O CRESCIMENTO DOS CRIMES CIBERNÉTICOS NO BRASIL APÓS A PANDEMIA DO COVID-19 À LUZ DO DIREITO PENAL

THE GROWTH OF CYBER CRIMES IN BRAZIL AFTER THE COVID-19 PANDEMIC IN THE LIGHT OF CRIMINAL LAW

MELLO, Leonardo Henrique Chain de[1]
MENDES, Gabriel de Paula Miranda[2]
OLIVEIRA, Vinícius Xingó Tenório de[3]

Doi: *doi.org/10.53426/unicad-2024.v3n1.001*

Recebido: 17 abr. 2024
Revisado: 24 mai. 2024
Aprovado: 09 jul.. 2024

RESUMO

O objetivo principal deste artigo é compreender o porquê de o Brasil ter um alto índice de crimes virtuais, bem como apresentar as principais modalidades de golpes virtuais, e a maneira de agir dos criminosos em cada uma delas. Como, também, abordar sobre os crimes sexuais contra crianças e adolescentes cometidos através da internet, e discorrer a respeito dos ataques às escolas e creches, que se tornou uma modalidade de crime recorrente nos últimos anos no Brasil. Com a deficiência das legislações brasileiras sobre os temas, buscou-se estabelecer uma relação entre o crescimento exacerbado da prática de tais crimes durante o período da pandemia do Covid-19, e o isolamento social imposto à sociedade no ápice do contágio do coronavírus, que trouxe, como consequência direta, a migração massiva das pessoas ao ambiente virtual para realizar atividades diárias, mas que por ora, estavam impedidas de serem realizadas de forma presencial, na tentativa de frear o avanço do número de pessoas contaminadas. A metodologia empregada no presente artigo consistiu na pesquisa descritiva, documental-bibliográfica, na qual o autor realizou a coleta de dados a partir de artigos acadêmicos, livros, doutrinas, legislações, revistas científicas, matérias jornalísticas, com abordagem qualitativa. Ao fim, considerou-se que há uma sensível relação entre o aumento dos crimes cibernéticos e o aumento significativo do uso da internet durante o período da pandemia.

Palavras-Chave: Crimes virtuais; Golpes virtuais; Legislação; Pandemia; Phishing.

ABSTRACT

The main objective of this article is to understand why Brazil has a high rate of virtual crimes, as well as to present the main types of virtual scams, and the way criminals act in each of them. As well as addressing sexual crimes against children and adolescents committed over the internet, and discussing attacks on schools and daycare centers, which have become a recurring type of crime in recent years in Brazil. With the deficiency of Brazilian legislation on the topics, we sought to establish a relationship between the exacerbated growth in the practice of such crimes during the period of the Covid-19 pandemic, and the social isolation imposed on society at the

[1] Docente do curso de Direito e Coordenador do Núcleo de Prática Jurídica da Faculdade Única de Ipatinga; leochain@gmail.com
[2] Bacharel em Direito pela Faculdade Única de Timóteo; gabrieldepaula2399@gmail.com
[3] Docente do curso de Direito; viniciusxingo2@gmail.com

height of the coronavirus contagion, which It brought, as a direct consequence, the massive migration of people to the virtual environment to carry out daily activities, but which for now were prevented from being carried out in person, in an attempt to slow the increase in the number of infected people. The methodology used in this article consisted of descriptive, documentary-bibliographical research, in which the author collected data from academic articles, books, doctrines, legislation, scientific journals, journalistic articles, with a qualitative approach. In the end, it was considered that there is a sensitive relationship between the increase in cybercrimes and the significant increase in internet use during the pandemic period.
Keywords: Cybercrime; Legislation; Pandemic; Phishing; Virtual scams.

1 – INTRODUÇÃO

O presente artigo tem como principal objetivo abordar a relevância da positivação do ordenamento jurídico em relação aos crimes cibernéticos, ressaltando a carência de normas concretas e eficazes envolvendo a culpabilidade das condutas ilícitas praticadas dentro do ambiente virtual, criticando a atuação do sistema jurídico brasileiro, tanto o Código Penal, quanto as atuais Lei nº 12.737/2012, Lei nº 12.965/2014, Lei nº 13.709/2018, Lei nº 13.964/2019 e a Lei nº 14.155/2021, que em vez de trazer uma segurança jurídica à sociedade, acabam gerando a sensação de perpetuação de impunidade desses criminosos (Brasil, 2012, 2014, 2018, 2019, 2021).

