrator que está dentro do local a ser fraudado seja ele um morador ou empregado ou mesmo um terceiro que esteja prestando serviço ou de passagem pelo local. Na prática dos crimes envolvendo fraudes virtuais, o usuário é induzido a fornecer seus dados financeiros ou pessoais. Parte das ações atualmente praticadas, os fraudadores tentam através das redes sociais maneiras de convencer usuários a fornecer dados pessoais.

## **2.4 DANO INFORMÁTICO**

O código penal brasileiro prevê o crime, em seu artigo 163, que versa: Art. 163: destruir, inutilizar ou deteriorar coisa alheia: Pena – detenção, de um a seis meses, ou multa.

No código penal brasileiro, o legislador protege o dano a “coisa” seja ela móvel ou imóvel conduta “coisa” denota algo que pode ser tocada, ou seja real. A época da elaboração do artigo 163 do cp o legislador não considerou o dano informático e atualmente ao aplicar a conduta do agente a conduta é relacionada a algo tangível como por exemplo computadores, servidores, pen-drives, conduto não há a deterioração destes, mas sim nós dados e informações eletrônicas nele contidos.

Não se pode aqui falar em uma interpretação analógica, o que não poderia ser feito, tendo em vista o princípio da legalidade, que proíbe a utilização de analogia do direito penal em situações que tragam prejuízos ao agente de conduta.

É impossível algo que é imaterial como material e hoje quando alguém pratica um dano informático a um terceiro mesmo que de forma dolosa este agente não tem conduta específica típica.

## **2.5 LIBERDADE DE EXPRESSÃO**

A liberdade de expressão está ligada ao direito de manifestação do pensamento, possibilidade de o indivíduo emitir suas opiniões e ideias ou expressar atividades intelectuais, artísticas, científicas e de comunicação, sem interferência ou eventual retaliação do governo. O artigo 19 da Declaração Universal dos Direitos Humanos define esse direito como a liberdade de emitir opiniões, ter acesso e transmitir informações e ideias, por qualquer meio de comunicação.

Importa ressaltar que o exercício de ambas as liberdades não é ilimitado. Todo abuso e excesso, especialmente quando verificada a intenção de injuriar, caluniar ou difamar, pode ser punido conforme a legislação Civil e Penal. A liberdade de expressão é um direito humano, protegido pela Declaração Universal dos Direitos Humanos, de 1948, e pelas constituições de vários países democráticos.

Segundo o artigo XIX da Declaração Universal dos Direitos Humanos:

“Todo ser humano tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras”.

## **2.6 ABUSO SEXUAL**

Assim, em termos legais, o conceito de abuso sexual costuma ser Inserção quando o pedófilo está envolvido. O ato criminoso de coagir ou coagir uma criança satisfaça seus desejos, que podem ser encontrados no direito penal, especificamente para a chave menor de 14 (quatorze). Comentário ao Código Penal Seção 218. “Seduz desejos sexuais em menores de 14 (catorze) outro”. O artigo 218-A do Código Penal também prevê os seguintes indivíduos: Cometer qualquer ato obsceno na presença de um menor, ou induzir um menor a testemunhar neste caso, para satisfazer o desejo próprio ou alheio: “Praticar, estar presente Menor de 14 (quatorze) anos, ou induzi-lo a presenciar relação sexual ou Outro ato indecente para satisfazer os desejos próprios ou de outrem. “Também vale a pena notar que o abuso sexual vai além da relação sexual. Qualquer conduta lasciva de um indivíduo envolvendo uma criança concorre com punição Representado pelo Código Penal, conforme consta no artigo 217-A: “As relações sexuais ou outra conduta indecente com menor de 14 (quatorze) anos. ” Deve-se notar que o abuso sexual de

crianças pode ser também com olhares, conversas com propostas maliciosas, ou qualquer tipo de mídia, um tema que será discutido posteriormente. Aqueles também as contribuições, seja por omissão ou divulgação, estão sujeitas às mesmas sanções legais.

