PUC GOIÁS

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
DEPARTAMENTO DE CIÊNCIAS JURÍDICAS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURIDICA

CRIMES CIBERNÉTICOS

QUESTIONAMENTOS ACERCA DA VULNERABILIDADE NOS CRIMES VIRTUAIS SEXUAIS

ORIENTANDO (A): SARAH RODRIGUES CHAVES
ORIENTADORA: PROF.ª MS. ELIANE RODRIGUES NUNES

GOIÂNIA
2020

SARAH RODRIGUES CHAVES

CRIMES CIBERNÉTICOS

QUESTIONAMENTOS ACERCA DA VULNERABILIDADE NOS CRIMES VIRTUAIS SEXUAIS

Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof.ª Orientadora: Ms. Eliane Rodrigues Nunes.

GOIÂNIA

2020

SARAH RODRIGUES CHAVES

CRIMES CIBERNÉTICOS

QUESTIONAMENTOS ACERCA DA VULNERABILIDADE NOS CRIMES VIRTUAIS SEXUAIS

Data da defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____Nota

Orientador (a): Prof. (a) Mestre Eliane Rodrigues Nunes

_____Nota

Examinador (a): Convidado (a): Prof. (a):

Dedico esta monografia a minha família que inquestionavelmente me apoiou nesta jornada acadêmica.

Agradeço primeiramente aos meus pais, Eduardo e Maria Edna, que sempre me apoiaram e incentivaram para tomar as decisões mais acertadas. A eles oferto o máxime de gratidão.

Agradeço a todos os mestres pertencentes ao Departamento do Curso de Direito da Puc-GOIÁS, que contribuíram com ensinamentos valiosos para minha formação acadêmica, e que serão levados para minha vida profissional.

Aos meus amigos de classe, em especial, àqueles que estiveram comigo e apoiaram durante a rotina acadêmica.

Por fim, a minha orientadora, a Professora Mestre Eliane Rodrigues Nunes, que foi de grande valia quanto a elaboração deste trabalho, transmitindo seus inestimáveis conhecimentos jurídicos.

SUMÁRIO

RESUMO

O atual cenário da *internet* nos permite questionar os limites dela. O modo como a tecnologia evolui faz com que a prática dos crimes também tenha evoluído, exigindo atenção da legislação penal. Crimes cibernéticos são uma realidade na sociedade atual e tomam proporções inovadoras a todo instante. A criação de uma legislação especifica, como a Lei 12.737/12, é necessária no combate e proteção das vítimas de tais delitos. Algumas questões são bastante polêmicas, como a sensação de anonimato que aumenta os crimes virtuais, bem como o meio facilita a obtenção de provas. Em outra análise, faz-se importante verificar a necessidade de prevenção quanto aos riscos de menores que utilizam os meios digitais. O presente estudo tem como base pesquisar acerca das normas que determinam a tipificação de tais condutas, em razão das mudanças constantes em sua prática. Além de verificar e analisar técnicas necessárias que poderia contribuir para evitar em golpes de criminosos cibernéticos.

Palavras-chave: Crimes cibernéticos. Vulnerabilidade. Lei 12.737/12. Crimes Sexuais Virtuais. Mecanismos de segurança.

INTRODUÇÃO

O presente trabalho tem como sustento o estudo das inovações tecnológicas e uma pesquisa acerca da garantia de segurança jurídica e punibilidade de crimes praticados no meio virtual. Os avanços na *internet* são inúmeros e constantes, tendo a necessidade de que haja limites para aqueles que usam evitando, assim, a denominação de que a *internet* seja uma “terra sem lei”.

São essenciais as pesquisas para avanços tão rápidos como o do meio virtual na legislação brasileira, considerando que é um novo bem jurídico a ser tutelado pela norma. Torna-se uma preocupação, nos dias atuais, o cuidado com a proteção de dados e a privacidade de quem utiliza as redes sociais, sejam estas para uso pessoal ou como ferramenta de trabalho.

Tendo em vista bens jurídicos relevantes para a pessoa, como por exemplo os crimes contra a dignidade sexual, na *internet* essa modalidade pode causar graves prejuízos, deixando vítimas sendo expostas de forma rápida e para qualquer lugar no mundo em questões de segundos. O caso da atriz Carolina Dieckmann, que teve fotos intimas expostas na internet causou grande repercussão geral e pressionou o legislador a criação de lei especifica (Lei 12.737/12) para que a matéria em pauta tivesse maior visibilidade e cuidado com o assunto.

O objetivo geral da presente monografia é discorrer sobre crimes virtuais e suas modalidades, bem como a eficácia e punibilidade dos mesmos, tratando da aplicação da lei nos casos específicos e as principais falhas legislativas para adequar às práticas.

A metodologia usada nesta pesquisa é a pesquisa bibliográfica como essencial, considerando que fornece um estudo teórico, embasado na lei e na jurisprudência, acerca dos princípios constitucionais bem como sobre as espécies dos crimes cibernéticos.

Quanto à estrutura, esta monografia está organizada em três capítulos. No capítulo I, apresentado o conceito deste crime, o contexto histórico no Brasil e diversas espécies do crime cibernético, baseados na Lei 12.737 de 2012.

Já no segundo capítulo do trabalho serão apresentados conceitos e categorias do crime, traçando-se ainda o perfil do criminoso, suas características e um contexto histórico no âmbito internacional.

Por fim, o último capítulo, será dedicado à análise das investigações policiais, como funciona o procedimento de apuração de provas, as formas de se chegar até os criminosos no ambiente virtual e, ainda, acerca da punibilidade dos crimes virtuais sexuais.

CAPITULO 1 – CRIMES CIBERNÉTICOS

1.1 CONTEXTO HISTORICO

Desde sempre se convive com as práticas de crimes, o ato de se corromper na sociedade é comum e aos primórdios já tiveram o trabalho de criar modos de disciplinar estas práticas. Mas o ambiente informático nem sempre existiu, e como se espera e como acontece, as leis tiveram que ir se adaptando para as novidades e modernidade do mundo.

Com o avanço da tecnologia e a criação da *internet* a forma de se comunicar se tornou mais rápida e instantânea no mundo todo, em fração de segundos se consegue comunicar com alguém no outro extremo do continente. A liberdade em utilizar esse meio é o que causa tamanha acessibilidade, e também, uma vulnerabilidade aos menos habilidosos na ferramenta.

A rede mundial de computadores, também denominada como *internet*, surgiu no período da guerra fria assim como o computador, com fins militares conforme diz Fabrizio Rosa:

> Criada inicialmente com fins exclusivamente militares, em 1969 foi criada a primeira rede nacional de computadores pelo departamento de defesa dos Estados Unidos da América, a ARPANET (Advanced Research Projects Administration – Administração de Projetos e Pesquisas Avançados), com intuito de compartilhar informações, pesquisas e estratégias militares conectando os computadores dos centros de pesquisas, universidades e instituições militares americanas. (ROSA, 2002, p. 29).

