**UNIVERSIDADE FEDERAL DE SANTA CATARINA**
**CENTRO DE CIÊNCIAS JURÍDICAS**
**DEPARTAMENTO DE DIREITO**
**CURSO DE DIREITO**

**KARINI NASCIMENTO**

# **A CIBERCRIMINALIDADE FRENTE AO DIREITO DA CRIANÇA E DO ADOLESCENTE:** uma análise da legislação brasileira mediante a constante exposição à rede.

Florianópolis
2023

**KARINI NASCIMENTO**

# **A CIBERCRIMINALIDADE FRENTE AO DIREITO DA CRIANÇA E DO ADOLESCENTE:** uma análise da legislação brasileira mediante a constante exposição à rede.

Trabalho de Conclusão de Curso submetido ao curso de Direito do Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Bacharela em Direito.

Orientadora: Profa. Dra. JOSIANE PETRY VERONESE

Florianópolis

2023

Nascimento, Karini
A CIBERCRIMINALIDADE FRENTE AO DIREITO DA CRIANÇA E DO ADOLESCENTE : uma análise da legislação brasileira mediante a constante exposição à rede. / Karini Nascimento ; orientadora, Josiane Petry Veronese, coorientador, Rosane Portella Wolff, coorientadora, Geralda Magella de Faria Rosetto, 2023.
70 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Graduação em Direito, Florianópolis, 2023.

Inclui referências.

1. Direito. 2. cibercriminalidade. 3. pedofilia . 4. crianças e adolescentes. 5. pornografia infantil. I. Petry Veronese, Josiane. II. Portella Wolff, Rosane. III. Magella de Faria Rosetto, Geralda IV. Universidade Federal de Santa Catarina. Graduação em Direito. V. Título.

KARINI NASCIMENTO

**A CIBERCRIMINALIDADE FRENTE AO DIREITO DA CRIANÇA E DO ADOLESCENTE:** uma análise da legislação brasileira mediante a constante exposição à rede.

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do título de Bacharela e aprovado em sua forma final pelo Curso de Direito.

Florianópolis, 30 de Novembro de 2023.

Prof. Francisco Quintanilha Veras Neto, Dr.

Coordenação do Curso

**Banca examinadora**

Documento assinado digitalmente
Josiane Rose Petry Veronese
Data: 04/12/2023 20:43:22-0300
CPF: ***.102.979-**
Verifique as assinaturas em https://v.ufsc.br

Profa. Dra. JOSIANE ROSE PETRY VERONESE

Orientadora

ROSANE PORTELLA WOLFF:4327
Assinado de forma digital por ROSANE PORTELLA WOLFF:4327
Dados: 2023.12.04 22:18:39 -03'00'

Msc. ROSANE PORTELLA WOLFF

Avaliadora

Documento assinado digitalmente
GERALDA MAGELLA DE FARIA
Data: 05/12/2023 08:23:09-0300
CPF: ***.732.531-**
Verifique as assinaturas em https://v.ufsc.br

Dra. GERALDA MAGELLA DE FARIA ROSETTO

Avaliadora

Florianópolis, 2023

**Um sonho concreto**

Um dia
me senti tocada
por um direito novo.
Poderia até dizer,
revolucionário.
Revolucionário por quê?
Porque traz ciência e amorosidade.
Sim,
verdadeiro direito.
Um direito que não se afasta do ser
o contempla,
o protege,
e sonha que seja reconhecido.
Não em favor de si próprio,
mas em favor
de crianças diversas,
muitas, inclusive, vulnerabilizadas
pela incapacidade,
egoísmo,
insensatez,
dos adultos.
Não podemos nos calar,
precisamos gritar sobre os montes, as torres.
As crianças precisam ser cuidadas,
protegidas,
as crianças precisam e merecem ser amadas.
(Josiane Rose Petry Veronese)

## AGRADECIMENTOS

Gostaria expressar minha profunda gratidão e reconhecimento a meus pais, Carlos Bento e Maria Terezinha, cujo apoio incansável e amor incondicional foram pilares fundamentais na jornada da realização deste trabalho de conclusão de curso. Suas orientações sábias, encorajamento constante e exemplos inspiradores foram fontes inestimáveis de motivação. A cada desafio, vocês estiveram ao meu lado, oferecendo suporte emocional e incentivo intelectual. Este trabalho é dedicado a vocês, que não apenas me proporcionaram oportunidades educacionais, mas também cultivaram em mim valores como perseverança e dedicação. A conquista deste marco acadêmico é, sem dúvida, um reflexo do amor e apoio inabaláveis que recebi ao longo de minha jornada. Muito obrigado, papai e mamãe, por serem a base sólida e inspiradora que tornou possível este feito.

Agradeço à minha professora orientadora, Josiane Rose Petry Veronese, por sua dedicação incansável e comprometimento durante todo o desenvolvimento deste trabalho de conclusão de curso. Este trabalho não seria o mesmo sem sua influência positiva e orientação valiosa. Muito obrigado, Professora Josiane, por ser uma mentora excepcional e contribuir significativamente para o meu crescimento acadêmico e profissional.

Profunda gratidão à minha amiga Julia Jacoby por sua compreensão e apoio durante o período em que optei por não participar das festas para me dedicar à conclusão deste trabalho. Sua compreensão, paciência e incentivo foram fundamentais para enfrentar os desafios e prazos apertados.

E claro, meu muito obrigada a minha amiga  Helena Carrara, por sua paciência inestimável e apoio durante o processo de ensaio da minha apresentação. Sua disposição em ouvir e oferecer feedbacks construtivos, mesmo após eu ter ensaiado mais de 10 vezes, foi crucial para aprimorar minha performance e confiança. Agradeço por dedicar seu tempo e atenção, contribuindo significativamente para o meu sucesso na apresentação final.

## RESUMO

A cibercriminalidade é um desafio em constante crescimento em um mundo cada vez mais digitalizado. Sua influência direta na vida de crianças e adolescentes, que usam a internet desde cedo para suas atividades diárias, é um tema de grande relevância. Esta monografia busca examinar a cibercriminalidade no contexto do direito da criança e do adolescente no Brasil, considerando a exposição constante dessa faixa etária à rede mundial de computadores. O estudo analisa as principais formas de cibercriminalidade que ameaçam os jovens, incluindo a exposição a conteúdos inadequados, a pedofilia online, grooming, a pornografia infantil e a cultura da sexualização da infância que temos em nosso país. Além disso, investiga a legislação brasileira em vigor, como o Estatuto da Criança e do Adolescente, a Constituição Federal e outras leis relacionadas à proteção infantil, visando avaliar sua eficácia na prevenção e repressão desses crimes virtuais. A importância deste trabalho está na necessidade de compreender e aprimorar os mecanismos legais e principalmente os preventivos, diante dos desafios impostos pela cibercriminalidade. Ao examinar o cenário atual da cibercriminalidade direcionada a crianças e adolescentes no Brasil, esta monografia visa contribuir para o fortalecimento do arcabouço jurídico e institucional com foco principal na necessidade da conscientização para prevenção desses crimes tão bárbaros. O objetivo é garantir um ambiente virtual seguro e saudável para essa parcela da população, sempre respeitando seus direitos fundamentais e liberdades individuais, tendo em vista que negar às crianças o acesso à internet, é o mesmo do que negar o acesso à cultura e a educação, o que se precisa é de um ambiente seguro, com supervisão, para que as crianças e adolescentes navegam pela internet de uma forma consciente e mais segura.

Para alcançar os objetivos propostos, esta pesquisa adotará uma abordagem metodológica dedutiva, embasada em revisão bibliográfica, legislação, crimes, e análise de material publicado. A metodologia adotada visa estabelecer um embasamento sólido para o desenvolvimento de uma análise abrangente e crítica sobre a intersecção entre cibercriminalidade e a salvaguarda dos direitos das crianças e adolescentes no contexto brasileiro.

**Palavras-chave:** cibercriminalidade, crianças e adolescentes, proteção infantil, pedofilia, pornografia infatil.

## ABSTRACT

Cybercrime is a constantly growing challenge in an increasingly digitized world. Its direct impact on the lives of children and adolescents, who use the internet early on for their daily activities, is a topic of great significance. This thesis aims to examine cybercrime in the context of child and adolescent law in Brazil, considering the constant exposure of this age group to the worldwide computer network. The study analyzes the main forms of cybercrime that threaten young people, including exposure to inappropriate content, online pedophilia, grooming, child pornography, and the culture of sexualizing childhood prevalent in our country. Additionally, it investigates the current Brazilian legislation, such as the Child and Adolescent Statute, the Federal Constitution, and other laws related to child protection, aiming to assess their effectiveness in preventing and prosecuting these virtual crimes. The importance of this work lies in the need to understand and enhance legal mechanisms, especially preventive ones, in the face of the challenges posed by cybercrime. By examining the current scenario of cybercrime targeting children and adolescents in Brazil, this thesis seeks to contribute to strengthening the legal and institutional framework with a primary focus on the necessity of awareness for the prevention of such heinous crimes. The goal is to ensure a safe and healthy virtual environment for this segment of the population, always respecting their fundamental rights and individual freedoms. It is crucial to provide a secure, supervised environment for children and adolescents to navigate the internet consciously and more safely, as denying them access to the internet is equivalent to denying access to culture and education.

To achieve the proposed objectives, this research will adopt a deductive methodological approach, grounded in literature review, legislation, crimes, and analysis of published material. The adopted methodology aims to establish a solid foundation for the development of a comprehensive and critical analysis of the intersection between cybercrime and the safeguarding of the rights of children and adolescents in the Brazilian context

**Keywords:** cybercrime, children and adolescents, child protection, pedophilia, child pornography.

# SUMÁRIO

## 1. INTRODUÇÃO

A sociedade contemporânea vive em um mundo cada vez mais digitalizado e interconectado, onde a tecnologia da informação e a internet desempenham um papel central na vida das pessoas, especialmente das crianças e adolescentes. No entanto, essa crescente dependência da tecnologia também abre portas para uma série de desafios, entre os quais se destaca a cibercriminalidade. O uso da internet e de dispositivos eletrônicos por parte de crianças e adolescentes é uma realidade incontestável, trazendo consigo uma série de riscos e vulnerabilidades que demandam uma análise aprofundada do ponto de vista jurídico.

Nesse contexto, esta monografia propõe-se a investigar a relação entre a cibercriminalidade e o direito da criança e do adolescente no Brasil, com foco na exposição constante dessa parcela da população à rede mundial de computadores. A proteção dos direitos das crianças e dos adolescentes é uma preocupação fundamental da sociedade e do Estado brasileiro, estando consagrada na Constituição Federal de 1988 e no Estatuto da Criança e do Adolescente (ECA). Contudo, a rápida evolução tecnológica e a disseminação da internet têm desafiado a eficácia desses instrumentos legais na preservação da integridade e bem-estar das crianças e adolescentes em um ambiente virtual complexo e muitas vezes hostil. Esta pesquisa buscará analisar as principais formas de cibercriminalidade que afetam crianças e adolescentes, tais como a exposição a conteúdos impróprios, a pedofilia online, a pornografia infantil e o *grooming*, entre outros. Além disso, será realizado um estudo aprofundado da legislação brasileira pertinente, avaliando sua adequação e eficácia no enfrentamento desses crimes virtuais e na proteção dos direitos das crianças e adolescentes. A relevância desta pesquisa reside na necessidade premente de compreender e aprimorar os mecanismos legais e de prevenção relacionados à cibercriminalidade, especialmente quando direcionada a um público tão vulnerável. Ao analisar o atual panorama da cibercriminalidade em relação às crianças e adolescentes no Brasil, esta monografia visa contribuir para o fortalecimento do arcabouço jurídico e institucional destinado a garantir um ambiente virtual seguro e saudável para essa parcela da população, ao mesmo tempo em que respeita suas liberdades individuais e direitos fundamentais.

Em paralelo, é fundamental destacar que nos últimos anos, a evolução da internet não apenas transformou de maneira exponencial os padrões de vida global, mas também gerou uma preocupante problemática: a utilização da internet para cometer crimes. O método utilizado foi por meio de revisão bibliográfica de artigos, livros e de material publicado, este estudo discute os desafios enfrentados nesse processo, especialmente os principais aspectos dos crimes cibernéticos, com foco na dificuldade de estabelecer um escopo preciso dos crimes de pedofilia e de pornografia infantojuvenil, os quais cresceram consideravelmente com a disseminação da internet.

De acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), em 2018, o número total de usuários da internet no Brasil ultrapassou 120,7 milhões, o que representava mais de 70% da população do país. Notavelmente, 89% dos jovens entre 10 e 15 anos tinham acesso à rede, refletindo a ampla penetração da internet em diferentes faixas etárias.

Contudo, essa era digital trouxe não apenas benefícios, mas também desafios significativos, pois os criminosos encontraram um ambiente propício para atividades ilícitas. Os crimes cibernéticos aumentaram em magnitude e complexidade, trazendo dificuldades consideráveis no combate a eles, especialmente na identificação dos infratores. Além disso, surge a preocupação com a vulnerabilidade das crianças no mundo digital. O uso desenfreado da internet e a falta de supervisão por parte dos responsáveis muitas vezes levam as crianças a compartilhar informações pessoais sem compreensão completa dos riscos associados, tornando-se inadvertidamente alvos de crimes cibernéticos.

Para alcançar os objetivos propostos, esta pesquisa adotará uma abordagem metodológica dedutiva, embasada em revisão bibliográfica, análise da legislação e análise de material publicado. Serão consultadas fontes acadêmicas, legislação pertinente, estudos de caso e relatórios que abordem a cibercriminalidade, especialmente aquelas que tangenciam a proteção da criança e do adolescente no contexto digital. A metodologia adotada visa estabelecer um embasamento sólido para o desenvolvimento de uma análise abrangente e crítica sobre a intersecção entre cibercriminalidade e a salvaguarda dos direitos das crianças e adolescentes no contexto brasileiro.

## 2. À HISTÓRIA E A ORIGEM DO CIBERCRIMES: UMA ANÁLISE DAS TENDÊNCIAS E EVOLUÇÃO DOS DELITOS CIBERNÉTICOS PRÓPRIOS E IMPRÓPRIOS

A emergência da tecnologia digital no século XXI não apenas trouxe inúmeras oportunidades, mas também deu origem a uma nova categoria de crimes, o cibercrime. Neste capítulo, exploraremos a origem e a evolução desse fenômeno contemporâneo que desafia a ordem legal global, bem como abordaremos não apenas o surgimento, mas a trajetória que levou ao estado atual do cibercrime, com o intuito de aprofundar nossa compreensão sobre como ele se desenvolveu e adaptou em sincronia com o avanço da tecnologia. A discussão não se limitará a uma narrativa histórica, mas se aprofundará na estruturação das categorias de crimes cibernéticos, com foco particular nas distinções entre os crimes cibernéticos próprios e impróprios. Dessa forma, isso permitirá compreender não apenas a evolução temporal desse fenômeno, mas também as complexidades intrínsecas às diferentes formas de cibercrimes e seus impactos na sociedade e na ordem legal

### **2.1.** O SURGIMENTO DO CIBERCRIME

A chegada da tecnologia digital e das redes de comunicação no século XXI representou um marco significativo, não apenas pela transformação nas formas de comunicação, produção e compartilhamento de informações, mas também pela emergência de uma nova categoria de crimes: os cibercrimes. À medida que a internet se tornou parte integrante da vida cotidiana, oferecendo oportunidades sem precedentes, ela também criou um terreno fértil para atividades criminosas (Júnior, 2019). A acessibilidade generalizada à internet, combinada com nossa crescente dependência dela para uma variedade de tarefas e transações, tornou-se um atrativo para indivíduos com intenções ilícitas.

Nesse contexto, a difusão da internet levou ao surgimento de especialistas altamente qualificados na linguagem informática, resultando na criação de uma ampla variedade de termos para descrever as infrações penais cometidas por meio de dispositivos conectados à rede mundial de computadores. Esses termos englobam cibercrimes, crimes cibernéticos, crimes informáticos, crimes na internet, crimes virtuais, crimes digitais, entre outros. Todos esses conceitos se referem a

atividades ilegais que envolvem o uso de computadores e redes de computadores, abrangendo desde ataques de negação de serviço (DDoS) e fraudes bancárias até espionagem cibernética. No entanto, é importante ressaltar que nem todas as atividades ilegais realizadas na internet se enquadram estritamente na categoria de cibercrimes, uma vez que essa designação abrange não apenas atividades criminosas em rede, mas também comportamentos ilegais, como cyberbullying, difamação e assédio online.

A história do cibercrime teve início no final dos anos 70 e início dos anos 80, quando os primeiros computadores pessoais começaram a surgir. Nesse período inicial, hackers pioneiros começaram a explorar as possibilidades da rede incipiente, desenvolvendo técnicas de invasão de sistemas e redes. A década de 90 testemunhou a popularização da internet, momento em que o cibercrime se tornou uma ameaça mais substancial para a sociedade. Durante essa década, o cientista britânico Tim Berners-Lee desenvolveu o primeiro navegador e servidor web, conhecido como World Wide Web (posteriormente renomeado para Nexus) (Souza, 2018). Em 6 de agosto de 1991, ele tornou-se o primeiro website público, explicando o que era a World Wide Web, seu funcionamento e como outras pessoas poderiam criar e hospedar páginas na web. A invenção de Tim Berners-Lee acelerou o desenvolvimento da internet, tornando a troca de informações e a comunicação global mais acessíveis e rápidas.

O crescente e lucrativo mercado da internet impulsionou o desenvolvimento de novas ferramentas e serviços, tornando a rede cada vez mais complexa e dinâmica. Atualmente, a World Wide Web faz parte integrante da vida moderna, sendo utilizada por bilhões de pessoas em todo o mundo para variadas finalidades, incluindo comunicação, educação, comércio e entretenimento. No entanto, essa mesma rede também serve como uma ferramenta para criminosos cibernéticos, que utilizam uma ampla gama de técnicas para perpetrar crimes online, como phishing, ransomware, malware, entre outros. A natureza desafiadora da rastreabilidade e da punição na internet e nas redes de computadores torna o ambiente virtual ainda mais atrativo para a prática de cibercrimes.

No Brasil, a história da internet teve seu início na década de 1980, acompanhando a evolução global da internet e seus impactos na sociedade. Em 1988, a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e o Laboratório Nacional de Computação Científica (LNCC) estabeleceram a primeira

conexão de rede no país, inicialmente voltada para fins acadêmicos e de pesquisa (Valverde, 2010). No mesmo ano, ocorreu o primeiro grande incidente de cibercrime, quando o estudante americano Robert Tappan Morris criou o "worm". O objetivo inicial do programa de Morris era avaliar a extensão da internet, mas ele se espalhou mais rapidamente e amplamente do que o previsto, interrompendo os serviços em cerca de 6.000 computadores, o que correspondia a 10% dos servidores de internet da época. Esse incidente foi considerado o primeiro grande caso de cibercrime e resultou na condenação de Morris sob a Lei de Fraude e Abuso de Computador dos Estados Unidos.

