FACULDADE DE ILHÉUS CESUPI

COLEGIADO DO CURSO DE DIREITO

COORDENAÇÃO DE TCC

ARTIGO CIENTÍFICO

CRIMES CIBERNÉTICO: DESAFIOS DA LEI 11.829/2008 NO COMBATE A PORNOGRAFIA INFANTIL

ILHÉUS – BA

2022

FACULDADE DE ILHÉUS CESUPI

COLEGIADO DO CURSO DE DIREITO

COORDENAÇÃO DE TCC

ARTIGO CIENTÍFICO

PAULO ANTONIO SILVA E SILVA

CRIMES CIBERNÉTICO: DESAFIOS DA LEI 11.829/2008 NO COMBATE A PORNOGRAFIA INFANTIL

Artigo Científico entregue para acompanhamento como parte integrante das atividades de TCC II do Curso de Direito da Faculdade de Ilhéus.

Orientadora: Professora Mª Thyara Gonçalves Novais

ILHÉUS – BA

2022

CRIMES CIBERNÉTICO: DESAFIOS DA LEI 11.829/2008 NO COMBATE A PORNOGRAFIA INFANTIL

PAULO ANTONIO SILVA E SILVA

Aprovado em: __ / __ / ____

BANCA EXAMINADORA

_____

Prof. Mª Thyara Gonçalves Novais

Faculdade de Ilhéus - CESUPI

Orientadora

_____

Prof.

Faculdade de Ilhéus - CESUPI

Avaliador I

_____

Prof.

Faculdade de Ilhéus - CESUPI

Avaliador II

Sumário

CRIMES CIBERNÉTICO: DESAFIOS DA LEI 11.829/2008 NO COMBATE A PORNOGRAFIA INFANTIL

CYBER CRIMES: CHALLENGES OF LAW 11.829/2008 IN THE FIGHT AGAINST CHILD PORNOGRAPHY

Paulo Antônio Silva e Silva [1] , Thyara Gonçalves Novais [2]

1. Discente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia. E-mail: paulocorretorilheus@gmail.com
2. Docente do curso de Direito da Faculdade de Ilhéus, Centro de Ensino Superior, Ilhéus, Bahia. E-mail:

RESUMO

Os crimes cibernéticos aqueles praticados em ambiente virtual, vem crescendo na mesma velocidade da globalização. Com isso a pornografia infantil se torna cada vez mais evidente, desta forma o Estatuto da Criança e do Adolescente alterada pela Lei 11.828 de 25 de novembro de 2008 pune as pessoas que reproduzem, fotografam, filmam ou registram, por qualquer meio, cena de sexo que envolvam menores de idade. Devido ao aumento do uso de dispositivos e redes sociais os crimes contra crianças e adolescente se torna um problema social, e que desafiam as autorizadas na punição dos infratores, pelo anonimato envolvido na internet. O objetivo central do estudo é analisar como a Lei de combate a pornografia infantil vem atuando no ambiente cibernético. O estudo justifica-se por haver números elevados de casos envolvendo menores dentro no universo virtual. Propõe-se, ainda, apresentar os desafios e desta forma analisar a influência da Lei no combate a esse tipo de crime, baseado no princípio que o crime contra menores, pode ser combatido com leis e penas mais severas para quem os pratica. Tendo como fontes coleta de informações de fontes secundárias, incluindo, plataformas de pesquisa, livros, materiais e autores significativos para o trabalho.

Palavras-chave: Direito Penal. Crimes Cibernéticos. Lei. Pornografia Infantil.

ABSTRACT

Cyber crimes, those practiced in a virtual environment, have been growing at the same speed as globalization. With this, child pornography becomes increasingly evident, in this way the Child and Adolescent Statute amended by Law 11,828 of November 25, 2008 punishes people who reproduce, photograph, film or record, by any means, a sex scene involving minors. Due to the increase in the use of devices and social networks, crimes against children and adolescents become a social problem, and they challenge the authorized in the punishment of offenders, due to the anonymity involved in the internet. The main objective of the study is to analyze how the Law to combat child pornography has been acting in the cyber environment. The study is justified by the high numbers of cases involving minors in the virtual universe. It is also proposed to present the challenges and thus analyze the influence of the Law in combating this type of crime, based on the principle that crime against minors can be fought with laws and

more severe penalties for those who practice them. Having as sources collect information from secondary sources, including research platforms, books, materials and authors significant to the work.

Keywords:Criminal Law. Cyber Crimes. Law. Child Pornograph

1 INTRODUÇÃO

Compreender o espaço virtual conhecido como Internet é fundamental para os juristas e para os que praticam o direito no século XXI. Essa nova tecnologia está cada vez mais presente em nosso dia a dia, principalmente na vida da nova geração nascida nesse mundo virtual, que é muito conveniente de usar os mais diversos dispositivos de informática.

No entanto, essas mentalidades novas e vulneráveis são alvos mais fácil para criminosos modernos explorarem no universo virtual para atividades ilegais, especialmente crimes envolvendo a exploração sexual de jovens. Existem vários métodos utilizados para distribuir grandes quantidades de material pornográfico, bem como estratégias para encontrar formas de realizar seus desejos sinistros. As responsabilidades dos juristas aumentaram, com a difícil tarefa de atualização das codificações para que sejam uma resposta firme e concreta às necessidades sociais do terceiro milênio. Os mundos virtuais não podem mais ser ignorados como fenômeno social, e sua regulamentação é iminente, principalmente para proteger os usuários.

Não se trata de interferência do Estado no livre fluxo de informações. A segurança pessoal deve existir tanto no mundo físico quanto no virtual, principalmente para os mais jovens. Dito isso, não há melhor maneira de modernizar o direito do que conhecer e entender o funcionamento desse caminho invisível que percorre na vida dos cidadãos. É com esse propósito que se propõe esta monografia: Compreender como a Internet, suas vulnerabilidades e insegurança, tornou-se um meio de ação para pedófilos e criminosos sexuais satisfazerem seus desejos pervertidos, e entender o avanço que a Internet trouxe em nossa legislação, para coibir esse comportamento, para obter uma visão geral da situação atual, das dificuldades que ainda persistem e possíveis caminhos para um maior aperfeiçoamento da nossa legislação.

Um breve histórico de seu surgimento e desenvolvimento, será discutida a ocorrência do crime virtual em geral e serão apresentados dados que revelam a necessidade de se discutir o tema.

Reconhecendo a gravidade da situação o artigo mostrará a legislação existente tanto no ordenamento jurídico internacional quanto no ordenamento normativo interno. O foco será nos dispositivos constitucionais que garantem a proteção da criança e do adolescente, bem como a implementação dessa proteção, como o Código Penal e o Código da Criança e do Adolescente.

Serão analisados os tipos de crimes trazidos pela Lei 11.829/08 para entender as inovações trazidas e as condutas típicas que configuram crimes contra bem jurídico tutelado. No entanto, à luz das Leis 12.735/12 e 12.737/12, será feito um breve comentário sobre as inovações que visam combater o crime virtual na Internet e os demais tipos de crime que o cercam. As situações analisadas vão desde questões anteriores à fase processual até questões discutidas e tratadas no âmbito da jurisdição do judiciário.

O trabalho justifica-se por atrair a atenção para algo que está no convívio das famílias e que muitas vezes só é percebido tarde demais, desta forma servirá como sinal de alerta

Para o presente estudo temático, a metodologia utilizada é bibliográfica, utilizando-se de textos e artigos científicos não só da ciência jurídica, mas também de diversas vertentes do conhecimento e da informática. Como esse é um problema relativamente novo, a quantidade de material disponível ainda é muito limitada, mas à medida que mais e mais estudiosos de diferentes áreas trabalham juntos para entender todos os detalhes desse fenômeno, dessa nova tecnologia cotidiana, torna-se cada vez mais importante todos os dias estão crescendo.

2 PORNOGRAFIA INFANTIL

Em primeiro lugar, é oportuno elucidar a origem da palavra pedofilia, que vem da combinação *paidós* (criança, em grego) e *philos* (amante, que gosta de) Consequentemente, no sentido original, um pedófilo seria uma pessoa que ama crianças. Posteriormente, esse conceito é usado para se referir a uma pessoa que tem interesse sexual em uma criança.

De acordo com a Classificação Internacional de Doenças (CID-10/OMS), a pedofilia é um transtorno de preferência sexual que geralmente afeta crianças antes ou no início da adolescência. Na Conceito Psiquiátrica (DSM-IV/APA), a pedofilia é um distúrbio sexual caracterizado pela formação de excitação sexual e fantasias intensas, excitação ou participação em comportamentos positivos em crianças pré-púberes, geralmente com 13 anos de idade ou menos. No entanto, para ser considerado pedófilo, ele deve ter pelo menos 16 anos e pelo menos 5 anos mais velho que a criança. A pedofilia pode levar a sofrimento clinicamente significativo ou prejuízo do funcionamento pessoal social e ocupacional.

Conforme o Art. 241-E do Estatuto da Criança e do Adolescente pedofilia infantil é qualquer representação de uma criança ou adolescente envolvida em atividades sexuais explícitas reais ou simuladas, ou qualquer representação dos órgãos sexuais de uma criança ou adolescente para fins primordialmente sexuais.

Na Grécia antiga, a fronteira entre a infância e a adolescência era marcada por aventuras eróticas com adultos. Não foram poucos os casos de filhas sendo estupradas por seus pais e, como resultado desses atos, a maioria das mulheres em Roma e na Grécia não tinha o hímen intacto. No entanto, não só as meninas foram submetidas a tais abusos, mas também os meninos foram abusados sexualmente constantemente, pois foram abusados sexualmente por homens mais velhos a partir dos 7 (sete) anos de idade até os 21 anos (AZAMBUJA, 2004).