Com esse surgimento pode-se entender que a internet não tinha a mesma utilidade que há usa-se hoje. Hoje é um material de comunicação e além disso uma ferramenta de trabalho no mundo todo, através da internet possibilitamos relações de comercio como a compra e venda, a possibilidade de aprendizado como pesquisas na *web*, a organização por meio de sistemas de uma empresa, o mundo jurídico se adaptando ao meio eletrônico tendo o processo digital e afins.

Não seria diferente com tamanho avanço, que os crimes também obtivessem novos avanços, o uso da *internet* para cometer crime se tornou existente cabendo as autoridades adaptarem leis para punir esses novos atos. Crimes antes cometidos na sociedade, tomaram rumos diferentes e adaptações para serem praticados no ambiente virtual com uma maior facilidade para o criminoso que utiliza do anonimato.

Os golpes constantes aplicados no meio virtual são preocupantes, pois o crime avança e atualiza a todo momento, compras na *internet* podem não ser tão seguras, o disparo em massa de *fake news* formando opiniões e revoltas na sociedade, o crime de ódio constante, o comercio de pornografia infantil crescente e ainda o *porn revenge* conhecida como pornografia de vingança.

O significado da palavra cibercrime indicado no dicionário é “crime cometido através da comunicação entre redes de computadores, notadamente através da *internet*. ” (PRIBERAM, 2008). Sendo assim, pode-se identificar que a materialidade do crime depende da internet para sua consumação. Já para Paulo Quintiliano, há uma diferença no conceito de crime de informática e crime cibernético, para ele “crimes de informática são todas as ações típicas, antijurídicas e culpáveis praticados com a utilização de computadores e/ou de outros recursos da informática. “ (NASCIMENTO, 2018).

Para o autor Sergio Marcos Roque o crime cibernético é “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”. (2007, p. 25). Entendendo melhor o significado dessa tipificação de crime é possível entender a proporção e agilidade em que o crime pode ser cometido em vários lugares ao mesmo tempo e a rapidez que pode ser consumado.

O Brasil possui índices muito altos de pratica de cibercrimes, segundo o *site* Computerword:

> O Brasil se tornou o segundo maior gerador de cibercrime do mundo. O País ocupa a primeira posição na América Latina e Caribe, sendo tanto fonte quanto alvo de ataques online. Para se ter uma ideia, padrões de malwares e fraudes online são desenvolvidos e utilizados por criminosos locais e gangues

> especializadas em atacar esquemas de serviços e pagamentos brasileiros. (PINHEIRO, 2015)

Sendo essas informações tão alarmantes é necessário que ainda se considere o reforço em leis e punibilidade para os crimes no país. Para ampliar o pensamento sobre o assunto, padrões de *malwares* e fraudes virtuais são desenvolvidos e utilizados por criminosos locais e gangues especializadas em atacar esquemas de serviços e pagamentos brasileiros.

Ainda segundo Felipe Machado para o site veja “as perdas das empresas brasileiras com crimes virtuais são de 10 bilhões de dólares (32,4 bilhões de reais) por ano. A estimativa consta de relatório da empresa de segurança digital McAfee” (MACHADO, 2018). Além dos crimes contra a honra que causam desgastes emocionais para as vítimas, os crimes com prejuízos financeiros são altos, principalmente entre financeiras e bancos.

1.2 A REALIDADE ATUAL

Em dezembro de 2019 o Brasil anunciou o início a adesão a convenção de Budapeste, que trata no combate aos crimes praticados pela internet, o que facilita a cooperação entre os países e ajuda na investigação do crime quando ultrapassa fronteiras. A convenção de Budapeste é composta pelos países da União Europeia, Estados Unidos, Canadá, Chile, Japão, Argentina, Paraguai e Republica Dominicana.

Rogério Romano explica o que propõe a convenção e seus objetivos:

> Esta Convenção propõe-se harmonizar a lei penal material no que se refere às previsões relativas à área do cibercrime, zelando para que na lei processual penal as autoridades competentes sejam dotadas dos necessários poderes de investigação e de combate a esta nova área da criminalidade. Cria igualmente um mecanismo rápido e eficaz de cooperação internacional. A Convenção prevê como crimes, designadamente, o acesso e intercepção ilegal em redes informáticas, o dano e sabotagem informática, o uso de vírus, e a posse, produção e distribuição de material de pornografia infantil na Internet. (ROMANO, 2019)

Para o Brasil é importante a adesão por ser o segundo pais com maior índice de crimes virtuais, assim essa cooperação facilitaria o combate ao cibercrime.

Em 2012, a denominada Lei Carolina Dieckmann foi sancionada que dispõe sobre a tipificação criminal de delito informático, objetivando suprir a falta legislativa sobre o tema anteriormente no pais. Para Artur Silveira:

> Anteriormente ao ano de 2012, a falta de legislação específica tornava muito difícil a apuração dos crimes virtuais, uma vez que a legislação até então vigente havia sido direcionada aos crimes de forma geral, independentemente do meio utilizado para a sua prática. Dessa forma, ante a não especificidade da legislação, era muito difícil a identificação dos sujeitos e a obtenção de provas para a condenação criminal quanto aos crimes virtuais, que exige certeza. (SILVEIRA, 2015)

Aproveitando a repercussão do caso da atriz no Brasil, a visão sobre essa forma de crime passou a ter mais importância legislativa e informação que chegasse à população, evidenciando a necessidade de alertar as vítimas de crimes virtuais.

No ano de 2020, a Polícia Federal intensificou operações ao combate ao crime virtual, especialmente os crimes relacionados a pornografia infantil. Na operação denominada “Guardiões da Inocência” a Policia Rodovia Federal em conjunto com a Policia Civil realizou diversão apreensões de suspeitos como computadores onde realizavam o armazenamento e compartilhamento de pornografia infantil em massa para diversos lugares do mundo.

Sobre a operação Guardiões da Inocência realizada em 12 Estados brasileiros, a maioria dos suspeitos que não possuía ainda o mandado de prisão expedido foram pegos em flagrante o que facilitou e corroborou para a eficiência da investigação.

Um caso de crime virtual que repercutiu em 2019 envolvendo pessoas públicas é o do jogador Neymar que segundo Luiz D’Urso:

> Recentemente foram noticiados dois casos de grande repercussão envolvendo investigações de cibercrimes. O suposto crime de vazamento de foto de nudez de terceiro, pelo jogador Neymar e a suspeita de invasões de celulares e aplicativos de agentes públicos ligados à operação Lava Jato.