O fato de existir uma carência de tipicidade dos crimes cibernéticos é deveras preocupante, pois esse substrato estudado no Direito Penal representa uma condição estritamente necessária para a fundamentação jurídica da responsabilização criminal dos indivíduos que praticam essas determinadas condutas delituosas.

Através desse artigo aborda-se as principais modalidades de golpes virtuais, bem como o *modus operandi* dos golpistas em cada uma delas, e o fato de que esse problema se apresenta em níveis alarmantes de milhares de indivíduos que acabam caindo nesses golpes durante os anos de 2020 e 2021, no ápice da pandemia do coronavírus, e que vêm se perpetuando até os dias atuais, diante da desinformação da maioria da população mundial.

Essa ausência de tipicidade, aliada às dificuldades de investigação e repressão dos crimes virtuais no Brasil gera um aumento nas modalidades criminosas efetuadas ou articuladas no meio virtual, como por exemplo os crimes de pedofilia, aliciamento, pornografia infantil, planejamento de ataques a escolas, estelionatos, fraudes, extorsão, roubo de dados, dentre outros golpes praticados através do ambiente virtual.

O momento vivido por todos no auge da pandemia do Covid-19 desencadeou uma série de impactos e repercussões globais, para além do âmbito da biomedicina e epidemiologia, mas também sociais, econômicos, políticos, culturais e históricos, sem nenhum precedente, por ter sido algo novo para toda a sociedade mundial, exigindo-se uma adaptação, ainda que lenta e gradativa de todas as pessoas. Tal cenário, aliado à sobredita carência legislativa gerou um ambiente propício para o aumento nos casos de crimes cibernéticos no Brasil.

Há relevância do tema que se aborda, visto que, a sociedade contemporânea é absolutamente tecnológica, encontrando-se conectada à internet diariamente, onde cada dia mais estão sendo criados aplicativos e plataformas digitais com o objetivo de facilitar a vida das pessoas, e torná-las de certa forma dependentes desse meio. No entanto, a maioria maciça dos usuários dessas tecnologias não tem pleno

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

conhecimento de como se prevenir de ataques de golpistas na internet, nem como proceder no caso de ser vítima de um crime cibernético.

Desta maneira, através deste artigo pretende-se responder ao seguinte problema: Como a falta de leis eficientes, aliada a outros fatores como a pandemia do Covid-19 e a ingenuidade de alguns usuários brasileiros, influencia no aumento das práticas de crimes virtuais nos últimos anos no Brasil?

Na tentativa de responder a esse problema, no presente artigo a metodologia científica usada é devidamente embasada e fundamentada em artigos acadêmicos, livros, doutrinas, legislações, revistas científicas, cartilhas e matérias jornalísticas, existentes até a presente data que possuem relação com o objeto do trabalho. Trata-se de uma pesquisa descritiva, documental-bibliográfica, com análise qualitativa de dados, voltada à resposta ao problema e objetivo central do estudo.

O estudo foi estruturado, além da presente introdução, em um referencial teórico, na seção 2, que visa o estudo de crimes cibernéticos no Brasil e sua repercussão perante o ordenamento jurídico brasileiro; na seção secundária 2.1, trata-se dos crimes cibernéticos e o modo como os criminosos os perpetram; na seção terciária 2.1.1, trata-se da relação da pandemia do coronavírus com o aumento de crimes cibernéticos no país; na 2.1.2, trata-se das principais modalidades conhecidas de crimes virtuais que têm ocorrido no Brasil; na seção 2.2, trata-se dos crimes sexuais praticados no país, usando a Internet como meio; na seção 2.3, trata-se do uso da Internet como meio preparatório de massacres em escolas e creches no país; na 2.4, trata-se da ineficácia e insuficiência da legislação brasileira para repressão a tais crimes; por fim, na seção 3, as considerações finais.