Portanto, na Grécia e no Império Romano, o uso de menores como objeto de gratificação pessoal adulta era difundido, apreciado e tolerado. A relação anal entre professores e alunos também era comum (AZAMBUJA, 2004).

Com a influência da religião, a prática sexual entre crianças e adultos assumiu contornos de reprovação à medida que o cristianismo passou a se opor vigorosamente a essas práticas (CARVALHO, 2002).

Com o cristianismo e a clara oposição a essas práticas, a Igreja conseguiu ao longo do tempo criminalizar essa reprovação e incorporá-la ao ordenamento jurídico estadual (CARVALHO, 2002).

Por volta do século XV, o sentimento de família prevalecia, mas os menores ainda eram submetidos à violência sexual no século XVII. Quando Portugal colonizou o Brasil, os decretos e leis que regem as crianças e os jovens eram aplicados por

representantes da Igreja Católica, pois a Igreja e o Estado andavam juntos, unindo conquista armada e religião (CARVALHO, 2002).

Dessa forma, os padres jesuítas cuidavam dos menores indígenas, com o objetivo de batizá-los e depois trazê-los para o trabalho. Movimentos religiosos, por exemplo, não aceitaram as formas de violência a que crianças e jovens eram submetidos e, por isso, fundaram abrigos para protegê-los. Após serem separados de sua tribo, esses pequenos índios foram ensinados as verdades do cristianismo, como o casamento religioso, além de outros dogmas para ensinar-lhes o modo de vida cristão no mundo (FALCONI, 1997).

Mudanças significativas ocorreram a partir do século 18 através da Reforma Protestante e da Contrarreforma Católica. A família tornou-se assim a pedra angular da moral cristã. Outro ladrão, a sodomia, foi visto com má visão e foi considerado depravado e abominável. No entanto, alguns filósofos se opuseram a essa ideia, entre os quais se destaca Jeremy Bentham, que defendia como permissível qualquer ato sexual que deixasse uma pessoa feliz (FALCONI, 1997).

Como em outras partes do mundo, o abuso sexual que ocorreu e está ocorrendo tem uma consequência do ponto de vista da criança. Na época do descobrimento do Brasil, muitos filhos eram enviados para acompanhar o rei e também para casar com os súditos da coroa (FELIPE, 2006).

Certas comunidades ribeirinhas da Amazônia tinham o costume de os pais iniciarem suas filhas na sexualidade, levando à pedofilia e ao incesto. Esse ato criou uma lenda muito comum na região, a lenda do boto rosa, que se transformava em um homem bonito nas noites de lua cheia e engravidava donzelas ingênuas (FELIPE, 2006).

O termo criança aparece pela primeira vez em 1823 porque as crianças precisam ser mais cuidadosas. Por outro lado, o tema da infância só ganhou importância com o estabelecimento das primeiras instituições de ensino superior, especialmente em medicina (FREUD, 1974).

Com a criação da Declaração dos Direitos da Criança em 1959, destacaram-se as condições degradantes em que viviam as crianças brasileiras. Na declaração acima foi previsto que toda criança tem, entre outros direitos, o direito à igualdade sem distinção de raça, religião ou nacionalidade, proteção especial para seu

desenvolvimento físico, mental e social. Mas foi somente em 1962, após a publicação de Kempe, que ele chamou de Síndrome da Criança Maltratada, que se iniciou o estudo das agressões a que as crianças eram submetidas, chamando a atenção dos profissionais de saúde e da sociedade principalmente para sua proteção (FREUD, 1974).

No entanto, deve-se ressaltar que a Lei da Infância e da Juventude, antes de descrever os direitos e obrigações, implementa a doutrina da proteção integral da criança e do jovem, definindo como criança a pessoa até os doze anos; e na adolescência, os de doze a dezoito anos (HISGAIL, 2007).

A partir da década de 1990, a violência sexual contra menores passou a preocupar a sociedade brasileira e até se tornou política pública no Brasil. A Constituição Federal do Brasil de 1988, o Estatuto da Criança e do Adolescente (Lei 8.069/90) e a Convenção Internacional dos Direitos da Criança de 1999 levaram a essa grande mudança (HISGAIL, 2007).

Percebe-se, assim, que a mudança na forma como as crianças são vistas se deve a mudanças sociais, políticas e culturais que alteraram o conceito de infância, família, instituições educacionais e, portanto, a forma como foram criadas e acompanhadas ao longo da vida.

2.1 Desafios da legislação no combate a pornografia infantil

Devido à existência desses ambientes virtuais de difícil acesso, a prática do crime, especialmente a pornografia infantil, é tão desenfreada. O compartilhamento e recebimento de fotos de abuso sexual infantil e juvenil na dark web e deep web ocorre constantemente sem que as autoridades consigam identificar a origem desses arquivos e quem tem acesso a eles (BAPTISTA, 2021).

No ambiente computacional, os usuários buscam segurança e privacidade para que possam usufruir tranquilamente da facilidade e dos benefícios que a World Wide Web oferece no dia a dia, tanto nas relações sociais quanto comerciais. Por outro lado, condutas ilícitas como fraudes, furtos e uso indevido de dados e tantos outros crimes cometidos pela Internet trazem cada vez mais insegurança e a sensação de que as autoridades são impotentes contra isto (BAPTISTA, 2021).

Analisando a legislação brasileira, fica claro que ainda faltam normas que caracterizem condutas ilícitas no ambiente virtual, as informações, dados, confiabilidade e segurança dos sistemas de informática e comunicações devem ser protegidos por lei criminal. Observando o desenvolvimento dos meios de comunicação e tecnologia da informação, constatamos que em determinados momentos a legislação penal não é adequada em termos de proteção legal contra crimes cibernéticos (BAPTISTA, 2021).

A adoção das Leis 12.735/2012, 12.737/2012 e 12.965/2014 não foi suficiente para combater efetivamente os crimes cometidos pela Internet, principalmente pela grande variedade de crimes cibernéticos e pela falta de legislação específica. Além disso, a completude do código penal brasileiro dificulta a aplicação de suas regras por analogia aos crimes cibernéticos (BAPTISTA, 2021).

Quando o crime diz respeito a contratos virtuais, são utilizados o Código Civil Brasileiro e o Código de Defesa do Consumidor, na ausência de regulamentação específica relacionada à área penal, já há também a aplicação de normas tipificadas no Código Penal, incluindo os artigos 240 e 241 da Lei nº 11.829/2008 do Estatuto da Criança e do Jovem; Artigo 12 da Lei n. 9.609/98 que trata dos crimes contra a pirataria de software; os artigos 138, 139, 140 e 147 do Código Penal Brasileiro, que descrevem respectivamente os crimes de difamação, difamação, agressão e ameaça (BAPTISTA, 2021).

Com os avanços da tecnologia e o constante compartilhamento de informações e ideologias nos meios virtuais, a sociedade atual carece de interferência governamental para ditar regras e regulamentos constitucionais para estender os princípios mencionados a todas as áreas onde a democracia estabelece as necessidades básicas da existência (BAPTISTA, 2021).

Pode-se observar que a internet brasileira é construída sobre três pilares formados pelos princípios de neutralidade da rede, privacidade e liberdade de expressão, que estão inter-relacionados. A neutralidade da rede é garantir que as operadoras não cobrem taxas diferentes dependendo do conteúdo que transportam, exceto em relação às velocidades que oferecem. Esse princípio visa democratizar o acesso à internet no país (BAPTISTA, 2021).

A referida Lei nº 12.737/2012 ficou conhecida como Lei Carolina Dieckmann, em decorrência do episódio de divulgação de imagens em sites pornográficos, após hackers penetrarem nos arquivos e acessarem ilegalmente os dados da atriz do canal

de TV brasileiro Fala Globo. A vítima recusou a chantagem de pagar a quantia em dinheiro para que suas fotos em poses íntimas não fossem amplamente divulgadas. O advento da regulamentação do cibercrime representou um marco na história do ordenamento jurídico brasileiro, pois trouxe um avanço significativo em relação ao crime de informática (BAPTISTA, 2021).

A Lei nº 12.737/2012 dispõe sobre a tipificação penal dos crimes de informática, com o intuito de atualizar a legislação penal vigente nos termos do art. 154-A do Código Penal, introduzido pelo art. 2º da Lei 12.737, declara a prática criminosa de hackear aparelho de informática de outra pessoa, conectado ou não à rede de computadores, mediante a violação ilícita de mecanismos de segurança para obter, adulterar ou destruir dados ou informações sem autorização do proprietário do aparelho para obter uma vantagem indevida (BAPTISTA, 2021).

Não é apenas qualquer dispositivo de computador hackeado que goza de proteção legal. Para que o crime ocorra, o dispositivo deve possuir um mecanismo de segurança (por exemplo, antivírus, firewall, senhas, etc.). Portanto, o dispositivo informático sem mecanismo de segurança não pode ser objeto material da conduta incriminada, pois o crime exige violação indevida do mecanismo de segurança. Dessa forma, introduzir ou construir vulnerabilidades em sistemas desprotegidos é um fato atípico. Francamente, essa falta de proteção legal não é compreendida com precisão para os indivíduos menos protegidos. É como se a legislatura assumisse que invadir uma casa com as portas abertas não é uma violação de invasão e ficar lá sem a permissão dos ocupantes e até mesmo contra seus desejos expressos! Não parece justo ou razoável supor que alguém que não instala proteção em seu computador permitirá tacitamente a intrusão, assim como deixar a porta ou portão de sua casa aberta ou destrancada de forma alguma significa que pretende intrometer alguém para deixá-la lar. O formulário vinculado fornecido de forma criminosa (por violação ilícita de mecanismos de segurança) pode muito bem não ter sido utilizado pelo legislador, que deve apenas alertar para intrusão ou instalação não autorizada e/ou injustificada. Isso seria feito simplesmente com a expressão por violação ilícita, sem a necessidade de mencionar mecanismos de segurança (BAPTISTA, 2021).