## **2.7 RACISMO E INJÚRIA**

Antes de conceituar o que é racismo no aspecto sociológico e jurídico, dele esclarecer qual o significado e a origem da classificação da palavra raça, e suas diferenças em relação à etnia e cor. Nota-se nos dias atuais, que a população, ou até mesmo muitos meios de comunicação social, empregam o termo raça com o mesmo significado de etnia e cor. Consta-se que o termo raça veio do vocabulário italiano *razão*, que por sua vez veio do latim *rate* que tem como significado sorte, espécie ou categoria. Verifica-se que em um primeiro momento o termo raça foi usado para classificação de animais e vegetais. Data-se que a primeira classificação étnica para seres humano registrada foi apresentada por Lineu, no século XVIII, conhecido como fundador da taxonomia, e dentro dessa classificação, abordava-se todos os tipos de seres vivos conhecidos. Lineu criou a designação do termo *homo sapiens* e subdividiu a espécie humana em quatro raças, sendo elas europeus (branco, sério e *speciality*), asiáticos (amarelo, melancólico e Preguiçoso), americanos (vermelho e mau temperamento) e africanos (preto, impassível e preguiçoso). Depois surgiram várias classificações, como Caucásico, Mongol, Etíope, americano e Malaio, baseadas em aspectos físicos. Porém, constata-se que as características físicas, revelam-se imprecisas quanto a uma definição exata da origem das diferentes raças do planeta<sup>32</sup>. Pesquisas apontam relações entre os tipos físicos de diferentes partes do planeta, sobre isso Eliane Azevedo, discute africanos e australianos não diferem quanto à cor da pele, mas apresentam a textura dos cabelos completamente diferente; europeus do Norte e europeus do centro têm a mesma cor da pele, mas têm índices cefálicos diferentes; europeus do Norte e africanos têm a cor da pele diferente, mas são iguais quanto ao índice cefálico. No século XVIII, conhecido como século das luzes, porque que fora a época que houve a revolução nos conhecimentos da humanidade pelos filósofos, até então concentrados nas mãos da igreja católica. Muitos filósofos debateram qual o conceito de evolução das raças em uma maneira racional, saindo do religioso. Nesse momento muitos abandonam as antigas teorias religiosas e monárquicas, para seguirem um novo campo de estudo, mais tarde chamada de História Natural, que posteriormente renomeada de

Biologia e Antropologia Física. Já no século XX, devido aos progressos da ciência e da tecnologia descobriu-se que alguns fatores genéticos eram mais precisamente herdados por Genéticas de sangue, do que por grupos raciais. Não obstante, constata-se que certas Doenças hereditárias eram encontradas mais em determinados grupos do que em Outros. Verifica-se que, identificadores genéticos de dois indivíduos de uma mesma Raça podem ser mais distantes, do que em relação a indivíduos de outras raças, a Exemplo um nigeriano pode ter características genéticas mais parecidas que um sueco, do que um congolês. Totem, nota-se que não existem raças puras, visto que a origem do ser vivo é Comum, sobre isso Eliane Azevedo destaca “Mesmo que esses grupos humanos Ficassem absolutamente isolados uns dos outros, eles jamais seriam puros em relação Uns aos outros, porque todos provêm de origem comum”. Observa-se que conceitos de raça pura como Hitler abordava em seus Discursos, e que foi muito usado em séculos passados é um mito, basta atentar que dos genes são iguais em todas as raças e que 30 que variam, o que zilches fazem iguais em Suas características básicas. Nesse sentido o Geneticista Bruce Wallace discorre. Não há nenhuma verdade na velha noção de raça “pura”, raças puras não Existem e quem quer que pense que existam está acreditando em bobagem. Como todos zilches membros de uma população diferem geneticamente, esta deve portanto, a definição mais correta de raça, que pode ser usada nos dias de hoje, é que raça é associada a aspectos biológicos, como características morfológicas, Como cor da pele, estatura, traços físicos etc. Vale ressaltar que uma raça pode não ser permanente, podendo-se moldar conforme a evolução da humanidade, ou seja, algum Membro de um determinado grupo ao se relacionar com alguém de culturas, origens, Línguas e traços diferentes, pode dar origem a uma nova raça. Por conseguinte, observa se que o conceito de raça, no aspecto biológico, é uma ideia imprecisa, e de difícil Delimitação.

### **3. AÇÃO PENAL**

Procedimentos criminais Arte. 154-B. Crime definido no art. 154-A, que só pode ser praticado por representante, salvo se o crime for dirigido contra a administração pública direta ou indireta de qualquer governo federal, estadual, distrital ou municipal ou contra franqueado de serviço público. “Arte. Terceira arte. Artigos 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, em vigor, com a seguinte redação: Interrupção ou interrupção de serviços de telégrafo, telefone, computador, telemática ou informações de serviços públicos Arte. 266. § 1º Incorrerá nas

mesmas penas quem interromper serviços telemáticos ou informações de utilidade, ou impedir ou dificultar sua reconstrução. § 2º Se o crime for cometido no contexto de calamidade pública, incide pena em dobro. ” (NR)