Em 1991, o Ministério da Ciência e Tecnologia estabeleceu a Rede Nacional de Ensino e Pesquisa (RNP) com o propósito de interligar instituições acadêmicas e de pesquisa em todo o território brasileiro. Três anos depois, em 1994, a RNP conquistou um marco significativo ao estabelecer a primeira conexão permanente à internet no Brasil, conectando universidades, centros de pesquisa e outras entidades científicas e tecnológicas. Ao mesmo tempo, em 1994, a Embratel estabeleceu a primeira conexão comercial ao backbone da internet, possibilitando o acesso à rede para empresas e provedores de serviços. Assim, em 1995, o cenário da internet comercial se estabeleceu no Brasil, com o respaldo do governo federal para que empresas privadas oferecessem serviços de conexão à internet. (Valverde, 2010). Durante essa fase inicial, o acesso à internet era predominantemente restrito à comunidade acadêmica e a algumas empresas. No entanto, a presença da web no Brasil começou a ganhar popularidade com a criação de websites, portais de notícias, lojas virtuais e serviços de e-mail. Consequentemente, ocorreu um crescimento exponencial da internet brasileira nos primeiros anos do século XXI, impulsionado pela expansão das conexões de banda larga e pelo aumento da oferta de serviços e conteúdo online. Na era contemporânea, a rede mundial de computadores transcende seus objetivos originais de comunicação e entretenimento, tornando-se uma plataforma essencial e poderosa para a economia global. Como resultado, ela está intrinsecamente entrelaçada em todos os aspectos da vida, abrangendo desde relações interpessoais até transações comerciais, bem como desempenhando um papel fundamental em setores como governança, segurança pública, educação, saúde e cultura (Valverde, 2010). Diante disso, evidencia-se as palavras de Mendes e Vieira, em que a sociedade da informação em rede traz consigo novos desafios para a sociedade e para o direito, em especial

para o direito penal. Os crimes cometidos pela internet são praticados em ambiente internacional, com ofensores e vítimas em diferentes países. A falta de fronteiras e de limites geográficos para a prática de delitos cibernéticos acarreta problemas para as autoridades, que muitas vezes encontram dificuldades em determinar o local da prática criminosa, a jurisdição aplicável e a efetivação de medidas de investigação e repressão. [...] apesar das facilidades e benefícios oferecidos pela internet, esse cenário também é propício para a prática de crimes. Cada vez mais, os criminosos se valem desse meio para praticar os mais variados tipos de crime. Pois, com o advento da internet, os crimes já tipificados pelo Código Penal passaram a ser praticados também no meio virtual, assim como, surgiram novas modalidades de crimes que passaram a ser praticados nesse meio (Mendes, Vieira, 2012).

Frente a isso, pelo desenvolvimento de tecnologias de comunicação hiper velozes, essa integração global também propiciou o crescimento tanto de atividades econômicas legítimas quanto de atividades criminosas em todo o mundo. Os meios virtuais, como motores de busca, provedores de acesso e conteúdo, bem como as redes sociais, se tornam propícios para diversas condutas criminosas de natureza diversa. Entre esses delitos, estão incluídos crimes como calúnia, ameaça, pornografia infantil, falsa identidade e pedofilia. (Kesikowski, Winter, Gomes, 2018). Mostra-se evidente que a circulação de informações pessoais na vasta rede de computadores torna as pessoas vulneráveis, uma vez que crimes anteriormente restritos ao âmbito nacional agora são cometidos internacionalmente. Além disso, é importante notar que o uso da internet não se restringe aos adultos, cada vez mais, crianças acessam a rede por meio de dispositivos como celulares, tablets e computadores. Infelizmente, muitos jovens compartilham informações pessoais na internet sem compreender completamente os riscos, tornando-se inadvertidamente alvos de crimes digitais. Essas situações de alto risco são resultado do uso desordenado da internet sem supervisão adequada por parte de seus responsáveis. (Eufrasio, 2015). Assim, é ainda mais alarmante considerar os crimes informáticos perpetrados por adultos que têm como alvo crianças, tendo em vista a natureza virtual e a habilidade de criminosos em explorar a anonimidade proporcionada pela internet, apresentando ameaças sérias à segurança das crianças e adolescentes. Os criminosos cibernéticos podem se envolver em uma ampla variedade de atividades prejudiciais, incluindo assédio, cyberbullying, exposição a conteúdo inadequado, grooming (o ato de adultos se passarem por crianças ou adolescentes

para ganhar a confiança das crianças e adolescentes com propósitos sexuais) e, em casos extremos, exploração sexual.

De acordo com uma pesquisa realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), em 2018, o Brasil contava com mais de 120,7 milhões de internautas, o que representava mais de 70% da população. Além disso, a pesquisa revelou que 89% das crianças entre 10 e 15 anos tinham acesso à internet. Embora seja inegável que a internet tenha proporcionado uma comunicação eficaz entre as pessoas, é fundamental reconhecer os desafios e riscos associados à falta de conhecimento e de cuidados básicos no acesso à rede. Isso pode resultar em prejuízos a diversos bens jurídicos protegidos (Eufrásio, 2015).

No entanto, o Direito Penal e suas legislações criminais especiais muitas vezes não conseguem acompanhar adequadamente as evoluções tecnológicas. Essa lacuna legal pode ser problemática, uma vez que a falta de normas específicas para certos comportamentos no ambiente virtual dificulta a aplicação de sanções adequadas aos seus perpetradores. Isso resulta em uma fragilidade do sistema legal diante da realidade social em constante evolução.

Diante desse cenário, é fundamental reconhecer que, embora a globalização tenha trazido benefícios significativos em diversos campos, como a economia e a indústria, ela também exige um aprimoramento dos mecanismos de combate à criminalidade transnacional e uma reavaliação da Ciência Criminal para enfrentar as novas modalidades criminosas que surgiram com o avanço tecnológico (Machado 2017).

O Brasil figura entre os quatro principais centros de disseminação de pornografia infantil globalmente, em concorrência com os Estados Unidos, Rússia e Coreia do Sul. Nesse contexto alarmante, a internet se apresenta como um facilitador significativo para criminosos, permitindo a troca de arquivos contendo informações, fotos e vídeos de teor ilícito (Ministério Público Federal, 2018).

Dentro desse cenário sombrio, torna-se evidente o perigo constante que as crianças enfrentam neste ambiente obscuro. Nele, uma ampla gama de crimes é cometida, com o potencial de causar danos psicológicos e físicos profundos, incluindo consequências devastadoras, como abuso sexual e até mesmo morte (Machado, 2017).

Infere-se, portanto, que a cibercriminalidade engloba uma ampla gama de atividades ilegais que ocorrem no ambiente virtual, abrangendo desde fraudes

financeiras até crimes contra a honra e exploração sexual infantil. Dessa forma, quando consideramos o direito da criança e do adolescente, torna-se ainda mais premente abordar esse tema, uma vez que a internet é um espaço onde jovens estão cada vez mais presentes, seja para fins educacionais, entretenimento ou interação social. Logo, a exploração sexual de crianças e adolescentes na internet é um dos aspectos mais sombrios da cibercriminalidade, ao ponto que criminosos podem usar a rede para se aproximar de jovens vulneráveis, explorando sua ingenuidade e confiança, diante disso, é fundamental que a legislação e as autoridades estejam atentas a essas ameaças, garantindo que medidas rigorosas sejam aplicadas contra os responsáveis por esses atos repugnantes. Além disso, o ciberbullying e a exposição de jovens a conteúdos prejudiciais também são questões críticas. A disseminação de informações difamatórias ou prejudiciais pode ter um impacto severo na saúde mental e emocional de crianças e adolescentes, afetando sua autoestima e bem-estar. Portanto, se evidencia fundamental que haja mecanismos legais eficazes para lidar com essas situações e proteger as crianças e adolescentes. Bem como, a privacidade online também é uma área de preocupação, crianças e adolescentes, muitas vezes, compartilham informações pessoais na internet, sem plena compreensão das consequências, sendo responsabilidade dos pais, educadores e das autoridades garantir que as crianças e adolescentes estejam cientes dos riscos associados à divulgação de informações pessoais online (Eufrásio, 2015). Por outro viés, é importante que o sistema legal também leve em consideração a idade e o entendimento limitado das crianças e adolescentes ao lidar com casos de cibercriminalidade cometida por menores de idades, ao ponto que as penas e medidas punitivas devem ser adequadas à idade e à situação específica da criança e adolescente infrator, priorizando, sempre que possível, a reabilitação em vez da punição severa. Em síntese, a cibercriminalidade é uma ameaça real ao direito da criança e do adolescente, exigindo uma abordagem abrangente que inclua educação, conscientização, legislação eficaz e medidas de proteção. É de responsabilidade coletiva, do estado, da sociedades e dos responsáveis legais, garantir que crianças e adolescentes possam aproveitar os benefícios da era digital de forma segura, enquanto combatem eficazmente a cibercriminalidade que os ameaça.

## 2.2. CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Nesse ínterim, mostra se importante destacar que existem principalmente duas categorias utilizadas para classificar os crimes cibernéticos, conforme esclarecido por Marcelo Crespo. Essas categorias compreendem os crimes informáticos próprios (ou puros) e os crimes informáticos impróprios (ou mistos).

> Crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas à pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas; e Crimes digitais impróprios ou mistos (conduta proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc. São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio. (Crespo, p. 140)

Portanto, os crimes informáticos abrangem tanto os delitos tradicionais já previstos na legislação brasileira, que são cometidos com o auxílio da rede mundial de computadores, quanto às condutas ilegais que envolvem sistemas informatizados e dados. Observa-se também que a rápida transformação dos hábitos da sociedade, impulsionada pelo uso de novas tecnologias, apresenta um desafio significativo na adaptação e definição de normas de conduta apropriadas. Muitas vezes, essas tecnologias são utilizadas de maneira inadequada e exploradas por indivíduos criminosos. Além disso, a internet possibilitou novas formas de interação social, que, por sua vez, facilitaram a aplicação de golpes e a prática de crimes. Embora o uso de computadores não seja algo novo na sociedade, é evidente que a legislação brasileira não está completamente preparada para lidar com as complexidades dos crimes eletrônicos. Portanto, é necessária uma revisão da legislação com o objetivo de tipificar adequadamente as diversas modalidades de crimes cibernéticos (Crespo, 2020).

O avanço constante da Tecnologia da Informação e Comunicação (TIC) deu origem a uma série de novos tipos de delitos que exploram a facilidade de acesso e disseminação de informações proporcionadas pela internet. Entre esses crimes, destacam-se a propagação de vírus e malwares, invasões de sistemas, subtração de informações pessoais e financeiras, espionagem cibernética e a prática de

phishing, um método que envolve a manipulação de usuários para obtenção fraudulenta de suas informações pessoais e financeiras. A emergência desses crimes cibernéticos é diretamente atribuída ao progresso tecnológico e à disseminação da internet. A Tecnologia da Informação, caracterizada por sua velocidade e flexibilidade, permite aos criminosos uma maior eficácia em suas atividades ilícitas, tornando desafiadora a tarefa das autoridades em reprimir e punir esses crimes. Dessa forma, é possível identificar diversas categorias de crimes cibernéticos, cada uma com suas próprias particularidades, como phishing, ransomware, botnets, malware e ataques DDoS, pornografia infantil, bem como o fenômeno do cyberbullying (Wendt, 2012).

Nesse contexto, a discussão sobre a invasão de privacidade na internet ganha relevância, pois muitos sites e aplicativos coletam dados pessoais dos usuários, frequentemente sem o seu consentimento, utilizando essas informações para fins comerciais. Para enfrentar esses desafios, é imperativo que empresas, governos e indivíduos adotem medidas eficazes de segurança cibernética. Além disso, as autoridades devem tomar medidas para reprimir e punir os criminosos cibernéticos, o que inclui a criação de legislações específicas e a cooperação internacional para identificar e responsabilizar os autores desses crimes. Muitos desses delitos são perpetrados por criminosos que atuam além das fronteiras nacionais, o que torna a extradição e a responsabilização mais complexas.

De acordo com informações do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, apenas no primeiro semestre de 2021, foram registrados mais de 1,6 milhão de incidentes de segurança na internet no país (Cert.br, 2020).

Diante desse cenário, os crimes cibernéticos podem ser classificados em duas categorias principais: os crimes cibernéticos propriamente ditos e os crimes cibernéticos impróprios. Os crimes cibernéticos impróprios envolvem atividades criminosas em que o computador ou a rede de computadores são usados como instrumentos para cometer o delito, como fraudes eletrônicas, clonagem de cartões de crédito e sequestro de dados. Já os crimes cibernéticos propriamente ditos abrangem atividades criminosas em que o computador ou a rede de computadores são o alvo do delito, incluindo acesso não autorizado a sistemas, disseminação de vírus e malware, e sabotagem de sistemas de informática (Wendt, 2012).

### **2.2.1** CRIMES INFORMÁTICOS IMPRÓPRIOS

Com a crescente utilização da Tecnologia da Informação e Comunicação (TIC), surgiram diversas categorias de crimes que exploram as vantagens da internet para a execução de atividades ilícitas. Entre essas categorias, destacam-se os chamados "crimes informáticos impróprios", que constituem crimes tradicionais aproveitando-se da tecnologia da informação como meio facilitador ou ocultador. Ao contrário dos crimes informáticos típicos, esses delitos não requerem conhecimentos técnicos aprofundados em informática ou sistemas de dados. Em vez disso, usam a internet como instrumento para alcançar seus objetivos, muitas vezes prejudicando bens jurídicos já protegidos por tipos penais existentes.

Essa classe de crimes engloba uma variedade de condutas criminosas, incluindo fraudes financeiras e estelionato, clonagem de cartões de crédito, sequestro virtual, invasões de dispositivos eletrônicos, divulgação não autorizada de informações pessoais, difamação, calúnia, falsificação de documentos eletrônicos, uso indevido de informações pessoais para transações financeiras ilegais, espionagem empresarial, sabotagem de sistemas de informática, assédio e perseguição virtual. Esses delitos podem resultar em sérias consequências para as vítimas, desde prejuízos financeiros até danos psicológicos, (Aras, 2001). Um exemplo crescente desses crimes é o "golpe do amor," em que criminosos criam perfis falsos em sites de relacionamento para enganar as vítimas e obter vantagens financeiras. Além disso, crimes que afetam a infância e adolescência, como a pedofilia e a pornografia infantil, são potencializados pela internet, mesmo diante das disposições do Estatuto da Criança e do Adolescente (ECA). Crimes de ódio, como o racismo, e crimes graves, como o terrorismo, também podem ser perpetuados ou amplificados online, representando uma ameaça significativa à sociedade. Portanto, apesar de a legislação já prever punições para essas condutas, é importante que os delitos clássicos, quando cometidos por meio da tecnologia da informação e do ambiente virtual, sejam tipificados adequadamente para garantir uma aplicação mais eficiente da justiça, (Dorigon, 2023). A investigação e repressão dos crimes informáticos impróprios enfrentam desafios significativos devido à sua natureza multifacetada e ao uso de técnicas sofisticadas para ocultar a autoria dos delitos. Além disso, muitas vezes, as vítimas não estão

cientes de que foram enganadas ou desconhecem seus direitos, dificultando a identificação e punição dos criminosos.

Diante desse cenário, é evidente que o computador e a internet são não apenas ferramentas de conveniência e produtividade, mas também meios para a prática de atividades ilícitas. Portanto, é essencial que haja uma compreensão clara desses crimes e de suas variantes digitais, bem como estratégias eficazes de prevenção, detecção e resposta. A legislação deve evoluir de acordo com o avanço da tecnologia, e os usuários devem estar cientes dos riscos associados ao uso da internet, contribuindo para um ambiente online mais seguro, (Aras, 2001).

### **2.2.2.** CRIMES CIBERNÉTICOS PRÓPRIOS.

Ao contrário dos crimes cibernéticos impróprios, que já existiam antes da revolução tecnológica e apenas foram adaptados para o contexto digital, os crimes cibernéticos próprios ou puros são uma categoria única que emergiu como resultado direto da digitalização e informatização de dados. Eles são intrinsecamente relacionados ao mundo digital e não possuem equivalentes diretos no mundo físico. Com a crescente dependência da sociedade em sistemas de informática, os criminosos encontraram novas oportunidades para suas atividades ilícitas, muitas vezes demonstrando conhecimento técnico especializado em computação e processamento de dados.

Os autores desses crimes geralmente são indivíduos ou grupos com grande experiência em tecnologia da informação, capazes de explorar brechas de segurança em sistemas e redes para a execução de suas atividades criminosas. Esses ataques cibernéticos visam diretamente os sistemas de dados, comprometendo a privacidade, integridade e disponibilidade das informações. As ações incluem a criação e disseminação de vírus de computador, invasões de sistemas (hacking) e ataques de negação de serviço (DoS e DDoS), cujo objetivo é tornar um serviço ou recurso indisponível.

Os crimes cibernéticos próprios afetam amplamente a segurança da informação, ameaçando a integridade dos sistemas e a confiabilidade das informações armazenadas. Eles exigem um alto grau de sofisticação técnica e um profundo conhecimento dos sistemas de informação, tornando-os particularmente desafiadores para a segurança cibernética.

Conforme definido pelo mestre Damásio de Jesus, os crimes eletrônicos puros ou próprios são aqueles praticados por meio de computadores e têm sua consumação no ambiente eletrônico. Neles, a informática, incluindo a segurança dos sistemas, a titularidade das informações e a integridade dos dados, é o objeto jurídico tutelado (Jesus, Aras, 2001).

A falta de uma legislação específica e abrangente para regulamentar o cibercrime pode criar lacunas legais. Em tal situação, ações que causam danos significativos podem não se enquadrar em categorias de crimes previamente definidas pelo Código Penal ou outras leis, sendo consideradas atípicas e não puníveis de acordo com o princípio da legalidade, que estabelece que ninguém pode ser punido por uma ação que não seja explicitamente considerada um crime por lei (Wendt, 2012).

Nesse cenário, a legislação precisa evoluir para abordar adequadamente esses novos tipos de crime, garantindo que os perpetradores possam ser identificados, processados e punidos de maneira eficaz. A prevenção, detecção e resposta a esses crimes requerem uma combinação de medidas de segurança robustas, legislação adequada e cooperação internacional, além da conscientização dos usuários sobre práticas seguras de uso da tecnologia. É importante destacar que a prevenção desempenha um papel crucial no combate aos crimes digitais, incluindo a implementação de medidas técnicas de segurança, como firewalls e programas antivírus, bem como a educação e conscientização dos usuários sobre os riscos e as práticas seguras de uso da internet. Um usuário informado e consciente é um dos melhores antídotos contra o crime cibernético, tornando possível combater eficazmente essa ameaça e garantir a segurança e integridade dos sistemas de informação na era digital (Santos, Ribeiro, 2018).

Além disso, é essencial ressaltar que a prevenção desempenha um papel crucial no combate aos crimes digitais. Isso envolve a implementação de medidas técnicas de segurança, como firewalls e programas antivírus, bem como a educação e conscientização dos usuários sobre os riscos e as práticas seguras de uso da internet. Um usuário informado e consciente é um dos melhores antídotos contra o crime cibernético, contribuindo para a proteção de seus próprios dados e sistemas.

