FACULDADE EVANGÉLICA DE GOIANÉSIA

BACHAREL EM DIREITO

ANÁLISE DOS ÍNDICES DE CRIMINALIDADE FRENTE AOS DELITOS PRATICADOS NO AMBIENTE VIRTUAL

JAIR ANTONIO RAPOSO MORAIS

GOIANÉSIA - GO
2021

JAIR ANTONIO RAPOSO MORAIS

ANÁLISE DOS ÍNDICES DE CRIMINALIDADE FRENTE AOS DELITOS PRATICADOS NO AMBIENTE VIRTUAL

Artigo Científico apresentado junto ao Curso de Direito da FACEG (Faculdade Evangélica de Goianésia), como exigência parcial para a obtenção do grau de Bacharel em Direito.

Orientador Profa. Ms. Cristiane Ingrid de Souza Bonfim

GOIANÉSIA - GO
2021

FOLHA DE APROVAÇÃO

ANÁLISE DOS ÍNDICES DE CRIMINALIDADE FRENTE AOS DELITOS PRATICADOS NO AMBIENTE VIRTUAL

Este Artigo Científico foi julgado adequado para a obtenção do título de Bacharel em Direito e aprovado em sua forma final pela banca examinadora da Faculdade Evangélica de Goianésia/GO- FACEG

Aprovada em, 17 de dezembro de 2021

Nota Final_____

Banca Examinadora

Prof. Ms. Cristiane Ingrid de Souza Bonfim
Orientador

Prof. Me. Adonis de Castro
Professor convidado 1

Prof. Esp. Mariana Ferreira Martins
Professor convidado 2

AGRADECIMENTOS

Agradeço primeiramente a Deus por todas as bençãos em minha vida, pois sem Ele nada seria possível. Sou grato ao Senhor por ter me guiado e ter me mantido firme em meu propósito, com saúde, e perseverança, sendo fundamentais durante minha jornada acadêmica.

Foram dias mal dormidos, corridos, de muita dificuldade, mas também de muita alegria e aprendizado, apesar das dificuldades encerro este ciclo com satisfação e a certeza de que serei recompensado.

Agradeço aos meus pais, Sr. Donizete Raposo e a Sra. Sueli de Morais que sempre foram os pilares da minha formação como ser humano, e que nunca deixaram de acreditar em mim e nos meus projetos e sonhos, ambos se desdobrando ao máximo para ver minha formação acadêmica.

Agradeço ao incentivo ofertado pelo Grupo Lírios e por toda compreensão durante toda jornada acadêmica.

Agradeço em especial meu amigo Túlio Mendes, por dividir essa jornada acadêmica, por sempre dar encorajamento e apoio durante a trajetória acadêmica, com certeza foi uma fonte inesgotável de apoio durante todo processo, pela sua presença em momentos difíceis.

Agradeço também aos meus amigos Ramon Silveira, Thales Oliveira, por sempre estarem ao meu lado tornando a vida mais leve diante das adversidades. Vocês foram meu apoio.

Por fim, agradeço especialmente minha orientadora, Professora Mestre Cristiane Ingrid de Souza Bonfim, pela sua generosidade e paciência, durante todo processo deste projeto.

ANÁLISE DOS ÍNDICES DE CRIMINALIDADE FRENTE AOS DELITOS PRATICADOS NO AMBIENTE VIRTUAL

ANALYSIS OF CRIME RATES IN RELATION TO CRIMES COMMITTED IN THE VIRTUAL ENVIRONMENT

JAIR ANTONIO RAPOSO MORAIS[1]
CRISTIANE INGRID DE SOUZA BONFIM[2]

1 Discente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail: jair_rps@hotmail.com
2Docente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail:cristiane481@hotmail.com

RESUMO

O Tema do estudo é uma análise dos índices de criminalidade em meio digital, considerando uma possibilidade de o presumir em ambiente de fácil impunidade. A justificativa do estudo é em analisar o atual cenário de danos ocasionados pelos crimes praticados pela internet, como também examinar a dificuldade que os Estados soberanos enfrentam na investigação e punição desses delitos. O objetivo geral do estudo é: analisar através do ordenamento jurídico brasileiro, a criminalidade praticada com os meios eletrônicos especialmente os que avançam na rede mundial de computadores. Os objetivos específicos do estudo foram: ponderar os principais aspectos do fenômeno dos crimes virtuais; pesquisar as possíveis consequências jurídicas aplicada atualmente na legislação vigente em nosso país segundo classificação doutrinária adotada; avaliar os aspectos que dificultam a identificação de autoria. O estudo visou compreender se é previsto no ordenamento jurídico brasileiro alguma ocorrência relacionada aos crimes cibernéticos? Quais os maiores desafios jurídicos desse meio? Como pode ser assegurada a segurança das vítimas e crimes virtuais?. O estudo detém a metodologia dedutiva, buscando compreender a temática de estudo a partir de premissas. A pesquisa é qualitativa, ressaltando ainda a pesquisa básica. A conclusão do estudo apresenta a existência de uma facilidade de anonimato no meio digital que permite a impunidade, vez que ante a falta de identificação é impossível constatar a autoria do crime e assim se vê frustrada a persecução penal, assim é necessária ação do Estado para impedir meios de anonimato ou privacidade extrema que seja utilizada para se esquivar da punição de crimes.

PALAVRAS-CHAVE: Crimes. Informática. Impunidade. Delitos.