2 – CRIMES CIBERNÉTICOS NO BRASIL

O Brasil se tornou uma seara fértil para a propagação de crimes cibernéticos. Esta seção busca explanar o que os teóricos argumentam sobre essas modalidades de crimes, além de um estudo sobre a eficácia da legislação brasileira na repressão.

2.1 – Dos Crimes Cibernéticos e seu *modus operandi*

O ordenamento jurídico brasileiro ainda se mostra falho e com lacunas evidentes pela ausência de legislações extravagantes que regulem e sancionem de forma severa e efetiva a prática de crimes cibernéticos. Essas lacunas na legislação impõem um ônus ao Magistrado, que, segundo seu próprio entendimento, analisa e aplica a norma que julga ser mais adequada a determinado caso concreto, que por vezes podem até resultar num conflito entre norma e fato no tocante a proporcionalidade (Jesus, 2022).

A carência mais evidente é a da mudança de postura individual de cada um dos operadores do direito, na busca por um órgão jurisdicional que preste um serviço de forma célere, eficaz e justo, visando a real efetivação dos direitos e garantias de todos os brasileiros que recorrerem a ele (Jesus, 2022).

Verifica-se, no Brasil, que um dos pontos que auxilia diretamente nesse crescimento dos crimes cibernéticos é a carência de uma norma penal atualizada que regula e sanciona a prática desse tipo de crime com rigor. O que se tem são normas arcaicas e que tratam de forma superficial essa nova modalidade de crime, sem falar nas penas previstas que são ínfimas, bem como da pequena quantidade de Delegacias Especializadas na repressão dos crimes cibernéticos no Brasil, que não conseguem atender essa quantidade absurda de demanda, o que suscita uma reanálise do processo investigativo e da própria organização das delegacias de polícias (Da Costa; Ribeiro; Wanderley, 2022).

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

O rastro do dinheiro perdido pela vítima, que se refere ao nexo causal entre a lesão ao patrimônio da mesma e o enriquecimento ilícito do criminoso, é o ponto mais árduo de ser averiguado, já que na maioria das vezes, todas essas condutas não são feitas por uma única pessoa, mas sim, por uma organização criminosa, com divisões internas tanto dos agentes, quanto dos indivíduos "laranjas", acima de quaisquer suspeitas, que emprestam suas contas bancárias para os criminosos em troca de uma porcentagem do montante ilícito. A definição desse tipo de organização, e a pena prevista aos indivíduos que já integraram uma organização dessa natureza é de 3 (três) a 8 (oito) anos de reclusão, e encontra-se prevista respectivamente no art. 1º, §1º; e art. 2º, caput, da Lei nº 12.850/2013 (Brasil, 2013).

É necessário "desmistificar" esse falso discurso de que "a Internet é terra sem lei", pois, assim como a sociedade global passou por diversas evoluções históricas no decorrer dos anos, com a Internet não seria diferente. Em pleno século XXI, pode-se perceber o quão importante a internet se tornou na vida das pessoas, seja para realizar tarefas simples do dia a dia como comprar e vender produtos sem ter o trabalho de sair de casa, bem como o aperfeiçoamento dos meios de comunicação entre os indivíduos, por meio das variadas redes sociais. Sem falar que a internet é uma "réplica virtual" do mundo material, portanto, assim como um indivíduo que infringe regras e normas no dia a dia recebe uma sanção da justiça, com aqueles indivíduos que infringem regras no ambiente virtual não pode ser diferente (Vidal, 2018).

Os aparelhos que permitem o acesso à internet passaram a possuir especificações técnicas cada vez mais sofisticadas, e consequentemente seus possuidores começaram a armazenar milhares de informações e dados pessoais neles, em sua grande maioria sem alguma proteção eficaz contra possíveis invasões, o que serve como um atrativo aos criminosos, que se valem da fragilidade dos usuários. Visando ter sucesso na prática de condutas ilícitas, os criminosos adequam-se às novas tecnologias para obterem êxito nos crimes virtuais, os smartphones e tablets passaram a ser o principal foco dos criminosos para praticar os cibercrimes (Cassanti, 2014).