### **3.1 LEI 12.737/12. CAROLINA DIECKMANN**

A Lei 12.737/12, conhecida como Lei Carolina Dieckmann trouxe à esfera correcional normatização para invasão de informações em computadores e outros equipamentos eletrônicos. Necessário é tratar este assunto por todos ziches membros da sociedade acadêmica ou não, para portar-se de forma coesa e ter conhecimento e respaldo jurídico. Este artigo irá apresentar as principais falhas como a terminologia utilizada na lei, a pena máxima branda, a precariedade da polícia técnica, objetivando discutir e reportar ao cidadão sobre a existência de uma lei que em suas linhas trouxeram falhas que podem dificultar e até impossibilitar a aplicabilidade para o fim pretendido, isto é, segurança jurídica contra crimes cibernéticos. Metodologicamente será utilizada a literatura da rede mundial de computadores (internet) e livros sobre o assunto. O artigo abordará como a imprensa brasileira conseguiu obter êxito através da pressão no Congresso para que se dessem respostas imediatas contra ziches crimes virtuais devido à violação virtual da intimidade da atriz Carolina Dieckmann, entretanto a legislação foi feita, tramitada, votada, promulgada e publicada, mas acabou contendo falhas no texto legal e sendo alvo de alguns pontos críticos.

Ressaltando-se a Lei nº12.737 que foi introduzida na legislação brasileira no dia 30 de Novembro de 2012, que dispõe sobre uma nova modalidade de crime, o de”; Invasão de Dispositivo Informático”; lei esta que ganhou repercussão nacional em razão da atriz Carolina Dieckmann, que foi vítima de invasão indevida de imagens privadas de seu sistema informático, e tal incidente influenciou o andamento do projeto de lei que tramitava, William mais célere a atualização do Código Penal em relação aos crimes de natureza virtual.

Outro ponto a ser exposto, recairá sobre ziches benefícios e malefícios que tal lei trouxe ao ordenamento. E por fim, aborda também ziches procedimentos realizados na persecução felonias dos crimes de natureza virtual.

## **3.2 MARCO CIVIL**

O marco civil da internet é a lei n° 12.965/2014 que entrou em vigor no desde o dia 23 de junho de 2014 é regulamenta o uso da internet.

Ela é responsável por estabelecer princípios e garantias para que a rede possa ser livre e democrática no Brasil. Ela que dita os direitos e deveres dos usuários e empresas provedoras de acesso e serviço online (Martins, 2015, online).

Assim como em qualquer meio que alguém esteja inserido há princípios a serem seguidos, no mundo virtual não é diferente, e para que haja uma harmonia também tem o papel de reger os deveres de que provê esse tipo de serviço.

O marco civil da internet proíbe que provedores de telecomunicações restrinjam conexão e velocidade de acordo com o conteúdo, origem, destino e acesso a rede para todos.

## **4 DA CLASSIFICAÇÃO DOS CRIMES**

Como vimos, o que define o crime de informática é a utilização do computador ou da Internet para a prática do ato. Assim, podem ser classificados como crimes Cibernéticos puros e impuros.

### **4.1 CRIMES CIBERNÉTICOS PUROS**

Os crimes cibernéticos puros ocorrem quando o agente quer atacar o sistema de Informática de um terceiro, seja este sistema um software, tecele, sistema e Meios de armazenamento de dados.

Segundo Damásio de Jesus Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por Computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico Tutelado.

Nota- se, que esta categoria de crime caracteriza- se quando um indivíduo, principalmente o hacker e o cracker, utiliza- se de um computador e/ ou internet para invadir a máquina de um terceiro, sendo que o crime se consome no próprio meio Virtual, não produzindo efeitos fora deste ambiente.

## **4.2 CRIMES CIBERNÉTICOS IMPUROS**

Crimes cibernéticos impuros ocorrem quando o agente utiliza-se da internet como Meio executório para prática de um crime tipificado em nossa legislação correcional, como por exemplo, a divulgação de fotografias pornográficas de crianças e adolescentes,

Tipificada no Art. 241 do Estatuto da Criança e do Adolescente. Damásio de Jesus, conceitua o referido crime da seguinte forma crimes eletrônicos impuros ou impróprios são aqueles em que o agente Se vale do computador como meio para produzir resultado naturalístico, que Ofenda o mundo físico ou o espaço “ real ”, ameaçando ou lesando outros Bens, não- computacionais ou diversos da informática.