ABSTRACT

The subject theme of the study is an analysis of crimes rates in digital media, considering the possibility of assuming it in an environment of easy impunity. The justification for the study is to analyze the current scenario of damage caused by crimes committed on the Internet, as well as to examine the difficulty that sovereign States face in investigating and punishing these crimes. The general objective of the study is: to analyze, through the Brazilian legal system, criminality practiced with electronic means, especially those that advance in the world wide web. The specific objectives of the study were: to consider the main aspects of the phenomenon of cybercrime; research the possible legal consequences currently applied in the legislation in force in our country according to the adopted doctrinal classification; assess the aspects that make it difficult to identify authorship. The study aimed to understand if any occurrence related to cyber crimes is foreseen in the Brazilian legal system? What are the biggest legal challenges in this medium? How can the security of victims and cyber crimes be ensured?. The study has the deductive methodology, seeking to understand the study theme from premises. The research is qualitative, also emphasizing basic research. The conclusion of the study shows the existence of an anonymity facility in the digital environment that allows impunity, since, given the lack of identification, it is impossible to verify the authorship of the crime and thus the criminal prosecution is frustrated, so State action is required to prevent means of anonymity or extreme privacy from being used to evade the punishment of crimes.

KEY WORDS: Crimes. Computing. Impunity. Offenses.

INTRODUÇÃO

À vista das evoluções tecnológicas, a internet vem sido usada como meio de trabalho, informação, lazer, pesquisas, e etc. Importante mencionar os dias atuais, onde a população sofre com a pandemia da Covid-19 e o meio virtual se mostrou de grande valia para impulsionar o mercado de trabalho sem que as pessoas precisassem sair de suas residências.

Ocorre que apesar de existirem inúmeros benefícios propiciados pelo desenvolvimento digital, este campo também é utilizado para a prática de crimes. Os indivíduos aproveitam a facilidade de expressão, o anonimato e a consequente dificuldade de se localizar o autor do fato e averiguar a conduta para cometerem delitos pressupondo a impunidade.

Dentre os crimes praticados no meio digital, merecem destaque e exemplo os crimes contra a honra; racismo; mediação de menores para fins libidinosos; invasão de privacidade; vendas fraudulentas ou de produtos ilegais; clonagem de cartões, divulgação de notícias falsas (as famosas fake news); roubo de senhas ou dados pessoais, entre outros.

Assim, a facilidade em se praticar crimes virtualmente se dá pelo fato de um sujeito conseguir se esconder atrás de diversas identidades. Logo, importante questionar: É previsto no ordenamento jurídico brasileiro alguma ocorrência relacionada aos crimes cibernéticos? Quais os maiores desafios jurídicos desse meio?

Sendo o objetivo geral do estudo o de Analisar através do ordenamento jurídico brasileiro, a criminalidade praticada com os meios eletrônicos especialmente os que avançam na rede mundial de computadores. Enquanto que os objetivos específicos são: Ponderar os principais aspectos do fenômeno dos crimes virtuais; Pesquisar as possíveis consequências jurídicas aplicada atualmente na legislação vigente em nosso país segundo classificação doutrinária adotada; Avaliar os aspectos que dificultam a identificação de autoria.

Assim, a presente pesquisa possui como intuito analisar o atual cenário de danos ocasionados pelos crimes praticados pela internet, como também examinar a dificuldade que os Estados soberanos enfrentam na investigação e punição desses delitos.

Esta pesquise estrutura-se em três tópicos, sendo o primeiro tratando de

um recorte teórico sobre o ambiente virtual e suas complexidades gerais, o segundo tópico apresenta normas principais que se aplicam especificamente ao ambiente virtual, e o terceiro tópico desenvolve conceitos e informações sobre a facilidade de impunidade quando os crimes sejam cometidos no ambiente virtual.

Os principais teóricos utilizados são IBGE (2018); Florillo (2017); Mendes (2012); Oliveira (2015); Pinheiro (2016); Rocha (2013); Rocha (2020); Souza (2020) e diversos outros que auxiliam o crivo teórico apresentado no estudo e as argumentações principais.

O estudo detém a metodologia dedutiva, buscando compreender a temática de estudo a partir de premissas. A pesquisa é qualitativa, de forma a buscar as qualidades dos itens e suas quantidades, ressaltando ainda a pesquisa básica que não se apresenta em nenhum caso específico e busca apenas conhecimento que solucione a problemática e atinja os objetivos apresentados.

1 RECORTE TEÓRICO: AMBIENTE VIRTUAL

Os ciberespaços são itens com história vasta e especialmente complexos, de forma que pode se considerar que estes ciberespaços ou ambientes virtuais não são uma inovação do século XXI e sim algo que surge no final do século XIX em razão da evolução dos meios de comunicação (OLIVEIRA, 2015)

Oliveira (2015) expõe que o desenvolvimento da informática e das revoluções dos meios de comunicação realmente só se viu no início do século XXI, com exceção de poucos casos, sendo desenvolvido inicialmente em ambientes empresariais, certas pesquisas do governo e indivíduos de classes mais elevada economicamente.

Conforme Souza (2020) o desenvolvimento da tecnologia e especialmente dos meios de comunicação são um item problemático desde a popularização do telefone no Brasil com as primeiras ligações públicas no início do século XX que serviam como meio de comunicação usado por criminosos. Existia ao período do século XX o uso inicial de comunicações tecnológicas para se cometerem crimes, porém não se pode considerar que ainda eram usos de ambientes digitais de fato.

O desenvolvimento da popularização da tecnologia ao final do século XX

começa a iniciar os primeiros ambientes virtuais, com o uso de comunicações como o telefone para criar conexões entre diversos usuários simultaneamente, assim permitindo uma forma de comunicação instantânea a partir de um ambiente que pode se considerar virtual. É certo que o ambiente virtual pode ser considerado como nascido no referido período e bem como sendo fruto das evoluções dos meios de comunicação (OLIVEIRA, 2015; SOUZA, 2020)

Souza (2020) expõe que as necessidades sociais e especialmente sua evolução para a solução de tais problemas é o que cria os meios digitais e especialmente a revolução tecnológica do século XXI, na qual existe a popularização de tecnologias de ponta e especialmente garantindo a possibilidade de usos infindáveis de tais tecnologias.