Em relação à legislação, é fundamental que esta evolua para abordar adequadamente os novos tipos de crime digital, garantindo que os perpetradores possam ser identificados, processados e punidos de maneira eficaz. Isso requer a

colaboração entre legisladores, especialistas em cibersegurança e juristas para criar leis específicas que abordem a complexidade do cibercrime (Santos, Ribeiro, 2018).

A proteção dos direitos e liberdades individuais na era digital também é um desafio importante. À medida que a tecnologia avança, é necessário garantir que as investigações e medidas de segurança respeitem esses direitos, equilibrando a aplicação da lei com a proteção dos cidadãos. Esse equilíbrio é essencial para garantir que a sociedade não apenas esteja segura contra crimes cibernéticos, mas também mantenha suas liberdades e privacidade. Por fim, a cooperação internacional desempenha um papel fundamental na luta contra o cibercrime, dada a natureza global da internet. Os crimes cibernéticos muitas vezes transcendem fronteiras, tornando necessária a colaboração entre países para rastrear e identificar criminosos cibernéticos. Acordos e tratados internacionais são fundamentais para garantir que os criminosos não encontrem refúgio em jurisdições estrangeiras. Em suma, a cibercriminalidade, seja na forma de crimes informáticos impróprios que se aproveitam da tecnologia para a prática de crimes tradicionais, ou crimes informáticos próprios que são exclusivos do ambiente digital, representa um desafio significativo para a sociedade moderna (Jesus, Aras, 2001). O combate a esses crimes exige uma abordagem multifacetada, que inclui legislação atualizada, conscientização pública, medidas técnicas de segurança e cooperação internacional. Somente com esses esforços coordenados podemos enfrentar eficazmente essa ameaça e garantir um ambiente digital mais seguro para todos.

## 3. OS MARCOS LEGAIS NACIONAIS E OS DIREITOS FUNDAMENTAIS

O advento das tecnologias digitais e da internet introduziu uma nova categoria de crimes, conhecidos como crimes cibernéticos, que são caracterizados por serem praticados no ambiente digital. A legislação brasileira tem passado por adaptações para lidar com essas novas formas de delinquência e oferecer respostas eficazes a essa crescente onda de criminalidade virtual. Por conseguinte, até 2012, o Brasil carecia de uma legislação específica para crimes cibernéticos próprios, ou seja, aqueles que só podem ser cometidos por meio de computadores e dispositivos tecnológicos. Vários projetos de lei foram apresentados no Congresso Nacional com o objetivo de estabelecer um marco legal para crimes cibernéticos. O Projeto de Lei nº 84/99, conhecido como Lei dos Crimes Digitais, proposto pelo deputado Luiz Piauhylino, visava tipificar ações como invasão de sistemas, roubo de senhas e criação de vírus, entre outros. Posteriormente, o senador Luiz Estevão apresentou o Projeto de Lei do Senado n.º 151/00, que propunha a obrigação de manter registros de conexão dos usuários da internet, buscando fortalecer o controle das atividades online e facilitar a investigação de crimes cibernéticos. Esses esforços resultaram na Lei nº 12.735/2012, também conhecida como Lei Azeredo, que incorporou novos tipos penais ao ordenamento jurídico. No entanto, a Lei Azeredo passou por simplificações que resultaram em uma integração dos novos tipos penais à Lei nº 12.737/2012. A evolução da legislação brasileira nesse contexto visou enfrentar a crescente onda de criminalidade cibernética.

No caso dos crimes cibernéticos impróprios, conforme explicado no item 2.2.1. deste estudo, a maior parte deles já está tipificada no Código Penal brasileiro. Esses delitos são caracterizados por utilizar a informática como meio para a prática do crime, sem que o bem jurídico afetado seja o dado informático em si. Este enfoque abrange uma série de infrações, incluindo fraudes, difamação e calúnia, que podem ocorrer tanto no mundo físico quanto no ambiente digital.

Apesar dos avanços legislativos no combate aos cibercrimes no Brasil, ainda existem desafios significativos. A legislação nacional deve se adaptar constantemente para regulamentar adequadamente o ambiente virtual, suas plataformas e reprimir tanto os crimes cibernéticos próprios quanto os impróprios. A rápida evolução do cenário cibernético e as novas modalidades de cibercrimes exigem uma atualização legislativa contínua. É essencial uma ampla discussão

sobre a melhor maneira de proteger os direitos dos cidadãos e combater os atos ilícitos no espaço digital, com foco especial na segurança de crianças e adolescentes.

Neste contexto, é fundamental explorar os desafios específicos relacionados à proteção de crianças e adolescentes no ambiente digital, uma vez que essa faixa etária está cada vez mais exposta a riscos cibernéticos.

No Brasil, a Lei nº 12.965, conhecida como o Marco Civil da Internet, é um exemplo de regulamentação que busca proteger os direitos das crianças e adolescentes no ambiente digital. Além disso, a Lei nº 13.441/2017, que trata sobre a infiltração de agentes policiais na internet, estabelece medidas de prevenção e combate a crimes de exploração sexual contra menores, reconhecendo os perigos online. No entanto, os desafios persistem, à medida que o mundo digital continua a evoluir rapidamente. A proteção de crianças e adolescentes no ambiente cibernético não é apenas uma questão de legislação, mas também de educação, conscientização e cooperação entre governo, sociedade e empresas de tecnologia. Compreender os desafios que o cibercrime impõe à proteção dos jovens é fundamental para desenvolver estratégias eficazes e garantir que a geração do futuro possa navegar pelo mundo digital com segurança e confiança. A proteção de crianças e adolescentes no ambiente digital é uma preocupação global que requer a atenção contínua de todos os setores da sociedade. A legislação brasileira precisa ser analisada à luz dessas questões, e medidas adicionais podem ser necessárias para garantir a segurança desses jovens no mundo virtual. Assim, este capítulo analisará a legislação atual e aprofundará essa análise, examinando como os principais ataques cibernéticos se alinham à legislação brasileira.

## 3.1. LEI Nº 10.695, DE 01 DE JULHO DE 2003

A evolução das tecnologias digitais e da internet trouxe consigo um conjunto de desafios jurídicos, incluindo a necessidade de adaptação da legislação brasileira para lidar com as novas modalidades de crimes cibernéticos. Uma área significativamente afetada é a proteção dos direitos autorais e dos direitos conexos, especialmente no contexto das crianças e adolescentes.

A Lei nº 10.695, promulgada em 01 de julho de 2003, introduziu modificações significativas no Código Penal e no Código de Processo Penal, relacionadas à

violação de direito autoral e direitos conexos. Antes dessa lei, a legislação brasileira tipifica como crime apenas a violação dos direitos autorais, negligenciando os direitos relacionados a artistas intérpretes ou executantes, produtores fonográficos e empresas de radiodifusão (Carboni, 2003). Essa lacuna foi preenchida pelo primeiro artigo da Lei nº 10.695, que promoveu alterações no artigo 184 do Código Penal. Esse artigo estabelece penalidades para a distribuição, sem fins lucrativos, de obras intelectuais, fonogramas e videofonogramas reproduzidos com violação do direito autoral. Segundo o texto, o infrator estaria sujeito a detenção por um período de seis meses a dois anos ou multa. Além de estender a proteção legal aos direitos conexos, a lei também incorporou, por meio de seu parágrafo terceiro, as ações realizadas com suporte tecnológico. Isso foi uma medida fundamental para combater a ciberpirataria, permitindo a apreensão e, quando apropriado, a destruição de cópias ou reproduções realizadas com violação dos direitos autorais e conexos. Além disso, a lei possibilitou a interdição de estabelecimentos que cometem esses delitos.

Essas mudanças na legislação têm implicações significativas para a proteção de crianças e adolescentes no ambiente digital. Como um grupo particularmente vulnerável, a exposição a conteúdo ilegal ou prejudicial é uma preocupação. A lei fortaleceu as medidas de repressão à distribuição de conteúdo protegido por direitos autorais que seja inapropriado para menores, contribuindo para um ambiente online mais seguro (Carboni, 2003).

Ao comparar a legislação brasileira com a Convenção de Budapeste, verifica-se que a salvaguarda dos direitos conexos se alinha ao que é estabelecido no artigo 10 da Convenção. A incorporação do terceiro parágrafo do artigo 184 do Código Penal do Brasil atende ao mandato da Convenção de Budapeste, especialmente no que se refere à perpetração de delitos por meio de sistemas informáticos. Essas mudanças na legislação refletem o esforço contínuo do Brasil em adaptar seu arcabouço jurídico à era digital, protegendo não apenas os direitos autorais, mas também a integridade de crianças e adolescentes na rede.

## 3.2.LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012

A Lei nº 12.735/2012, conhecida como Lei Azeredo, representa um marco importante na luta contra os crimes cibernéticos no Brasil. Proposta pelo Senador

Eduardo Azeredo, sucedendo os projetos de lei nº 89/2003, nº 76/2000 e nº 137/2000, e sancionada em 30 de novembro de 2012, essa legislação teve como propósito principal tipificar condutas realizadas por meio de sistemas eletrônicos digitais, ou similares, e aquelas perpetradas contra sistemas informatizados e seus equivalentes.

Os primeiros artigos da Lei 12.735/2012 focaram na tipificação de delitos praticados no ambiente virtual. As condutas relacionadas à falsificação de cartão de crédito, já previstas no Código Penal e no Código Penal Militar, foram inicialmente contempladas nos artigos 2º e 3º, mas foram vetadas na sanção final da lei. Além disso, a lei contemplou aspectos processuais e penais no combate aos crimes digitais. O artigo 4º fundamentou a criação de órgãos especializados para lidar com esses delitos, reconhecendo a importância de profissionais tecnicamente preparados para investigar crimes cibernéticos, que muitas vezes requerem a localização e análise de equipamentos informáticos e dos dados armazenados neles.

Por outro lado, o artigo 5º alterou a redação do §3º do Art. 20 da Lei nº 7.716/1989, que define crimes decorrentes de preconceito de raça ou cor, com o intuito de coibir a disseminação de preconceito e intolerância racial por meio das novas tecnologias.

A origem da Lei Azeredo remonta ao Projeto de Lei nº 84/1999, que buscava definir os crimes cibernéticos, tornando certas condutas praticadas no ambiente cibernético passíveis de prisão e multa. Esse projeto inicial foi, por vezes, denominado de "AI-5 Digital" devido à amplitude e rigidez de suas propostas, o que o colocou em espera por alguns anos. O deputado Eduardo Azeredo retomou a discussão em 2008 e, após mudanças significativas e a retirada de vários artigos, a Lei 12.735/2012 foi finalmente promulgada em 2012, embora tenha sofrido veto parcial da então presidente Dilma Rousseff. Embora a Lei Azeredo tenha sido criada especificamente para tipificar os crimes cibernéticos, este papel acabou sendo atribuído à Lei 12.737 de 2012, promulgada no mesmo ano. Assim, a Lei Azeredo desempenhou um papel crucial na evolução da legislação brasileira sobre crimes cibernéticos, estabelecendo as bases para a legislação subsequente.

### 3.3.LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012

A Lei nº 12.737/2012, também conhecida como Lei Carolina Dieckmann, foi um marco crucial na legislação brasileira no combate aos crimes cibernéticos. Apresentada pelo Deputado Federal Paulo Teixeira e promulgada em 30 de novembro de 2012, seu rápido processo de implementação foi impulsionado pela pressão da mídia, resultado do notório caso da atriz Carolina Dieckmann. Este incidente, onde fotos íntimas foram roubadas e divulgadas após a invasão de sua conta de e-mail por cibercriminosos, instigou a necessidade urgente de regulamentar os crimes virtuais, ganhando a lei o apelido popular de "Lei Carolina Dieckmann".

Esta legislação inovou no ordenamento jurídico brasileiro ao tipificar novos delitos, ampliando o alcance da legislação sobre crimes digitais. Introduziu no Código Penal artigos que visam tratar da invasão de dispositivo informático, interrupção ou perturbação de serviço telemático ou de informação de utilidade pública, e a falsificação de cartão.

Um aspecto crucial é o artigo 2º da Lei, que trata das ações relacionadas à "invasão de dispositivo informático". Esta medida expandiu o Código Penal ao introduzir os artigos 154-A e 154-B, visando penalizar aqueles que invadem, adulteram ou destroem a privacidade digital de terceiros, ao violar mecanismos de segurança. Entretanto, a lei exige a existência de um mecanismo de segurança no dispositivo eletrônico da vítima para que a ação seja considerada um crime.

O artigo 154-A, incluído pela Lei 12.737/2012, busca combater condutas criminosas baseadas na invasão de dispositivos informáticos de terceiros, conectados ou não à internet, e condiciona a criminalização à violação concreta e indevida de mecanismos de segurança. Este artigo também considera os efeitos patrimoniais da invasão. Por sua vez, o artigo 154-B estabelece que a ação penal para o crime de "invasão de dispositivo informático" será pública, condicionada à representação da vítima, exceto nos casos em que o delito for cometido contra a administração pública direta ou indireta.

Essas alterações têm uma correlação com a Convenção de Budapeste. O artigo 154-A está alinhado com o artigo 2 da Convenção, que trata de acesso ilegítimo. Além disso, o parágrafo 1 do artigo 154-A está parcialmente em conformidade com o item 1.a.i do artigo 6 da Convenção, que aborda o uso abusivo de dispositivos.

Além disso, a Lei nº 12.737/2012 também alterou os delitos tipificados nos artigos 266 e 298 do Código Penal, incluindo o serviço informático, telemático ou de informação de utilidade pública no artigo 266, tornando sua interrupção um crime. No artigo 298, foi incluído o delito de falsificação de cartão.

Em suma, a Lei Carolina Dieckmann foi um passo significativo para preencher as lacunas normativas, visando uma repressão e punição mais eficazes dos ilícitos no ambiente virtual. No entanto, apesar das melhorias trazidas por essa lei, o combate a esses crimes ainda apresenta desafios significativos, devido à constante evolução tecnológica e globalização, que tornam o ambiente virtual propício para a atuação de criminosos.

## 3.4.LEI Nº 12.965, DE 23 DE ABRIL DE 2014

Antes do advento do Marco Civil da Internet, o Brasil carecia de legislação abrangente para regulamentar questões relacionadas à internet. As resoluções estabelecidas pelo Poder Executivo eram o principal recurso para suprir a lacuna legal em meio a questões emergentes no ambiente online. O Projeto de Lei que culminou na Lei nº 12.965/2014 iniciou em 2009, com o projeto de lei nº 2.126/2011. Esse texto foi submetido a um processo de consulta pública em várias localidades do país, no qual diversas sugestões relacionadas ao tema foram discutidas no Legislativo e muitas delas foram incorporadas ao texto final.

O Marco Civil da Internet, correspondente à Lei nº 12.965, promulgada em 23 de abril de 2014, estabelece princípios, diretrizes, garantias, direitos e deveres para o uso da internet no Brasil, aplicáveis a usuários, governo e provedores de serviços e acessos. Foi desenvolvido com o propósito de promover o uso ético da internet, assegurando os direitos dos usuários, especialmente no que se refere à inviolabilidade da intimidade e vida privada, embora não tipifique condutas.

A lei aborda de modo especial a liberdade de expressão e a proibição da censura, expressamente garantidas nos artigos 2º e 19. Além disso, o artigo 3º, I, estabelece princípios essenciais do uso da internet, como a liberdade de expressão, comunicação e manifestação do pensamento. A Lei nº 12.965/2014 também enfatiza a importância da privacidade, garantindo a inviolabilidade da intimidade e vida privada, preservando o sigilo das comunicações transmitidas ou armazenadas,

e proíbe a divulgação de dados coletados pela internet sem o consentimento prévio do usuário.

O registro e a guarda dos logs de acesso dos usuários à rede são contemplados no Marco Civil da Internet. O artigo 14 estabelece que os provedores de acesso e conteúdo na internet não podem armazenar registros de acesso sem o consentimento prévio do usuário, enquanto o artigo 13 impõe a obrigação de guardar esses registros pelo período mínimo de um ano. Da mesma forma, estabelece regras para a responsabilidade civil dos provedores de internet em casos de ofensa aos direitos da personalidade. Assim, os provedores podem ser responsabilizados por danos decorrentes de conteúdos publicados em suas plataformas caso não os removam após ordem judicial. Ademais, o artigo 29, juntamente com seu parágrafo único, reconhece o direito do usuário da internet de instalar em seu computador pessoal programas de controle parental, para filtrar conteúdo considerado inadequado para menores.

Apesar dessas disposições, a proteção oferecida pela lei penal ainda não está plenamente efetivada. A inviolabilidade da intimidade e vida privada e o sigilo das comunicações ainda são tratados de maneira restrita no artigo 7º da lei. De maneira similar, a Lei de Proteção de Dados, Lei 13.709/2018, ainda carece de inovações legislativas para uma proteção mais abrangente dos bens jurídicos.

O Marco Civil da Internet representa um avanço significativo ao estabelecer os direitos e deveres para o uso da internet, assegurando liberdade de expressão, intimidade e vida privada, além de estabelecer as bases para a responsabilidade civil dos provedores de internet em caso de violação dos direitos individuais. No entanto, sua aplicação integral ainda enfrenta desafios, especialmente no âmbito da legislação penal, abrindo espaço para debates contínuos sobre como reforçar a proteção dos direitos do usuário na era digital. Sendo uma legislação pioneira, busca equilibrar a liberdade de expressão e a privacidade dos usuários na internet, embora ainda esteja em fase de avaliação para determinar seu impacto total e a completa efetivação de seus preceitos.

### 3.5. LEI nº 13.964, DE 24 DE DEZEMBRO DE 2019

A Lei nº 13.964, conhecida popularmente como Lei Anticrime, foi promulgada em 24 de dezembro de 2019, introduzindo uma série de modificações no sistema jurídico penal brasileiro, impactando significativamente o Código Penal, o Código de Processo Penal, a Lei de Execução Penal, e outras legislações correlatas.

Uma das mudanças mais notáveis estabelecidas por essa lei foi a criação do "juiz de garantias", uma nova figura responsável por atuar durante a fase de inquérito policial. Seu papel envolve a análise e decisão sobre solicitações como quebra de sigilo e emissão de mandados de prisão preventiva, com a finalidade de assegurar um julgamento mais imparcial. Outro destaque da Lei Anticrime é a introdução do Acordo de Não Persecução Penal (ANPP). Esse acordo permite que o Ministério Público proponha uma alternativa de acordo ao acusado em casos de crimes sem violência ou grave ameaça, desde que a pena mínima prevista seja inferior a 4 anos. Além disso, a legislação trouxe alterações significativas na progressão de regime para condenados por crimes hediondos e ampliou o conceito de legítima defesa para incluir agentes de segurança pública. Novas regras para o cumprimento de penas também foram estabelecidas, determinando que, para progressão de regime, o condenado deverá cumprir 40% da pena se for reincidente, ou 25% se for primário.