Desta forma, crimes impuros são aqueles em que o agente utiliza-se do Computador e da internet como ferramenta meio para produzir um resultado que Afeta outros bens tutelados pelo nosso ordenamento jurídico que não sejam relacionados aos meios virtuais.

## **4.3 PRINCÍPIO DA INOCÊNCIA**

O responsável por tutelar a liberdade dos indivíduos, sendo previsto pelo art. 5º, LVII da Constituição de 1988, que enuncia: “ninguém será considerado culpado até trânsito em julgado de sentença penal condenatória”.

## **4.4 PRINCÍPIO DA LEGALIDADE**

Nenhum crime será punido sem que haja uma lei. Também de acordo com o Princípio da Legalidade ninguém está obrigado a fazer ou deixar de fazer algo, a menos que seja previsto em lei.

## **4.5 LAVAGEM DE DINHEIRO**

Lavagem de dinheiro é uma expressão que se refere a práticas econômico financeiras que têm por finalidade dissimular ou esconder a origem ilícita de determinados ativos financeiros ou bens patrimoniais, de forma que tais ativos aparentem uma origem lícita ou que, pelo menos, a origem ilícita seja difícil de demonstrar ou provar.

Em outras palavras, lavar dinheiro é simular uma operação financeira para justificar valores obtidos por meios ilícitos ou não declarados. Um exemplo seria a

emissão de notas fiscais falsas (por advogados, consultores, médicos.) Serviços não prestados de fato (totem, notas falsas) para justificar o recebimento de valores que, na verdade, foram recebidos por propina, venda de drogas ou simplesmente não declarados ao fisco no momento correto. É uma forma de se justificar a existência de valores ou bens obtidos de forma inidônea através de falsas operações idôneas.

#### **4.6 ROUBO**

Esse tipo de crime no código penal brasileiro, ao nível virtual, é praticado para desviar fundos, obter os dados pessoais, fraudar, cometer plágio e pirataria. Art. 157 – Subtrair coisa móvel alheia, para si ou para outrem, mediante grave ameaça ou violência a pessoa, ou depois de havê-la, por qualquer meio, reduzido à impossibilidade de resistência: Pena – reclusão, de quatro a dez anos, e multa.

#### **4.7 PORNOGRAFIA INFANTIL**

Nos últimos anos o Brasil avançou na luta contra os crimes praticados contra a dignidade sexual na internet. Criou-se dispositivos úteis ao enfrentamento destes crimes, tanto na esfera processual quanto na penal (BARRETO, 2021). A pornografia infantil é uma conduta criminosa, um tipo de violência sexual cometida contra vulneráveis (criança e adolescentes), que acabou ganhando força com a atual facilidade de acesso à internet. A prática desse crime está tipificada no Estatuto da Criança e do Adolescente (ECA), e no Código Penal, assim como também Na Convenção dos Direitos da Criança da ONU, de 1989.

Os artigos 240 a 241-E, do ECA, descrevem as condutas que tipificam a Pornografia infantil, visando criminalizar a aquisição e a posse de tal material, bem como, combater à produção, venda e distribuição de pornografia infantil. O art. 240, salienta ser crime contra vulneráveis as seguintes condutas: Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:

Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa

Ademais, a pornografia infantil não é praticada apenas por aqueles que Querem prazer próprio, é praticado também por aqueles que visam lucro com a criação E comercialização de material pornográfico.

Neste sentido, dispõe o artigo 241, do ECA:

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.

Ainda, aquele que de alguma maneira compartilha, troca, publica, divulga, oferece, possui ou armazena, bem como, simula (por adulteração, montagem, Modificação) a participação de crianças ou adolescentes em cenas de conteúdos Pornográficos, mesmo que sem intenção lucrativa, também concorre a sanções Estabelecida pelo ECA, conforme seus artigos 241- A, 241-B e 241-C.

Esse crime aumentou drasticamente com a expansão da internet e criação da dep. web, a qual não será abordada amplamente no presente trabalho, mas em Suma trata-se de uma plataforma quase não conhecida pela população, de difícil Acesso e que permite a prática de condutas ilícitas por meio de sites considerados “invisíveis”, uma vez que, não aparecem nos mecanismos de busca tradicionais como O Google. Por meio dessa plataforma são praticados os mais diversos crimes, o que Dificulta ainda mais o trabalho das autoridades em descobrir os agentes dessas Condutas, posto que, o acesso a deep web é complexo e os agentes se escondem Através do anonimato.