A evolução da sociedade é um fator que impacta uma série de complexidades das relações sociais e especialmente das complexidades intrínsecas de toda a população. O ser humano se atualiza constantemente na busca por melhorias de sua convivência e de benefícios que melhorem sua vida, porém essas constantes atualizações também auxiliam em mudanças de mundo, tal qual o aquecimento global, o desenvolvimento de problemas sociais e especialmente a possibilidade de maiores cometimentos de crimes. (PINHEIRO, 2016)

> Acredita-se que os crimes cibernéticos vêm sendo praticados no mundo por mais de cinco décadas, desde as primeiras referências até os dias atuais, propagando e se desenvolvendo conforme a globalização dessa nova era digital. O que se sabe, é que foi na década de 1970 que os hackers começaram a ser citados e relacionados aos crimes virtuais, todavia, tenha sido em 1980 o maior alastramento dos mais diferentes delitos pertinentes aos crimes cibernéticos. (BRASIL, 2018, p. 271)

A modernidade e as complexidades sociais desenvolveram a tecnologia e as mídias digitais como uma forma de comunicação, a comunicação digital, de forma que se tornou pouco a pouco mais fácil desenvolver uma série de ações sem a necessidade de contato físico. Tais atualizações e modernidades das comunicações sociais permitiram uma revolução social sem precedentes, garantindo segurança de comunicações e especialmente a possibilidade de contatos de uma forma muito maior que em períodos pré-tecnológicos como o atual da contemporaneidade. (PINHEIRO, 2016)

Desde o surgimento dos usos das tecnologias digitais os seus usos não

pareciam controlados por nenhum órgão e existindo um ambiente novo de livres possibilidades de uso. A primeira década do século XXI é marcada pela explosão das redes sociais e o desenvolvimento da informática, com isso se popularizando o conhecimento sobre a rede mundial de computadores (internet) e bem como o nascimento de vários locais para acesso a esta vasta rede de conhecimento. (OLIVEIRA, 2015; SOUZA, 2020)

Esta explosão da internet e especialmente os usos cada vez mais frequentes das redes sociais e dos meios de comunicação virtuais podem ser ditas como uma complexidade que popularizou o meio digital e o fez extremamente acessível a qualquer um do povo. Ocorre que na primeira década do século XXI não se vê uma regulamentação direta dos usos de tais meios e somente se aplicando as normas gerais e abrangentes do direito pátrio para se punir e evitar usos indevidos.

O meio digital ainda detém uma grande complexidade que é o acesso praticamente ilimitado de qualquer indivíduo de qualquer local com recursos básicos como eletricidade, hardware computacional e acesso a rede mundial de computadores. Com essa facilidade de acesso qualquer indivíduo pode acessar uma quantidade de conhecimento infindável e ter acesso facilitado de comunicação com pessoas em todo o mundo. Essas facilidades criam um ambiente perfeito para o anonimato e falsidade ideológica, de forma que é simples se comunicar com alguém sem a possibilidade de fisicamente se expor (BRASIL, 2018)

O anonimato que é possibilitado pelas redes digitais permite que o usuário possa alterar facilmente a sua auto-exposta identidade, isso sendo um dos maiores problemas de tais redes de comunicação e especialmente das redes sociais, nas quais a identidade do indivíduo usuário é auto exposta e não detém comumente um agente ou órgão regulador e que valide a identidade dos usuários (STRASSER, 2019)

De acordo com os estudos de Strasser (2019) o anonimato nas redes digitais é muitas vezes essencial, dando a privacidade necessária e protegendo o ambiente de práticas como usos indevidos de dados pessoais, porém em certas redes sociais e especialmente em certos centros de comunicação e comércio tal anonimato é utilizado para garantir a impunidade e bem como uma barreira que impede a identificação do indivíduo que já não se pode atingir fisicamente.

O ambiente digital ainda detém uma flexibilidade tamanha, especialmente a as redes sociais permitem o desenvolvimento de locais de bate-papo, comércio, relacionamento, compartilhamento de informações, ensino e até mesmo locais de

simples humor e lazer. Certo é que existe uma complexidade com os ambientes digitais e uma flexibilidade em seu uso, dependendo apenas da vontade do usuário e da permissibilidade das redes.

É diante desta complexidade de novos caminhos e contatos tecnológicos que nascem os crimes cibernéticos ou ainda conhecidos como crimes digitais, estes que são uma complexidade no direito moderno pois permitem uma via de cometimento de crimes não prevista por parte do legislador. (PINHEIRO, 2016)

Oliveira (2015) informa que estes tipos de crimes podem até mesmo ser encaixados na norma pátria, vez que se considera especialmente à vontade em cometer o crime e em muitos delitos não se importa a forma de cometimento ou o seu meio.

> O elemento central no estudo dos crimes ou da teoria do delito é a conduta, a qual pode ser comissiva ou omissiva, dolosa ou culposa. No campo da conduta, o Direito Penal pátrio adotou a teoria finalista da ação, elaborada por Welzel. Para essa teoria, a conduta é o comportamento humano voluntário dirigido a um fim.
> A conduta deve estar definida em lei como crime anteriormente à sua prática para que possa ser punida pelo Estado, atendendo-se ao princípio da legalidade insculpido no inciso XXXIX, do art. 5º, da Constituição Federal, segundo o qual não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Tal princípio também está presente no art. 1º do Código Penal Brasileiro. (BRASIL, 2018, p. 120)

Ocorre que certos crimes detém uma complexidade que necessita de definição específica e de que estejam previstos em lei para que realmente sejam um crime punível no direito brasileiro, tal qual o compartilhamento de fotos intimas que foi uma luta por tal durante muito tempo no direito brasileiro.