. O contexto que cerca a gênese da Lei 12.737/12 mostra que havia uma brecha legal para caracterizar crimes cometidos na Internet e que foi somente após o crime envolvendo a atriz Carolina Dieckmann que a questão foi efetivamente debatida e a

lei aprovada com urgência, marcando um grande avanço na legislação brasileira no combate ao cibercrime (BAPTISTA, 2021).

Investigar e combater crimes cibernéticos não é uma tarefa fácil, pois as práticas desses crimes podem ocorrer em qualquer lugar, desde que o criminoso tenha acesso à rede. Nesse contexto, a Internet desempenha o papel de grande intermediária na perpetração desses crimes devido à dificuldade em encontrar o responsável pelo crime (BARRETO, 2017).

Em geral, a aplicação da lei pode ser dividida em duas fases, investigações criminais e processos criminais. A primeira fase limita-se à recolha de provas, verificando a autoria e a substancialidade do facto criminoso, enquanto a segunda fase destina-se à persecução e julgamento (BARRETO, 2017).

Tanto no direito penal como no direito penal digital, cibernético ou eletrônico, os termos crime, delito, ato e efeito são utilizados da mesma forma, com as principais diferenças relativas à territorialidade e coleta de provas, bem como a criação de novos tipos de crime devido ao surgimento de infrações penais cometidas exclusivamente por meio eletrônico (BARRETO, 2017).

Na investigação de crimes cibernéticos, há uma fase inicial, técnica, e uma fase subsequente, de investigação. O principal objetivo da fase técnica é localizar o computador ou dispositivo usado para cometer o comportamento criminoso. Nessa fase, são realizados alguns procedimentos iniciais, que são a análise das informações contadas pela vítima e o entendimento dos fatos que surgiram na internet, bem como a orientação da vítima buscando preservar as provas materiais de o crime e seu respaldo virtual, início da Prova em ambiente virtual, formalização do comportamento criminoso por meio do registro do boletim de ocorrência e início do procedimento, primeira coleta de dados na World Wide Web, sobre possíveis autores, origem de e-mails, registros e hospedagem de domínios. Formalização das provas colhidas e investigação preliminar, representação no judiciário para obtenção de autorização judicial para violação de dados, conexão ou acesso (BARRETO, 2017).

A partir da identificação e localização do computador que possibilitou a conexão e acesso criminoso à Internet, tem-se a chamada fase de atendimento de campo, na qual há a necessidade de os policiais avançarem para a realização de diligências para obtenção de informações operacionais. lugar de reconhecimento para promover. Essa diligência deve ser sempre feita de forma discreta, pois pode ser necessário requerer medida cautelar no processo penal, geralmente uma representação, para que o

judiciário possa expedir o mandado de busca e apreensão. Ocorre imediatamente nos casos de identificação do endereço correspondente a um local de residência e/ou rede não corporativa (BARRETO, 2017).

No Brasil, foi implementada a criação de outros métodos de combate aos crimes virtuais, incluindo a criação de departamentos especializados em crimes cibernéticos. Essa atividade de policiamento, realizada tanto no mundo offline quanto no mundo online, e que é de responsabilidade da polícia federal ou civil, deve ser regida por uma política de segurança pública e organizada por meio de dados e informações, característicos do local ou assunto às quais as autoridades policiais estão ligadas (BARRETO, 2017).

A infiltração de agentes policiais no mundo virtual é lícita para apuração de crimes de organização criminosa, tráfico de drogas, pornografia infantil, pedofilia e ciberterrorismo. A Lei 13.441/1733 regulamenta o contrabando de policiais na Internet para fins de apuração de crimes contra a dignidade sexual de crianças e jovens. Nas investigações, assim como os criminosos possuem técnicas que os mantêm anônimos na rede, as autoridades policiais rastreiam possíveis vulnerabilidades desses criminosos coletando provas de crimes, aproveitando também o anonimato oferecido pela deep web e dark web (BARRETO, 2017).

Também nesse sentido, os acordos internacionais de cooperação e combate ao cibercrime ratificados pelo Brasil favorecem a comunicação entre os países e seu apoio e comunicação no combate ao cibercrime (BARRETO, 2017).

No Brasil, a Polícia Federal lançou duas grandes operações de crimes cibernéticos, ambas com o objetivo de combater a pornografia infantil. Usando um método investigativo inédito, a polícia conseguiu burlar o anonimato proporcionado por ambientes obscuros da Internet onde não é possível identificar o IP e identificou mais de 90 usuários que acessam e controlam o compartilhamento de pornografia infantil. Essas operações demonstram que o Serviço Brasileiro de Investigação tem feito avanços significativos no ambiente virtual, apesar de todas as falhas na lei e dos benefícios que a Deep Web e a Dark Web oferecem aos criminosos (BARRETO, 2017).

O abuso sexual é um grave problema social no Brasil, sendo a segunda forma mais comum de violência contra crianças segundo levantamento do Ministério da Saúde publicado em 2012. As consequências de tais ações levam a diversos transtornos físicos e psicológicos tanto nos acometidos quanto na própria sociedade.

A pornografia infantil é um tipo de violência sexual contra menores, tipificada como crime pela Lei da Criança e do Adolescente (ECA), Lei Federal 8.069/1990, alterada pela Lei 11.829/2008. De acordo com as estatísticas, o número de denúncias de pornografia infantil é crescente, apesar dos inúmeros esforços dos órgãos policiais, há um aumento no número de prisões e acusações criminais. Em 2014, o Nacional Central de Denúncias de Crimes Cibernéticos considerou a pornografia infantil o crime cibernético mais comum no Brasil. Em 2015, a mesma linha direta recebeu e processou 43.182 denúncias anônimas de pornografia infantil envolvendo 17.433 sites diferentes (dos quais 5.142 foram removidos), hospedados em 4.956 hosts diferentes e conectados à internet por meio de 3.956 IPs diferentes que são atribuídos a 54 países em 5 continentes (BARRETO, 2017).

As principais soluções encontradas atualmente para detectar automaticamente pornografia infantil podem ser divididas em quatro métodos: comparação de assinaturas de arquivos únicos; detecção de pele em conteúdo digital; identificação de partes do corpo humano; e métodos de classificação por conjunto de recursos visuais. O método de análise de assinatura única consiste em atribuir um número único - obtido através da função hash do arquivo - a cada imagem (ou mídia) que já foi comprovadamente material pornográfico infantil e criar um banco de dados (BARRETO, 2017).

A partir daí, para cada apreensão de arquivos suspeitos, sua assinatura única é calculada e comparada com os registros existentes, que foram definidos como ilegais. Essa metodologia também pode ser utilizada continuamente para monitoramento de redes de transferência de arquivos entre usuários (peer-to-peer), verificação de tráfego de mídia com assinatura exclusiva já conhecida e registrada. A limitação de usar a análise de assinatura única é que ela só é aplicável a arquivos que já foram catalogados. Não pode ser usado em casos novos que ainda não foram descobertos, bem como em imagens editadas, pois possuem um hash diferente das imagens originais cadastradas na base de dados. As técnicas baseadas na detecção da pele e na identificação de partes do corpo pressupõem que o conteúdo visual das imagens pornográficas infantis a serem destacadas é composto em grande parte por pele e forma humana. Para tanto, utiliza mecanismos de filtragem para detectar a pele infantil aliado ao uso de algoritmos computacionais para perceber a nudez. É aqui que o trabalho da NuDetective se destaca com impacto global. As abordagens baseadas no método de detecção da pele possuem uma grande limitação que já foi apresentada

em trabalhos científicos e comprovada empiricamente: a ocorrência de falsos positivos. Essa característica pode ser facilmente observada, pois a exposição da pele (ou exposição explícita dos genitais) em arquivos digitais não está necessariamente relacionada à pornografia infantil. No entanto, estudos mostram que, apesar das limitações, ferramentas desse tipo têm sido utilizadas como filtro inicial para agrupar arquivos suspeitos e são utilizadas de forma complementar em cenas de crime em todo o mundo forense. Devido às limitações descritas nos dois primeiros métodos apresentados, diversas pesquisas seguiram para utilizar meios de extração e classificação de características visuais (BARRETO, 2017).

Muitos comportamentos que prejudicam claramente o interesse da sociedade em manter os bens jurídicos mais fundamentais em termos de equilíbrio e harmonia na convivência social ainda ocorrem hoje sem uma perspectiva preventiva geral ou especial pela falta de tipificação do direito penal como ilegalidade (BRASIL, 2012).

Hoje, a tecnologia da informação possibilita causar danos ou ameaças de dano à propriedade moral e material dos indivíduos, e muitas vezes da própria comunidade, que, por sua gravidade, deveria ser objeto de crime (BRASIL, 2012).

As facilidades e confortos decorrentes da evolução tecnológica trouxeram consigo a fragilidade da insegurança que seu uso indevido traz. Isso tem resultado em fraudes, invasões ilícitas de privacidade, ataques e danos às esferas pública e privada (BRASIL, 2012).

Crime organizado, espionagem, interferência na segurança do Estado e na prestação de serviços públicos, o próprio Estado, em nome do que considera princípios legítimos, mas de legitimidade duvidosa ou ilegitimidade duvidosa, como no caso recente dos Estados Unidos, espionando a privacidade dos cidadãos nos nomes de contraterrorismo estão entre as principais ofensas no uso da gratificação tecnológica (BRASIL, 2012).