No âmbito do combate ao crime organizado, a Lei Anticrime fortaleceu o uso de mecanismos como as colaborações premiadas e a infiltração de agentes, além de endurecer a legislação relacionada às organizações criminosas. Ela também fez modificações na Lei nº 9.296/96, que trata das interceptações telefônicas. Nesse contexto, a lei introduziu o artigo 10-A, que caracteriza a prática de realizar captação ambiental de sinais eletromagnéticos, ópticos ou acústicos para fins de investigação ou instrução criminal sem a devida autorização judicial. Essa lei representa um marco fundamental no sistema penal brasileiro, trazendo várias mudanças destinadas a aprimorar a justiça penal e a eficácia no combate ao crime. No entanto, é relevante destacar que certos aspectos dessa legislação têm sido alvo de debates intensos na comunidade jurídica e na sociedade, indicando que a aplicação e efetividade da lei serão continuamente discutidas e avaliadas no futuro. Embora essa nova tipificação criminal esteja em conformidade com as disposições do artigo 3º da Convenção de Budapeste, é crucial observar que o crime só se configura

quando a captação de sinais é realizada com a finalidade específica de investigação ou instrução criminal. Outras formas de captação de sinais, que não estejam vinculadas a esses propósitos, não são consideradas crimes de acordo com essa legislação.

### 3.6.LEI Nº 14.155, DE 27 DE MAIO DE 2021

A Lei 14.155, sancionada em 27 de maio de 2021, trouxe mudanças significativas na legislação penal brasileira, especialmente em relação aos crimes cibernéticos. Seu foco primário foi a ampliação das penalidades para delitos cometidos por meio da internet, com ajustes em diversas seções do Código Penal.

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. ...
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

No que diz respeito à invasão de dispositivos informáticos, a Lei buscou aumentar a punição, eliminando a exigência anterior de que a invasão ocorresse por meio de violação de mecanismos de segurança. Essa alteração teve o intuito de tornar as penas mais severas para os invasores, mesmo sem a necessidade de quebra de barreiras de segurança. Adicionalmente, houve mudanças no crime de furto qualificado, estipulando penas mais duras quando o delito é praticado com o uso de fraude eletrônica ou programas maliciosos, especialmente quando a vítima é idosa ou vulnerável. No contexto do estelionato, a nova legislação inaugurou o "estelionato eletrônico", onde a utilização de informações induzidas por meio de redes sociais, ligações telefônicas ou e-mails fraudulentos, é considerada um agravante, com aumento de pena para os casos que envolvem servidores mantidos fora do território nacional ou quando a vítima é idosa ou vulnerável.

Entretanto, as penalidades estabelecidas pela Lei 14.555/2021 geram debates sobre a justiça das punições para crimes digitais. Em alguns casos, as sanções são mais severas do que aquelas aplicadas a crimes que afetam diretamente a vida ou a saúde das pessoas. Essa disparidade destaca o desafio

que os legisladores enfrentam ao tentar equilibrar a necessidade de punir e prevenir os delitos digitais sem comprometer a consistência do sistema penal.

Além das mudanças na legislação, ações preventivas e educacionais são fundamentais no combate aos crimes digitais. Informar o público sobre os riscos online e incentivar práticas seguras na internet são componentes vitais para reduzir a ocorrência desses crimes. Assim, as estratégias para combater delitos cibernéticos devem ser abrangentes, envolvendo não apenas a aplicação efetiva da lei, mas também a promoção da segurança digital e a educação tecnológica. Consequentemente, a Lei 14.555/2021 representa um marco significativo na legislação penal brasileira, introduzindo penas mais rígidas e estendendo a jurisdição para crimes eletrônicos. No entanto, a discussão persiste em torno de certos aspectos da lei, como a determinação da jurisdição baseada no domicílio da vítima, o que pode dificultar a eficiência das investigações e do processo penal. A contínua revisão e aprimoramento da legislação são essenciais para garantir uma resposta justa e adequada aos crimes cibernéticos, considerando a complexidade inerente a esses tipos de delitos.

### 3.7. O surgimento da proteção da Criança e do Adolescente

Ao longo das últimas décadas, houve uma notável evolução no reconhecimento dos direitos de crianças e adolescentes, guiada por diversos movimentos e marcos legais internacionais. Esse progresso é reflexo de uma mudança de paradigma, que passou de considerar a criança como mero objeto de proteção para reconhecê-la como um sujeito de direitos merecedor de proteção especial.

As convenções da Organização Internacional do Trabalho (OIT) em 1919 constituíram marcos importantes para os direitos das crianças, abordando especificamente suas condições no contexto laboral. Duas das seis convenções aprovadas tratavam diretamente dos direitos das crianças: a Convenção sobre a idade mínima para o trabalho na indústria e a Convenção que proibia o trabalho infantil em certas atividades. Esses avanços surgiram após uma série de greves na Europa entre 1917 e 1918, onde crianças foram exploradas como mão-de-obra, trabalhando longas horas e recebendo salários injustos em comparação com os adultos (Ribeiro, Veronese, 2021).

O primeiro documento internacional que teve como foco os direitos da criança foi a Declaração de Genebra, em 1924, também conhecida como Carta da Liga sobre a criança, surgiu após a Primeira Guerra Mundial devido à criação da Associação Salve as Crianças na Inglaterra. Esta declaração, adotada pela Liga das Nações (atual ONU), foi o primeiro documento amplo sobre o tratamento da infância, indo além da abordagem centrada no trabalho infantil. Embora não tenha reconhecido a criança como um sujeito de direitos, estabeleceu importantes alertas de proteção e pavimentou o caminho para futuras conquistas nessa área.

A Declaração Universal dos Direitos Humanos, proclamada pela ONU em 1948, mencionou a necessidade de atenção e cuidados especiais para as crianças, embora de maneira implícita, indicando a importância de garantir seus direitos e liberdades.

Em 1959, aprovou-se a Declaração Universal dos Direitos da Criança, complementar à Declaração Universal dos Direitos Humanos. Essa Declaração representou um marco, pois reconheceu a vulnerabilidade das crianças e a necessidade de proteção por meio de uma legislação especial. No entanto, o Brasil demorou quase 20 anos para adotar essa doutrina, instituindo o Código de Menores em 1979, quando poderia ter antecipado essa abordagem integral para a proteção da infância. Essa declaração apresentava dez princípios, mas assim como a Declaração Universal dos Direitos Humanos, carecia de pactos para tornar-se efetiva (Ribeiro, Veronese, 2021).

A Convenção sobre os Direitos da Criança, apesar de ter tido seus debates iniciados em 1979, foi aprovada somente em 1989, a Assembleia-Geral das Nações Unidas aprovou, por unanimidade, a Convenção Internacional sobre os Direitos da Infância. Este tratado tornou-se o mais ratificado na história, representando um marco significativo na proteção integral de crianças e adolescentes, estabelecendo a prioridade e o interesse supremo da criança como regras fundamentais. No entanto, com o tempo, ficou claro que apenas a Convenção era insuficiente, necessitando de abordagens mais específicas para temas como exploração infantil, envolvimento em conflitos armados, prevenção da delinquência na infância e adolescência,, administração da justiça para crianças e privação da liberdade de crianças e adolescentes (Ribeiro, Veronese, 2021).

Já antes da aprovação desta Convenção pela Assembleia Geral da ONU, o Brasil havia introduzido, em 1988, na Constituição Federal, a doutrina da proteção

integral, evidenciada no artigo 227. Este artigo constitucional estabeleceu um sistema focado na proteção dos direitos fundamentais de crianças e adolescentes, com responsabilidade compartilhada entre Estado, família e sociedade.

Com base na Constituição Federal e nos documentos internacionais existentes, foi promulgado o Estatuto da Criança e do Adolescente (ECA), em 1990, substituindo o antigo Código de Menores. O ECA foi orientado pela doutrina da proteção integral e mudou o foco da legislação, reconhecendo crianças e adolescentes como sujeitos de direitos. O Estatuto classificou como criança a pessoa com até 12 anos incompletos e como adolescente aquele entre 12 e 18 anos, em contraste com a normativa internacional que considera criança a pessoa até 12 anos (Ribeiro, Veronese, 2021).

O princípio da proteção integral é um dos pilares do ECA, garantindo a proteção de crianças e adolescentes de forma absoluta, tanto pelo Estado quanto pela família, pelas entidades comunitárias e pela sociedade em geral, como estipulado no artigo 4º do Estatuto. Este princípio se reflete no artigo 1º do ECA, assegurando essa proteção de maneira integral e priorizada.

A legislação do ECA e as normas internacionais ressaltam os direitos fundamentais das crianças e adolescentes, salientando o papel compartilhado de diferentes instâncias na garantia desses direitos, refletindo a preocupação com o desenvolvimento saudável e o bem-estar dessa população (Ribeiro, Veronese, 2021).

A promulgação da Lei nº 8069 em 13 de julho de 1990 marcou a criação do Estatuto da Criança e do Adolescente. Este estatuto emergiu do contexto democrático e das discussões que envolveram a formulação do artigo 227 da Constituição Federal de 1988, introduzindo paradigmas inovadores na proteção dos direitos desses indivíduos, agora considerados sujeitos de direito, em um estágio peculiar de desenvolvimento, destinados a receber prioridade absoluta. Os dispositivos presentes nesse Estatuto têm como objetivo primordial a proteção dos direitos das crianças e adolescentes de maneira exclusiva e abrangente. O Artigo 3º desse Estatuto delineia diretrizes específicas, estabelecendo ações e procedimentos que visam garantir e aprimorar os direitos dessa parcela da população, enfatizando a importância da proteção integral e do cuidado especial com essa faixa etária.

> Art. 3º A criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, assegurandose-lhes, por lei ou por outros meios, todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade. Parágrafo único. Os direitos enunciados nesta Lei aplicam-se a todas as crianças e adolescentes, sem discriminação de nascimento, situação familiar, idade, sexo, raça, etnia ou cor, religião ou crença, deficiência, condição pessoal de desenvolvimento e aprendizagem, condição econômica, ambiente social, região e local de moradia ou outra condição que diferencie as pessoas, as famílias ou a comunidade em que vivem (BRASIL, 1990).

Dessa forma, os dispositivos deste Estatuto têm a função de assegurar os direitos de crianças e adolescentes, de forma específica e ampla, estabelecendo diretrizes e procedimentos para a manutenção e aprimoramento de seus direitos, conforme expresso no artigo 3º deste Estatuto (Ribeiro, Veronese, 2021).

Os princípios fundamentais que guiam o direito da criança e do adolescente são essenciais para estabelecer equilíbrio e justiça nas relações jurídicas, visando garantir seus direitos fundamentais com normas protetivas distintas das aplicadas aos adultos. Esses princípios são embasados na Constituição Federal de 1988 e consolidados pelo Estatuto da Criança e do Adolescente. Dentre esses princípios, o princípio do melhor interesse da criança e do adolescente remonta ao instituto protetivo do direito anglo-saxônico. Com a adoção da doutrina da proteção integral pela Convenção Internacional sobre os Direitos da Criança, os direitos fundamentais para a infância e adolescência foram reconhecidos, transformando a aplicação desse princípio, estabelecendo que suas necessidades devem ser a prioridade máxima (Cury, 2005).

O princípio da prioridade absoluta, consagrado no artigo 227 da Constituição Federal de 1988 e reforçado pelo Estatuto da Criança e do Adolescente, destaca-se pela necessidade de aplicação invariável dessa norma em todos os casos envolvendo crianças e adolescentes. A Constituição Federal coloca a vida, saúde, educação, lazer, dignidade, entre outros, como prioridades absolutas desses indivíduos, exigindo que o Estado, a sociedade e a família garantam esses direitos em primeiro plano, sem exceção. O princípio da municipalização está ligado à descentralização das ações governamentais e assistenciais para facilitar o atendimento aos programas de assistência às crianças e adolescentes. O município tem um papel essencial nesse cenário, já que é capaz de perceber as necessidades

específicas dessa população e aplicar a doutrina da proteção integral, sem prejudicar a responsabilidade conjunta dos Estados e da União. O princípio da brevidade se concentra na aplicação de medidas socioeducativas privativas de liberdade, estabelecendo um tempo limite para a manutenção dessas medidas. A privação de liberdade, como uma medida de proteção específica, deve ser cumprida em um local distinto daquele destinado ao abrigo, garantindo a separação entre internados, levando em conta a gravidade dos atos infracionais e a necessidade de um ambiente propício para a reintegração social. Por fim, o princípio da convivência familiar assegura o direito fundamental da criança e do adolescente de viver junto à sua família natural ou subsidiariamente à sua família extensa. Constitucionalmente reconhecido, este princípio estabelece que o Estado, a sociedade e a família devem assegurar o direito à vida, à saúde, à alimentação, à educação e à convivência familiar e comunitária desses indivíduos, protegendo-os de qualquer negligência, violência ou crueldade (Cury, 2005).

Infere-se, portanto, que estes princípios representam a espinha dorsal para a garantia e proteção dos direitos da infância e adolescência, alinhando a legislação e a atuação dos diversos setores para assegurar um ambiente saudável e promissor para o desenvolvimento desses jovens cidadãos. Dessa forma, a Constituição Federal de 1988, juntamente com o Estatuto da Criança e do Adolescente, estabeleceu um novo paradigma, conferindo prioridade absoluta aos direitos dessas crianças e adolescentes. Os princípios do melhor interesse da criança, da prioridade absoluta, da municipalização, da brevidade e da convivência familiar servem como pilares fundamentais para garantir o desenvolvimento saudável e protegido de cada criança e adolescente. Assim, a aplicação desses princípios não é apenas uma responsabilidade legal, mas um compromisso moral e social que envolve a família, a sociedade e o Estado. Eles exigem uma abordagem holística, buscando sempre o melhor para as crianças e adolescentes, colocando seus interesses e necessidades em primeiro plano.

No entanto, é importante notar que o progresso legislativo é apenas o primeiro passo. A efetiva implementação e cumprimento desses princípios demandam uma ação contínua e coerente, isso acaba por envolver a atuação comprometida de todos os setores da sociedade, garantindo não apenas a existência de leis protetivas, mas também sua efetiva aplicação em situações reais,

assegurando a criação de um ambiente seguro, saudável e propício para o crescimento e desenvolvimento de todas as crianças e adolescentes.

## 4. A EROTIZAÇÃO DA INFÂNCIA POR MEIO DOS VEÍCULOS DE COMUNICAÇÃO SUA CONSEQUÊNCIA SOCIAL E O CIBERCRIME

A medida em que observamos o constante avanço da era tecnológica, juntamente com o frequente uso das redes sociais na vida das pessoas, especialmente das crianças e adolescente que, atualmente nascem e se desenvolvem imersos nesse cenário, torna-se imperativo analisar os possíveis impactos negativas que podem vir a serem acarretadas neste panorama. As implicações decorrentes desta nova era tecnológica são notórias no comportamento do indivíduo, no desenvolvimento como membro da sociedade e na formação de seu pensamento, principalmente quando se considera a idade tão tenra dos envolvidos (Borges, Javorski, 2022).

As implicações negativas mencionadas anteriormente influenciam diversos aspectos do crescimento da criança, são exemplos destes, danos físicos, mentais, sociais e sexuais. No tocante deste último tema, é notório que atualmente, fazendo uma observação do cenário mundial mas com principal foco no panorama brasileiro, há uma grande erotização da infância, erotização a qual decorre das mais variadas formas. Nota-se diariamente, nos principais veículos de comunicação utilizados em nosso país, tais quais, televisão e redes sociais, uma grande vinculação publicitária da imagem de crianças com produtos adultos, publicidades muitas vezes passadas em rede nacional, onde são expostas crianças com maquiagens, sapatos, bolsas e roupas “adultizadas” o que estimula as crianças a se portarem como adultos (Bolzan, Silva, 2019).

As mensagens mercadológicas possuem uma grande influência sobre as pessoas, impactando em suas formas de se vestir, de se comportar e de ver a realidade e, as crianças e adolescentes são hipervulneráveis a isso. Esta influencia exercida pelas publibicidades não se resumem somente à preocupação de que nossas crianças serão mais tendenciosas ao consumismo pois, em contrapartida a esta óptica, tem-se a questão de como a sociedade passará a enxergar estas crianças após a normalização dessa erotização infantojuvenil feitas pelos veículos de comunicação (Bolzan, Silva, 2019).

Em decorrência desses conteúdos publicitários e do fácil acesso a internet, onde crianças acabam tendo acesso muito precocemente a conteúdos não apropriados para suas idades, acaba dando-se origem às chamadas “Kids Growing

Older Younger", sigla "KGOY", que faz alusão às crianças que se comportam como adultas de forma precoce, comportamento o qual decorre justamente o excesso de informação que acaba estando disponível em todas as plataformas como um todo (Bolzan, Silva, 2019). Por conseguinte, os resultados derivados tantos da erotização da infância pelas mídias, tanto como resultado desses fatos, que são às crianças se comportarem como adultos, torna-se fundamental reforçar a atenção para os desafios decorrente da exposição de conteúdo erotizando o público infantil, visto que "o erótico é distorcido em relação à idade e entra como mais uma forma de atração, fascínio e sedução. Os próprios significados são dados de fora para dentro"(Bolzan, Silva, 2019).

Apesar de haver uma resolução criada pelo Conselho Nacional dos Direitos da Criança e do Adolescente, especificamente a de número 163 artigo 2º de 2014, que dispõe em sua redação as publicidades que são consideradas abusivas (Bolzan, Silva, 2019), há ainda uma grande cultura em nossa sociedade no que versa a forma de ver a criança e no que se é entendido por infância. Um grande exemplo que comprova a visão deturpada e normalizada supramencionada é o caso da empresa "Valisere Ind. e Com. Ltda – Meu 1º Valisere", que em meados de 2013 foi denunciada devido à autoria de uma propaganda onde haviam cartazes e catálogos que faziam a oferta de pijamas e lingeries, tendo como seu público alvo a faixa etária entre 8 a 12 anos, expondo meninas e seus corpos infantis usando essas peças intimas e posando para as fotos e desfiles da mesma forma que as modelos adultas a fariam, sugerindo exposição erótica (Bolzan, Silva, 2019).

Mediante a fatídica denúncia que havia sido feita ao Projeto Criança e Consumo, a referida empresa demonstrou surpresa ao ser informada sobre a promoção desse tipo de conteúdo utilizando crianças, alegou também que este tipo de conteúdo não tinha respaldo algum na empresa e nem na sua política de marketing e se comprometeu em notificar seus lojistas da proibição do uso de crianças para a promoção daquele tipo de produto, o que resultou no arquivamento do processo. Apesar de arquivado o processo e retirados de ar a campanha que continham estes conteúdos, é de muito fácil acesso a estas imagens pela plataforma "Google", tornando contínua e duradoura a exposição de corpos infantis (Bolzan, Silva, 2019).