> É fato que vários crimes estão migrando para a Internet, isto ocorre, pois, os criminosos acreditam tratar-se de um local mais seguro para cometer delitos, além de ser um ambiente pelo qual trafega grande quantidade de informações valiosas. (D'URSO, 2019).

A importância de noticiar esses crimes envolvendo pessoas públicas é o alerta e a informação chegar a maior quantidade de pessoas, pois, apesar da propagação e alerta sobre crimes virtuais, muitas pessoas ainda são vítimas. Os golpes em compras *on-line* são um dos mais comum, diariamente pessoas fazem compras online de sites inseguros ou aplicativos abertos que pessoas conseguem vender produtos de procedências duvidosas.

A pornografia de vingança também é muito comum atualmente, esse termo consiste na divulgação de imagens, vídeos ou informações intimas e pessoais na *internet.* A vítima desse crime acaba ficando em situação constrangedora e vexatória diante da sociedade, tendo o objetivo do ofensor sendo concretizado apenas pelo fato de causar a vingança e promover tais sentimentos a vítima.

Com a quantidade de criadores de conteúdos e *influencers*, os crimes de ódio são crescentes também, o interesse por expor a opinião de forma anônima cresce pela falta de punição a quem expõe o ódio. Os crimes contra a honra previstos nos arts. 138 a 140 do Código Penal Brasileiro, são eles, injúria, difamação e calúnia. É importante ressalvar a diferença entre os crimes, A calúnia é uma falsa imputação de fato criminoso a outro alguém, a difamação é a imputação a alguém de um fato ofensivo a sua reputação e a Injúria é imputar a alguém uma qualidade negativa seja ela falsa ou verdadeira.

A *fake news* também se fez muito presente no cenário nas eleições em 2018, o disparo em massa de mensagens com notícias falsas por todo o pais formou opiniões contestáveis a respeito de diversos candidatos. Gabriele Silva explica o significa e origem do termo:

> O termo vem do inglês fake (falsa/falso) e news (notícias). Dessa forma, em português, a palavra significa notícias falsas. Apesar de ter se destacado recentemente, a expressão é bem mais antiga e data do final do século XIX. Fake News são as informações falsas que viralizam entre a população como se fosse verdade. Atualmente, elas estão, principalmente, relacionadas às redes sociais. (SILVA, 2019).

No Brasil, o uso de *fake news* tem sido comum desde então para diversos assuntos, na pandemia do Covid-19 a grande quantidade de disparo dessas mensagens se tornou alarmante pois causava desespero na população com tantas mensagens de pânico sobre a situação de calamidade. Alguns médicos no Brasil tiveram que prestar esclarecimento e se retratarem perante a justiça e a sociedade sobre estarem disparando essas falsas notícias para causar tumulto entre as pessoas.

Para Raul Galhardi com base em estudos de pesquisas o Brasil é o país que mais acredita em notícias falsas e o que mais se preocupa com a veracidade de informações na *internet*:

> O Brasil vive um paradoxo. Pesquisas recentes revelaram que nós somos a sociedade que mais acredita em notícias falsas, ao mesmo tempo em que somos o país que afirma se preocupar mais com o que é falso e verdadeiro dentre as informações que circulam na internet. De acordo com estudo realizado em 2018 pelo instituto Ipsos, intitulado “Fake news, filter bubbles, post-truth and trust”, 62% dos entrevistados no Brasil admitiram ter acreditado em notícias falsas até descobrirem que não eram verdade, valor muito acima da média mundial de 48%. (GALHARDI, 2019).

Essa soma de noticia negativas com a quantidade de mensagens falsas, causa um sentimento de impotência perante a população e a alarma ainda mais sobre os problemas sociais que convivemos.

1.3 DIREITO COMPARADO

Tratando da pornografia de revanche, em 2009, as Filipinas criminalizaram essa pratica com penas entre três e sete anos no país, além de multa, ficou permitido a responsabilização à pessoa jurídica, e em caso de o criminoso ser estrangeiro a deportação do mesmo. Em Israel, a punição é de até cinco anos de prisão. Segundo o site InternetLab:

> Em 2009, entrou em vigor o *Anti-Photo and Voyeurism Act* que criminaliza o ato de gravar uma imagem de alguém em situação sexual ou similar ou capturar uma imagem das áreas íntimas. É uma das primeiras leis específicas sobre o assunto. Lei específica: Anti-Photo and Video Voyeurism Act of 2009. (INTERNETLAB, 2018)

Nos Estados Unidos a Califórnia foi o primeiro a dar um passo na legislação acerca desde assunto. No Reino Unido foi criado a própria lei de pornografia de revanche, com punições de até dois anos de prisão e multa. *

No Japão em 2014 foi aprovada a lei que penaliza as condutas com até três anos de prisão e aplica multas de até trezentos mil ienes, e ainda por determinação da justiça os provedores de *internet* tem o prazo máximo de dois dias para excluir os conteúdos publicados das redes. No Brasil ainda não temos uma lei especifica que trate da determinação da exclusão dos conteúdos criminosos. *

Conforme enuncia Alesandro Barreto em sua obra é ressaltada a importância da exclusão do conteúdo da *internet*:

> Ressalte-se que, em razão da gravidade dos fatos, os quais podem levar as vítimas a atitudes extremas – como no caso da adolescente de 17 anos que se suicidou no estado do Piauí no ano de 2013, ao ter um vídeo seu difundido em um aplicativo de troca de mensagens –, há a necessidade de criminalização mais severa da pornografia de vingança, a fim de inibir a prática de tal ato. Adequar conduta tão covarde e reprovável apenas como atentatória à honra, quando se tratar de conteúdo de maiores, é alimentar pensamentos machistas, ao repetir a exposição vexatória de vítimas, especialmente mulheres. (BARRETO, 2016, p.165)

A cooperação jurídica entre os países se torna necessária e importante no combate a essa espécie de crimes, há uma crescente interdependência entre os Estados cada vez maior, tendo como destaque a cooperação entre países. O conceito de soberania sofre modificações passando a ser visto como uma assistência mutua.

Assim, essa cooperação acaba representando uma das principais formas de combater os crimes supranacionais, fazendo ser necessário uma harmonia legislativa, para que sejamos capazes de solucionar um problema globalizado nesta nova realidade.

Nos Estados Unidos, Ana Karolina Calado da Silva aponta os dois patamares de combate ao crime informático:

> No âmbito federal encontrou-se a Lei de Proteção aos Sistemas Computacionais (*Federal Computer System Protection Act of 1981)* – que determinava como conduta delituosa o uso de

> computadores com o objetivo de praticar fraudes, furtos ou espécies de apropriação indébita. Em seguida, em 1982 surgiu a *Eletronic Funds Transfer Act* – lei que trata da regulamentação de transferências eletrônicas de fundos, incriminando as fraudes informáticas que não continham relações interpessoais. (SILVA, 2013).