Muitas dessas graves violações dos direitos humanos básicos já são classificadas como infrações penais no direito penal. Outros são examinados para digitação. A evidência desses comportamentos ainda está em terreno instável, carecendo de legislação processual adequada de uma hermenêutica quanto aos princípios constitucionais de salvaguarda que equilibrem mais claramente a proporcionalidade prevalecente dos valores individuais e sociais. O Tribunal de Justiça Federal já decidiu que as garantias constitucionais não podem ser convertidas em escudo protetor contra a delinquência social (BRITO, 2020).

No plano internacional, é preciso avançar efetivamente em relação à ocorrência de extraterritorialidade do direito penal quando os crimes decorrem de atos praticados fora do território nacional ou em espaço virtual cibernético (BRITO, 2020).

Por motivos puramente didáticos e para melhor estruturar a apresentação do assunto deste artigo, adota-se a classificação proposta pela União Internacional de Telecomunicações, que divide os delitos em:

- Direitos autorais;
- Conteúdo relacionado;
- Contra a confidencialidade, integridade e disponibilidade dos sistemas informáticos;
- Relacionados a computadores (BRITO, 2020).

A história da classificação de crimes cibernéticos no Brasil começa com questões relacionadas à proteção da propriedade intelectual de programas de computador. Em dezembro de 1987, o Congresso Nacional aprovou a Lei nº 7.646 que criminaliza a violação de direitos autorais e a importação, exibição e depósito de programas de computador não registrados de origem estrangeira para fins comerciais. Esta lei foi revogada pelo número 9.609 em 1998, mantendo o primeiro tipo de delito com a mesma pena e abolindo o segundo (BRITO, 2020).

Esta categoria inclui atividades ilegais relacionadas a material erótico, pornografia, pornografia infantil, racismo, discurso de ódio, incitação à violência, ofensas religiosas, jogos online ilegais, difamação ou desinformação, spam e outras formas de conteúdo ilegal (BRITO, 2020).

O crime de pornografia infantil é regulamentado pela Lei da Criança e do Adolescente (Lei nº 8.069 de 1990), nos artigos 240, 241 e 241-A a 241-EA. A primeira alteração ao texto original da Lei sobre questões de pornografia infantil foi feita em 2003 por força da Lei nº 10.764 de 2003, que lhe deu um conteúdo diferente dos conceitos do art. 240 e 241. No entanto, as mudanças mais significativas foram trazidas pela Lei nº 11.829 de 2008, que, além de alterar novamente os artigos acima, acrescentou novos tipos de crimes (241-A a 241-E) Finalidade, para acompanhar os passos da modernidade e da tecnologia que cada vez mais se difundem entre os jovens, com acesso gratuito e fácil aos mais diversos conteúdos (BRITO, 2020).

Nesse sentido, a referida lei ampliou a possibilidade de punição, aumentou a pena e buscou punir a guarda de fotografias e outros registros de menores de 18 (dezoito) anos envolvidos em cenas pornográficas ou de sexo explícito. Também passou a punir o comportamento de quem, por qualquer meio, trocasse, transmitisse, disponibilizasse, publicasse ou divulgasse gravações que continham cena de sexo explícito ou pornográfico envolvendo crianças ou adolescentes. Também visava penalizar montagens de filmes e lançamentos em geral que continham imagens sexuais de jovens. Qualquer pessoa que falsifique explicitamente sexo ou pornografia com crianças e jovens falsificando, montando ou alterando fotografias (BRITO, 2020).

Entre as práticas mais importantes, vale, portanto, destacar a difamação, calúnia, insulto, ameaças, coação ilícita, identidade falsa, assédio ou perturbação da paz. Neste último caso, não se trata de um crime, mas de uma infração penal que permite punir quem passa a assediar ou perturbar a paz por motivo ofensivo ou condenável (BRITO, 2017).

Esta categoria descreve ações que prejudicam a confidencialidade, integridade e disponibilidade de sistemas de computador (CARNEIRO, 2012).

A Lei nº 12.737 de 2012 criminalizou a interrupção e interrupção de serviços telemáticos ou de informação pública, com a inclusão dos artigos 1º e 2º no artigo 266 do Código Penal. Esse crime está localizado no Título VIII do Código Penal, Capítulo II, que ataca a segurança pública no que diz respeito à segurança midiática e, se categoriza como crime de periculosidade geral, o que é essencial para que comportamentos típicos causar perigo para todo o sistema mencionado. Portanto, se apenas a comunicação ou conversa entre duas pessoas for interrompida, o crime se enquadra no art. 151, §1º, III do Código Penal (CARNEIRO, 2012).

A segurança pública é protegida sob o aspecto particular da regularidade do funcionamento dos serviços de telégrafo, telefone, computador, transmissão de dados ou informação de utilidade pública. Portanto, a normalidade dos serviços de telecomunicações está protegida (CARNEIRO, 2012).

A natureza criminosa de invadir outro dispositivo informático, violando ilicitamente um mecanismo de segurança e com o objetivo de obter, manipular ou destruir dados ou informações sem a permissão expressa ou tácita do proprietário do dispositivo, ou instalar vulnerabilidades para obter um acesso ilícito benefício recebido, foi introduzido no ordenamento jurídico brasileiro por força da Lei nº 12.737 de 2012 (CARNEIRO, 2012).

No sentido do legislador, dispositivos de informática são computadores pessoais, computadores em formato de prancheta (tablets), telefones celulares (especialmente aqueles com acesso à Internet), meios de armazenamento externo como CD-ROMs, DVDs e similares. na exposição de motivos ao Projeto de Lei 2.793 de 2011 que resultou na referida lei. É condição essencial que o dispositivo informático pertença a outra pessoa que não o autor do crime, caso contrário o comportamento torna-se atípico (CARNEIRO, 2012).

O elemento subjetivo do tipo é a intenção, representada pela vontade livre e consciente do autor, de obter, manipular ou destruir dados ou informações sem a autorização expressa ou tácita do proprietário do dispositivo, ou instalar vulnerabilidades para obter uma vantagem ilegítima (CAVALCANTE, 2016).

A natureza criminosa acima também representa um elemento subjetivo de dolo desleal ou específico, caracterizado pela intenção do autor de obter, manipular ou destruir dados ou informações sem a autorização expressa ou tácita do proprietário do dispositivo, ou de instalar vulnerabilidades para obter uma informação ilegítima para ganhar vantagem (CAVALCANTE, 2016).

Fica sujeita ao autor a fabricação, oferta, venda ou distribuição de vírus ou dispositivos informáticos com o objetivo de permitir a intrusão no dispositivo informático, seja para obter, manipular ou destruir dados ou informações, ou instalar vulnerabilidades para impedir a obtenção de vantagem ilícita. com a mesma pena do caput do art. 154-A, que é crime semelhante. No caso do elemento subjetivo, que expressa a finalidade de instalar vulnerabilidades para obter vantagem injustificada, o autor deve estar ciente de que está obtendo vantagem injustificada, pois quando devido é legal ou justo, a natureza penal é não mantida (CAVALCANTE, 2016).

Se a invasão resultar na obtenção de conteúdos privados de comunicações eletrônicas, segredos comerciais ou industriais, informação confidencial na acepção da lei, ou controlo remoto não autorizado do dispositivo invadido, a pena é de prisão de 6 (seis) meses a 2 (dois) anos. e multa, a menos que o crime seja mais grave (CAVALCANTE, 2016).

A pena é aumentada se os dados ou informações obtidos forem divulgados, comercializados ou cedidos a terceiros a qualquer título ou se o crime for cometido contra o Presidente da República, governadores e prefeitos; Presidente do Tribunal de Justiça Federal; Presidente da Câmara dos Deputados, do Senado Federal, da Assembleia Legislativa do Estado, da Câmara Legislativa do Distrito Federal ou da

Câmara Municipal; ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou distrital (CAVALCANTE, 2016).

É um crime formal porque, embora seja descrito um resultado, não precisa ser verificado para que ocorra a consumação (DORIGON; SOARES, 2018).

Em 2000, as alterações ao Código Penal introduzidas pela Lei nº 9.983 introduziram novos crimes relacionados ao uso indevido de sistemas de informação, tais como: além de modificar os crimes de quebra de sigilo funcional (§ 1º do art. 325) e divulgação de sigilo (DORIGON; SOARES, 2018).

Essas mudanças foram motivadas pela necessidade de coibir fraudes previdenciárias, que em vários casos foi perpetrada por meio do uso indevido da tecnologia da informação (DORIGON; SOARES, 2018).

Artigo 313–A criminaliza a inserção ou facilitação da inserção de dados falsos, modificação indevida ou exclusão de dados verdadeiros nos sistemas informáticos ou bases de dados da administração pública para obter vantagem ou prejuízo injustificados para si ou para outrem (DORIGON; SOARES, 2018).

O artigo 313-B criminaliza a modificação ou alteração de qualquer sistema de informação ou programa de computador sem permissão ou solicitação de autoridade competente. Embora pareçam ser considerados sinônimos, para efeitos do texto, a ação de modificar expressa uma mudança radical no programa ou sistema de informação, enquanto a mudança representa uma mudança no programa que também ocorre, não o desnatura completamente (DORIGON; SOARES, 2018).

O objeto material refere-se a um sistema de informação ou programa de computador utilizado pela administração pública, ambos elementos normativos da avaliação extrajurídica (DORIGON; SOARES, 2018).

§ 1º ao art. 325, que criminaliza o comportamento do empregado que abusar do acesso restrito aos sistemas, bem como atribuir, fornecer e emprestar senha ou de outra forma permitir o acesso de pessoas não autorizadas aos sistemas de informação ou bases de dados da Administração Pública (DORIGON; SOARES, 2018).