A forma que os criminosos usam para captar dados pessoais de vítimas se dá a partir de condutas fraudulentas e sutis, que induzem as vítimas ao erro, para que estas enviem todos os dados solicitados, imaginando se tratar de uma solicitação lícita. O termo "engenharia social" consiste em uma técnica tida como base de sustentação usada pelos criminosos que atuam no ambiente virtual precipuamente para induzir usuários ao erro, para que enviem dados confidenciais, ou que cliquem em links que os direcionem a sites infectados por vírus e *malwares*, onde seu dispositivo informático ou telemático fica vulnerável a ataques (AO Kaspersky Lab, 2023).

Nesse sentido, a principal distinção entre um simples ataque virtual e o ataque de engenharia social, é que naquele o invasor irá buscar por vulnerabilidades no servidor da vítima, enquanto neste o engenheiro social irá empregar técnicas de persuasão, através da enganação e exploração da confiança da vítima, sempre estimulando emoções, como a simpatia, a curiosidade, o medo, ou a ganância para obter o acesso remoto ao dispositivo da vítima, e ter livre acesso a suas informações e dados pessoais (Cassanti, 2014).

Outra técnica que serve como base para a prática de crimes virtuais diz respeito ao cibercrime conhecido pelo termo "*phishing"*, que se deriva da junção das palavras em inglês "*fishing*" (que significa pesca; pescaria) e "*phreaks*" (termo que eram conhecidos os primeiros *hackers*), com surgimento na década de 1990, sendo

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

referenciado inicialmente em um fórum de notícias da provedora American Online (AOL) (Araújo; Chicre; Rebello, 2016).

Segundo foi informado pela empresa de segurança de dados mundial Kaspersky Lab. Segundo ela, no ano de 2022 o seu sistema anti-phishing conseguiu bloquear mais de 500 milhões de tentativas de acesso a algum conteúdo fraudulento, o dobro do número de ataques que fracassaram no ano de 2021. Os especialistas da referida empresa conseguiram levantar informações a respeito das principais tendências dentro desse cenário da prática do "*phishing"* em pleno 2022, onde puderam perceber um aumento na ocorrência desses ataques por meio dos seguintes aplicativos de mensagens: WhatsApp, Telegram e Viber, onde seu sistema anti-phishing obteve êxito no bloqueio das tentativas criminosas em 82,71%, 14,12% e 3,17% respectivamente (AO Kaspersky Lab, 2022).

Dentre as principais ações que envolvem o "*phishing"*, vale mencionar os e-mails ou mensagens que contêm links que direcionam o usuário para sites maliciosos; e-mails ou mensagens com oferta de grandes lucros em pouco tempo; publicidades que contêm links para outros sites de notícias, boatos e fofocas de celebridades e famosos; e-mails e mensagens de falsos bancos e de falsos cartões virtuais, entre outros meios (Cassanti, 2014).

Relevante trazer à memória um caso de "*phishing"* que teve grande repercussão, no ano de 2011, em que a atriz brasileira Carolina Dieckmann foi vítima de um ataque de um grupo de hackers, os criminosos obtiveram acesso ao computador pessoal da atriz via e-mail, onde obtiveram várias imagens íntimas da atriz. Os criminosos, não satisfeitos com apenas a posse das fotos, passaram a ameaçar e extorquir a atriz para que ela pagasse quantias exorbitantes evitando que divulgassem tais fotos, a atriz não realizou nenhum pagamento, e sua atitude culminou na divulgação das fotos na internet pelos hackers (Pompeu, 2022).

Diante da exposição da intimidade da atriz, somado ao fato de que até o ano de 2011 inexistia no Brasil uma legislação específica que punisse essa prática criminosa, a justiça brasileira tomou uma providência diante da repercussão midiática em âmbito internacional, e criou a Lei nº 12.737/2012, que ficou "apelidada" de Lei Carolina Dieckmann, onde foi incluído ao Código Penal a previsão legal do crime de Invasão de dispositivo informático e a natureza da ação penal na ocorrência desse delito, respectivamente através do art. 154-A e 154-B, que mais tarde sofreu outra alteração por meio da Lei nº 14.155/2021 (Pompeu, 2022).