Atualmente existem seis ondas legislativas em diversos países visando a proteção do bem jurídico e a segurança jurídica, são eles: proteção de privacidade, Direito Penal econômico, proteção da propriedade intelectual, conteúdo ilegal e lesivo e as leis de segurança. Para Ana Karolina Calado da Silva, sobre o cibercrime no Brasil:

> Em relação aos crimes virtuais o Brasil tem avançado cada vez mais quanto à criação de núcleos de investigação especializados no combate e prevenção dos delitos cometidos por meios eletrônicos, como a criação das Delegacias Especializadas de Repressão a Crimes contra Informática e Fraudes eletrônicas. No âmbito Federal é possível contar com a Unidade de Perícia Informática da Polícia Federal, criada desde de 1996 e denominada como SEPFIN (Serviço de Perícia em Informática). Ademais, devido à crescente criminalidade eletrônica e a necessidade de criar meios preventivos para reduzir tal criminalidade, foram desenvolvidas no Brasil iniciativas privadas especializadas no recebimento de denúncias de crimes que violem os direitos humanos praticados pelo meio virtual. Este é o caso da organização não governamental SaferNet Brasil, em parceria com o Ministério Público Federal. (SILVA, 2013).

Por estes motivos essa cooperação jurídica entre os países é de tamanha importância para o cuidado com as vítimas como também com ajuda na investigação de crimes que superam fronteiras em fracções de segundos e causam danos e descontentamento com quem sofre com o crime cibernético.

CAPITULO 2 – CONDUTAS SEXUAIS VIRTUAIS

2.1 CRIMES SEXUAIS VIRTUAIS

Entende-se como dignidade sexual a liberdade dos indivíduos de se relacionarem com qualquer parceiro de sua vontade sem discriminação ou intervenção. Estando relacionado esse conceito com o princípio fundamental da Constituição Federal que é o da dignidade da pessoa humana, o conceito de dignidade explicado por Artur Motta é a seguinte:

> A dignidade é essencialmente um atributo da pessoa humana pelo simples fato de alguém "ser humano", se tornando automaticamente merecedor de respeito e proteção, não importando sua origem, raça, sexo, idade, estado civil ou condição sócio-econômica. (MOTTA, 2013).

Com a liberdade de acesso à *internet* e informações, o meio digital passou a ter conteúdo com viés sexual, conteúdos de fácil acesso e sem nenhum tipo de filtro, popularizando essas práticas.

Com a Lei 12.015/2009 foi incluso ao código penal a expressão “crimes contra a dignidade sexual” com objetivo de proteger diversos bens jurídicos, sendo eles a liberdade sexual da pessoa humana, a vida e a saúde.

No ambiente virtual se torna simplificada a forma de cometer crimes, o estupro é um deles, a dificuldade do legislador de encaixar ao crime do art. 213 do Código Penal no ambiente virtual é notada, o que demonstra uma falha na reforma legislativa quando a criação de um artigo especial ou modificação do atual artigo que tipifica o crime.

Outra pratica comum no ambiente virtual é o *revenge porn*, que consiste na pornografia de vingança, onde a vítima tem vídeo e imagens com conteúdo sexual e intimo divulgados como forma de vingança. O autor desse crime geralmente usa do descontentamento de um fim de relacionamento para justificar a conduta cometida provocando a violação da dignidade sexual da vítima.

“Sextorsão” a junção das palavras sexo e extorsão, é o termo que se usa para definir o crime em a uma exigência de enviar materiais com cunho pornográfico

e sexual por meio de ameaças muitas vezes direcionadas a espalhar o conteúdo ou divulgar segredo intimo da vítima. O termo foi usado pela primeira vez nos Estados Unidos em um caso de uma mulher que foi chantageada sexualmente para enviar imagens intimas suas ao chantagista, afirma Isabella Otto.

Isabella Otto em seu artigo explica sobre o motivo do termo não ser tão ouvido e os motivos para isso:

> A palavra assusta, até porque é recente e você pode ainda não estar tão familiarizada com ela. Além disso, o crime não é tão discutido, geralmente porque é abafado pela própria vítima, que sente medo de expor o chantagista e sofrer consequências ainda mais duras, como ameaças de morte. De acordo com um relatório realizado pelas empresas Thorn e Crimes Against Children Research Center, uma em cada três vítimas não fala sobre o abuso sofrido por vergonha, embaraço e/ou culpa. Uma em cada oito vítimas ainda tem sua rotina afetada e muda de casa para tentar escapar da chantagem sexual. (OTTO, 2019).

A pratica mais comum da sextorsão é no meio virtual apesar de ainda ser possível a pratica no meio real, ou seja, pessoalmente. Como ainda não é um crime especifico pelo Código Penal, o legislador costuma enquadrar essa pratica no art. 213 desta lei.

A importunação sexual, descrita no caput do art. 215-A do Código Penal Brasileiro: "Art. 215-A. Praticar contra alguém e sem a sua anuência ato libidinoso com o objetivo de satisfazer a própria lascívia ou a de terceiro:" (BRASIL,1940). Ou seja, é realizar um ato libidinoso na presença de alguém sem o seu consentimento, com o interesse de satisfazer lascívia própria ou de terceiros.

Andreza Matos tem seu posicionamento sobre a aplicação desse crime no meio virtual:

> Guilherme Nucci (2019) preceitua que o crime de importunação sexual será praticado por “Qualquer um que realize ato libidinoso com relação a outra pessoa (com ou sem contato físico, mas visível e identificável)”. Desse entendimento, pode-se concluir que mesmo no âmbito virtual, se a vítima for exposta a prática do ato libidinoso, direcionado a ela, e violando dessa forma sua liberdade e dignidade sexual, estará, portanto, praticado tal crime. Então, esse restaria consumado, por exemplo, por meio de encaminhamento de vídeos ou imagens

> do autor praticando atos libidinosos em face da vítima, sem o seu consentimento, objetivando satisfazer sua lascívia. (MATOS, 2020).

No meio digital o art. 218-C, visa a preservação das vítimas que possuem imagens intimas divulgadas, punindo com a pena do artigo mencionado aquele que divulga e compartilha essas imagens. No caput é possível observar a quantidade de verbos capazes de descrever o crime:

> Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia. (BRASIL, 1940).