O segredo funcional, elemento normativo do tipo, é tudo o que se sabe e não pode ser conhecido senão por determinadas pessoas ou uma determinada categoria de pessoas em virtude de sua profissão (DORIGON; SOARES, 2018).

O bem jurídico a tutelar é o normal funcionamento da administração pública, que resguarda os seus interesses, sendo certos segredos necessários ao bom funcionamento do Estado e outros no art. 327 § 1º do Código Penal, que também

protege interesses privados, por meio da devida publicação os dados sigilosos que se encontram na área de acesso restrito do órgão público poderão ser danificados (DORIGON; SOARES, 2018).

No delito de divulgação de segredo, a divulgação de informações confidenciais ou reservadas nos termos da lei sem motivo válido, estejam ou não contidas nos sistemas de informação ou bancos de dados da administração pública, não é pré-requisito para o tipo Autor configuração. ofensa oficial, como nos tipos descritos acima. O delito tem potencial ofensivo médio porque, enquanto a pena máxima imposta ultrapassa dois anos de prisão, a pena mínima não é superior a um ano (DORIGON; SOARES, 2018).

Os tipos de crimes relacionados à espionagem estão descritos no ordenamento jurídico brasileiro pelo Código Penal Militar (Decreto-Lei nº 1.001 de 1969) e pela Lei de Segurança Nacional (Lei nº 7.170 de 1983) possibilitado pelo uso da tecnologia da informação, em particular a Internet (DORIGON; SOARES, 2018).

Esta categoria inclui crimes que são inevitavelmente cometidos através de sistemas informáticos, tais como, por exemplo, fraude electrónica, phishing, contrafacção electrónica (DORIGON; SOARES, 2018).

O número de fraudes eletrônicas não é encontrado no ordenamento jurídico brasileiro, pois é um termo utilizado por alguns autores para se referir a fraudes cometidas por meio de sistemas informatizados (MATSUYAMA, 2019).

Típico do delito de peculato é o artigo 171 do Código Penal e consiste em dar a si ou a outrem vantagem ilícita em detrimento de outrem, enganando ou mantendo alguém em erro por astúcia, ardil ou outros meios fraudulentos (MATSUYAMA, 2019).

Característica fundamental do desfalque é a fraude, utilizada pelo agente para enganar ou ludibriar a vítima com o objetivo de obter ganho ilícito (MATSUYAMA, 2019).

Para enquadrar o crime, é imprescindível que o benefício seja ilícito e decorra de erro cometido pelo agente, ou seja, que o benefício seja consequência deste. A existência do erro decorrente da fraude não é suficiente, é necessário que o ato conduza a uma vantagem ilícita (MATSUYAMA, 2019).

O Projeto de Lei nº 5.485 de 2013, em tramitação no Congresso Nacional, propõe a criminalização da fraude eletrônica configurada pelo envio de mensagens digitais de qualquer natureza e que se faz passar por empresa, instituição ou pessoa,

com o objetivo de induzir terceiros a fazê-lo, divulgar informações pessoais, identidade ou senhas de acesso (MATSUYAMA, 2019).

Estritamente falando, o phishing é criminalizado, e o simples envio de mensagens destinadas a atingir vítimas que estão fornecendo suas informações pessoais a indivíduos mal-intencionados é punível com a mesma pena de apropriação indébita. Se a vantagem injusta é obtida em prejuízo de outrem, ou seja, se o mal não passa de fraude sem maior potencial de dano, ela é absorvida por ela, conforme previsto no caso do STF (MATSUYAMA, 2019).

A fraude eletrônica em sistemas bancários pode ocorrer com o uso de cartões de débito, cartões de crédito, por meio do acesso a contas de internet banking (home banking) e call centers (MEDEIROS; UGALDE, 2020).

Os golpes de home banking geralmente são feitos por meio da distribuição de programas maliciosos que coletam informações confidenciais dos usuários e as enviam ao cibercriminoso pela própria Internet (MEDEIROS; UGALDE, 2020).

Nesses casos, é importante identificar qual malware foi usado ou qual outra estratégia de ataque foi usada para encontrar a melhor maneira de resolver o problema e planejar adequadamente os procedimentos de investigação (MEDEIROS; UGALDE, 2020).

Por fim, a Lei 12.737 de 2012 equiparou o cartão de crédito ou débito a um documento particular para auxiliar no combate à fraude bancária (MEDEIROS; UGALDE, 2020).

A inviolabilidade do sigilo de cartas, telégrafos, dados e telefones é garantida pela constituição federal de 1988 incl. XII do seu art. 5º, sendo esta última regida pela Lei nº 9.296, de 1996, que trata das escutas telefônicas e do fluxo de comunicações em sistemas informatizados e telemáticos de qualquer natureza para fins probatórios em investigações criminais e instruções processuais criminais (MEDEIROS; UGALDE, 2020).

A rigor, interceptar significa interromper, cortar ou impedir. No entanto, a vigilância de que trata a lei pertinente tem o significado de uma intervenção com o objetivo de recolher informações (MEDEIROS; UGALDE, 2020).

A espionagem é proibida se não houver provas suficientes de autoria ou envolvimento em um crime; se a prova puder ser fornecida por qualquer outro meio disponível; se o facto apurado constituir infracção penal punível com pena de prisão máxima (MEDEIROS; UGALDE, 2020).

Ao contrário das escutas telefônicas, que estão sujeitas à mesma lei e já estabelecidas, as escutas telemáticas apresentam uma série de desafios técnicos e jurídicos (MEDEIROS; UGALDE, 2020).

Enquanto o uso de serviços telefônicos apresenta obrigações bem definidas para concessionárias e usuários, essa relação não existe na Internet, por se tratar de uma tecnologia cujo uso não é disciplinado ou regulamentado pelo Estado brasileiro (MEDEIROS; UGALDE, 2020).

No campo jurídico, a constitucionalidade da legislação sobre interceptação do fluxo de comunicações em sistemas informáticos e telemáticos foi questionada pela Ação Direta de Inconstitucionalidade nº 1.488 proposta pelo Sindicato dos Delegados de Polícia do Brasil. A ação inclui um pedido de liminar para suspender o funcionamento do regulamento impugnado (MEDEIROS; UGALDE, 2020).

O autor alega que o parágrafo único do art. 1 e art. 10 da referida lei viola os incisos XII e LVI do art. 5º da Constituição Federal de 1988 ao introduzir a possibilidade de espionagem do fluxo de comunicações em sistemas informatizados e telemáticos (MEDEIROS; UGALDE, 2020).

Os argumentos apresentados beiram a letra do dispositivo constitucional que prevê a inviolabilidade do sigilo das cartas e das comunicações telegráficas, de dados e telefônicas, salvo neste último caso por ordem judicial, nos casos e na forma prevista em lei para a finalidade da investigação criminal ou da instrução processual penal estabelecida (MEDEIROS; UGALDE, 2020).

De acordo com a interpretação dos denunciantes, somente conversas telefônicas poderiam ser violadas, desde que cumpridas as formalidades legais. Como consequência direta dessa impossibilidade, os relatórios de gravação de comunicações telemáticas seriam inadmissíveis em provas, por violarem o Inc. LVI do art. 5 (provas obtidas ilicitamente não são permitidas no processo) (MEDEIROS; UGALDE, 2020).

O Supremo Tribunal Federal analisou a ação direta quanto à pertinência de sua fundamentação, mas indeferiu o pedido de liminar por considerar a inexistência de Periculum em Mora como justificativa para a suspensão da provisão impugnada (MEDEIROS; UGALDE, 2020).

Quanto ao mérito, a denúncia não foi analisada, pois seu seguimento foi indeferido pelo relator em 2001 com fundamento na ilegalidade ativa dos autores. Apesar do pronunciamento informal da Justiça Federal, o Supremo Tribunal Federal

demonstrou o reconhecimento da constitucionalidade do parágrafo único do artigo 1º da Lei nº 9.296 de 2006 e respaldou suas decisões a partir do Habeas Corpus nº 2002, em que reconhece que a legislação integrativa de os cânones Constitucionais no âmbito da persecução penal com autorização judicial permite a intercepção do fluxo de comunicação em sistemas informáticos e telemáticos (MEDEIROS; UGALDE, 2020).

Após esse julgamento, outros seguiram na mesma direção, como o julgamento do Habeas Corpus nº 101.165/PR, que reconhece a legalidade da interceptação telemática quando, aliada à presença de indícios de autoria, se baseia em a especificidade des modus operandido delicto, a única evidência para esclarecer os fatos (MEDEIROS; UGALDE, 2020).

Outra norma sobre serviços de escuta telefônica e telemática é a Resolução nº 59, editada em 2008 pelo Conselho Nacional de Justiça, com o objetivo de disciplinar e padronizar rotinas para proteger o procedimento de escuta telefônica de comunicações telefônicas e sistemas de informação para aprimorar a tecnologia e telemática nos órgãos de jurisdição do Poder Judiciário a que se refere a Lei nº 9.296, de 1996. Este regulamento trata de aspectos relacionados à movimentação de documentos para garantir o sigilo das ações judiciais e estabelecer controles para coibir o uso indevido dessas provas (MEDEIROS; UGALDE, 2020).

Uma inovação trazida pela Lei nº 12.683, de 2012, foi a possibilidade de o Ministério Público e a Polícia Judiciária solicitarem, diretamente e sem mediação judicial, os dados cadastrais dos inquiridos que constam nos bancos de dados do Tribunal Eleitoral, das companhias telefônicas, instituições financeiras, provedores de Internet e empresas de cartão de crédito (MEDEIROS; UGALDE, 2020).