Ao mesmo passo em que em nossa sociedade contemporânea têm usado cada vez mais as crianças como um veículo de consumo, usando a imagem destas

muitas vezes de forma indiscriminada, acaba se tendo cada vez mais a concepção da infância como um objeto digno de desejo, apreciação, como se houvesse, e de fato há, uma normalização “inconsciente” que instiga uma espécie de ideologia a pedofilia, de forma que a incita de formas “veladas”, tendo assim um resultado negativo decorrente da excessiva exposição sem as devidas supervisões e limitações (Bolzan, Silva, 2019).

No contexto em que vivemos, a partir do momento em que um conteúdo é disseminado na internet, torna-se basicamente impossível a sua remoção ou esquecimento, o que afeta diretamente na eficácia das solicitações de remoção de conteúdo após sua indevida publicação. A partir do momento que algo é publicado nas redes, o conteúdo se espalha rapidamente e, nada pode impedir que este conteúdo seja salvo, compartilhado ou arquivado pelos visualizadores com as mais diversas finalidades, incluindo a postagem nas redes de pornografia (Bolzan, Silva, 2019).

É possível afirmar que, apesar de todo o trâmite que se tem previsto para a solicitação da remoção de determinada postagem ou conteúdo, por mais eficaz que seja o procedimento e independentemente do tempo que tenha demorado para ser deferido, as imagens ainda estarão disponíveis a acesso, é algo que foge do controle da jurisdição atual, fazendo com que a jurisdição existente não seja suficiente, havendo a urgência de uma ação conjunta para que se evite essa exposição problemática feita em diversas publicidades para que só assim não restem vestígios de tais imagens deturpadas que atentam contra o verdadeiro sentido da infância (Veronese, 2019).

## **4.1** VIOLAÇÃO SEXUAL DE INFANTES PELA INTERNET. CIBERCRIME, PEDOFILIA E A PORNOGRAFIA INFANTIL

O direito penal brasileiro exerce função de tutela em diversos direitos que devem ser resguardados pelas leis, dentre esses direitos tutelados tem-se a liberdade sexual das pessoas. No código penal brasileiro, há previsões específicas destacando e tipificando os delitos que têm na figura de vítima crianças e adolescentes. No que tange a liberdade sexual dos infantes, nosso ordenamento possui uma preocupação maior, tendo em vista a não existência de consentimento para menores de 14 anos e também observando a fase de desenvolvimento em que

se encontram, pois qualquer ato de violação sexual nessa fase de desenvoltura acarretarão traumas que acompanharão essas vítimas pelo restos de suas vidas (Neumann, 2016)

A violação da liberdade sexual das pessoas infelizmente existe desde os primórdios, acompanhando a evolução do homem na sua história, todavia é inegável o fato de que a ascensão da internet contribui muito para o aumento e a facilitação do cometimento deste tipo de delito. Há várias pesquisas que tange sobre a questão do acesso de criança às redes e, em uma dessas pesquisas, especificamente a que foi feita pela BitDefender (empresa especializada em segurança na internet), com um número superior a 1500 pais, apresenta que, 95% dos que foram entrevistados afirmaram ter total ciência de que seus filhos acessam ou então já acessaram conteúdo adultos. Quando indagados sobre de que forma passaram a supervisionar e controlar esse tipo de atividade  informarem que foi através de instalação de software de controle, programas os quais podem ser facilmente burlados pelas crianças (Neumann, 2016).

No contexto societário atual, é inegável o fato de que as crianças passam a ter acesso à internet cada vez mais precocemente, que de uma certa óptica pode ser visto como um ponto positivo, tendo em vista que a facilitação ao acesso às redes pode sim ajudar na formação educacional delas. Por um outro lado, esse dado pode ser alarmante, pois essas crianças e principalmente os adolescentes se tornam diariamente mais viciados e dependentes dos meios de veículos de informação, acessando essas plataformas diariamente e na maioria delas sem supervisão dos responsáveis, consequentemente se tornando alvos fáceis de cibercriminosos, muito deles com transtornos psiquiátricos (Neumann, 2016).

Em 1990 houve uma grande explosão da internet, onde as pessoas que tinham acesso às redes faziam uso diário e, segundo a exposição de Hisgail:

> “Na década de noventa, a exploração comercial e sexual infantil vitimou milhões de crianças e adolescentes no mundo. Devido à pobreza, o desemprego, e desestruturação familiar e a banalização da sexualidade, a pedofilia surge na calada da vida cotidiana como perversão sexual, a ponto de interferir de forma drástica no desenvolvimento psíquico infantil provocando traumas irreversíveis e doenças transmissíveis por sexo. A infância, convocada pelo adulto a assumir uma identidade sexual, mostra-se nas imagens eletrônicas da pornografia infantil. Esse fenômeno, criado pela cultura moderna se destaca como um sintoma do mal-estar da atualidade, ao mesmo tempo em que mobiliza legiões contra a pornografia infantil”. (Hisgail, 2007, p. 17)

Dentre todos os aplicativos e meios de acesso possíveis à internet, podemos colocar como principal meio facilitador para o cometimento de crime contra vulneráveis às redes sociais. Com a popularização e frequente uso de rede social pelos indivíduos, torna-se muito fácil se passar por outras pessoas na internet a partir da criação de perfis falsos para que, a partir desses, se permita aproximar das vítimas de forma online e posteriormente, criar-se a possibilidade de um encontro físico.

O comportamento citado anteriormente é muito recorrente aos pedófilos. Segundo Breier Trindade, "A palavra pedofilia, etimologicamente, deriva do grego paidofilia, a partir das matrizes paidós (criança) e philia (amor, a amizade), significando, originalmente, “amor por crianças”, (Trindade, 2010). De acordo com a autora  Raquel Fernandes Tavares de Moraes, a classificação da pedofilia é compreendida como: “Um transtorno psiquiátrico classificado entre os chamados transtornos da preferência sexual ou parafilias, caracterizado por fantasias, atividades, comportamentos ou práticas sexuais intensas e recorrentes envolvendo crianças ou adolescentes menores de 14 anos de idade. Isso significa que o portador de pedofilia é sexualmente atraído exclusivamente, ou quase exclusivamente, por crianças ou indivíduos púberes” (Balteri, 2015) . No que tange a classificação dos pedófilos e da própria pedofilia há estudiosos que defendem a questão de que esse desejo por se relacionar com crianças não se trata de uma doença psiquiatrica, pois os pedofilos teriam a capacidade de discernir o que é certo e o que é errado, entretanto, foi classificada pela Organização Mundial dá Saúde como sendo, sim, uma doença. Danilo Antônio Baltieri também é um dos estudiosos que afirmam que se trata sim de um transtorno psiquiátrico e, pensando desta forma, tais criminosos na hora de sua condenação deverão receber tratamento diferente dos demais,  recebendo a condenação de internação (Neumann, 2016), entretanto a legislação brasileira não pune objetivamente o crime de pedofilia por não haver nenhuma tipificação legal para tal, o que ocorre é a aplicação de penalidades análogas já previstas no código penal, sendo elas a punição por abuso sexual ou estupro de vulnerável.

Segundo matéria fornecida pelo próprio Ministério público de Santa Catarina, destaca-se que, de acordo com a Classificação Internacional de Doenças (CID-10/OMS)e os critérios diagnósticos estabelecidos, a pessoa que é considerada

pedófila deve ter pelo menos 16 anos de idade e ser no mínimo 5 anos mais velha que a criança que desperta seu interesse sexual. Isso implica que a pedofilia se refere a adultos ou adolescentes mais velhos que experimentam atração sexual inapropriada por crianças.

Os perfis dos considerados Pedófilos, normalmente, segundo investigações da Polícia Federal, é de possuir idade entre 30 e 45 anos, tratando-se geralmente de pessoas mais inseguras, consequentemente mais reservadas e solteiras. Também é levantado que, em muitos casos, o consumo de pornografia infantil decorre apos a saturação do consumo de conteúdo pornográfico adulto em excesso.

O modus operandi dos pedófilos que optam por agir pela internet normalmente se dá pela criação de perfis falsos na internet ou então, até mesmo fazendo uso de jogos de comunidade infantil em que há interação entre os usuários, se passando também por crianças com o objetivo de seduzi-las para fins sexuais, ação denominada como grooming, para conseguir realizar essa primeira interação. Posterior a essa primeira ação, obter o acesso aos dados pessoais das vítimas fica muito fácil para esses agentes, que normalmente costumam pedir de praxe seus respectivos números de telefone e, por meio de textos trocados, passam a enviar às mais diversas mensagens até o momento em que avançam para o compartilhamento de conteúdo sexual por meio de fotos e vídeos.

Uma outra técnica muito utilizada por esses criminosos, se aproveitando da ingenuidade das crianças, é o envio de imagens pornográficas usando personagens de filmes infantis para que as crianças se sintam mais “tranquilas” ao ver aquele conteúdo pela primeira vez (Neumann, 2016). Durante essas conversas, esses cibercriminosos buscam sempre ter a certeza de que quem eles estão conversando são de fato crianças e, para obter essa informação, normalmente solicitam que as vítimas enviem fotos e vídeos e, após o recebimento das mídias requeridas, os pedófilos passam a ter a missão de conquistar a confiança de quem está do outro lado da tela, iniciando a solcitação de imagens obscenas e de cunho sexual onde apareçam seus corpos infantis, incluindo suas partes íntimas (Tanaka, 2016), dando posteriormente aos criminosos o poder de compartilhar essas imagens nos mais diversos e variados sites que compactuam com a disseminação da pornografia infantil, como por exemplo, a deep web.

O histórico de comercialização de pornografia infantil é bastante extenso, por muito tempo este tipo de conteúdo foi armazenados em ferramentas muito pouco

tecnológicas, como por exemplo, CDs, DVDs, Disquetes e nos primeiros computadores criados, que mal possuiam a conexão que temos na atualidade. O mundo virtual faz com que seja extremamente complexo a criação de normas que de fato sejam eficientes nesse âmbito, fazendo com que a legislação brasileira tenha um novo desafio a cada dia (Fernandes, 2022).

A lei nº 8.069/1990 que trata sobre a proteção integral à criança e ao adolescente, prevê na redação de seu artigo 241-A no tocante sobre o compartilhamento de material pornográfico infantil, que:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> § 1 o Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; (Incluído pela Lei nº 11.829, de 2008)
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
> § 2 o As condutas tipificadas nos incisos I e II do § 1 o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)

Tal dispositivo tem como objetivo tutelar o bem jurídico da integridade moral e física dos infantes, que neste caso, serão sempre os sujeitos passivos do crime, tendo como sujeito ativo qualquer pessoa. O referido artigo tipifica como crime às fotografia, vídeos e registros que possam possuir qualquer tipo de cena explicita de sexo em que envolva crianças ou adolescentes nos atos. Aduz também os meios que podem ser utilizados para efetuar o compartilhamento desse material, sendo estes, por meio de sites ou redes sociais, neste último caso, com uma ou com um grupo de pessoas que podem vir a fazer essa troca de conteúdo ilícito contendo imagens de violência ou posse sexual de crianças, por meio de mensagens privadas ou públicas em determinada página. Aquele que realiza o compartilhamento descrito neste tipo de delito pode ser punido com uma pena que varia de três a seis anos de prisão, além de multa. Essa penalização é considerada relativamente leve, uma vez que esse crime viola os direitos de pessoas que frequentemente não têm a

capacidade de se proteger por conta própria, ou até mesmo de reconhecer quando estão sendo vítimas desse ato ilícito. Em 25 de dezembro de 2008 foi promulgada a lei nº 11.829/2008 que alterou o referenciado dispositivo da lei nº 8.069/1990 com o objetivo de tornar mais eficaz a luta contra a produção, comercialização e disseminação de pornografia envolvendo crianças, e também com o objetivo de penalizar a aquisição e a posse desse tipo de conteúdo, além de abordar outras práticas relacionadas à exploração infantil na internet.

Apesar da expressa previsão legal na legislação brasileira, este tipo de conteúdo é diariamente compartilhado nas redes, mesmo diante da proteção legal, o Brasil figura entre os quatro principais centros de disseminação de pornografia infantil globalmente, em concorrência com os Estados Unidos, Rússia e Coreia do Sul. Segundo dados fornecidos pela associação Safernet, conhecida por defender os direitos humanos na web, o número de denúncias por exploração sexual e abuso na internet no ano de 2022 foi de 111.929, o que totaliza uma média de 306 denúncias por dia. Também foi informado que 2023 foi o segundo ano consecutivo em que se é ultrapassado o numero de 100 mil denuncias referente a pornografia infantil, a ultima vez que esse número foi batido foi no ano de 2011.

Entre 2016 e 2018, houve um aumento de 83% no número de imagens e vídeos contendo pornogradia infantil. Além disso, a presença de crianças e pré-adolescentes (3-13 anos) em imagens e vídeos relacionados à exploração e abuso sexual aumentou de 56% do material ilegal total (122.276) em 2016 para 79% (148.01) em 2017 e 89% (223.999) em 2018 (Unesco, 2020). De acordo com o relatório do Fórum Brasileiro de Segurança Pública de 2023, observou-se um aumento nos números absolutos dos crimes de "pornografia infanto-juvenil" e exploração sexual infantil, com acréscimos de 7,0% e 16,4%, respectivamente. Em 2021, os casos de exploração sexual infantil atingiram o ápice entre as idades de 10 a 17 anos, representando 48,7% das vítimas de 0 a 17 anos. Já em 2022, esse percentual elevou-se para 58,0%, indicando uma média de idade das vítimas mais jovens. Adicionalmente, nota-se uma alteração no pico da curva, que anteriormente ocorria aos 15 anos e passou a ocorrer aos 14 anos (Fórum, 2023)

A associação Safernet também aponta que, no início do ano de 2023, teve-se um aumento significante de denúncias referente a imagens contendo pornografia infantil no Brasil, um aumento de 70%, tento sido o maior número registrado desde o ano de 2022 (Safernet, 2023). De acordo com a Operação Luz na Infância, no ano

de 2022, no Brasil, foi encontrado o equivalente a 4 mil gigabytes contendo conteúdo de pornografia infantil, o que resultou, após as investigações, em 125 mandados de busca e apreensão, resultando em 43 prisões em flagrante (Brasil, 2023).

Tratando-se de dados em níveis mundiais, no ano de 2008 obteve-se o número de 42.396 sites de pedofilia em todo mundo, dados colhidos através de diversas denúncias feitas a associação Italiana na época. Importante também destacar que o número fica ainda mais alarmante quando se leva em consideração que o número de acessos à internet diariamente no ano de 2008 era muito inferior aos números de acessos atuais. Esses sites de pedofilia mencionados tiveram maior concentração na Holanda, Alemanha e Estados Unidos. Em 2008, a organização Internet Watch Foundation do Reino Unido recebeu aproximadamente 34 mil denúncias de conteúdo de pornografia infantil na internet. Entre os casos verificados, cerca de 74% estão relacionados a sites comerciais, ou seja, aqueles que comercializam material de pornografia infantil o que demonstra que este mercado tem grande potencial de histórico de movimentar milhares de cifras pelo mundo segundo informações do Ministério Público.

Um dos meios extremamente utilizados para o compartilhamento desses arquivos ilegais é a chamada “Deep Web” que tem como tradução literal “internet profunda”. Trata-se de uma parte mais obscura da internet, que inclusive não é de tão fácil acesso como o “google” por exemplo, fica oculta da maior parte do público, mas é extremamente utilizada para a venda e compartilhamento dos mais variados tipos de conteúdos ilegais (Neumann, 2016).

Essa ferramenta obscura supramencionada é composta por milhares de páginas e, nessas páginas é possível encontrar diversos vídeos, imagens, blogs, banco de dados e fóruns que ficam em anonimato. Por gozar desse grande anonimato, essa ferramenta se torna um grande paraíso para o cometimento de cibercrimes e para a facilitação do compartilhamento de mídias que possuem como conteúdo atos ilícitos. A questão do anonimato é tão grande que se torna até impossível a identificação do IP de determinados usuários, o que dificulta muito o trabalho das autoridades.

Em entrevistas feitas pela “ANDI, Comunicações e Direito” com agentes que atuam na área de combate a este tipo de compartilhamento, foi declarado que nosso país utiliza como maior forma de combate a esse tipo de crime à repressão

criminal e, segundo a Polícia Federal, o órgão além de atuar contra o combate ao crime de pornografia também é responsável por fazer a identificação das vítimas desses crimes por meio de policiais civis e federais especializados, conseguindo assim indentificar a efetuar a apreensão dos criminosos. Também é enfatizado que além dessa repressão criminal direta, faz-se necessário instaurar uma cultura de prevenção e combate, que devem ter iniciativa pelo governo federal pois, mesmo com as diversas delegacias especializadas nessa abordagem, através delas não é possível prevenir o crime (R7 Notícias, 2023).

O ato de aplicar a punição cabível após a consumação do crime não é a melhor forma de lidar com esses delitos, tendo em vista que estamos falando sobre crianças que são vítimas de crimes sexuais, é necessário prevenir que crianças sejam vítimas diárias dessas condutas. Eva Dengler, uma das entrevistadas e gerente do programa de relações empresariais da Childhood Brasil, afirma que mesmo diante de toda repressão e os avanços nas prisões destes delinquentes, somente 7% dos casos tem sido denunciado às autoridades, o que reforça mais uma vez a carência que nossa país tem sobre a conscientização e prevenção desses crimes ainda mais diante do cenário da pornagrafia que é enorme, que perpassam às mais profundas camadas da internet tornando quase impossível o trabalho das autoridades competentes. Diante dessas afirmações conclui-se que, a melhor maneira além da repressão para o combate da exploração sexual infantil é, e sempre será, o diálogo que deve ser feito desde a sociedade como um todo, até pelas pessoas mais próximas e responsáveis pelos infantes (R7 Notícias, 2023).

Algo muito recorrente nesse cenário virtual é o denominado aliciamento sexual de crianças e adolescentes, que não necessariamente estará ligado de forma direta com a pernografia infantil, mas sim com a consumação de fato do ato de abuso sexual. O aliciamento sexual se divide em três etapas: a persuasão, o envolvimento da vítima e a instauração da relação sexual abusiva (Tanaka, 2016).

A primeira etapa, de persuasão, trata-se daquela já mencionada neste capítulo, na qual, o agressor conquista a confiança da vítima e passa a receber dela suas informações pessoais como endereço, idade, escola onde estuda, dentre outras. Após deter essas informações dá-se início ao chamado “posicionamento estratégico” onde ocorreria um ponto de encontro. Sempre pensando em assegurar a confiança do infante, esses pontos de encontro normalmente são em lugares

públicos como shoppings, parques e praças e, a partir deste encontro se abre a oportunidade do início de um suposto relacionamento com a vítima (Tanaka, 2016).

A segunda etapa tem como foco envolver a vítima em uma relação enganosa em que o agressor normalmente tenta transparecer uma falsa amizade para que a vítima se sinta mais segura e dificulte ainda mais a identificação por parte dela da relação em que de fato está se envolvendo. As consequências dessa relação normalmente são fáceis de identificar, há um isolamento por parte da vítima em seus comportamentos físicos e mentais (Tanaka, 2016).