No caso do jogador Neymar Junior que, em maio de 2019, foi acusado de estupro e na tentativa de se defender em suas redes sociais, expôs conversas com a vítima demonstrando imagens intimas e o nome da mesma borrados. Pode-se entender como uma forma da pratica do crime previsto no art. 218-C. Para Mariano Junior:

> A situação que será apreciada em juízo consiste no fato de se analisar se constitui o crime do art. 218-C do CP divulgar fotos e vídeos íntimos, mesmo com recurso que impossibilite o reconhecimento da vítima, ainda que no decorrer da divulgação seja possível identificar o rosto e o nome da pessoa em imagem diversa. Considerando que foi uma divulgação de uma conversa em aplicativo de mensagem instantânea, entendo que configura o delito do art. 218-C do CP, visto que o tipo penal foi criado para evitar que pessoas que enviaram cenas de nudez, sexo para alguém não tenha sua vida íntima exposta em público, o que aconteceu. (MARIANO JUNIOR, 2019).

Como conclusão do caso do jogador, pode-se entender que, por mais que esteja sendo acusado de forma injusta, usar a imagem de outrem e divulga-las, configura um crime e será apurado.

Na Lei 12.015, um capitulo é reservado para tratar de crimes contra vulneráveis, que é acobertado pela Constituição Federal em seu art. 227, parágrafo 4º que diz: “A lei punirá severamente o abuso, a violência e a exploração sexual da

criança e do adolescente. Ocorre que muitos pedófilos aproveitam da vulnerabilidade da *internet* para aliciar menores, no art. 241-B do Estatuto da Criança e do Adolescente é tipificado o crime:

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

Ainda sobre o ECA, está descrito o crime de pornografia infantil no art. 241-C que prevê reclusão de um a três anos e multa:

> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo

Sendo importante a monitoração de menores quanto ao uso das redes sociais, para evitar que possam ser constrangidos a passar informações pessoais, marcar encontros e até enviar imagens intimas em troca de jogos e até brinquedos.

2.2 O PERFIL DA VITIMA – VULNERABILIDADE

Quando não se toma os devidos cuidados ao utilizar a *internet* fica-se vulneráveis e expostos a *hackers* e criminosos que estão disponíveis para aplicar golpes constantes. Na grande maioria as mulheres são as maiores vítimas de crimes virtuais sexuais, esse espaço de maior interação entre as pessoas reflete na sociedade que ainda pratica muitos crimes relacionados a gênero.

A falta de informação muitas vezes corrobora para o perfil de vítima de golpes nas redes. Orientar quem usa a *internet* nunca é demais, alertar sobre como conferir se um site é de fato confiável, evitar o compartilhamento de informações confiáveis por meio eletrônico e dentro outros cuidados básicos para não ser uma vítima.

O sentimento de impunidade que perpetua quando se trata de um crime virtual, muitas vezes considerado anônimo o autor do crime, aumenta o número de casos de práticas de crimes virtuais cada vez mais, tornando ao assunto a necessidade de falar e divulgar mais sobre os riscos do uso da *internet*.

Por meio da Central de Ajuda *SaferNet* as vítimas de crimes virtuais podem buscar informações e orientações sobre como reagir ao se deparar com essa situação. Vejamos o que diz o site sobre sua plataforma:

> A SaferNet Brasil oferece um serviço de orientação sobre crimes e violações dos Direitos Humanos na internet, de forma anônima e sigilosa. Nossa equipe é formada por profissionais especializados para orientar sobre como prevenir algumas violências online, o que fazer para denunciar e, quando possível, facilitar a identificação de instituições de saúde e/ou socioassistenciais que possam realizar um atendimento presencial o mais próximo possível da sua cidade/região. (SAFERNET, 2020).

É importante ressaltar que o site, preserva a imagem e a privacidade de quem o utiliza na busca de ajuda:

> Nosso canal mantém o sigilo (segredo) e confidencialidade de todas as informações fornecidas pelos usuários. As mensagens são acessadas apenas pela equipe especializada e só poderão

> ser reveladas às autoridades em situações de suspeita ou confirmação de grave violência contra crianças e adolescente, obedecendo o previsto no Art. 245 do Estatuto da Criança e Adolescente. Utilizamos técnicas de criptografia (segurança dos dados) para proteger suas informações. Como nenhum sistema de informática é 100% seguro, sugerimos: cuide da proteção de seu equipamento; acesse de um local no qual se sinta seguro e com privacidade e guarde bem sua senha e não divulgue. (SAFERNET, 2020).

Ainda assim, é importante destacar que nem todos sabem e conhecem dessa ferramenta para buscar uma solução quando se deparam com esse tipo de situação. Caso a vítima não conheça um aparo pela própria *internet* onde sofreu o delito, o ideal é ir à delegacia para colher informações de como proceder e realizar o boletim de ocorrência.

Além disso, caso a vítima não tenha a possibilidade de se dirigir até uma delegacia para realizar a denúncia pode ser feita por meio dos telefones de emergências disponíveis em todo o país: 190 para polícia militar, 197 para polícia civil e 180 para denuncia de violência doméstica.

2.3 O PERFIL DOS INFRATORES

Por um lado, analisar o perfil dos infratores é importante para investigação e para se precaver de ser vítima de um deles. Para Rodrigo Santos, existem algumas motivações para o criminoso fazer suas vítimas, seria elas a demonstração de poder, o prestigio, motivações financeiras, motivações ideológicas e também motivações comerciais:

> Muitos cibercriminosos podem agir pela simples possibilidade de mostrarem o que podem fazer. A ação é comumente acompanhada de tentativas de solicitações de pagamento para que a prática não ocorra novamente. Sendo os cibercriminosos seres humanos, também estão sujeitos a falhas e ações emotivas ou reativas a posicionamentos políticos e sociais. (SANTOS, 2020)

Assim, é perceptível que a mente do infrator muitas vezes é motivada por sentimentos de grandezas, anonimato e por questão de moral. Esse sentimento de superioridade sobre a vítima, causa a sensação de prazer e impunidade ao cibercriminoso.

Quem está navegando pela rede e se depara com perfis com promessas muito boas e fora de comum é importante ficar alerta. Muitas vezes a promessa de um ótimo ganho de dinheiro, anúncios de produtos mais baratos que o valor de mercado e propostas de trabalho muito convidativas pela própria *internet* geralmente é o mais comum.

O perfil do parceiro vingativo também é muito comum, aquele que não aceita o termino do relacionamento ou ver sua ex-companheira seguir em frente, que acaba usando da intimidade da vítima para denegrir sua imagem e sua moral usando as redes sociais e grupos de aplicativos de comunicação como ferramenta de vingança.