2.1.1 – Da relação da pandemia do Covid-19 com o aumento dos crimes cibernéticos

Há uma relação entre o momento da implantação compulsória do isolamento social no Brasil, no auge da pandemia do Covid-19, e como os criminosos tiraram proveito dessa vulnerabilidade mental das pessoas que estavam de certa forma deprimidas e desesperançosas com o futuro de suas vidas naquele cenário. O uso massivo da internet no mundo todo, durante o período de *lockdown*, acabou servindo como válvula de escape do tédio, ansiedade, medo, depressão e da vida monótona, mas que acabaram criando o ambiente perfeito para os criminosos, que viram grandes oportunidades para terem êxito em seus objetivos de obter lucro econômico de maneira ilícita (Da Costa; Ribeiro; Wanderley, 2022).

O isolamento social contribuiu como retrocesso para a sociedade contemporânea, no que diz respeito à vulnerabilidade e exposição dos usuários desinformados em sites e plataformas virtuais que não são seguros. Os criminosos

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

virtuais agem contra aqueles que julgam mais vulneráveis e o número de vítimas desses tipos de crimes não para de subir (Da Costa; Ribeiro; Wanderley, 2022).

Segundo o então Corregedor Nacional de Justiça, Ministro Humberto Martins, durante sua participação em um Seminário Virtual realizado em 2020, intitulado como *"Criminalidade em tempos de Covid-19: atuação do sistema de justiça"*, é necessária a adequação do ordenamento jurídico brasileiro a essas novas condutas delitivas no ambiente cibernético, cabendo ao Estado aprimorar ordenamento para impedir a prática desses crimes, evitando prejuízos financeiros e patrimoniais às pessoas, às empresas e ao poder público" (Martins, 2020).

2.1.2 – Das Principais Modalidades de Golpes Virtuais

Essa seção tratará de modalidades mais recorrentes de crimes cibernéticos e como se operam, visando maior esclarecimento e entendimento de como as vítimas são influenciadas a ceder à ação dos criminosos.

2.1.2.1 – *Do Golpe de clonagem do WhatsApp*

Nessa modalidade, o estelionatário entra em contato com a pessoa através de ligação telefônica ou por mensagem de *WhatsApp*, se passando por funcionário de um banco, ou de site de compra e venda online, ou de rede social. Usando de sua *expertise* criminosa, ele informa à pessoa que é necessário que ela envie para ele o código que chegará por SMS no seu smartphone, pois, esse código "seria" para regularizar uma situação cadastral daquela pessoa na plataforma representada pelo golpista. Esse código, é o *PIN*, um código de autenticação da conta de *WhatsApp*, que permite que aquela conta possa ser acionada em outro smartphone, no caso em posse do criminoso, para que este tenha livre acesso a tudo que esteja armazenado na conta do *WhatsApp* da vítima (DPE-DF; DPE-TO; PCDF; PCMG; PCRS; PCSP, 2022).

2.1.2.2 – *Do Golpe do "PIX Falso"*

Outra modalidade que diariamente faz diversas vítimas é o golpe do "PIX falso", que consiste na ação daqueles criminosos que entram em contato com a vítima, seja por meio de chamada telefônica ou o mais comum pelo aplicativo *WhatsApp*, se passando por comprador e demonstrando interesse real em comprar algum produto anunciado pela pessoa em uma plataforma de comércio online, porém, no momento de realizar o pagamento de fato, ele envia à pessoa a foto do comprovante de pagamento PIX falso, ele edita com auxílio de aplicativos a foto do comprovante, inserindo nele seu nome, número do CPF, e o valor da quantia paga, induzindo a pessoa a acreditar que o pagamento foi realizado (DPE-TO; PCRS; PCSP, 2022).

2.1.2.3 – *Do Golpe do Boleto Falso*

Também existe a modalidade do golpe do boleto falso, na qual o criminoso emite um boleto bancário falso e o envia para a vítima, em nome de uma empresa que a própria vítima tem uma confiança e/ou vínculo comercial, e esta acaba realizando o pagamento daquela quantia achando que está pagando por um produto ou serviço, quando na verdade o boleto em si não representa nenhum tipo de compra (DPE-DF; DPE-TO; PCMG; PCRS; PCSP, 2022).