Por último tem-se a terceira etapa, em que de fato ocorre a consumação do abuso sexual e, a partir desse estágio, o agressor passa a ter a preocupação de que a vítima mantenha o ocorrido em sigilo fazendo com que isso ocorro pelas mais variadas formas de coação para que haja o convencimento da criança agredida (Tanaka, 2016).

Analisando diretamente a legislação brasileira, podemos observar algumas das previsões referente a proteção sexual das crianças e adolescentes. Primeiramente podemos começar mencionando o código penal do Brasil, que traz na redação de seu artigo 217-A o delito de estupro de vulnerável, que consiste em ter conjunção carnal ou a pratica de outro ato libidinoso com menores de 14 anos independentemente de seu consetimento, ja que não há consentimento para essa faixa etária de idade,, estendendo tal tipificação também a pessoas que portem algum tipo de deficiência mental ou enfermidade (Tanaka, 2016). Também está em vigor em nossa legislação o artigo 241-A da Lei nº 8.069/1990 que legisla sobre a prática do crime da comercialização de pornografia infantil, tipificando esta como sendo o compartilhamento ou comercialização de de fotografias, videos ou qualquer tipo de conteúdo deste cunho. Esta promulgada também desde 2014 a Lei nº 12.965, que ficou popularmente conhecida como Marco Civil da internet pois possui como objetivo regulamentar o uso da internet no Brasil a partir de princípios, garantias direitos e deveres que são estabelecidos aos usuários também adotando medidas que ajuda na proteção dos dados e na privacidade de seus respectivos usuários.

Como pioneira das leis que tratam sobre proteção de dados, tem-se a conhecida Lei Carolina Dieckmann, a Lei nº 12737/2012, que foi promulgada após a atriz brasileira Carolina Dieckmann ter seus dados violados e fotos íntimas vazadas nas redes. No momento do ocorrido, apesar de a invasão virtual já ser considerada

crime no código penal, especificamente no artigo 154-A que dispõe sobre a invasão de dispositivo informático, ainda não existia legislação específica que tratava sobre o assunto, pois tal matéria não era recorrente em nosso ordenamento (Neumann, 2016). Existem mais leis que tange sobre a proteção de dados e, apesar de a legislação brasileira ter avançado nesse sentido de enfrentamento dos crimes cometidos por meios virtuais através da criação de leis específicas que abordam o assunto, ainda há muito desafios que tem de ser superados para que seja possível ter de fato a garantia da efetividade de tais leis.

## **4.2** AS LACUNAS E DIFICULDADES DA LEGISLAÇÃO E ÓRGÃOS PÚBLICOS BRASILEIROS NO COMBATE E PREVENÇÃO DA PORNOGRAFIA INFANTIL

Diante dos diversos desafios enfrentados mundialmente no combate aos crimes virtuais, foi promulgado pelo ordenamento jurídico brasileiro a Lei nº 12.375/2012 que, dentre seus artigos, dispõe que os órgãos de polícia judiciária serão responsáveis por setores e equipes especializadas, com o objetivo de combater ações delituosas que podem vir a serem cometidas nos meios virtuais, apesar da devida previsão, essas equipes especializadas muitas vezes carecem de recursos, devido a complexidade dos crimes de natureza virtual pois, na maioria das vezes, os infratores fazem uso de sistemas extremamente complexos, tornando cada vez mais difícil a efetividade no combate a comercialização da pornografia infantil, a identificação dos criminosos e a devida punição dos responsáveis (Neumann, 2016).

Foram promulgadas outras leis em nosso ordenamento jurídico durante o processo de globalização e frequente uso da internet, entretanto, ao mesmo passo que surgiram leis para resguardar os direitos dos usuários, foram surgindo também lacunas decorrentes dessas próprias leis. Como exemplo podemos mencionar a Lei nº 12.965/2014, conhecida como Marco Civil da internet, mencionada anteriormente nesta sessão, que trata sobre as garantias e os deveres dos usuários. Em seu artigo 13 dispõe quanto a prestação de serviços de internet, instituindo que é responsabilidade do administrador de sistemas autônomo manter os registros de conexões em ambiente seguro e sigiloso no período de um ano, um pouco mais abaixo, em seu artigo 15 é previsto que quando os provedores de aplicações de internet são pessoas jurídicas e exercem atividade organizadas com fins

econômicos, o registro de acesso a aplicações de internet também devem ser mantidos em ambientes seguros e sigilosos porém com o prazo de 6 meses. Às previsões desses dois artigos inframencionados faz com que a atividade de investigação policial se torne mais difícil, já que a lei prevê o prazo de um ano a 6 meses para que se possa se desfazer dos registros armazenados, restando pouco tempo para as investigações e eliminando os possíveis IPs que poderiam fazer papel importante durante as investigações, por exemplo.

Quando adentramos a chamada Deep Web, as dificuldades encontradas pelos órgãos públicos tornam-se ainda maiores, uma vez que em muitos dos crimes praticados na Web, quando de fato conseguem identificar o criminoso, tem-se mais um grande desafio: o Princípio da Territorialidade, que dispõe que às leis penais de um determinado país somente são aplicáveis aos crimes cometidos dentro daquele determinado território. Os delitos virtuais podem vir a ser cometidos de qualquer país do mundo e, para que seja possível aplicar a devida punição quando se é encontrado o autor do delito, faz-se necessário determinar qual jurisdição é considerada relevante e aplicável para determinado caso, dividindo assim o iter criminis e necessitando obrigatoriamente de uma cooperação entre os possíveis países envolvidos nos casos concretos.

Dado este panorama, informa-se que a comercialização de pornografia infantil normalmente ultrapassa às fronteirais territoriais brasileiras, dificultando a devida atuação de nossa legislação que, alem de carecer de leis especificas para o caso, muitas vezes, as que ja possuem previstas, não podem vir a serem aplicadas, pelo fato de entrar em conflito com questões internacionais que possuem diferentes regulamentações, leis, prioridades e dificuldades na cooperação entre os países. No tocante às incompatibilidades jurisdicionais, é um ponto que se deve ter grande observância, visto que algumas nações podem ter abordagens sobre o tema de forma mais ampla ou então restritivas, que acaba implicando nas questões de extradição dos investigados. Além das questões mencionadas, tem de ser observada a relevância que cada país dá para o tema de pornografia infantil, visto que se não houver uma política de grande foco de combate aos crimes em determinado território, mais difícil será a questão da aplicação da lei, visto que será extremamente vasta por não ser vista como relevante, somada com a grande dificuldade na cooperação de investigação conjunta.

Além da questão territorial, é extremamente necessário para as investigações o conhecimento técnico sobre o processo de investigação já que, os agentes de investigação, normalmente se deparam com sistemas extremamente complexos, onde os agentes agem de forma anônima com seus IPs quase que irrastreável na maioria das vezes. A Lei nº 13.105/2015, em seus artigos 156 ate 158 discorre sobre o funcionamento do processo de investigação no caso em questão. É previsto ao decorrer de sua redação do artigo 156 que é permitido ao juiz solicitar o auxílio de um perito técnico na área quando, em determinado caso, necessite conhecimento especializado para a produção da prova. O trabalho realizado pelo perito é indispensável para a investigação dos cibercrimes, uma vez que a maioria deles possuem sistemas extremamente complexos que precisam ser adentrados.

Para a investigação desses crimes, um outro grande aliado usado pelos órgãos públicos é a denominada perícia forense computacional, que tem competência de realizar a análise e coletas das possíveis evidências encontradas em dispositivos que estão sendo objeto de investigação. Mesmo com uma perícia específica para esse tipo de investigação, ainda assim são encontrados diversos obstáculos na coleta de supostas provas  devido a complexidade de alguns dispositivos.

No tocante às provas, quando de fato são coletadas, os investigadores se veem diante da quase impossibilidade de provar a autoria de prova que fora coletada, classificando os crimes virtuais como quase perfeitos, pois carecem de arma do crime e objetos que possam ligar o delito ao autor, por exemplo. Após a coleta das provas, é necessário ter um cuidado para preservá-las, com a finalidade de que esta continue sendo uma prova válida. Uma das alternativas de preservação da prova disposta pelo código penal brasileiro é a ata notarial, fazendo com que haja a preservação da prova mesmo que ela não seja física.

De uma forma conclusiva, podemos elencar em ordem as principais dificuldades e lacunas na nossa legislação, sendo a primeira, a questão de que as equipes investigativas carecerem de recursos necessários para as investigações desde as mais simples até as mais complexas; a segunda seria a questão dos prazos previstos em leis em que permite se desfazer dos registros eletrônicos no prazo entre 6 meses a um ano a depender do caso, o que acaba encurtando o tempo de investigação que as equipes governamentais possuem; no que tange a Deep web, tem-se a dificuldade de rastrear os autores e, quando obtém-se

efetividade nas buscas deparam-se com a questão da territorialidade e de qual país compete a devida aplicação da legislação vigente e, por final, tem-se a questão da dificuldade de ligar a autoria dos fatos às provas coletadas

Diante das diversas lacunas e dificuldades anteriormente mencionados, mostra-se cada vez mais evidente o fato de que além das leis criadas por nossa legislação para combater os crimes virtuais ainda existem muitas dificuldades referente às investigações e principalmente a prevenção desses crimes e, de acordo com a Constituição Federal brasileira, a responsabilidade sobre às crianças e adolescentes é uma responsabilidade conjunta, sendo um dever da sociedade como um todo, tendo os pais ou responsáveis um papel crucial na conscientização e monitoramento de seus infantes na internet (Borges, Javorski, 2022).

## **4.3** A RESPONSABILIDADE E A INFLUÊNCIA PARENTAL FRENTE A EXPOSIÇÃO À INTERNET E O USO DE REDES SOCIAIS PELOS INFANTES

A Constituição Federal brasileira de 1988 prevê em seu artigo 227 que:

> Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.(Brasil, 1988).

No contexto da legislação vigente, é constitucionalmente prevista uma tríplice responsabilidade entre a sociedade, o estado e a família incumbindo a garantia dos direitos elencados no artigo anteriormente mencionado, tendo como objetivo principal assegurar que as crianças estejam ambiente seguro, isentos de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão. No entanto, lamentavelmente, essa proteção muitas vezes não se concretiza na prática.

No presente contexto, a ubiquidade da conectividade à internet é incontestável, tal realidade também se aplica às crianças e adolescentes que já nascem e se desenvolvem em um ambiente tecnologicamente imersivo. O contexto do desenvolvimento da tecnologia propicia amplas oportunidades para o aprendizado e aquisição de conhecimento, ao mesmo tempo que sujeita essa faixa

etária a uma exacerbada exposição aos perigos inerentes aos crimes cibernéticos. Excluir a internet da vivência das crianças é percebido como uma restrição que obstaculiza o acesso a informação, socialização e aprendizado. A questão central reside, não na proibição do uso da internet pelas crianças, mas sim na necessidade de estabelecer limites discerníveis para a utilização da internet no que concerne à contribuição benéfica na formação das crianças, bem como à mitigação do risco que essa mesma exposição pode vir a apresentar (Borges, Javorski, 2022).

Quando falamos de mitigação de riscos às crianças, apesar da previsão expressa da constituição da tríplice responsabilidade de proteção entre a sociedade, estado e a família, faz-se necessário frisar que a instituição familiar encontra-se em vantagem dos demais, considerando a proximidade e convívio direto com os infantes. Tal vantagem não implica que a sociedade e o estado encontram-se em posição em que possam eximir-se de suas respectivas responsabilidades, relegando a atenção às crianças e adolescentes exclusivamente de forma subsidiária, muito pelo contrário, apenas enfatiza que mesmo diante da mesma responsabilidade, possuem funções diferentes (Borges, Javorski, 2022).

O Código Civil concede tanto aos pais biológicos quanto aos pais socioafetivos a responsabilidade legal sobre seus filhos, até que estes atinjam a maioridade, que é estabelecida aos 18 anos. Esta responsabilidade é denominada "poder familiar". O poder familiar é uma instituição jurídica que atribui aos pais a autoridade e a obrigação de cuidar e tomar decisões na vida civil em nome dos filhos menores de idade. Essa responsabilidade legal é crucial para garantir que os interesses e o bem-estar das crianças sejam protegidos e promovidos, uma vez que elas podem não ter a capacidade plena de compreender e decidir sobre diversos assuntos. O poder familiar, portanto, estabelece uma estrutura legal que permite aos pais ou responsáveis legais representar os interesses de seus filhos em questões legais e administrativas. É importante notar que essa responsabilidade legal não se limita apenas às questões de caráter patrimonial ou financeiro, mas também abrange aspectos que envolvem o desenvolvimento integral da criança, tais como a orientação educacional, a tomada de decisões em relação à saúde e a garantia de um ambiente seguro e propício ao crescimento saudável. Também é previsto no Código Civil a responsabilização de terceiros sobre às crianças em caso de ausência ou abandono por parte dos pais, entretanto, independente sobre quem recaia a responsabilidade de garantir os direitos dos infantes, fato é que, de acordo

com a lei, sempre haverá alguém que compõem a instituição familiar tendo contato direto com a criança (Borges, Javorski, 2022).

Considerando as implicações da responsabilidade civil dos pais em relação aos seus filhos, emerge a essencial incumbência dos genitores de proporcionar a seus descendentes um desenvolvimento digno, possuindo autonomia na criação, educação e formação como pessoa, respeitando sempre os limites previstos nas leis. Todavia, a autonomia concedida aos pais na criação de seus filhos também pode levar a situações de negligência, nas quais as crianças se veem expostas a diversos tipos de riscos, principalmente no âmbito das interações virtuais. Essa negligência pode manifestar-se de diversas formas, frequentemente como resultado de omissões deliberadas ou mesmo abuso, em muitos casos perpetrados de forma intencional (Borges, Javorski, 2022).

O termo autonomia e era digital, quando fazendo menção a crianças e suas devidas criações, implicam em diversos riscos. No contexto da era digital, a negligência parental pode se tornar ainda mais complexa, uma vez que crianças e adolescentes, imersos na tecnologia desde cedo, podem ser suscetíveis a ameaças virtuais que variam desde o cyberbullying até a exploração online. Portanto, é imperativo que os pais exercem uma supervisão ativa e proporcionem orientação para ajudar seus filhos a navegar com segurança no mundo digital sob pena de estarem violando direitos previstos na constituição, como os de garantir a saúde e o bem estar de seus dependentes já que, a assistência aos filhos é um dever constitucional (Borges, Javorski, 2022).

Como já mencionado anteriormente, internet é uma ferramenta poderosa que pode ser usada para fins educativos, recreativos e sociais. No entanto, ela também pode ser um lugar perigoso para crianças e adolescentes, que podem ser expostos a conteúdo inadequado, cyberbullying, grooming e outros riscos. Por isso, é importante que os pais supervisionem o uso da internet de seus filhos. Essa supervisão pode ser realizada de várias maneiras, como: estabelecer limites de tempo e de conteúdo onde os pais devem definir quanto tempo seus filhos podem passar na internet e quais tipos de conteúdo eles podem acessar; Usar software de controle parental, esses softwares permitem que os pais bloqueiem sites e aplicativos inadequados; Conversar com os filhos sobre os riscos da internet: os pais devem conversar com seus filhos sobre os riscos de se exporem a conteúdo inadequado ou de serem vítimas de cyberbullying, grooming ou outros crimes

cibernéticos e claro, sempre ver com quem os filhos interagem na internet olhando suas conversas. Muitos dizem que olhar a conversa de filhos menores na internet seria uma invasão de privacidade mas, na verdade, trata-se de um ato de cuidado e prevenção.

A internet é um espaço público, diferentemente de um quarto ou de uma sala de estar, onde qualquer pessoa pode acessar informações e interagir com outras pessoas. Por isso, é importante que os pais estejam cientes do que seus filhos estão fazendo online, ainda mais que as crianças e adolescentes são mais vulneráveis aos riscos da internet, pois ainda estão em desenvolvimento e podem não ter a maturidade necessária para identificar e lidar com esses riscos e, a supervisão parental é uma oportunidade para os pais educarem seus filhos sobre os riscos da internet e sobre como usar a internet de forma segura e responsável.

É de responsabilidade direta dos pais ou responsáveis que fazem parte do cotidiano dos infantes intervir, monitorar e impor limites no uso dos meios digitais, tendo como função compreender a grandiosidade da internet e das redes sociais juntamente com os perigos que emergem destas. Os pais precisam atuar em prol da delimitação do uso das tecnologias, tendo em vista que a não supervisão das atividades virtuais dos filhos podem gerar consequências negativas físicas e mentais e, detendo o conhecimento sobre os risco do uso indiscriminado da internet sem a devida supervisão dos pais que tem responsabilidade civil e constitucional sobre os filhos, pode vir a implicar em negligência, omissão e violação de direitos previstos na constituição (Borges, Javorski, 2022).

Inúmeras vezes as crianças são instigadas pelos próprios pais a fazer uso de redes sociais pois, desde novos são fotografados e postados em suas respectivas redes, expondo-as, ocasionalmente, a usuários cujas identidades os pais desconhecem por completo. Essa exposição precoce às câmeras de celulares acabam despertando curiosidade nas crianças, que se entretém com o que lhes é apresentado, gerando um desejo precoce de se fotografar e, por consequência, criar redes sociais, tornando-se suscetíveis cada vez mais cedo aos riscos virtuais (Borges, Javorski, 2022).

## 5. AS REDES SOCIAIS E SUAS DIRETRIZES NEGLIGENCIADAS DE CRIANÇAS E ADOLESCENTES

A presença de crianças nas redes sociais já é uma realidade que não pode ser ignorada. As crianças nativas digitais cresceram em um mundo onde a internet e as redes sociais desempenham um papel central em suas vidas. Elas são fluentes em tecnologia desde tenra idade, utilizando as redes sociais de maneira natural e espontânea, como se fosse uma extensão de suas vidas. A tendência é que esse fenômeno se intensifique à medida que a tecnologia continue avançando a passos largos. Consequentemente, estamos testemunhando um aumento significativo no número de menores de idade navegando livremente pelas redes sociais, o que suscita questões importantes sobre segurança, privacidade, educação digital e diretrizes eficientes.

No cenário atual, a diversidade de redes sociais disponíveis é impressionante. De acordo com uma pesquisa abrangente envolvendo cerca de 2,6 mil crianças, cujos resultados foram publicados no site UOL, podemos identificar as redes mais populares entre os adolescentes. Os líderes indiscutíveis são o WhatsApp, utilizado por incríveis 80% dos entrevistados, seguido pelo Instagram, com 62% de adeptos, e o TikTok, que conquistou 58% dos jovens. Além disso, a pesquisa revelou que, ao navegar na internet, a maioria das crianças tem objetivos bem definidos. Surpreendentemente, 84% delas buscam principalmente entretenimento, seja assistindo a filmes e séries ou explorando conteúdo de lazer. Logo em seguida, com 79% das respostas, surge a intenção de trocar mensagens instantâneas, indicando a importância da comunicação online em suas vidas. Os jogos online que permitem conexão com outros jogadores também ganharam relevância, com 66% das crianças admitindo utilizá-los. Por último, 58% dos jovens declararam o interesse e o uso para as atividades escolares, destacando a versatilidade das redes sociais e da tecnologia como um todo no contexto educacional. Essas estatísticas evidenciam a complexidade das interações das crianças e adolescentes com o mundo digital, assim como a necessidade de considerar suas necessidades e segurança em ambientes online (Estadão, 2022).