Déborah Oliveira, questiona em seu artigo sobre o perfil de cibercriminosos:

> Afinal, que tipo de criminoso está por trás de ameaças como essa? Segundo Fabio Assolini, analista sênior da equipe Global de Investigação e Análises da Kaspersky Lab, há dois perfis. “O primeiro é o *script kiddie*, que tem pouca ou nenhuma habilidade técnica. Geralmente, ele tem acesso à códigos maliciosos disponíveis no Git Hub. Ele assiste à vídeos no YouTube e aprende algumas técnicas. Por outro lado, há o superprofissional, que faz ataques em série, criando códigos indecifráveis”, descreve ele. Assolini comenta que no caso do cibercriminoso do Dilma Locker, nota-se que se trata de um hacker, de certa forma, amigável. “No texto de pedido de resgate, ele até se dispôs a negociar o valor de R$ 3 mil. Ele afirmou, ainda, que pratica crimes cibernéticos porque não tem tantas operações para viver com dignidade dentro do sistema”, detalha o executivo. (OLIVEIRA, 2017)

Entender a mente desses criminosos e como é avançado seu conhecimento e as ideias para realizar seus delitos não é atividade fácil e é importante especialistas na área para entender e investigar os crimes, as novas modalidades de praticarem e os avanços tecnológicos.

CAPITULO 3 – OS MEIOS DE PREVENÇÃO E PUNIÇÃO

3.1 AS INVESTIGAÇÕES POLICIAIS E APURAÇÃO DOS FATOS

As investigações desses crimes estão em constante revolução e mudanças, pois a *internet* está em variações a todo instante e os métodos sempre evoluindo. Diego Braga preceitua as investigações cibernéticas como:

> A investigação dessa modalidade criminosa evolui constantemente. Passou-se das pioneiras investigações encentradas em floppy disk[1], subsequentemente substituídos por técnicas mais sofisticadas, até a recente hipótese de análise de dados contidos em sistema de cloud computing, social network, smartphone, pen-drive, arquivos musicais etc. Hoje, a tecnologia informática permite formas de intrusões particularmente invasivas da esfera privada da pessoa submetida a inquérito policial, através de programas espiões denominados trojan, que se articulam mediante o monitoramento, seja do fluxo de comunicações de sistemas informáticos e telemáticos, seja de seu respectivo conteúdo. (BRAGA, 2019).

Conforme exposto o uso de programas espiões é o método que facilita essas investigações, visto que assim a autoridade policial investigativa tem acesso a todo o conteúdo disponível no computador do suspeito, podendo monitora-lo e assim iniciar um inquérito policial.

Quando se tem um crime informático passa a ser necessária a investigação do mesmo, para garantir provas para uma possível ação penal, tornando impreterível o uso de diversos métodos e recurso para investigar. Uma pessoa possui seu registro geral, um número que nos identifica, um aparelho eletrônico, seja computador, celulares ou tablets, também possuem seu número de registro conhecido como IP.

Braga ainda, preceitua a dificuldade de identificar o IP:

> Sendo assim, devido as suas características, o endereço IP é um dos pontos para que o agente do crime seja identificado. Entretanto, as dificuldades iniciam na tentativa de obter este endereço IP, pois apesar de poderem ser descobertos com o provedor de Internet ou com os gerenciadores do site, obter os dados do usuário que estava acessando naquele certo momento

> é complexo e burocrático. Sem contar as ferramentas que podem mascarar e dissimular o número do IP. (BRAGA, 2019)

Essa dificuldade em identificar o IP pode provocar a falta de provas pela quantidade de delitos cometidos, o excesso de informações e a demora na apuração dos fatos no inquérito policial pode causar a perca desses dados. Além da dificuldade quando se trata de crime que envolve outros países, o acesso aos dados se torna mais difícil e moroso para a justiça brasileira.

Uma barreira que também atrapalha essa investigação são os chamados *proxies* uma espécie de servidor que ocultam os números de IP.

Quando é possível identificar o IP do aparelho eletrônico é necessário buscar o endereço MAC, que é o endereço onde se encontra o local físico que se encontra esse aparelho, a dificuldade é quando está sendo utilizado uma rede aberta em local público, podendo ser logo alterada.

A Convenção de Budapeste trata sobre essa cooperação na parte investigativa dos crimes cibernéticos, Braga cita algumas medidas preceituadas na referida Convenção:

> São medidas processuais recomendadas pela referida Convenção Europeia: i) determinação ou ordem de preservação de dados armazenados em sistemas de computadores (expedited preservation of stored computer data),com duração de até noventa dias, que permite às autoridades pleitear posteriormente uma ordem de abertura ou revelação (disclosure) de tais dados, o que seria equivalente à quebra de sigilo prevista no Brasil (art. 16); ii) ordem de preservação e parcial abertura de fluxo de dados (expedited preservation and partial disclosure of traffic data); iii) ordem de fornecimento de dados às autoridades (production order- art. 18); iv) busca e apreensão para acessar sistemas e dados de computadores, incluindo meios de armazenamento de dados eletrônicos (mídias e similares - art. 19); v) obtenção, coleta ou gravação em tempo real de fluxo de dados (real-time collectionof traffic data- art. 20); vi) interceptação de dados/conteúdo (interception of content data) transmitidos por meio de comunicação eletrônica, em tempo real. (BRAGA, 2019)

Sendo assim, os Estados que fazem parte dessa Convenção são obrigados a adequarem suas legislações para atender os requisitos acima. Luciana Boiteux ressalva a necessidade de capacitação aos profissionais que irão exercer essa investigação:

> Além da previsão legal de medidas processuais para se obter a evidência em cibercrimes, é essencial que se tenha uma polícia científica desenvolvida, com pessoas capacitadas e treinadas no campo da informática e que dominem as novas tecnologias. Além de bem equipadas com computadores de última geração, para que possam periciar e avaliar os dados coletados, tendo em vista o alto grau de especialização deste tipo de atividade (BOITEUX, 2010).

A busca sistemática é um dos procedimentos mais utilizados na investigação cibernética, sendo um modelo de investigação de forma preventiva, que depende de iniciativa da autoridade policial, aquela sensação de anonimato na *internet* é falsa e por isso corrobora e facilita essas investigações.

A engenharia social é outro método eficaz e importante para a investigação desses crimes. A engenharia social pode ser definida como um conjunto de atos que influenciam uma pessoa a realizar uma determinada ação de interesse (SOCIAL-ENGINEER, 2015).

Diego Braga preceitua sobre o uso da engenharia social em investigação cibernética:

> Em geral, para se conquistar o objetivo durante o procedimento de engenharia social, se abusa da ingenuidade do alvo ou se procura ganhar a sua confiança, utilizando-se, por exemplo, de símbolos de instituições confiáveis, como órgãos públicos, grandes empresas, etc para obter informações desejáveis ou invadir computadores. Geralmente, o investigador influencia a pessoa a ser “conquistada” utilizando-se de sentimentos de medo, ambição, curiosidade, solidariedade, montando uma armadilha. (BRAGA, 2019)

Usando esse método de investigação é necessário que o agente crie vários perfis falsos, e que esses perfis em redes sociais aparentem serem verdadeiros. Assim, eles conseguem infiltram em perfis de gangues, criminosos, pedófilos, quadrilhas dentre outros.