O direito brasileiro necessita de atualização para compreender não somente tipos penais modernos que possam estar ligados aos delitos modernos e a ações que façam mal social e sejam cometidas por meio digital. Desta forma, passam a nascer itens, bens jurídicos, que são necessários de tutela por parte do Estado. (OLIVEIRA, 2015)

> Se de um lado a modernidade, marcada pelo uso em comum da internet e pelo início da era homo digitalis, trouxe elementos facilitadores ao desenvolvimento social, por outro também criou amplos desafios daqueles que têm por objetivo e função primordial a manutenção dos direitos e da paz social. O enfrentamento e a

> punibilidade dos chamados crimes informáticos – cometidos essencialmente por meio da internet ou de dispositivos eletrônicos vindos até a sociedade moderna, graças à evolução tecnológica – ainda representam grandes problemáticas ao Direito, que, em muito, encontra-se preso aos bens jurídicos edificados a partir das antigas revoluções. (BRASIL, 2018, p. 216)

Ocorre que, dada a complexidade destas novas tecnologias e especialmente a falta de controle do Estado sobre estes meios de comunicação, não é fácil a fiscalização das redes de informática ou de meios digitais por sua complexidade, criptografia e até mesmo a privacidade que é aplicada em tais redes. Assim testando apenas a tutela do Estado em meios públicos nas redes de internet e conexões das quais detenha controle. (BRASIL, 2018)

> É de grande importância frisar desde logo que também não há um conceito unívoco do que vem a ser delito informático, repetindo a discordância que ocorre com o ramo maior, que é o direito informático. Com base nas lições do festejado pesquisador Augusto Eduardo de Souza Rossini, há quem chame de “criminalidade do computador”, “criminalidade da informática”, “delitos cibernéticos”, além dos já citados vocábulos. (BRASIL, 2018, p. 205)

Diante de tais informações é evidente em como os ambientes virtuais, as redes sociais e os meios de comunicação na nova geração, isto é, os meios de comunicação tecnológicos são uma complexidade e especialmente sendo amplamente flexíveis para seu uso. Tal flexibilidade e complexidade permite um ambiente fértil para golpes, auxiliado por parte do fácil anonimato e falta de controle do Estado.

2 APONTAMENTOS LEGAIS ACERCA DOS CRIMES PRATICADOS NO AMBIENTE VIRTUAL

O direito brasileiro vem se adequando a modernidade com certa lentidão, porém desenvolvendo claros itens de apoio e especialmente proteção a população em face de ações que podem ser nocivas a sociedade. Algumas normas são disciplinadas desde 2012, com projetos em face de crimes digitais desde o período de 2010. É evidente que diversas ações foram tomadas por parte do legislativo para coibir

as ditas ações danosas a sociedade, mesmo que elas não sejam bem compreendidas ou sejam ações não muito praticadas como o furto e roubo. (PINHEIRO, 2016)

> No plano nacional há dispositivos legais penais voltados especialmente para a proteção de dados informáticos, como é o caso do caput do art. 154-A do Código Penal, acrescentado pela Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann), o qual tipifica a conduta de 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, punindo tal conduta com a pena de detenção de três meses a um ano e multa. O referido artigo ainda descreve nos seus parágrafos algumas hipóteses qualificadoras e causas de aumento de pena. (BRASIL, 2018, p. 123)

É importante salientar em como esta norma criada para coibir o compartilhamento de imagens privadas foi desenvolvida por meio de uma grande comoção da atriz Carolina Dickman e de diversas outras vítimas de ações danosas a suas reputações cometidas por meio online. (BRASIL, 2018)

Em mesmo sentido as informações de Souza (2020) apresentam que o marco da Lei Carolina Dickman foi apresentado mediante proposta de Lei popular e somente se desenvolveu em razão da comoção popular diante do caso. A repercussão nacional dada ao caso o tornou facilmente evidente e toda a população passou a conhecer tanto o caso quanto a lei advinda dele, assim gerando uma redução dos crimes de invasão digital.

Compreende-se ainda em como a complexidade da diversidade de meios em que podem ser cometidos tais crimes criam uma falta de possibilidade de o Estado estar no controle da rede, especialmente considerando que a maioria dos dispositivos de informática prezam por uma ação de criptografar seus dados e especialmente garantir a privacidade do usuário, o que pode dar segurança aos criminosos para manter-se no anonimato. (BRASIL, 2018)

> São inúmeros os meios de comunicação via internet atualmente disponíveis (computador, smatphone, tablet, smartTV), bem como os espaços virtuais, como as redes sociais (Facebook, Twitter, Linkedin, Instagram) e demais páginas da internet onde se publicam conteúdos que passam a ser acessíveis a todos que estejam conectados. Portanto, fácil é a difusão de ideias via internet e rápido o alcance a um número cada vez maior de pessoas. Dessarte, devida e necessária

> a proteção contra as palavras, imagens e vídeos racistas publicados no campo virtual.
> Realçando a importância do tema, houve um caso notório na mídia nacional em que a apresentadora negra Maria Júlia Coutinho, do Jornal Nacional, da Rede Globo de televisão, sofreu inúmeras ofensas em virtude de sua cor em rede social (Facebook), dando azo à discussão nos meios de comunicação.
> Tal caso, conforme nosso entendimento, caracterizou injúria racial, conduta insculpida no tipo do art. 140, § 3º, do Código Penal, muito embora haja interpretações de que também havia se caracterizado o crime de racismo. (BRASIL, 2018, p. 211)

É observado que os crimes digitais podem ser cometidos de uma forma bem ampla e especialmente tendo alguns crimes que mesmo sem a mudança do tipo penal podem se adequar com simples entendimento doutrinário para abarcar ações de crimes digitais. O racismo parece ser o crime digital, injuria racial, mais possível de se ver sendo cometido e aplicando a norma sem alterações, vez que o meio digital se tornou apenas uma ferramenta no desenvolvimento do delito, não servindo mais que igual a um papel e caneta; no caso da injuria racial. (BRASIL, 2018)

> Ressalta-se que, apesar da legislação brasileira suprir algumas necessidades no direito nacional, ainda, há muitos lapsos a serem preenchidos, pois, as leis citadas neste trabalho não são totalmente eficientes, vez que o índice de criminalidade virtual ainda é crescente. Desta forma, faz-se essencial a educação e conscientização da sociedade em respeitar os limites do mundo virtual, a intimidade, privacidade alheia para então se evitar os crimes cibernéticos. (PINHEIRO, 2016, p. 342)

A norma brasileira necessita de uma clara atualização para considerar as complexidades presentes no direito digital e especialmente as formas de desenvolver ações danosas para a sociedade em meios digitais, isso pois, a norma atualmente existente parece não considerar as necessidades de proteção em meios digitais.