Conforme dados revelados por uma pesquisa conduzida pelo TIC KIDS ONLINE NO BRASIL, a plataforma mais amplamente adotada no país em questão de uso e atividade dentro do aplicativo, é o TikTok, que superou tanto o Instagram

quanto o Facebook em popularidade. Esta rede social específica atrai um público predominantemente composto por crianças e adolescentes com idades entre 9 e 17 anos. De acordo com os resultados do estudo, impressionantes 93% das crianças e adolescentes no Brasil estão ativos na internet, com o Instagram e o WhatsApp destacando-se como as plataformas com o maior número de perfis de usuários. No entanto, quando se trata de uso frequente e postagens, o TikTok assume a liderança, consolidando seu papel como a rede social preferida entre as gerações mais jovens, evidenciando sua rápida ascensão e influência no cenário digital brasileiro (Silva, 2022).

Em teoria, as redes sociais têm uma política que não permite a criação de contas de usuários com menos de 13 anos, o que é um contraponto aos dados apresentados na pesquisa, que mostram que crianças de até 9 anos estão ativas nessas plataformas. Tomando o TikTok como exemplo, de acordo com as diretrizes do aplicativo, a idade mínima exigida para criar um perfil é de 13 anos, mas não é necessária nenhuma forma de comprovação da idade. Recentemente, o TikTok implementou algumas mudanças nas configurações de perfis de menores de idade de 13 a 15 anos. Agora, todos esses perfis são automaticamente definidos como privados, com comentários restritos. No entanto, uma conta de perfil privado implica que apenas aqueles autorizados pelo titular da conta, neste caso, menores de idade, podem acessar o conteúdo postado. Isso, infelizmente, não é uma proteção eficaz, uma vez que para um cibercriminoso, como um pedófilo, ter acesso aos conteúdos protegidos, pode facilmente criar uma conta falsa e tentar seguir a conta privada, na esperança de ser aceito pela criança. Além disso, se uma criança não quiser que sua conta seja automaticamente privada, ele pode facilmente falsificar sua idade, o que coloca em destaque a necessidade de medidas mais rigorosas para proteger a privacidade e segurança das crianças online. Essas questões ressaltam a urgência de se regulamentar e fiscalizar as políticas de idade mínima nas redes sociais e de educar tanto os pais quanto as crianças sobre os riscos e boas práticas online. (G1, 2021)

Quando nos referimos ao Instagram, que, de acordo com as pesquisas apresentadas, conta com 80% dos entrevistados possuindo perfis em sua plataforma, observamos que suas diretrizes para menores de idade são em grande parte semelhantes às do TikTok. A plataforma configura automaticamente os perfis com faixa etária entre 13 e 15 anos como privados, permitindo que apenas aqueles

autorizados pelo titular da conta tenham acesso às postagens. No entanto, é importante ressaltar que o Instagram, da mesma forma que o TikTok, não exige qualquer forma de comprovação de idade durante o processo de criação de uma conta. Os usuários são solicitados a fornecer apenas sua data de nascimento, o que pode ser facilmente falsificado por indivíduos mais jovens. A empresa por trás do Instagram justifica essas restrições de contas como uma medida destinada a evitar que os usuários recebam mensagens de outros usuários desconhecidos. No entanto, a eficácia dessas medidas permanece questionável, uma vez que não existe um mecanismo eficiente para verificar a idade real dos usuários, o que pode potencialmente permitir que crianças e adolescentes tenham acesso a conteúdo inapropriado ou interajam com estranhos na plataforma. Isso sublinha a necessidade de uma revisão das políticas de idade mínima e a implementação de medidas mais robustas para proteger os usuários mais jovens nas redes sociais. (Agência o Globo, 2021)

À medida que crianças cada vez mais jovens acessam essas plataformas, surgem preocupações significativas sobre a eficácia das políticas de idade mínima. Tanto o TikTok quanto o Instagram, apesar de suas diretrizes, não apresentam mecanismos eficazes para verificar a idade real dos usuários, deixando uma brecha para crianças menores de 13 anos acessarem essas plataformas. Além disso, mesmo com medidas como a configuração automática de perfis privados para menores de idade, a proteção oferecida é limitada, uma vez que é relativamente fácil para estranhos se infiltrarem e interagirem com as crianças por meio de contas falsas. Essas lacunas nas políticas de idade mínima destacam a necessidade urgente de regulamentações mais rigorosas e fiscalização eficaz por parte das autoridades e das próprias empresas de tecnologia. Além disso, a educação dos pais sobre os riscos e boas práticas online é fundamental para garantir a segurança das crianças na era digital. Sem dúvida, a crescente presença das crianças nas redes sociais representa um desafio contínuo em um mundo digital em constante evolução. É crucial que se reconheça a importância de um esforço conjunto, envolvendo não apenas reguladores e empresas de tecnologia, mas também educadores, pais e responsáveis, a fim de garantir que as crianças possam explorar o espaço online com segurança.

As políticas de idade mínima precisam ser revistas e aprimoradas, buscando maneiras eficazes de verificar a idade dos usuários, ao mesmo tempo em que se

promove uma educação digital abrangente e informada. Além disso, as próprias redes sociais devem desempenhar um papel ativo na proteção das crianças, implementando medidas de segurança mais robustas, como verificações de idade mais eficazes e um controle mais rígido sobre o conteúdo e a interação dentro de suas plataformas. É crucial que essas empresas reconheçam sua responsabilidade na proteção das crianças e tomem medidas proativas para garantir um ambiente virtual seguro.

## CONSIDERAÇÕES FINAIS

Diante de tudo o que foi exposto ao decorrer deste estudo, torna-se evidente a situação alarmante na qual o Brasil se encontra. Estamos diante de um complexo cenário que envolve não apenas lacunas legislativas, mas também negligências por parte dos pais, que não possui preocupação com o tema e não tem políticas públicas para conscientizar e informar a população sobre os dados crescentes; dos responsáveis legais das crianças e adolescentes que não supervisionam a atividade destes na internet; a ausência de diretrizes eficazes nos aplicativos e, ainda mais preocupante, a normalização a nível nacional da sexualização da imagem de crianças. Esses fatores interconectados lançam uma sombra sobre a segurança e o bem-estar das gerações futuras, destacando a urgente necessidade de ações coordenadas por parte da sociedade, do governo e das empresas de tecnologia para proteger as crianças e preservar a integridade de sua infância.

O advento do avanço da tecnologia de forma alguma deve ser visto como um inimigo das crianças e adolescentes, uma vez que desempenham um papel fundamental na obtenção de conhecimento e enriquecimento cultural, quando utilizados de maneira apropriada. O que se faz necessário é estabelecer uma cultura de conscientização acerca dos riscos associados à navegação livre das crianças nas redes. É crucial compreender que as leis que visam punir os crimes que podem ser cometidos contra crianças e adolescentes na internet, não são, por si só, suficientes para a prevenção. A devida punição dos criminosos não consegue restituir a infância que foi roubada da vítima que sofreu o crime. É urgente a necessidade que sejam reforçadas as medidas de prevenção, envolvendo não apenas o reforço das leis, mas também a educação das crianças, pais e responsáveis sobre os perigos on-line.

Como previsto em nossa própria Constituição Federal, é um dever da família, da sociedade e do Estado assegurar às crianças e aos adolescentes os direitos básicos necessários para que cresçam e desfrutem de uma vida digna, garantindo que estejam inseridos em ambientes seguros. É notório que muitos pais, devido ao receio compreensível de que algo de ruim possa ocorrer em uma sociedade frequentemente marcada pela violência, não permitem que seus filhos andem desacompanhados pelas ruas de suas próprias cidades. No entanto, é notável que esses mesmos pais, por vezes, permitem que seus filhos naveguem na internet sem

a devida supervisão, expondo-os a riscos potencialmente maiores dentro das paredes de suas próprias casas, por meio de seus celulares e computadores. Esta aparente contradição destaca a cultura que os brasileiros possuem de não se atentar no quão nociva a internet pode ser, principalmente quando se fala de infância e adolescência. Com frequência, muitos pais compartilham fotos e vídeos de seus filhos em suas redes sociais, e, em muitos casos, essas imagens incluem crianças com idade inferior a 10 anos, expondo seus rostos a uma ampla gama de usuários, alguns dos quais são desconhecidos dos próprios pais. A prática de expor a imagem de crianças nas redes sociais não deve ser encarada como algo normal. É importante ressaltar que existem inúmeros criminosos ativos nas redes, dedicados a vasculhar essas imagens, que para pais e familiares são simples registros afetuosos da infância de seus filhos. No entanto, para indivíduos com intenções prejudiciais, como pedófilos, por exemplo, a imagem de uma criança, especialmente quando exposta de forma inadequada, pode ser explorada de maneira extremamente perturbadora. Isso sublinha a necessidade urgente de conscientizar os pais sobre os riscos associados à exposição excessiva de seus filhos nas redes sociais, o equilíbrio entre compartilhar momentos felizes e garantir a proteção dos pequenos é essencial em um mundo cada vez mais conectado digitalmente.

Um outro ponto importantíssimo que foi levantado é a questão da cultura da sexualização da infância em nosso país. Torna-se cada vez mais comum propagandas incitando crianças a usarem roupas e acessório usados normalmente por pessoas adultas, o que não parece algo problemático se visto de forma superficial, fato é que, o compartilhamento desse tipo de ideia, disseminada em nossa sociedade um desejo doentio por crianças. Esse desejo subliminarmente instigado por essas propagandas desencadeia muitos problemos sociais, faz com que os pedófilos sintam-se cada vez mais instigados, compartilhando imagens de cunho sexual infantil e assediando crianças pela internet de forma cada vez mais intensa, fazendo com que nossos legisladores tenham cada vez mais a necessidade de instituir leis para que seja possível fazer com que o número de crimes e compartilhamento desse tipo de conteúdo perturbador diminua. Por consequência de toda essa questão cultural, nosso governo passa a ter que lidar com sistemas complexos, com a Deep Web, carecendo de recursos, e até lidar com questões de territorialidade, já que estamos falando de um crime que ultrapassa fronteiras.

Essa corrente de sucessões de problemáticas englobam todos, envolve os país, os legisladores, as empresas de aplicativos que negligenciam as crianças e adolescentes com suas diretrizes meramente ilustrativas e, principalmente, o estado como um todo. O estado brasileiro não possui cultura de prevenção contra crimes cibernéticos que atingem os infantes, tendo uma grande parcela de culpa nesses números que não param de crescer, até porque, é muito mais inteligente prevenir do que punir. A cultura punitivista é falha, e a falta de prevenção em crimes que tem como vítima crianças e adolescentes, é assustadora. Todos no estado brasileiro negligenciam as crianças, deixando-as à mercê de criminosos que navegam de forma anônima, quase que irrastreável, criminosos que roubam infâncias, sorrisos, ingenuidades e, em alguns casos, até a vida.

A família, os legisladores, o estado, e as empresas de redes sociais, sabendo de todos esses perigos, precisam urgentemente mudar suas condutas e assumirem posturas de proteção e prevenção pois, atualmente se encontram na posição de negligentes. Aplicar penas brandas para esses criminosos pode ser até algo satisfatório para a sociedade como um todo, mas não possui influência nenhuma no dano causada aquele que, com idade tão tenra, foi vítima de um crime que, em muitos casos, se supervisionado pelos três elemento citados no começo desse parágrafo, poderia ter sido evitado. Quando a fiscalização ultrapassa os limites possíveis da família, e da conscientização da população brasileira como um todo, torna-se ainda mais evidente a urgência de estabelecer uma regulamentação eficaz e de intensificar a fiscalização das políticas de idade mínima nas redes sociais.

É imperativo que sejam implementadas medidas mais rigorosas para verificar e validar a idade dos usuários, a fim de cumprir a promessa de impedir o acesso de crianças menores de 13 anos. Além disso, é essencial promover a conscientização entre os pais e responsáveis sobre a importância de monitorar ativamente as atividades de seus filhos nas redes sociais. A educação dos pais é crucial para entender os riscos potenciais que as crianças enfrentam no ambiente digital, assim como para fornecer orientação e suporte no uso responsável da internet.

Em um mundo cada vez mais conectado, a segurança das crianças online deve ser uma prioridade absoluta, e isso requer ações coordenadas que envolvam empresas de tecnologia, legisladores, educadores e famílias. A proteção das crianças contra os perigos virtuais exige uma abordagem multifacetada que trate tanto a regulamentação como a educação, para que só assim a previsão de

proteção da criança no ordenamento se faça vital, garantindo a tão prometida infância feliz e saudável.

## REFERÊNCIAS


ANDRADE, Mariah Dourado de. BENTES, Dorinethe dos Santos. GUIMARAES, David Franklin da Silva. **Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais.** Revista Vertentes do Direito. Disponível em https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/4171#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime.. Acesso. 05.nov.2023

ARAUJO, Nádia de. **A importância da cooperação jurídica internacional para a atuação do estado brasileiro no plano interno e internacional.** Manual de Cooperação Jurídica Internacional e Recuperação de Ativos. Brasília: Ministério da Justiça, 2012.

BARRETO, Alesandro Gonçalves. SANTOS, Hericson dos. Deep Web: **investigação no submundo da internet.** 1. Ed. Rio de Janeiro: Editora Brasport, 2019. BRASIL. Supremo Tribunal Federal. Informativo STF n° 286/2002. Disponível em http://www.stf.jus.br//arquivo/informativo/documento/informativo286.htm.. Acesso. 05.nov.2023

BALTERI, Danilo Antônio. Pedofilia como transtorno comportamental psiquiátrico crônico e transtornos comportamentais assemelhados. Disponível em < http://www.ambr.org.br/pedofilia-como-transtorno-comportamental-psiquiatrico-cronico-e-transtornos-comportamentais-assemelhados/>Acesso. 05.nov.2023

BECK, Ulrich. **Sociedade de risco: rumo a uma outra modernidade.** Tradução de Sebastião Nascimento. São Paulo: Ed. 34, 2010.

BECK, Ulrich.. **Sociedade de risco mundial:** em busca da segurança perdida. Edições 70, 2015.

BITTAR, Carlos Alberto. **Os Direitos da Personalidade.** Rio de Janeiro: Forense Universitária, 1989.

BRANCO, Paulo Gustavo Gonet; COELHO, Inocêncio Mártires; MENDES, Gilmar Ferreira. **Curso de Direito Constitucional**. 4ª. ed. São Paulo: Saraiva, 2008. p. 404.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. Supremo Tribunal Federal. **Informativo STF n° 393/2005.** Disponível em http://www.stf.jus.br/arquivo/informativo/documento/informativo393.htm. Acesso. 12.out.2023

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário n° 125.556/PR**. Disponível em http://www.stf.jus.br/. Acesso em 06 de setembro de 2020. BRASIL. Supremo Tribunal Federal. MS 24.405-4-DF. Rel. Min. Carlos Velloso. Disponível em http://www.stf.jus.br/. Acesso. 12.out.2023

BRASIL. Supremo Tribunal Federal. **HC 82.424. Rel. p/ o ac.** Min. Presidente Maurício Corrêa. Disponível em http://www2.stf.jus.br/portalStfInternacional/cms/verConteudo.php?sigla=portalStfJurisprudencia_pt_br&idConteudo=185077&modo=cms. Acesso. 20.set.2023

BRASIL. Supremo Tribunal Federal. **Ação Direita de Inconstitucionalidade n° 1969- 2007**. Rel. Min. Ricardo Lewandosvik. Disponível em http://www.stf.jus.br/. Acesso em 08 de setembro de 2020. Brasil adere à Convenção de Budapeste e se posiciona contra crimes cibernéticos. Disponível em https://diariodoturismo.com.br/brasil-adere-a-convencao-de-budapestee-se-posiciona-contra-crimes/. Acesso. 20.set.2023

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso. 21.set.2023

BRASIL. DECRETO 75.699, DE 6 DE MAIO DE 1975. Promulga a **Convenção de Berna para a Proteção das Obras Literárias e Artísticas,** de 9 de setembro de 1886, revista em Paris, a 24 de julho de 1971. Disponível em https://www.planalto.gov.br/ccivil_03/decreto/1970-1979/d75699.htm. Acesso 25.set. 2023

BRASIL. **Lei 8.069, de 13 jul. 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso. 19.set.2023

BRASIL. **Lei 9.279, de 14 de maio de 1996.** Regula direitos e obrigações relativos à propriedade industrial. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l9279.htm Acesso 20.set.2023

BRASIL. **Lei 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm.Acesso. 20.set.2023

BRASIL. **Lei 9.610, de 19 de fevereiro de 1998.** Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l9610.htm Acesso. 20.set.2023

BRASIL. **Lei nº 9.983, de 14 de julho de 2000.** Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9983.htm. Acesso 11.out.2023

BRASIL. **Lei 10.695, de 01 de julho de 2003.** Altera e acresce parágrafo ao art. 184 e dá nova redação ao art. 186 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal, alterado pelas Leis nos 6.895, de 17 de dezembro de 1980, e 8.635, de 16 de março de 1993, revoga o art. 185 do Decreto-Lei no 2.848, de 1940, e acrescenta dispositivos ao Decreto-Lei no 3.689, de 3 de outubro de 1941 – Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.695.htm. Acesso 11.out.2023

BRASIL. **Lei 11.829, de 25 de novembro de 2008.** Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso 11.out.2023

BRASIL. **Lei 12.735, de 30 nov. 2012.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso 11.out.2023

BRASIL. **Lei 12.737, de 30 nov. 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso 01.out.2023

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm; Acesso em 27.set.2023

BRASIL. **Lei 13.869, de 5 de setembro de 2019.** Dispõe sobre os crimes de abuso de autoridade; altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 8.906, de 4 de julho de 1994; e revoga a Lei nº 4.898, de 9 de dezembro de 1965, e dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13869.htm#art45. Acesso 01.out.2023

BRASIL. **Lei nº 13.964 de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm.

BRASIL**.Lei 14.155, de 27 de maio de 2021**. Aperfeiçoa a legislação penal e processual penal. Disponível em http://https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso 01.out.2023

BRASIL. **Marco civil da internet:** Lei n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015.