Mais um método de investigação é a utilização de fontes abertas, o que facilita a entrada nos *sites*, pois são gratuitos e de livre acesso. Mas essas fontes abertas devem ser verificadas e autenticadas para um futuro processo penal.

3.2 PUNIBILIDADE DOS CRIMES VIRTUAIS SEXUAIS

Quanto à aplicabilidade dos crimes cibernéticos é utilizada o Código Penal Brasileiro e algumas leis especificas que tratam do tipo penal, como é o caso da Lei Carolina Dieckmann. A forma como esses delitos crescem a frente da criação de leis especificas acaba tornando muitas vezes difícil de processar e julgar os autores desses crimes.

A Lei 12.737/12 tipificou diversas condutas como a falsificação de documento particular, a invasão de dispositivo informático alheio dentre outros, porém apesar de ser uma lei especifica foi redigida pelo legislador com uma grande pressão da sociedade pelo caso de a atriz ter se tornado público e gerado revolta social.

Enunciado da Lei n° 12.737/12 versa:

> Art. 1o Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
> Art. 2o O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes artigos; 154-A e 154-B:
> **Invasão de dispositivo informático**
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;

> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. ”

Conforme entendimento jurisprudencial, demonstra o gravidade e periculosidade de quem invade dispositivos informáticos.

> HABEAS CORPUS. INVASÃO DE DISPOSITIVO INFORMÁTICO E FALSIDADE IDEOLÓGICA. NEGATIVA DE AUTORIA. ATO COATOR. FUNDAMENTAÇÃO IDÔNEA E SUFICIENTE. COVID-19. MEDIDAS CAUTELARES DIVERSAS DA CUSTÓDIA PESSOAL. 1. A alegação de negativa de autoria só logra conhecimento no Habeas Corpus quando amparada em prova pré-constituída robusta, haja vista o rito mandamental não prever dilação probatória.2. Verificado que o ato coator expõe a necessidade e adequação da prisão preventiva do paciente com base na gravidade concreta da conduta, na elevada periculosidade pessoal dele e no grave risco que a sua liberdade implica à ordem pública, à regularidade processual e eventual aplicação da lei penal, inexiste constrangimento ilegal a ser debelado. 3. A simples alegação de necessidade de relaxamento ou substituição da cautela pessoal do paciente ante a possibilidade de contágio pelo novo coronavírus (COVID-19) não basta ao deferimento da ordem, posto que as unidades prisionais estão adotando as medidas sanitárias de prevenção e o paciente não possui nenhuma comorbidade que recomende cuidados e/ou medidas excepcionais. 4. Parecer ministerial acolhido. WRIT CONHECIDO EM PARTE. ORDEM DENEGADA. (TJGO, Habeas Corpus Criminal 5250886-10.2020.8.09.0000, Rel. Des(a). EUDÉLCIO MACHADO FAGUNDES, 2ª Câmara Criminal, julgado em 28/06/2020, DJe de 28/06/2020)

Deixa-se lacunas e diferentes interpretações entre os legisladores quanto a invasão de dispositivo mediante violação de mecanismo de segurança, gerando críticas como a de poder realizar invasão de dispositivo que não tenha mecanismos de segurança dentre outras. Além disso alguns tipos penais não inseridos nesta lei tiveram que ser usadas e interpretadas por analogia ao Código Penal por não possui lei especifica.

Zaqueu e Antônio explicam sobre a forma de fazer analogia de crimes virtuais com o Código Penal Brasileiro, “Quanto a aplicabilidade penal dos crimes virtuais estes serão penalizados pelo Código Penal pátrio, ainda que não esteja tipificado diretamente, faz-se por analogia. ” (SILVA, MELLO, 2019).

Diante disso e apesar das buscas pela punibilidade dos crimes virtuais sexuais o poder judiciário ainda é lento em apurar e julgar os casos e muitas vezes, provas de crimes como esses acabam sumindo no universo virtual visto que muitos criminosos conseguem eliminar seus rastros após cometer seus abusos.

Muitos pedófilos, por exemplo, aliciam suas vítimas por meio de aplicativos de mensagens que possuem criptografia, o que acaba dificultando a investigação por exigir que autoridades policiais tenha autorização para ter acesso as mensagens, e com isso correr o risco de perder todo o histórico de conversas durante o tramite para conseguir essa autorização.

CONCLUSÃO

O presente estudo partiu de uma análise do tema crimes virtuais, abordado em suas várias espécies e meios de prática, sendo assim analisada a problemática da ausência de segurança jurídica na legislação brasileira referente aos crimes cibernéticos. O alvo importante foi a análise da Lei 12.737/12, bem como o artigo 154-A do Código Penal Brasileiro, que trata da invasão de dispositivos informáticos.

A lei especifica, denominada Lei Carolina Dieckmann, buscou trazer inovações legislativas para esse meio de crime, porém, trouxe consigo algumas falhas legislativas, deixando então dificuldades para o legislador encaixar condutas e puni-las de formas adequadas e eficaz, deixa-se como questionamento se há de fato uma segurança jurídica trazida por essa lei.

Tendo sido evidenciada a importância e o crescimento tecnológico, faz - se necessário o cuidado com quem utiliza as redes de computadores, para que tenha suas privacidades preservadas, que *sites fakes* e perfis de golpistas sejam banidos com maior agilidade evitando maiores fraudes.

A pesquisa traçou desde métodos de investigação policial dos crimes bem como salientou o perfil dos infratores, sendo de maior facilidade para que seja identificado quando estiver diante de alguma fraude. Também apresentou o perfil de vítimas e pessoas expostas nas redes a esses tipos de crimes.

Concluindo assim que são tantos os pontos negativos na lei para o tratamento e punibilidade dos casos de delitos virtuais, e que, ainda há ausência de atenção ao preparo de profissionais para atuarem nos casos, bem como a falta de mais delegacias especializas pelo país, que faz com que tamanha seja a importância de atentar-se para esse meio e buscar avanços e melhorias na questão virtual e tecnológica do pais.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves. Manual de investigação cibernética à luz do Marco Civil da Internet. Rio de Janeiro: Brasport, 2016.

BRAGA, Diego Campos Salgado. Métodos de investigações no âmbito cibernético. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 24, n. 5681, 20 jan. 2019. Disponível em: https://jus.com.br/artigos/71463. Acesso em: 14 set. 2020.