A norma está em consonância com a Constituição Federal de 1988, uma vez que a recuperação direta de dados cadastrais de telefonia e telemática não se confunde com a medida investigatória criminal de escuta telefônica regulamentada na Lei nº XII da Constituição Federal de 1988 requer homologação judicial. Tampouco se confunde com a violação do sigilo bancário prevista na Emenda à Lei nº 105 de 2001, segredo cuja retirada revela a vida financeira do suspeito e pode indicar outros elementos de sua personalidade (MEDEIROS; UGALDE, 2020).

Os dados cadastrais não estão protegidos por direitos de personalidade (art. 5º, X, Constituição Federal), conforme demonstram diversos acórdãos do Superior Tribunal Regional, como o Pedido de Assistência Jurídica nº 000297, no Habeas

Corpus nº 83.338/DF, em agravo de instrumento contra o Mandado de Segurança nº 25.375/PA (MEDEIROS; UGALDE, 2020).

Portanto, a partir de agora, o Ministério Público, as polícias criminais (polícias federal e civil dos estados) e as polícias militares (na condução de inquéritos policiais militares) podem, com base no art. 17-B da Lei nº 9.613 de 1998, consultas diretas às pessoas jurídicas detentoras dos dados cadastrais, ordens que devem ser obedecidas sob pena de desobediência (MEDEIROS; UGALDE, 2020).

O uso indevido dessa atribuição pelo membro do Ministério Público ou pela autoridade policial pode ser qualificado como contraordenação ou como quebra de sigilo funcional e também um ato de desonestidade administrativa e a Serapurada deve ser disciplinada (MEDEIROS; UGALDE, 2020).

Atualmente, não há justificativa específica de responsabilidade criminal para provedores de acesso e provedores de conteúdo e armazenamento. A complexidade da questão está ligada à dificuldade enfrentada pelo provedor de acesso e conteúdo em identificar o tipo de conteúdo que é transmitido ou armazenado em seus servidores. Se o provedor tomar conhecimento de conteúdo nocivo em um site hospedado por ele, ele deve parar de publicar esta página imediatamente para não ser responsabilizado civil ou mesmo criminalmente. Isso está previsto na Lei da Criança e do Adolescente (Lei nº 8.609 de 13 de julho de 1990) em decorrência das alterações introduzidas pela Lei nº 11.829 de 2008 (MEDEIROS; UGALDE, 2020).

Nos termos do § 2º do art. 241-A do referido diploma, as condutas tipificadas nos incisos I e II do § 1º do art. 241-A são punível se o responsável legal pela prestação do serviço, oficialmente notificado, não bloquear o acesso aos conteúdos ilícitos referidos no caput deste artigo (MEDEIROS; UGALDE, 2020).

A obrigação de manter registros (logs) de acesso à Internet não é um procedimento regulamentado por lei ou regulamento de abrangência nacional, mas limita-se a iniciativas locais de governos estaduais e municipais, o que limita as investigações criminais traz consigo (MEDEIROS; UGALDE, 2020).

Em nível estadual, os ISPs são obrigados a manter os logs, ou entidades que fornecem cobrança ou acesso gratuito à grande rede para cadastrar usuários: Alagoas (Lei nº 6.891 de 2007), Amapá (Lei nº 3.173 de 2007) e Lei nº 3.351 de 2008), Bahia (Lei nº 11.608 de 2009), Espírito Santo (Lei nº 8.777 de 2007), Paraíba (Lei nº 8.134 de 2006), Paraná (Lei nº 16.241 de 2009), Pernambuco (Lei nº 14.001 de 2009), Piauí (Lei nº 5.747 de 2008), Rio de Janeiro (Lei nº 5.132 de 2007), Rio Grande do Sul (Lei

nº 12.698 de 2007) e Santa Catarina (Lei nº 5.132 de 2007; 14.890 de 2009), São Paulo (Lei nº 12.228 de 2006) (MEDEIROS; UGALDE, 2020).

No âmbito distrital e municipal, destacam-se iniciativas como o Distrito Federal com a Lei Distrital nº 3.437 de 2004 e o Município do Recife com a Lei Municipal nº 17.572 de 2009 (MEDEIROS; UGALDE, 2020).

Criar uma obrigação para os ISPs manterem registros não esgota os recursos necessários para identificar o autor de um crime cometido pela Internet, mas pode ajudar muito na sua identificação (MEDEIROS; UGALDE, 2020).

Muitos dos padrões internacionais existentes surgiram da conclusão de tratados e convenções internacionais entre os Estados. Historicamente, os tratados têm servido a uma ampla gama de propósitos, entre os quais se destacam o estabelecimento de alianças militares-defesas, a celebração da paz, a demarcação de fronteiras entre os países e a intensificação dos intercâmbios econômicos e culturais (MEDEIROS; UGALDE, 2020).

De acordo com o artigo 38 do Estatuto da Corte Internacional de Justiça, promulgado pelo Brasil pelo Decreto nº 19.841 de 1945, as convenções internacionais são fontes do direito internacional; costume internacional; os princípios gerais do direito reconhecidos pelas nações civilizadas; sujeito ao disposto no art. 59, as decisões judiciais e os ensinamentos dos mais qualificados juristas das diversas nações, como meio de determinar as normas de direito (MEDEIROS; UGALDE, 2020).

Um tratado é um acordo formal celebrado entre sujeitos de direito internacional e destinado a produzir efeitos jurídicos. As variantes terminológicas concebíveis do contrato em português são: acordo, ajuste, arranjo, ato, ato, código, juízo, estatuto, declaração, memorando, pacto, protocolo, regulamento assinado em 23 de novembro de 2001, na cidade de Budapeste, Hungria, ainda não ratificado pelo Brasil (MEDEIROS; UGALDE, 2020).

Devido ao fenômeno da globalização, os crimes internos em particular, onde o princípio da territorialidade é aplicado em sua totalidade, podem exigir a adoção de mecanismos de cooperação internacional para sua investigação (MEDEIROS; UGALDE, 2020).

A cooperação internacional em justiça criminal compreende uma série de mecanismos que facilitam a cooperação dos Estados na implementação da justiça criminal, levando em consideração procedimentos ou processos específicos. Nesse contexto, não deve ser confundida com a cooperação administrativa internacional, que

visa o aprimoramento tecnológico, a troca de informações e estratégias de ação entre os órgãos envolvidos (MEDEIROS; UGALDE, 2020).

A discussão sobre os fundamentos da cooperação criminalística internacional está cada vez mais rompendo com o paradigma da territorialidade ou extraterritorialidade na punição dos delitos. A regra geral é a territorialidade, podendo os crimes praticados fora do território nacional basear-se na nacionalidade do infrator (princípio da personalidade ativa), na nacionalidade da vítima (princípio da personalidade passiva), no bem jurídico envolvido (princípio da defesa ou princípio real) e o local onde o crime foi cometido, deve ser processado (princípio da representação) e características do crime, se pode ou não prejudicar valores da comunidade internacional (princípio da justiça universal) (NASCIMENTO, 2017).

3 LEGISLAÇÃO ATUANTE EM NOSSO ORDENAMENTO

3.1 Direito digital

O combate ao cibercrime, justamente por ser praticado em ambientes virtuais, exige um olhar mais específico. Uma das razões para o aumento da criminalidade nesse ambiente é a própria integração digital.

Segundo Cardoso (2014), de acordo com o Mapa de Segurança Global, projeto da organização independente CyberDefcon, o Brasil ficou em 33º lugar em segurança cibernética em um ranking de 219 países. À frente do Brasil, por exemplo, Rússia, Japão e Índia.

No Brasil não existe legislação especial, aplica-se a legislação geral (Código Penal); A Lei 12.737/2012 introduziu alguns de seus próprios crimes cibernéticos no CP: Por exemplo, a Lei 12.737/30.11.2012 - Lei Carolina Dieckmann, que no artigo 2º insere o art. 154-A, no CP e o projeto de lei № 236/2012 aprimora a lei 12.737. No que diz respeito à pornografia infantil, é típico no art. 240 e 241 DO ECA e está configurado para simplesmente retratar crianças em poses sensuais, mesmo sem mostrar a genitália, segundo o STJ.

A polícia realiza várias operações. Entre eles, no dia 18 de maio, Dia Nacional de Combate à Violência e Exploração Sexual de Crianças e Adolescentes, foi lançada a Operação Luz na Infância.

De acordo com o site da Fundação Abrinq:

> Com o objetivo de mobilizar a sociedade brasileira e convocar o combate às violações dos direitos sexuais de crianças e adolescentes, o dia 18 de maio foi instituído como o Dia Nacional de Enfrentamento à Violência e Exploração Sexual de Crianças e Adolescentes. Somente em 2014, foram registradas 24.575 denúncias de abuso sexual de crianças e adolescentes no Brasil. Destes, 19.165 foram violência e 5.410 foram exploração sexual de crianças. Esses dados divulgados pela linha direta de direitos humanos mostram o quão importante é combater essa realidade. E maio é o mês dessa luta.
> Por que 18 de maio?
> Naquele dia, em 1973, uma menina de 8 anos de Vitoria (ES) foi sequestrada, estuprada e brutalmente assassinada. Seu corpo foi carbonizado seis dias depois, e seus agressores nunca foram punidos. Com as consequências deste caso e a forte mobilização do movimento pela proteção dos direitos da criança e do adolescente, o dia 18 de maio foi instituído como o Dia Nacional de Combate à Violência e Exploração Sexual de Crianças e Adolescentes. Desde então, este dia tem sido um dia para a população brasileira se unir e se opor a esse tipo de violência.
> O que é violência sexual?
> Esta é uma situação em que uma criança ou adolescente é usado para o prazer sexual de uma pessoa idosa. Ou seja, qualquer ato de interesse sexual, consumado ou não. Trata-se de uma violação dos direitos sexuais de crianças e adolescentes, pois abusa ou explora o corpo e a sexualidade, seja pela força ou outra forma de coação, envolvendo crianças e adolescentes em atos sexuais impróprios para sua idade ou física, e psicológico desenvolvimento.
> Contra a exploração
> A violência sexual pode ocorrer de duas maneiras diferentes. O abuso sexual é qualquer forma de contato e interação sexual entre um adulto e uma criança ou adolescente em que um adulto em poder ou autoridade usa a condição para sua própria estimulação sexual, criança ou adolescente. , ou terceiros, que podem ou não ocorrer por meio de contato físico. A exploração caracteriza-se pela exploração sexual de crianças e adolescentes com fins lucrativos, sejam eles financeiros ou não. Existem quatro formas de exploração sexual: através da prostituição, pornografia, tráfico de seres humanos e turismo sexual. (FUNDAÇÃO ABINQ, 2015)

A melhor forma de combater o abuso sexual de crianças e adolescentes é por meio da prevenção. Ao reunir a família, a sociedade, os profissionais da educação e o Estado para fornecer e proteger o trabalho de informação, conscientizar e fornecer apoio adequado, alcançaremos o objetivo de acabar com a pornografia infantil.