A jurisprudência é dura na aplicação das penas envolvendo essas Condutas, podendo ser destacado a decisão do Superior Tribunal de Justiça, a qual Estabelece que quando praticado na internet tem caráter transnacional. Veja-se:

HABEAS CORPUS Nº 413.069 – SP (2017/0208680-6)  
RELATOR: MINISTRO JOEL ILAN PACIORNIK  
IMPETRANTE: DEFENSORIA PÚBLICA DA UNIÃO  
ADVOGADO: DEFENSORIA PÚBLICA DA UNIÃO  
IMPETRADO:

TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO  
PACIENTE: MICHAEL LEME DE QUEIROZ DECISÃO  
Cuida-se de habeas corpus substitutivo de Recurso próprio, com pedido de liminar, impetrado em benefício de MICHAEL LEME DE QUEIROZ, contra acórdão do Tribunal Regional Federal da

3ª Região (APC n. 2016.61.14.002516-6). Consta dos autos que o paciente foi condenado em primeiro grau pela prática dos crimes do 20 art. 241-A e 241- B, do Estatuto da Criança e do Adolescente c.c. art. 69 do Código Penal, à Pena de 4 (quatro) anos de reclusão, em regime aberto, consistentes em Prestação de serviços à comunidade e prestação pecuniária. O Tribunal Regional Federal da 3ª Região, por sua vez, negou provimento ao recurso Defensivo e deu parcial provimento ao recurso ministerial, conforme ementa A seguir transcrita: DIREITO PENAL. PROCESSO PENAL APELAÇÕES CRIMINAIS. PORNOGRAFIA INFANTO-JUVENIL. LEI 8.069/90. ARTIGOS 241-A E 241-B. PROGRAMA DE COMPARTILHAMENTO DE DADOS. USO. COMPETÊNCIA. JUSTIÇA FEDERAL. DOLO CARACTERIZADO NO COMPARTILHAMENTO DOS ARQUIVOS ILÍCITOS. AUTORIA E MATERIALIDADE INCONTROVERSAS. ABSORÇÃO. INOCORRÊNCIA NO CASO CONCRETO. CONDENAÇÃO MANTIDA. DOSIMETRIA.

ALTERAÇÕES. 1. Réu flagrado em posse de acervo de fotografias e vídeos de pornografia infanto-juvenil, acervo este armazenado digitalmente em Discos rígidos de sua propriedade. Teria, ainda, compartilhado arquivo do Mesmo teor anteriormente. [...] em outros termos: ao disponibilizar arquivos de conteúdo pornográfico infanto-juvenil em servidor mundialmente acessível, o que há é a disponibilização/divulgação de pornografia infanto-juvenil além das fronteiras nacionais, o que torna claro seu caráter Transnacional. [...]

3. Por sua vez, a constatação da internacionalidade do Delito demandaria apenas que a publicação do material pornográfico tivesse Sido feita em “ambiência virtual de sítios de amplo e fácil acesso a qualquer Sujeito, em qualquer parte do planeta, que esteja conectado à internet” e que “o material pornográfico, envolvendo crianças ou adolescentes tenha estado Acessível por

alguém no estrangeiro, ainda que não haja evidências de que Esse acesso realmente ocorreu” [...] Publique-se. Intime-se. Brasília (DF), 23 De fevereiro de 2018. (STJ – HC: 413069 SP 2017/0208680-6, Relator: Ministro Joel Ilan Paciornik, Data de Publicação: DJ 28/02/2018) O Superior Tribunal Federal, ainda estabelece que a mera divulgação do Conteúdo sexual envolvendo os vulneráveis já se consuma o crime de pornografia Infantil. In verbais: Primeira turma do STF: ESTATUTO DA CRIANÇA E DO ADOLESCENTE – Art. 241 – Inserção de cenas de sexo explícito em rede de computadores (Internet) – Crime caracterizado – Prova pericial necessária para apuração Da autoria. “Crime de computador”; publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores Atribuída a menores – Tipicidade – Prova pericial necessária à demonstração Da autoria – Habeas Corpus deferido em parte. 1. O tipo cogitado – na Modalidade de “publicar cena de sexo explícito ou pornográfica envolvendo Criança ou adolescente” – ao contrário do que sucede por exemplo aos da Lei De Imprensa, no tocante ao processo da publicação incriminada é uma normal Aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica Do veículo utilizado à difusão da imagem para número indeterminado de Pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar Lacuna da lei incriminadora por analogia: uma vez que se compreenda na Decisão típica da conduta incriminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da Lei penal: a invenção Da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a Solução da controvérsia de fato sobre a autoria da inserção incriminada do Conhecimento do homem comum, impõe se a realização de prova pericial. Destarte, a pornografia infantil é um crime doloso, o qual exige-se apenas