BRASIL, Lei 12.015, de 7 de agosto de 2009. Dispõe sobre os crimes hediondos. Diário oficial da União, Brasília, 7 de agosto de 2009. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12015.htm. Acesso em 27 de julho de 2020.

BRASIL, Lei 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Diário oficial da União, Brasília, 30 de novembro de 2012. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 27 de julho de 2020.

BRASIL, Lei 2.848, de 7 de dezembro de 1940. Dispõe sobre o Código Penal Brasileiro. Diário oficial da União, Brasília, 7 de dezembro de 1940. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 24 de agosto de 2020.

BRASIL, Lei 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário oficial da União, Brasília, 13 de julho de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em 21 de setembro de 2020.

BRASIL, Tribunal de Justiça do Estado de Goiás, Habeas Corpus Criminal 5250886-10.2020.8.09.0000, Rel. Des(a). EUDÉLCIO MACHADO FAGUNDES, 2ª Câmara Criminal, julgado em 28/06/2020, DJe de 28/06/2020. Acesso em 14 de outubro de 2020.

BOITEUX, Luciana. Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual. Doutrinas Essenciais de Direito Penal. vol. 8, 2010.

D’URSO, Luiz Augusto Filizzola. Em tempos de cibercrimes. 2019. Disponível em https://canalcienciascriminais.jusbrasil.com.br/artigos/752483002/em-tempos-de-cibercrimes?ref=serp. Acesso em 17 de junho de 2020.

GALHARDI, Raul. Brasil é terreno fértil para fake news. 2019. Disponível em http://www.observatoriodaimprensa.com.br/crise-na-imprensa/brasil-e-terreno-fertil-para-fake-news/. Acesso em 01 de junho de 2020.

INTERNETLAB. Como países enfrentam a disseminação não consentida de imagens íntimas. 2018. Disponível em https://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/. Acesso em 08 de outubro de 2020.

MACHADO, Felipe. Brasil perde US$ 10 bilhões por ano com cibercrime, diz McAfee. 2018. Disponível em https://veja.abril.com.br/economia/brasil-perde-us-10-bilhoes-por-ano-com-cibercrime-diz-mcafee/. Acesso em 27 de maio de 2020.

MARIANO JÚNIOR, Alberto Ribeiro. Divulgar cena de sexo, nudez ou pornografia é crime: breves comentários sobre o caso Neymar e o art. 218-C do CP. 2019. Disponível em: https://jus.com.br/artigos/74450. Acesso em 25 de agosto 2020.

MATOS, Andreza. Assédio com teor sexual praticado pelas redes sociais pode ser considerado crime. 2020. Disponível em https://andrezamaatos.jusbrasil.com.br/artigos/897480242/assedio-com-teor-sexual-praticado-pelas-redes-sociais-pode-ser-considerado-crime?ref=feed. Acesso em 26 de agosto de 2020.

MOTTA, Artur Francisco Mori Rodrigues. A dignidade da pessoa humana e sua definição. 2013. Disponível em https://ambitojuridico.com.br/cadernos/direitos-humanos/a-dignidade-da-pessoa-humana-e-sua-definicao/#:~:text=No%20art.,dos%20princ%C3%ADpios%20fundamentais%20da%20Rep%C3%BAblica. Acesso em 27 de julho de 2020.

NASCIMENTO, Talles. Crimes cibernéticos. 2018. Disponível em https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em 14 de maio de 2020.

OLIVEIRA, Déborah. Qual o perfil dos cibercriminosos no Brasil. 2017. Disponível em https://www.itforum365.com.br/qual-o-perfil-dos-cibercriminosos-no-brasil/. Acesso em 07 de setembro de 2020.

OTTO, Isabella. O que é Sextorsão e como ocorre o crime de estupro virtual. 2019. Disponível em: https://capricho.abril.com.br/comportamento/o-que-e-sextorsao-e-como-ocorre-o-crime-de-estupro-virtual/. Acesso em 02 de setembro de 2019.

PINHEIRO, André. Por que o Brasil se tornou o segundo maior gerador de cibercrime do mundo. 2015. Disponível em https://computerworld.com.br/2015/06/16/por-que-o-brasil-se-tornou-o-segundo-maior-gerador-de-cibercrime-do-mundo/. Acesso em 27 de maio de 2020.

PRIBERAM, "cibercrime", in Dicionário Priberam da Língua Portuguesa, 2008, Disponível em https://dicionario.priberam.org/cibercrime. Acesso em 11 de maio de 2020.

ROMANO, Rogério. Convenção de Budapeste e cibercrimes. 2019. Disponível em https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes. Acesso em 27 de maio de 2020.

ROQUE, Sérgio Marcos. Criminalidade informática: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007.

ROSA, Fabrizio, Crimes de informática, Campinas: Bookseller, 2002.

SAFERNET. Perfil, Helpline. 2020. Disponível em: https://new.safernet.org.br/helpline. Acesso em 01 de setembro de 2020.

SANTOS, Rodrigo. Crimes Cibernéticos: Por Trás Da Mente Dos Hackers. 2020. Disponível em: https://www.compugraf.com.br/crimes-ciberneticos-por-tras-da-mente-dos-hackers/. Acesso em 05 de setembro de 2020.

SILVA, Ana Karolina Calado Da. O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira. 2013. Disponível em: https://ambitojuridico.com.br/edicoes/revista-109/o-estudo-comparado-dos-crimes-ciberneticos-uma-abordagem-instrumentalista-constitucional-acerca-da-sua-

producao-probatoria-em-contraponto-a-jurisprudencia-contemporanea-brasileira/. Acesso em 02 de junho de 2020.

SILVA, Gabriele. O que são as fake news. 2019. Disponível em https://www.educamaisbrasil.com.br/educacao/dicas/o-que-sao-fake-news. Acesso em 01 de junho de 2020.

SILVA, Zaqueu de Almeida; MELLO, Antônio Cesar de. 2019. Uma análise jurídica dos crimes virtuais e a eficácia da legislação brasileira. Disponível em https://www.boletimjuridico.com.br/artigos/direito-penal/4423/uma-analise-juridica-crimes-virtuais-eficacia-legislacao-brasileira. Acesso em 17 de setembro de 2020.

SILVEIRA, Artur. Os crimes cibernéticos e a Lei nº 12.737/2012 (“Lei Carolina Dieckmann”). 2015. Disponível em https://jus.com.br/artigos/35796/os-crimes-ciberneticos-e-a-lei-n-12-737-2012-lei-carolina-dieckmann. Acesso em 27 de maio de 2020.

SOCIAL-ENGINEER. Security through education. 2015. Disponível em: www.social-engineer.org. Acesso em 16 de setembro de 2020.