O Ministério Público de Minas Gerais foi o primeiro Ministério Público do Estado a contar com um Ministério Público especializado no combate ao cibercrime em todas as áreas especializadas.

3.1.1 Crimes cibernéticos

Os criminosos estão interessados no anonimato, que pensam que não será descoberto, mas há oportunidades para identificar os culpados. Os crimes mais

comuns são o desfalque, o comércio online tem ceifado muitas vidas, mas a pornografia infantil é uma grande preocupação, e o combate à pornografia infantil na Internet é uma medida preventiva dirigida à sociedade.

A pornografia infantil na Internet está se tornando um grande problema para as autoridades, pois é importante identificar o autor do crime. No entanto, muitos invasores utilizam outras identidades pessoais, *fakes*, páginas em redes sociais com autoria incerta, o que dificulta a identificação das autoridades, com apenas o endereço da máquina denominada *Internet Protocol* - IP localizado com um código digital, porém, a maioria dos agressores o faz não usam seus computadores para cometer atos ilegais, eles usam máquinas públicas, como *lan-house* ou computadores na escola, mas a máquina é, e o agente não.

O princípio da Intranscendência determina que a ação deve ser movida apenas contra pessoas a quem a prática da violação é atribuída, sem permitir a transferência da punição para outras pessoas. Portanto, sem a determinação da autoria e da materialidade, é impossível ter uma finalidade punitiva.

Gabriel Cesar Zacarias de Inellas (2004) entende que a prova pericial é a prova mais eficaz no crime cibernético, e a perícia computacional deve ser utilizada nesse ato.

Cibele de Souza Silva argumenta que

> a maioria das meninas e adolescentes prostituídas no Brasil são motivadas pela necessidade de sobrevivência, que é o segmento mais vulnerável da pirâmide social (...) Milhares de meninas e adolescentes trocam sexo por comida ou abrigo. Nesses casos, o usuário ou cliente da menina, bem como aqueles que facilitam o tráfico de seu corpo, estão sujeitos a processo criminal e podem ser condenados à prisão. (SILVA, 1999, p. 25)

Sabe-se que esse problema ocorre em todo o Brasil, principalmente nas estradas. As meninas muitas vezes são vendidas por suas próprias famílias, enganadas pela possibilidade de uma boa vida, e acabam em bordéis, estupradas e escravizadas.

A imaterialidade do ambiente virtual, que a falta de limites espaciais e temporais oferece, contribuiu, portanto, para o surgimento dos chamados crimes virtuais. Dentre os diversos crimes existentes no contexto virtual está a pornografia infantil, que consiste no compartilhamento ou comercialização de fotos e vídeos pornográficos envolvendo crianças e jovens. Essa prática criminosa está tipificada no Código Penal e no Estatuto da Criança e do Adolescente (ECA) (ABREU, 2014).

Os crimes cometidos no ambiente virtual são denominados crimes virtuais, digitais, informáticos, telemáticos, crimes de alta tecnologia, crimes informáticos, fraude informática, crimes cibernéticos, crimes transnacionais, entre outros. Estas se dividem em puras (ou próprias) aquelas praticadas por meio eletrônico em sentido mais amplo, sendo a tecnologia da informação o objeto jurídico protegido, enquanto as impuras (ou impróprias) são aquelas em que o agente utiliza o computador como meio, para obter resultados. naturalista que ofende o mundo físico ou o espaço real, ameaça ou prejudica ativos que não sejam a tecnologia da informação (ABREU, 2014).

O conceito de crime informático pode ser definido como a conduta típica e ilícita que constitua crime ou contravenção, dolosa ou culposa, comprometedora ou omissão, praticada por qualquer pessoa, física ou jurídica, utilizadora de tecnologia da informação, dentro ou fora de uma rede, e que ataca direta ou indiretamente a segurança digital, cujos elementos são integridade, disponibilidade e confidencialidade (ABREU, 2014).

3.2 Estatuto da Criança e do Adolescente

A pornografia infantil é uma forma de violência sexual contra crianças e jovens. No Brasil, a prática desse crime está tipificada na Lei da Criança e do Adolescente (ECA) e no Código Penal, bem como na Convenção das Nações Unidas sobre os Direitos da Criança de 1989 (AJEJE, 2018).

Deve-se deixar claro que o crime de pornografia infantil não deve ser confundido com pedofilia, que segundo a Organização Mundial da Saúde (OMS) é uma doença, um transtorno mental em que o indivíduo tem desejo sexual antes da puberdade em crianças. Assim, o pedófilo não é um criminoso, mas um paciente, mas se ele traz sua patologia para fora e ela se enquadra em qualquer crime contemplado pelo ordenamento jurídico, o pedófilo se torna um criminoso (AJEJE, 2018).

A Lei 11.829/08, alterou a Lei 8.069/90, Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil e criminalizar a aquisição e posse desse material, sob outras condutas relacionadas à pornografia infantil na internet (AJEJE, 2018).

A proliferação desse tipo de conteúdo na Internet dificulta a identificação das origens de quem o distribui. Essa prática criminosa é difundida na deep web, local que

torna quase impossível a identificação do criminoso, além da facilidade de viralização que a internet oferece, bem como o envio e recebimento de arquivos, como fotos e vídeos a cada lugar ainda mais prefere esta prática (ALMEIDA, 2015).

A utilização do ambiente virtual por crianças e jovens, principalmente redes sociais e jogos online, sem supervisão dos pais ou responsáveis, facilita ainda mais a existência desse crime e torna esses menores alvos fáceis para criminosos que muitos criam perfis falsos. nas redes sociais para comunicar com as vítimas facilmente e sem suspeitas (ALMEIDA, 2015).

3.2.1 Lei 11.829/2008 – Pedofilia na Internet

Além disso, é importante que os pais ou a família prestem atenção nas fotos tiradas no dia a dia onde essas crianças ou jovens estão nus, pois tais arquivos podem ser facilmente invadidos e utilizados por criminosos invadindo um Dispositivo Computacional e proliferação na Deep Web (ALMEIDA, 2015).

Chama-se Deep Web, o local onde os materiais de difícil acesso pode ser encontrados na Internet. Esses materiais são para usuários selecionados e o acesso a tal conteúdo requer seus próprios links, dificultando o acesso do público leigo (ALMEIDA, 2015).

A Deep Web, também conhecida como as profundezas da Internet, é o lugar onde seu conteúdo não está tão prontamente disponível para todos os usuários como nos mecanismos de busca populares da Internet como Google ou Yahoo, mas sua expansão é igual à da Internet convencional (ALMEIDA, 2015).

A internet usual, a superfície web, consiste em computadores cujo conteúdo é conectado por uma rede mundial. Nesse ambiente, é possível acessar a localização de cada computador utilizando o endereço IP (Internet Protocol), que é um endereço único presente em cada computador, permitindo o acesso à Internet. Para ter acesso ao conteúdo da deep web são necessários mecanismos específicos que não tenham apenas o endereço IP, desta forma fica claro o quão limitado é o acesso a este ambiente virtual (ALMEIDA, 2015).

A dark web, uma rede ainda mais anônima, surgiu da propagação da existência da deep internet, que atraiu a atenção de cada vez mais usuários ao longo do tempo. A Dark Web é predominante em países onde o governo restringe e bloqueia o acesso

a determinados sites, e esse ambiente ainda mais profundo da rede usa criptografia para dificultar ainda mais a identificação de usuários e criminosos (ALMEIDA, 2015).

Esse ambiente é muito mais propício para cometer crimes em comparação com a Deep Web, pois garante o anonimato de seus agentes. Infelizmente, é muito comum na dark web a prática de diversos crimes como tráfico de drogas, fraudes bancárias, assassinos de aluguel e principalmente pornografia infantil justamente pelo sigilo do ambiente de informações do usuário (ALMEIDA, 2015).

Para utilizá-lo, são necessários mecanismos que garantam o anonimato do usuário, dentre os quais o mais conhecido é o TOR (The Onion Router), consiste em uma rede de túneis virtuais que permitem a identificação dificultam para computadores acessarem determinados conteúdos, um mecanismo desenvolvido pela Marinha dos Estados Unidos para estabelecer comunicações seguras pela Internet (BAPTISTA, 2021).