Fiorillo (2017) informa que o novo marco da internet, também conhecido como Marco Digital, de 2014 e atualizado ao longo dos anos é especialmente complexo, isso pois, seu texto no anteprojeto era extremamente rígido e não se encaixava com o modelo digital e da internet contemporânea.

Fiorillo (2017) desenvolve a compreensão que o marco da internet não fez muito por parte do direito digital e sequer expondo itens que protegem a população com grande força, até mesmo os ditos delitos nela compreendidos como a responsabilidade do uso, não desenvolvem punições ou sequer delimitam um tipo

penal.

O que se pode informar sobre o marco da internet é que ele foi desenvolvido com intenções de desenvolver um marco para a internet, porém acarretou em uma ação de menor força do que o esperado, isso pois, o local da internet já está em um desenvolvimento que vai além dos poderes do Estado. (FIORILLO, 2017)

> Não obstante, fato notório é a expansão da odiosa prática de violação da intimidade de diversas mulheres por intermédio da rede mundial de computadores, com a divulgação não autorizada de imagens, áudios, dados e informações pessoais, que a ela pertencem, motivo que bastou para o nascimento do citado projeto com o propósito de engrandecer a lista de formas de violência doméstica e familiar contra a mulher.
> Sabe-se que isso abre espaço para a chamada “pornografia de vingança”, também conhecida por revenge porn, que pode ser conceituada como uma das várias formas de violência moral, mas somada ao objeto sexual, pela qual alguém publica em redes virtuais e distribui por meio de outros aparelhos conectados à rede, sem o consentimento da vítima, fotos ou vídeos de conteúdo sexual explícito ou com nudez. (BRASIL, 2018, p. 214)

A norma do marco da internet tratou de dar um benefício para a proteção nas redes que foi a possibilidade de adequar os crimes atuais para as possibilidades em que se utilize a internet como meio de cometer qualquer crime, inclusive criando mais complexidades para os delitos de compartilhamento de imagens intimas, como a lei Carolina.

> Por isso, ao modificar a Lei Maria da Penha e acrescentar um novo delito ao Código Penal, o Projeto de Lei nº 5.555/2013 – hoje em trâmite perante o Senado Federal, aguardando votação – mostra-se essencial para assegurar às pessoas, em especial às mulheres, maior proteção no âmbito da moral subjetiva e no ambiente familiar, erradicando cada vez mais a violência doméstica.
> A proposta tende a acrescentar valores indispensáveis à comunidade brasileira, que procura incessantemente instrumentos capazes de combater a criminalidade dos tempos modernos, sobretudo no que se refere aos direitos de dignidade das mulheres, além de incluir o direito à comunicação como condição fundamental para o nivelamento dos direitos femininos no Brasil. (BRASIL, 2018, p. 217)

É importante ainda observar o percurso histórico da Lei 12.735/2012 que dispõe sobre crimes cometidos na área de informática, sendo seu maior item a criação de órgãos especializados da polícia judiciária para o combate a crimes em rede de computadores.

A Lei 12.735/2012 nasce como o Projeto de Lei (PL) 84/1999, mais conhecido como a Lei Azeredo, em razão de seu propositor do projeto Eduardo Azeredo. Dornelas (2020) apresenta que esta norma é de extrema importância para o combate de crimes cibernéticos, vez que criou polícia especializada com conhecimento técnico para investigar crimes em meio digital,

Dornelas (2020) ainda apresenta que o desenvolvimento desta lei se vê em parte concretizada, existindo sim as delegacias especializadas e e policia própria para o combate dos crimes em meio digital, porém sem a efetividade devida e sem meios de punição devida dos crimes em meio digital, diante de uma lei penal omissa e falta de recursos.

Há ainda a Lei Geral de Proteção de Dados (LGPD) que visa uma proteção do meio digital e especialmente uma ação de desenvolvimento de limites para armazenamento de dados dos usuários em meios digitais. Tal norma é vista como uma proteção ao consumidor, ao usuário digital e bem como um marco para evitar a manipulação digital. (SOUZA, 2020)

Tais normativas servem para garantir a proteção do usuário, garantia de punibilidade para crimes cometidos em meio digital. As informadas normas ainda prestam o papel de atualizam o ordenamento brasileiro para garantir a aplicação de leis comuns no meio digital.

3 ANÁLISE ACERCA DA IN(EFICÁCIA) DA LEGISLAÇÃO PENAL FRENTE A INCIDÊNCIA DOS CRIMES CIBERNÉTICOS

Os crimes cometidos por meio de locais digitais detêm a complexidade de serem de difícil identificação, podendo acarretar em fácil impunidade para os criminosos e ainda mais mascarar o crime e assim este sequer chegando a ser investigado.

O meio digital permite o anonimato para a pessoa usuária de redes sociais, perfis digitais e até mesmo em certas prestações de serviços. Este anonimato dá aos usuários tanto uma segurança para a sua privacidade e bem como impedem a sua identificação em casos de crime ou de abusos dos meios digitais que violem termos de serviço ou qualquer direito autoral. (SILVA, 2012)

O Meio digital apresenta não somente um anonimato básico de proteção a identidade do usuário, mas sim podendo existir um anonimato em absoluto, sem a possibilidade de identificação de nenhuma forma. O Anonimato extremo das redes digitais ocorre em razão do usuário pode se negar a apresentar informações verdadeiras no momento de cadastro em um portal ou uma rede social e se utilizar de meios de criptografia para impedir seu rastro digital. (SILVA, 2012)

Já para Pinheiro (2016) o anonimato na rede digital é uma questão que não é tratada por parte do direito e deveria ser, isso pois, muito embora o anonimato seja possível no mundo real, há a necessidade de informar sua identidade acertas autoridades, quando necessário.