BRANCO, Paulo Gustavo Gonet. COELHO, Inocêncio Mártires. MENDES, Gilmar Ferreira. Curso de Direito Constitucional. 4ª. ed. São Paulo: Saraiva, 2008.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Âmbito Jurídico.** Disponível em http://www.ambitojuridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revist a_caderno=17. Acesso. 13. out.20233

CAVALCANTE. Márcio André Lopes. Lei 14.155/2021: **promove alterações nos crimes de violação de dispositivo informático, furto e estelionato** https://www.dizerodireito.com.br/2021/05/lei-141552021-promove-alteracoes-nos.html. Acesso. 3. set.20233

CANUTO, Luiz Cláudio. CPI **constata dificuldade em rastrear e punir crimes de internet.** Disponível em https://www.camara.leg.br/noticias/467819-cpi-constatadificuldade-em-rastrear-e-punir-crimes-de-internet/. Acesso. 3. set.20233

CARBONI, Guilherme C. **A Lei nº 10.695/03 e seu impacto no Direito Autoral Brasileiro. 2003.** Disponível em https://www.migalhas.com.br/impacto-no-direito-autoral-brasileiro.Acesso. 6. set.20233

CARDOSO, Luiz Eduardo; FALAVIGNO, Chiavelli Facenda. **Do Pacote Anticrime ao Código Penal**: uma análise comparativa da disciplina da perda alargada na Lei n. 13.964/2019. 2020. No prelo.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Âmbito jurídico, 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-umareflexao-sobre-o-problema-na-tipificacao/.

CARVALHO, Paulo Sergio de. **Noções Gerais de Direitos autorais**. Escola Nacional de Administração Pública - ENAP. 2014. Acesso 02.nov.2023

CENTRO DE PREVENÇÃO, TRTAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO. **Abuso de Sítio Web.** Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/abuso-de-sitio-web. Acesso 02.nov.2023

CENTRO DE PREVENÇÃO, TRTAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO. **Incidentes.** Disponível em: https://www.gov.br/ctir/ptbr/assuntos/ctir-gov-em-numeros/incidentes . Acesso 02.nov.2023

CERT.br. **Cartilha de Segurança para Internet.** Versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso 18. out. 2023

CERT.br. **Incidentes reportados ao CERT.br:** Janeiro a Junho de 2020. 2020. Disponível em: https://www.cert.br/stats/incidentes/2020-jan-jun/fraude.html. Acesso 18. out. 2023

CERT.br. **Vazamento de Dados.** 2021. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf. Acesso 03.nov.2023

CISO Advisor. S**TJ comunica superação do incidente cibernético com ransomware.** 2020. Disponível em: https://www.cisoadvisor.com.br/stj-comunica-superacao-do-incidentecibernetico-com-ransomware/.

CONVENÇÃO de Budapeste. 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacaotematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-dobrasil/docs_legislacao/convencao_cibercrime.pdf. Acesso 17.out.2023

COUTINHO, Isadora Caroline Coelho. **Pedofilia na era digital.** Ambito Juridico. 2011. Disponível em: https://ambitojuridico.com.br/edicoes/revista-94/pedofilia-na-era-digital/amp/. Acesso 20.out.2023

COMISSÃO EUROPEIA. Proteção de dados nas instituições e outros organismos da UE. Disponível em https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pt#:~:text=O%20Regulamento%20(UE)%202018%2F,Dados%20na%20Aplica%C3%A7%C3%A3o%20da%20Lei. Acesso em 28.set.2023

CRESPO, Marcelo. **Ransonware e sua tipificação no Brasil.** Canal Ciências Criminais. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/artigos/249364352/ransonware-e-suatipificacao-nobrasil#:~:text=A%20pr%C3%A1tica%20do%20ransonware%20%C3%A9,se%20nota%20pel
a%20reda%C3%A7%C3%A3o%20t%C3%ADpica).&text=Ent%C3%A3o%20um%20crime%20grave%20como,do%20modus%20operandi%20do%20criminoso. Acesso 20.out.2023

CUNHA, Rogério Sanches. Pacote Anticrime: Lei n. 13.964/19 - **Comentários às alterações no CP, CPP e LEP.** Salvador: Juspodivm, 2020b.

CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade.** Revista científica eletrônica do curso de direito. 13ª Ed. Disponível em http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso 20.out.2023

CURY, Munir. Estatuto da Criança e do Adolescente comentado: comentários jurídicos e sociais. São Paulo: Malheiros, 2005.

**Declaração Universal dos Direitos do Homem.** Disponível em http://pfdc.pgr.mpf.mp.br/atuacao-econteudos-de-apoio/legislacao/direitos-humanos/declar_dir_homem.pdf. Acesso 20.out.2023

DIANA, Daniela. **História da internet.** Disponível em https://www.todamateria.com.br/historia-dainternet/. Acesso em 14 out. 2023.Acesso 03.nov.2023

DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Disponível em https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indiciosda-autoria-e-prova-da-materialidade. Acesso 05. set. 2023

ELIAS, João Roberto. **Comentários ao Estatuto da Criança e do Adolescente**: Lei n. 8.069, de 13 de julho de 1990. São Paulo: Saraiva, 1994.

ELIAS, João Roberto**. Direitos fundamentais da criança e do adolescente.** São Paulo: Saraiva, 2005

ESTADÃO. **Estudo revela quais as redes sociais mais acessadas por crianças e adolescentes.** Disponível em <https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2022/08/17/estudo-revela-quais-as-redes-sociais-mais-acessadas-por-criancas-e-adolescentes.htm> Acesso 02.nov.2023

FERNANDES SOBRINHO, Rodrigo. Crimes cibernéticos evolução no período pandêmico e combate. 2022.

FUNDAÇÃO Escola Superior do Ministério Público. **Lei Carolina Dieckmann:** Você sabe o que essa lei representa? 2021. Disponível em: https://fmp.edu.br/lei-carolina-dieckmannvoce-sabe-o-que-essa-lei-representa/. Acesso 05.nov.2023

FUTURE. **Brasil: um dos líderes em controle de botnet.** 2017. Disponível em: https://www.future.com.br/blog/brasil-um-dos-lideres-em-controle-de-botnet/. Acesso 10.nov.2023

GATEFY. **BEC e phishing ainda continuam na moda, diz o relatório do FBI**. 2021. Disponível em: https://gatefy.com/pt-br/blog/bec-phishing-continuam-moda-diz-relatoriofbi/.

GIACCHETTA, André Zonaro. **A nova arma no combate à pirataria - a Lei Nº 10.695, de 2.7.2003.** Migalhas, 2003. Disponível em: https://www.migalhas.com.br/depeso/2275/a-novaarma-no-combate-a-pirataria---a-lei--n---10-695---de-2-7-2003. Acesso 20.out.2023

GIDDENS, Anthony. **As consequências da modernidade.** São Paulo: Editora UNESP, 1991

GUARAGNI, Fábio André. RIOS, Rodrigo Sanchez. **Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea.** Revista de Estudos
Criminais. Porto Alegre, v. 18, n. 73. p. 181. 2019.

GUARAGNI, Fábio André. RIOS, Rodrigo Sanchez. **Novas tendências de combate aos crimes cibernéticos:** cooperação internacional e perspectivas na realidade brasileira contemporânea. Revista de Estudos Criminais. Porto Alegre, v. 18, n. 73. p. 181. 2019.

O GLOBO.Instagram muda regras de acesso para menores de 16 anos, que terão contas privadas por padrão. Disponível em < https://revistapegn.globo.com/Banco-de-ideias/Mundo-digital/noticia/2021/07/instagram-muda-regras-de-acesso-para-menores-de-16-anos-que-terao-contas-privadas-por-padrao.html> Acesso 20.nov.2023

INTERPOL. **Cybercrime: Covid-19 Impact.** 2020. Disponível em: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats. Acesso 10.nov.2023

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

JESUS, Damásio De. ARAS, Vladmir. Crimes de informática: **Uma nova criminalidade.** Disponível em .https://jus.com.br/artigos/2250/crimes-de-informática. Acesso 20.out.2023

JUNIOR, Júlio Cesar Alexandre. **Cibercrime: um estudo acerca do conceito de crimes informáticos**. Revista Eletrônica da Faculdade de Direito de Franca. Disponível em . Acesso em https://www.revista.direitofranca.br/index.php/refdf/article/view/602#:~:text=Cibercrime%20est%C3%A1%20associado%20ao%20%E2%80%9Cfen%C3%B3meno,12). Acesso. 10 set. 2023.

KASPERSKY. **Ciberataques crescem 23% no Brasil em 2021**. 2021. Disponível em: https://www.kaspersky.com.br/blog/panorama-ciberameacas-brasil-2021-pesquisa/18020/. Acesso 20.set.2023

KAMINSKI, Omar. **Conheça o Tratado Internacional contra crimes na Internet.** Revista Consultor Jurídico. Disponível em . https://www.conjur.com.br/2001-nov-4/convencao_lanca_tratado_internacional_cibercrimes. Acesso 19.out.2023

KESIKOWSKI, Sabrina Cunha; WINTER, Luis Alexandre Carta; GOMES, Eduardo Biacchi. Atuação do Grupo Mercado Comum frente à criminalidade organizada transnacional. Revista de Direito Internacional, v. 15, n. 2, p. 353-369, 2018

LEON, Lucas Pordeus. **Brasil tem 152 milhões de pessoas com acesso à internet.** AgênciaBrasil, Brasília, 2021. Disponível em: Brasil tem 152 milhões de pessoas com acesso à internet | Agência Brasil (ebc.com.br).

Legislação Informatizada - **LEI Nº 11.829, DE 25 DE NOVEMBRO DE 2008** - Publicação Original. Disponível em < https://www2.camara.leg.br/legin/fed/lei/2008/lei-11829-25-novembro-2008-584363-publicacaooriginal-107102-pl.html. Acessado 08. nov. 2023. Acesso 15.out.2023

LIMA, Renato Brasileiro de. **Pacote Anticrime:** Comentários à Lei 13.964/2019 artigo por artigo. Salvador: Juspodivm, 2020. Acesso. 29.set.2023

LIMA, Caio Souza Pitta. Evolução histórica do sistema internacional de proteção aos direitos humanos de crianças e adolescentes. In. Boletim Consultor Jurídico, 16 out. 2015. Disponível em: http://www.conteudojuridico.com.br/artigo,evolucao-historica-do-sistemainternacional-de-protecao-aos-direitos-humanos-de-criancas-e-adolescentes,54545.html. Acesso 20.out.2023

LOURENÇO, Gabriel D. **Ataque da Mão Fantasma: novo golpe brasileiro rouba a vítima diante dos próprios olhos.** Olhar Digital, 2021. Disponível em: https://olhardigital.com.br/2021/08/31/seguranca/ataque-da-mao-fantasma/ .

NASCIMENTO, Talles Leandro Ramos. Crimes cibernéticos. Conteúdo Jurídico. Disponível em . https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso 20.out.2023

NEUMANN, Josieli Pinto. Pedofilia virtual: consequências reais. Disponível em: <http://bibliodigital.unijui.edu.br:8080/xmlui/bitstream/handle/123456789/3771/Josieli%20Pinto%20Neumann.pdf?sequence=1>. Acesso 20.out.2023

MACHADO, Thiago José Ximenes. **Cibercrime e o crime no mundo informático.** Tese apresentada no Programa de Mestrado em Criminologia da Universidade Fernando Pessoa, sob a orientação da Professora Rita Rola. Porto, 2017, p. 7.

MATIAS, Juliana. **Crimes digitais: 'Atual legislação vive de puxadinhos', diz desembargadora do TJSP.** Disponível em https://www.jota.info/jotinhas/crimes-digitais-atual-legislacao-vive-de-puxadinhos-diz-desembargadora-do-tjsp-09062022. Acesso 15.set.2023

MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges. **Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica.** Disponível

em
http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e a-necessidade-de-legislacao-especifica-2. Acesso. 14 de set..2023

MENDONÇA, Cláudia da Silva. **Guerra Cibernética: Desafios de uma Nova Fronteira.** Rio de Janeiro, 2014.

MILAGRE, José Antônio. **Lei Azeredo, AI-5 digital e a cultura do contra. Uma visão pessoal sobre o manifesto contra a Lei de Crimes de Informática**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 14, n. 2216, 26 jul. 2009. Disponível em: https://jus.com.br/artigos/13211. Acesso 12.set.2023

MINISTÉRIO DA JUSTIÇA DE SEGURANÇA PÚBLICA. **Convenção de Budapeste é promulgada no Brasil.** Disponível em https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso 10.set.2023

MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO.. **Marco Civil da Internet: Perspectivas gerais e apontamentos críticos.** São Paulo.

MINISTÉRIOS DAS RELAÇÕES EXTERIORES. **Processo de adesão à Convenção de Budapeste** -Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Disponível emhttp://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de. Acesso 10.set.2023

MORAES, Alexandre de. **Direito constitucional.** 15. Ed. – São Paulo: Atlas, 2004. p. 74

MORAES, Paulo Francisco Cardoso de. **A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores.** Revista Âmbito Jurídico. Disponível em https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/. Acesso: 2.set.2023.

PINHEIRO, Patrícia Peck, **Sobre a adesão do Brasil à Convenção de Budapeste**. Disponível em https://www.telesintese.com.br/peck-sobre-a-adesao-do-brasil-a-convencao-de-budapeste/. Acesso 12.set.2023

PINHEIRO, Patrícia Peck, Direito digital. 6.ed., atual. e ampl. São Paulo: Saraiva, 2016.

PROPRIEDADE INTELECTUAL, **Estratégia Nacional de Propriedade Intelectual.** 2021. Disponível em
https://www.gov.br/pt-br/propriedade-intelectual/estrategia-nacional-de-propriedade-intelectual Acesso 28.set.2023

POR G1. **Brasil tem 306 denúncias de pornografia infantil por dia na internet, aponta levantamento.** Disponível em
<https://g1.globo.com/tecnologia/noticia/2023/02/07/brasil-tem-306-denuncias-de-pornografia-infantil-por-dia-na-internet-aponta-levantamento.ghtml>

POR G1.**TikTok altera contas de usuários com idade entre 13 e 15 anos para modo privado.** Disponível em

<https://g1.globo.com/economia/tecnologia/noticia/2021/01/13/tiktok-altera-contas-de-usuarios-com-idade-entre-13-e-15-anos-para-modo-privado.ghtml> Acesso 20.set.2023

RAINS, Tim. **CybersecurityThreats, Malware Trends, andStrategies: mitigateexploits, malware, phishingandother social engineeringattacks**. Birmingham: PacktPublishing Ltd, 2020. 429 p.

ROVER, Tadeu. **Violência virtual: internet facilita crimes e dificulta investigação, estimulando a impunidade.** Disponível em https://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais. Acesso 5.set.2023

ROMANO, Rogério Tadeu. CONVENÇÃO DE BUDAPESTE E CIBERCRIMES. Disponível em. https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes. Acesso em 5. set. 2023.

SAFERNET, Brasil - Protegendo os Direitos Humanos na Sociedade da Informação. **Parcerias com o MPF.** Disponível em https://www.safernet.org.br/site/institucional/parcerias/mpf. Acesso 01 out. 2023

SANCHES, Ademir Gasques. ANGELO, Ana Elisa de. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil. Acesso 02.set.2023

SANTOS, Elaine Gomes dos. RIBEIRO, Raisa Duarte da Silva. **Restrições à liberdade de expressão e crimes cibernéticos: a tutela penal do discurso de ódio nas redes sociais.** Revista dos Tribunais. vol. 997. ano 107. p. 527. São Paulo: Editora RT. novembro 2018.

Secretaria Geral da Presidência da República. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**. Disponível em https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica. Acesso 9.set.2023

SEGURANÇA,Justiça. **A Convenção de Budapeste é promulgada no Brasil**. Disponível em https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso 10.set.2023

SENADO. C**ombate ao cibercrime é urgente, afirmam especialistas na CCT.** Disponível https://www12.senado.leg.br/noticias/materias/2021/12/15/combate-ao-cibercrime-e-urgente-afirmam-especialistas-na-cct. Acesso 20.set.2023

SENADO. **Comissão de Relações Exteriores e Defesa Nacional.** Disponível https://www25.senado.leg.br/web/atividade/notas-taquigraficas/-/notas/r/10148 Acesso. 18. set.2023

SENADO FEDERAL. **Projeto de Lei n. 6.341, de 2019.** 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/140099. Acesso 20.out.2023

SEGURANÇA PÚBLICA, **Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos.** 2022. Disponível em https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos. Acesso. 18. mai.2023

SILVA, Rita de Cássia Lopes. **Direito Penal e Sistema Informático**. Revista dos Tribunais, 2003.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS.** Disponível em. https://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras. Acesso 02.set.2023

STEINBERG, Joseph. **Cibersegurança para leigos**. 1 ed. Rio de Janeiro: Alta Books, 2021.

Symantec; Organizações dos Estados Americanos. Relatório '**Tendências de Cibersegurança na América Latina e no Caribe**". 2014. Disponível em https://www.broadcom.com/404-symantec?sourceURL=http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc-annex.pdf?

TANAKA, Caroline Yumi de Oliveira. OS CRIMES CONTRA A HONRA E A INTERNET. 2016. Disponível em: <http://repositorio.uniceub.br/bitstream/235/9234/1/21204599.pdf>.

TRUZZI, Gisele. **Direitos autorais e internet: como usar conteúdo de terceiros sem problemas**. Disponível em https://www.conjur.com.br/2020-ago-24/gisele-truzzi-direitos-autorais-internet. Acesso 20.out.2023

VALVERDE, Danielle Novaes de Siqueira. **Crimes Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso.** Revista da ESMAPE. Recife. v. 15. n. 32. p. 236.

VERONESE, Josiane Rose Petry. **Lições de Direito da Criança e do Adolescente:** Volume 2 [recurso eletrônico] -- Porto Alegre, RS: Editora Fi, 2022.

VERONESE, Josiane Rose Petry; SILVA, Rosane Leal da (Orgs.) **A Criança e seus Direitos: entre violações e desafios [recurso eletrônico]** -- Porto Alegre, RS: Editora Fi, 2019.

RIBEIRO, Joana; VERONESE, Josiane Rose Petry. **Princípios do Direito da Criança e do Adolescente e Guarda Compartilhada: estudos de casos com a Família ampliada ou extensa** [recurso eletrônico] / Joana Ribeiro; Josiane Rose Petry Veronese -- Porto Alegre, RS: Editora Fi, 2021.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes Cibernéticos: Ameaças e procedimentos de investigação**. 3 ed. Rio de Janeiro: Brasport, 2021.

WINDER, Davey. **This 20-Year-Old Virus Infected 50 Million Windows Computers In 10 Days:** Why The ILOVEYOU Pandemic Matters In 2020. FORBES, 2020. Disponível em: https://www.forbes.com/sites/daveywinder/2020/05/04/this-20-year-old-virus-infected-50-million-windows-computers-in-10-days-why-the-iloveyou-pandemic-matters-in2020/?sh=10aa7f8b3c7c.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 17° Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf.
Acesso em: 31 ago. 2023.

SAFERNET. Denúncias de imagens de abuso e exploração sexual infantil online compartilhadas pela Safernet com as autoridades têm aumento de 70% em 2023. 2023. Disponível em: https://new.safernet.org.br/content/denuncias-de-imagens-de-abuso-e-exploracao-sexual-infantil-online-compartilhadas-pela. Acesso em: 27 set. 2023.

UNESCO. Segurança online de crianças e adolescentes: Minimizar o risco de violência, abuso e exploração sexual online. 2020. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000374356. Acesso em: 19 set. 2023.