É importante mencionar que nenhum desses mecanismos de acesso a esses ambientes, que obscurecem a identificação dos dispositivos utilizados, é totalmente seguro, sendo possível a violação de dados e a descoberta do servidor ou computador utilizado. Apesar disso, é quase impossível para as autoridades combater esses ambientes de internet profunda, bem como identificar criminosos que operam nesses ambientes (BAPTISTA, 2021).

4 CONSIDERAÇÕES FINAIS

A Internet e a tecnologia da informação começaram a mudar o modo de vida das pessoas O homem, causando mudanças constantes, revoluciona a mente do indivíduo, e como vemos e entendemos a sociedade moderna. No entanto, como em todos os grandes e nobres etapas evolutivas percorridas pelo ser humano, algumas pessoas se aproveitaram delas ferramenta de auto-serviço, explorando a ignorância ou a inocência dos usuários da Internet, bem como táticas obscuras e de alta tecnologia.

As possibilidades do ambiente virtual, principalmente o anonimato, tornaram essa ferramenta um meio adequado para ações penais, com o qual é possível elucidar as implicações jurídicas dos crimes virtuais e quais instrumentos jurídicos podem ser levados em consideração em seu julgamento. Dessa forma, o crime cibernético

tornou-se comum, pois o público está pouco informado sobre suas implicações legais e sociais.

A exploração sexual de adolescentes online é gravíssima, seja por meio de distribuir pornografia infantil, ou através do ato de encorajar e distribuir pornografia infantil ou mesmo o comportamento que incentiva essas práticas sexuais nocivas.

A democratização do uso da World Wide Web não só trouxe enormes benefícios, mas também facilitou a prática de crimes, e é evidente o quão difícil é para as autoridades identificar e combater esses criminosos. Com o desenvolvimento do comportamento criminoso no ambiente virtual, a inteligência policial também precisou ser aprimorada e, assim, a injeção de agentes no ambiente cibernético tornou-se essencial no combate ao cibercrime.

Assim, os legisladores nacionais agiram para garantir a proteção dos direitos das vítimas crianças e jovens em todos os níveis e em todos os aspectos, especialmente no o direito à liberdade e à dignidade sexual desses indivíduos em desenvolvimento. Apenas as recentes alterações à Lei da Criança e do Adolescente, Principalmente, a Lei 11.829/08 protege melhor esses direitos ações ilegais através da internet e ferramentas, a tecnologia tem sido prescrita em vários tipos de penalidades que dependendo do grau de dano aos interesses legítimos declarados, diferentes ações são tomadas.

A adoção das Leis 12.735/2012, 12.737/2012 e 12.965/2014 não foram suficientes para o combate efetivo aos crimes cometidos pela Internet, principalmente pela grande variedade de crimes cibernéticos e pela falta de legislação específica. Além disso, a completude do código penal brasileiro dificulta a aplicação de suas regras por analogia aos crimes cibernéticos.

Apesar da ação legislativa, o código ainda tem vários erros a existência, tanto substantiva quanto processual, cria brechas permite que os infratores escapem das punições, mais sério que isso são as dificuldades estruturais enfrentadas por agências investigativas e repressivas, muitas vezes não há meios específicos ou pessoal dedicado para realizar o combate ao crime no ciberespaço. Embora o tema desta monografia seja a pedofilia e suas consequências na internet, fica claro que medidas mais amplas são necessárias para combater essas práticas. O espaço virtual precisa ser regulamentado, o que ajudará a combater todos os tipos de também estão acontecendo nesta área, o que levará a uma maior segurança dos usuários. Entretanto, é preciso ressaltar que "regulação" não pode ser entendida como censura,

pois a internet é um espaço aberto e livre e deve ser preservado para continuar desenvolvimento, a padronização deve visar apenas a prevenir violações de direitos.

A violação desarrazoada de um mecanismo de segurança é um elemento normativo de antilegalidade e implica na obrigação das vítimas de garantir a segurança dos seus dados, o que indica o seu direito à privacidade.

5 REFERÊNCIAS

MINISTÉRIO DA MULHER, DA FAMÍLIA E DOS DIREITO HUMANOS. **Exposição de crianças e adolescentes na internet ocupa 5ª posição no ranking do Disque 100**. Disponível em: https://www.gov.br/mdh/pt-br/assuntos/noticias/2020-2/novembro/exposicao-de-criancas-e-adolescentes-na-internet-ocupa-quinta-posicao-no-ranking-de-denuncias-do-disque-100. Acesso em: 2 mai. 2022.

EDUARDA, Maria. Cibercrime: Conceitos, modalidades e aspectos jurídicos-penais Âmbito Juridico. Disponível em:https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/. Acesso em: 18 mai. 2022BUTCHER, Isabel. 89% das crianças e dos adolescentes brasileiros são usuários de Internet. Teletime. Disponível em: https://teletime.com.br/23/06/2020/89-das-criancas-e-dos-adolescentes-brasileiros-sao-usuarios-de-internet/. Acesso em: 16 mai. 2022.

LIMA, Rubens Fellipe; ALMEIDA, Sérgio. **Crimes virtuais: uma análise sobre os crimes cibernéticos e a dificuldade na aplicação da legislação**. João Pessoa. 23 p Dissertação (Direito) - Centro Universitário de João Pessoa - Unipê.

DORIGON, Alessandro; OLIVEIRA, Renan Vinicius. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade**. 2018. Disponível em: https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade/3. Acesso em: 28 abr. 2022.

INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS. 2020. Disponível em: https://www.ibccrim.org.br/noticias/exibir/7216/. Acesso em: 16 abr. 2021.

PAIXÃO, Gleice Kelly Silva. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na deep web e dark web**. Goiânia, 2019.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na internet**. São Paulo: Editora Juarez de Oliveira, 2004.

LANDINI, Tatiana Savoia. **Pornografia infantil na internet: violência sexual ou pornografia?** Sociologia, USP. S.Paulo, 2000.

CARDOSO, Fabio Fettuccia**. O brasil está atrasado em estratégias de combate a crimes cibernéticos. 2014**. Disponível em: </fabiofettuccia.jusbrasil.com.br/noticias/180688777/brasil-esta-atrasado-em-estrategias-de-combate-a-crimes-ciberneticos> Acesso em: 20 de Maio de 2022

SILVA, Cibele de Souza. **Inocência em perigo:** Abuso Sexual de Crianças, pornografia infantil e pedofilia na Internet. Rio de Janeiro: Garamond, 1999.

BRUNES, Carla Roberta. **Exploração sexual de criança e adolescente por meio de rede de computadores**: diferença entre citação curta e citação longa nas

normas da ABNT. Anápolis. 57 p. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/16842/1/Monografia%20-CARLA%20ROBERTA%20DE%20PAULA.pdf. Acesso em: 6 abr. 2021.

ABREU, Eduardo Franco. **Os entraves à repressão aos crimes cibernéticos.** 2014.

AJEJE, Gisele Ajeje de Carvalho. **A persecução penal no crime cibernético e a aplicabilidade da norma penal.** 2018. Número total de folhas, 55. Trabalho de Conclusão de Curso, Graduação em Direito – Faculdade Anhanguera, Campinas. 2018.

ALMEIDA, Jessica de J. **Crimes cibernéticos.** Caderno de Graduação-Ciências Humanas e Sociais-UNIT-SERGIPE. 2015.

BAPTISTA, Rodrigo. **Lei com penas mais duras contra crimes cibernéticos é sancionada.** 2021.

BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei n. 12.737/2012.** 2017.

BRASIL. **Lei 12.735 de 30 de novembro de 2012.** 2012.

BRITO, Maximo. **A pratica das feke news e a falsa sensação de anonimato.** 2020.

BRITTO, Gladstone Avelino; FREITAS, Maristella Barros. **Ciberataques em massa e os limites do poder punitivo na tipificação de crimes informáticos.** Revista de Direito Penal, Processo Penal e Constituição. 2017.

CARNEIRO, Adeneele Garcia. **Crimes Virtuais:** Elementos Para uma Reflexão Sobre o Problema na Tipificação. 2012.

CAVALCANTE, Waldek Fachinelli. **Crimes Cibernéticos:** noções básicas de investigação e ameaças na internet. 2016.

DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. **Crimes cibernéticos:** dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. Revista Jus Navigandi, ISSN 1518-4862, Teresina. 2018.

MATSUYAMA, Keniche Guimarães; LIMA, JAA. **Crimes cibernéticos:** atipicidade dos delitos. 2017.

MEDEIROS, Gutembergue Silva; UGALDE, Júlio César Rodrigues. **Crimes Cibernéticos:** Considerações Sobre a Criminalidade na Internet. 2020.

NASCIMENTO, Cláudia Rufino. **Crimes Cibernéticos à Luz Da Lei 12.737/2012:** Avanços e Retrocressos. Revista de Trabalhos Acadêmicos Universo Recife. 2017.

RAMOS, Eduardo Dulcetti. **Crimes cibernéticos:** análise evolutiva e legislação penal brasileira. 2017.

AZAMBUJA, Maria Regina Fay. **Violência sexual intrafamiliar:** é possível proteger a criança? Porto Alegre: Livraria do Advogado. 2004.

CARVALHO, Olavo de. **Cem anos de Pedofilia.** Jornal O globo. São Paulo. 2002.

FALCONI, Romeu. **Lineamentos do direito penal.** 2. Ed. São Paulo: Icone. 1997.

FELIPE, Jane. **Afinal, que é mesmo pedófilo?** Cad. Pagu, Campinas. 2006.

FREUD, S. **A dissolução do complexo de Édipo.** Edição Standard Brasileira das Obras Psicológicas Completas (Vol. XIX, pp. 215-226). Rio de Janeiro: Imago. 1974.

HISGAIL, Fani. **Pedofilia:** Um estudo psicanalítico. São Paulo, Iluminuras. 2007.