> O Direito Digital tem o desafio de equilibrar a difícil relação existente entre interesse comercial, privacidade, responsabilidade e anonimato, gerada pelos novos veículos de comunicação. Esta equação só pode ser equilibrada se socialmente aceita e cobrada mediante procedimentos de vigilância e punibilidade que devem ser determinados pelo próprio Direito Digital. (PINHEIRO, 2016, p. 53)

Pinheiro (2016) defende a necessidade de um ramo específico de direito digital, que trata da aplicação e regramentos específicos do meio digital, isso pois, a maioria das normas atuais não foi pensada para aplicação em meio digital e com isso sendo necessárias de atualização.

Certo é que as normas brasileiras não foram pensadas para aplicação quando há um crime em meio digital, assim podendo existir uma fácil possibilidade de o agente do fato criminoso se esquivar do tipo penal por argumento de não ser ele o agente do fato, não existir provas do fato e até mesmo se utilizar de quistos como o *in dubio pro reo* para se esquivar da punição. (BRASIL, 2018)

> O crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual; contudo, em certos casos, o crime não (PINHEIRO, 2016, p. 164)

O meio digital e sua complexidade em identificar a pessoa que faz diversas ações neste meio ainda dá a margem para que o agente do fato criminoso conteste a

autoria do crime, podendo ser informado que um usuário com seu nome não é de fato ele ou que sua conta foi indevidamente invadida para cometer o fato criminoso. (BRASIL, 2018)

Neste sentido, surge a dúvida sobre as provas no meio digital, como pode se obter provas eletrônicas e a validade de tais provas, vez que são essenciais para punir o criminoso e até mesmo para poder dar a materialidade e autoria do fato criminoso.

> Não há nenhuma legislação brasileira que proíba ou vete a utilização de prova eletrônica. Ao contrário, o Código Civil e o Código de Processo Civil aceitam completamente o seu uso, desde que sejam atendidos alguns padrões técnicos de coleta e guarda, para evitar que esta tenha sua integridade questionada ou que tenha sido obtida por meio ilícito]. Logo, o que realmente existe, novamente, é o preconceito quanto ao tipo de prova, pois todos nós temos medo (insegurança) daquilo que não conhecemos. (PINHEIRO, 2016, p. 118)

É certo que itens eletrônicos servem, no direito civil, como uma prova melhor que algumas provas físicas, tais como controles de acesso que em sua forma eletrônica são mais confiáveis do que os livros físicos que podem facilmente ser alterados. (MENDES, 2012)

Quanto a provas em direito criminal, o uso de provas colhidas do meio digital é mal aplicado no país, isso pois, encontrar provas de tal fato delituoso costumam apenas dar a materialidade e não a autoria do crime. Mendes (2012) apresenta que a falta de leis específicas sobre provas do meio digital torna o papel do Ministério Público árduo, não podendo utilizar provas que são circunstanciais e sequer obrigar órgãos digitais, como redes sociais, que tenham provas sobre autoria e materialidade a fornecer as informações de imediato.

> Podemos afirmar que a tecnologia trouxe mais ferramentas para validação jurídica das provas, algo que se busca há muito, e hoje, por certo, já há força legal muito maior numa prova composta por um email do que apenas um testemunho oral ou um mero fax; o mesmo para uma assinatura digital ou biométrica do que apenas o número de um RG ou CPF anotados a mão sem conferência do documento, ou cuja foto, normalmente, está desatualizada. Afinal, para todos nós, o teste de DNA continua sendo considerado prova inequívoca de autoria, apesar de não ter lei e não ser 100% de certeza (PINHEIRO, 2016, p. 120)

Os dados do Ministério Público apresentam a possibilidade de uso de

agentes infiltrados, busca por rastros digitais, apreensão de materiais físicos que contenham dados de informática e acesso a contas e perfis por meio de quebra de sigilo telemático como os principais meios de prova de crimes digitais. (BRASIL, 2018)

Nota-se que a ação de obrigar meios digitais como as redes sociais a fornecer informações é ato que não faz parte dos meios principais por busca de provas para constatar a autoria e materialidade de um fato criminoso. Isto ocorre em razão da maioria dos meios digitais de redes sociais prezar por criptografia de seus dados, prezar também por um direito ao anonimato e privacidade dos usuários. Assim, o próprio meio digital das redes sociais mais comuns, como Twitter, Facebook e Instagram, permitem e até auxiliam o anonimato que pode vir a favorecer a impunidade de crimes digitais. (BRASIL, 2018)

O fato das redes criptografadas e ainda mais a possibilidade de o usuário utilizar de meios rígidos de criptografia, com o auxílio de programas ou até da própria rede digital, permite e facilita o anonimato e esconde os rastros digitais. Com isso, a busca por provas de autoria fica prejudicadas e pouco se pode fazer em casos de existência de criptografia. Este fato auxilia a impunidade e ainda mais permite o desenvolvimento de um anonimato criminoso para propagas crimes de ódio, racismo, calunia e injuria. (FIORILLO, CONTE, 2017)

Fiorillo e Conte (2017) apresentam que crimes em ambiente digital são facilitados e até recorrentes, porém não sendo investigados e muito menos punidos em razão da baixa possibilidade de punição e da permissibilidade do ambiente digital em manter o usuário anônimo.

Souza (2020) apresenta que apesar de existirem indivíduos especializados em desenvolver invasão de dispositivos, roubo de dados e crimes cibernéticos específicos, tais como os hackers e crackers, porém a maior parte de crimes do meio digital são comuns e direcionados a pessoas, como os crimes contra a honra.