O dano potencial, não necessitando de dano material efetivo para ser consumado, Tendo como objeto material a foto, o vídeo ou a imagem contendo pornografia ou sexo Explícito envolvendo criança ou adolescente e, ainda, tendo como objeto jurídico a Proteção à formação moral da criança ou adolescente (NUCCI, 2016). Ainda, nos termos do art. 241-A, parágrafo 2º, a autoridade policial ou Ministério Público podem oficiar o responsável técnico dos sites os quais contenham Fotos, vídeos ou qualquer outro registro que tenha sexo explícito ou pornografia envolvendo menores, requisitando sua remoção em 24 horas, sob pena de 03 a 06 de Reclusão e multa.

Além disso, a solicitação também pode ser feita pelos pais ou Representantes da vítima, e em caso de descumprimento recomenda-se a instauração de inquérito e posterior indiciamento do investigado (BARRETO, 2021)

## **CONSIDERAÇÕES FINAIS**

Os delitos cometidos através da internet são presentes em todo o mundo, entretanto, o Brasil encontra-se atrasado por não dispor de uma legislação específica e adequada à regulamentação e punição àqueles que cometem as condutas delituosas em questão.

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. *REVISTA DA FACULDADE DE DIREITO DA UFMG*, 2013, 2013.62: 139-178.

A falta de tipificação adequada para os delitos praticados no ambiente cibernético, promove insegurança tanto para a sociedade quanto para o âmbito jurídico brasileiro. As tentativas fracassadas de projetos de lei ou mesmo a publicação apressada de legislações, como é o caso da Lei nº 12.737/2012, geraram inúmeras consequências em desfavor da adequada classificação e regulamentação dos crimes em questão. É necessária cautela na instauração de um ordenamento sob o referido tema, tendo em vista que o ambiente virtual está em constante evolução, devendo ser estudado de forma adequada. Sendo assim, a favor da segurança do desenvolvimento da sociedade e da

segurança do âmbito jurídico brasileiro, faz-se necessário um maior investimento no âmbito de segurança da informação, além de treinamento especializado dos agentes para que haja uma persecução penal efetiva e atual, lembrando que o Código Penal brasileiro é de 1940, período em que não existia as tecnologias usadas atualmente e notoriamente, não existiam os crimes cibernéticos (FERNANDES, 2013). Com a existência de condutas atípicas que não podem ser punidas em decorrência do princípio da legalidade ou da reserva legal, é essencial a elaboração de um ordenamento específico além da adoção do Brasil a tratados internacionais que disciplinam sobre o conteúdo em questão para adequação da legislação interna, como é o caso da Convenção de Budapeste. Diante a expansão do espaço cibernético em todo o mundo, a adoção à Convenção consistiria no dever preventivo do Estado, tendo em vista que promoveria a utilização de normas claras e eficientes, de modo que promova segurança à sociedade e punição àqueles que se utilizam de meios escusos para provocar danos materiais e morais a terceiros.

## REFERÊNCIAS

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. Jus Navigandi, Teresina, ano 5, p. 51, out. 2001. Disponível em: <<https://Jus.com.br/artigos/2250/crimes-de-informatica>>. Acesso em: 10 out. 2017.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2011

<http://advivo.com.br/blog/luiz-claudio-tonchis/redes-sociais-privacidade-perfis-fake-e-crimes-virtuais> Acesso em 04 de nov. 2017.  
<https://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lein-12737-12-art-154-a-do-codigo-penal> Acesso em 04 de nov. 2017  
<http://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-do-roubo-das-fotos-decarolina-dieckmann-sao-descobertos.html> Acesso em 02 de nov. 2017.

<https://www.conjur.com.br/2009-jul-25/identificar-autores-crimes-eletronicos-cadavez-possivel> Acesso em 03 de nov. 2017.

<https://www.dgti.ufla.br/site/lei-de-crimes-informaticos/> Acesso em 04 de nov. 2017.

CRESPO, Marcelo. As Leis nº 12.735/2012 e 12.737/2012 e os crimes digitais: certos e equívocos legislativos. Abr 2015. Disponível em: < <http://canalcienciascriminais.com.br/asleis-no-12->

7352012-e-12-7372012-e-os-crimes-digitais-acertos-e-equivocos-legislativos/>. Acesso em:  
Nov 2016.