Pinheiro (2016) segue o mesmo sentido, informando que muito embora existam indivíduos especializados em cometer crimes digitais, a ação criminosa pode se enquadrar em um crime comum, tal como extorsão ou estelionato. Assim, os indivíduos mais comuns com poucos conhecimentos que cometem crimes digitais são pessoas comuns e até sem conhecimento especializado no ramo da informática

Em exemplo de como pessoas comuns sem conhecimento técnico específico de informática comentem tais crimes, o Projeto de Lei (PL) 2068/2020 visa aumentar as penas para o crime de estelionato cometido por indivíduo preso que se

utilize de aparelho de comunicação móvel. A exposição de motivos desta norma se dá em razão de quadrilhas e criminosos individuais recorrentemente cometendo crimes por meio de celulares, em ligações e até mesmo em redes sociais, mesmo estando em estabelecimentos prisionais. (BRASIL, 2021)

Em mesmo sentido o famoso Golpe dos Nudes que são formas de estelionato cometidos por meio das redes sociais, ficando bem famosos no período de 2020 e 2021. Tal golpe se constitui como a criação de um laço do criminoso com a vítima, levando a troca de imagens sensuais e posterior ameaça de exposição a sociedade ou um simulado boletim de ocorrência, assim requerendo valores para evitar a exposição vexatória ou a suposta persecução penal. Normalmente os indivíduos que cometem tais crimes são quadrilhas com pouco conhecimento de informática e apenas com conhecimento básico do uso das redes sociais ou indivíduos presos com acesso a smartphones. (ISTO É, 2021)

Existe ainda até o fato de crimes graves serem cometidos por meio digital, como extorsão e até mesmo o estupro mediante ameaça e sem contato físico, em tais casos é comum o agente do fato se blindar e buscar o anonimato com a finalidade de cometer o crime e se esquivar da persecução penal. Oliveira (2015) informa que em diversos casos existe uma engenharia social para obter dados das vítimas de um crime com a finalidade de extorsão ou ameaça para obter vantagem sexual, em tais casos o agente criminoso inicia sua campanha criminosa já no anonimato e com diversas barreiras que impedem a sua identificação.

No caso de crimes sexuais, existe a possibilidade até de estupro sem contato físico, quando o agente imputa grave ameaça a vítima para que aquele satisfaça suas lascívias. Tal possibilidade é pouco vista no direito pátrio, mas já se concretizou em diversos casos e em sua maioria existindo a impunidade em razão do anonimato.

É evidente que o meio digital dá margens plenas para que o agente criminoso possa se blindar com o anonimato e ainda mais se esquivar da persecução penal após cometer o crime. Assim há uma clara necessidade de regulamentação deste direito de privacidade e de um indevido anonimato para cometimento de crimes.

Existe ainda uma grande complexidade do meio digital com itens econômicos, isso pois, a revolução do dinheiro digital permite até mesmo um anonimato de pagamentos e criando ordenamento econômico diverso daquele controlado por parte do Estado. Souza (2020) expõe que as moedas de *blockchain*,

isto é, o dinheiro digital garante um anonimato em pagamentos de qualquer valor.

Souza (2020) apresenta que a evasão fiscal é facilitada com as moedas digitais e até mesmo permitindo uma forma de lavagem de dinheiro que seja advindo de fonte ilícita como o tráfico de drogas. O meio digital permite complexas formas de movimentar valores fora do controle do Estado e assim se utilizar deste meio para cometer crimes financeiros.

Souza (2020) informa que os meios digitais permitem o uso do anonimato como a principal forma para se esconder de crimes, sejam crimes financeiros, crimes contra a honra, contra a dignidade e liberdade sexual e até mesmo incitação criminosa em fóruns para este fim específico.

O anonimato parece ser o grande fator que demonstra a possibilidade de se evadir das punições, isso pois, o Estado ou o ofendido não pode buscar a punição quando não se sabe a autoria do fato criminoso. Essa impunidade é recorrente em redes sociais que não cooperem com os órgãos de justiça ou até mesmo prezem por um direito ao anonimato e extrema proteção a informações pessoais.

Fica claro como o ambiente digital permite até mesmo crimes graves como a extorsão e estupro, porém a punição de tais crimes fica prejudicada diante de um anonimato e até mesmo uma possibilidade de existir uma ação dos meios digitais em proteger a privacidade ou anonimato.

CONSIDERAÇÕES FINAIS

Diante de todas as informações apresentadas, considerando a flexibilidade do ambiente virtual e a falta de grandes normas brasileiras que regulamente corretamente o meio digital, existe uma clara facilidade no anonimato nas redes e assim possibilitando a impunidade.

O meio ambiente é especialmente flexível e permite a qualquer indivíduo com acesso à rede mundial de computadores a acessar tal meio, assim podendo o fazer facilmente na atual era digita. É evidente que, no Brasil, o acesso ao meio eletrônico é bem disseminado e difundido na sociedade.

Este meio ambiente digital é comumente de finalidade social, isto é, utilizado para se comunicar com outros indivíduos ou grupos de pessoas,

especialmente sendo utilizado para acesso de redes sociais e meios de relacionamento.

O direito brasileiro não trata especialmente de normas gerais para regulamentar o meio digital, apenas em casos extremos de grande comoção social ou em tentativas de corrigir problemas graves é que existe uma ação do poder público para editar normas específicas do meio digital.

As maiores normas que se observa no direito brasileiro e que tratam especificamente de questões digitais são a Lei Geral de Proteção de Dados (LGPD) que trata especificamente de armazenamento e distribuição de dados de usuários, a Lei Carolina Dieckmann (Lei 12.737/2012) que trata de invasão de dispositivos informáticos e visa punir a violação de privacidade digital de uma pessoa, existindo ainda o Marco Civil da Internet (Lei 12.965/2014) que trata de princípios e garantias no meio digital e dá a aplicação dos crimes comuns ao meio digital.

É certo que o meio digital é não impede a aplicação das normas comuns para crimes cometidos neste ambiente, assim a lei penal pode ser aplicada em tais meios sem prejuízos. Aplicação da norma é certa, porém a persecução penal fica prejudicada diante da falta de meios para se investigar crimes que ocorrem em um meio que auxilia o anonimato e a privacidade de informações.

A grande complexidade constatada foi a existência de fácil anonimato no meio digital, assim impedindo que a autoria do fato criminoso fique clara e consequentemente frustrando a persecução penal. Os meios de redes digitais, tais como redes sociais, permitem uma privacidade extrema de dados e até mesmo auxiliando no anonimato de indivíduos.

O anonimato frustra a constatação da autoria do crime e consequentemente impedindo a punição do criminoso, isso gera uma impunidade clara e pode permitir que os meios digitais sejam utilizados recorrentemente para que uma pessoa cometa crimes dos mais diversos sem ser punida.

Há uma necessidade de regulamentação sobre a identificação de pessoas no meio digital, deve haver uma forma de impedir o anonimato para se cometer crimes e possibilitar a persecução penal. O cenário atual é de facilidade para a impunidade, diante de um meio digital flexível e sem regulamentação devida, o que permite um usuário ficar impune de violações penais.

REFERÊNCIAS

BUANI, Patrícia Berto. **A compatibilidade entre o ordenamento jurídico brasileiro e a convenção sobre cibercrimes**. Instituto Brasiliense de Direito Público – IDP. Escola de Direito de Brasília – EDB. Curso de Graduação em Direito, 2020.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2**. Crimes cibernéticos** / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília : MPF, 2018.

BRASIL, **PL 2068/2020,** Altera o art.171 do Decreto-Lei n° 2.848, de 7 de dezembro de 1940 – Código Penal, para estabelecer novas hipóteses de estelionato majorado. Folha de Tramitação do Senado. 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2250300. Acesso em 05 Nov. 2021

DORNELAS, Natália Alves. **A resposta estatal quanto aos crimes cibernéticos: uma análise direcionada às leis nº 12.735/2012 e 12.737/2012.** Repositório de Trabalhos de Conclusão de Curso, 2020. Disponível em: http://pensaracademico.unifacig.edu.br/index.php/repositoriotcc/article/view/1727. Acesso em 04 Nov. 2021

FIORILLO, Celso Antonio Pacheco. **O Marco Civil da Internet e o meio ambiente digital na sociedade da informação**: Comentários à Lei n. 12.965/2014. Saraiva Educação SA, 2017.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digita**l. Saraiva Educação SA, 2017.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social** / Antonio Carlos Gil. - 6. ed. - São Paulo : Atlas, 2008.

IBGE. **Pesquisa nacional por amostra de domicílios contínua** - PNAD contínua. Divulgação anual. 2018. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/ liv101631_informativo.pdf. Acesso em: 15/02/2021.

ISTO É, **“Sextortion”: entenda como funciona o golpe dos nudes na internet**. Matéria jornalística, redação Isto É Dinheiro, publicado em 20 de Outubro de 2021. Disponível em: https://www.istoedinheiro.com.br/sextortion-entenda-como-funciona-o-golpe-dos-nudes-na-internet/. Acesso em 05 Dez. 2021

KLEIN, Esther. Teletrabalho e ensino à distância na pandemia: quais são as consequências?. **Revista Arco. Jornalismo Científico e Cultural**. Publicado em 01/10/2020, 10h51. Atualizado 01/10/2020, 15h06. Disponível em:< https://www.ufsm.br/midias/arco/teletrabalho-ead-pandemia/> Acesso em: 15/04/2021.

MENDES, Maria Eugenia Gonçalves; VIEIRA, Natália Borges**. Os Crimes Cibernéticosno Ordenamento Jurídico Brasileiro e a Necessidadede Legislação**

Específica. 20-08-2012 Disponível em: < http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2>. Acesso em 27/03/2021.

OLIVEIRA, Alisson Cortez. **Crimes Cibernéticos**: Ordenamento Jurídico Brasileiro. Curso de Direito da Faculdade São Lucas – FSL. Porto Velho. 62 p. 2015.

PINHEIRO, P. P. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016.

ROCHA, Carolina Borges. **A evolução criminológica do Direito Penal**: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. Jus navegandi, 2013. Disponível em: <http://jus.com.br/artigos/25120/a-evolucao-criminologica-do-direito-penal-aspectos-geraissobre-os-crimes-ciberneticos-e-a-lei-12-737-2012>. Acesso em 27/03/2021.

ROCHA, Lilian Rose Lemos et al. **Caderno de Pós-Graduação em Direito**: Crimes Digitais. Brasília: UniCEUB: ICPD, 2020. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/14602/1/Crimes%20digitais.pdf. Acesso em 29 Nov. 2021.

SANTOS, Samuel Fernandes dos; GOMES, Magno Federici. O meio ambiente digital em face da sociedade de risco: estupro virtual e sextorsão, fenômenos em ascensão. **Direito Público**, v. 15, n. 86, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3097. Acesso em 29 Nov. 2021.

SILVA, Regina Beatriz Tavares da. **Responsabilidade civil :** responsabilidade civil na internet e nos demais meios de comunicação / Regina Beatriz Tavares da Silva, Manoel J. Pereira dos Santos, coordenadores. 2. ed. — São Paulo : Saraiva, 2012.

SOUZA, Allan Rocha de. **Direito digital:** direito privado e internet / Allan Rocha de Souza...[et al.] ; organizado por Guilherme Magalhães Martins, João Victor Rozatti Longhi. - 3. ed. - Indaiatuba, SP : Editora Foco, 2020.

STRASSER, Francislaine de Almeida Coimbra; DE OLIVEIRA, Myllena Gonçalves. **O advento da internet e seus desafios no campo jurídico brasileiro**: breve análise dos dispositivos legais sobre o mundo digital. Colloquium Socialis, Presidente Prudente, v. 03, n. 4, p.6-19 out/dez 2019. Disponível em: 10.5747/cs.2019.v03.n4.s080. Acesso em 21 Nov. 2021