2.1.2.4 – *Dos Golpes praticados nas Plataformas de Compra e Venda Online*

Os golpes praticados nas plataformas de compra e venda online, como: OLX, Facebook Market, WebMotors buscam pessoas que anunciaram determinado produto, entram em contato com o vendedor, expressando o interesse em comprá-lo,

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

enviam um falso comprovante de TED, e na data marcada da entrega do produto, evitam demorar conversando sobre a venda, e rapidamente pegam o produto e fogem, sendo que as vítimas só se dão conta que caíram em um golpe quando percebem que o depósito não ocorreu (DPE-DF; DPE-TO; PCRS; PCSP, 2022).

2.1.2.5 – ***Dos Golpes praticados por meio da criação de Sites Falsos ou dos Perfis Fakes nas Redes Sociais***

Outra hipótese de atuação dos criminosos diz respeito à criação de sites ou perfis falsos nas redes sociais como Instagram, Facebook, Telegram, *WhatsApp*, mediante o envio de spams para o e-mail do comprador; a oferta de produtos com valor muito abaixo do valor de mercado; anúncios e propagandas através de links patrocinados; etc (DPE-DF; DPE-TO; PCMG; PCRS; PCSP, 2022).

2.1.2.6 – ***Do Golpe do Falso Emprego***

Após a pandemia do coronavírus muitas pessoas perderam o emprego e ficaram numa situação financeira bem complicada. A forma de agir dos criminosos resume-se no envio de mensagem de texto via SMS e *WhatsApp* para a vítima ofertando uma vaga de emprego em uma grande empresa nacional ou em filial de uma empresa estrangeira, com a promessa de um alto salário, e na modalidade *home office.* Nessa mesma mensagem, os criminosos adicionam um link, e solicitam que a pessoa interessada realize o cadastro através dele, no qual a pessoa é redirecionada a um site falso, que capta seus dados e documentos (DPE-DF, 2022).

2.1.2.7 – ***Do Golpe da Selfie***

Outra modalidade de golpe praticado no ambiente virtual, e que vêm fazendo milhares de vítimas até os dias atuais, é o golpe da selfie. Criminosos enviam um e-mail "*phishing"* para pessoas, passando-se por um banco, rede social, ou empresa de pagamentos online, com uma mensagem, que diz que, por medidas de segurança, é necessário que a pessoa clique em um link para confirmar sua identidade. Quando a pessoa clica nesse link, é redirecionada para outra página, exigindo-se que preencha um formulário, escrevendo suas informações pessoais como endereço, número de telefone, e também o upload de uma foto tipo selfie da pessoa, com algum documento de identificação pessoal. Uma vez munidos dessas informações pessoais, os golpistas podem realizar diversas compras, além de abrir outras contas em bancos online em nome da vítima. (DPE-TO; PCSP, 2022).

2.1.2.8 – ***Das Fraudes no Recebimento do Auxílio-Emergencial***

Durante os dois anos de pandemia do coronavírus foi instituído tal benefício para compensar o afastamento de algumas pessoas do seu trabalho. Houve muitos casos em que pessoas reclamaram de tentar se inscrever e receberem a mensagem do aplicativo da Caixa Econômica Federal de que aquele número de CPF, já havia recebido o auxílio, o que certamente foi feito por criminosos que se passaram pela vítima (PCRS, 2022).

2.1.2.9 – ***Do Golpe do Amor ou do Namoro Virtual***

Os criminosos também passaram a induzir a erro indivíduos fragilizados emocionalmente, que buscavam novos relacionamentos, notadamente na pandemia, quando uma parcela da sociedade passou a adotar cada vez mais os relacionamentos

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

a distância, recorrendo às redes sociais e aplicativos de relacionamento (Gonçalves, 2022).

Entraram em cena os conhecidos golpe do amor, golpe do aplicativo Tinder, golpe do "Don Juan", golpe do namoro virtual, em que os criminosos direcionam sua atuação na criação de perfis fakes de homens e mulheres atraentes, nos aplicativos de relacionamentos como o Tinder, onde fazem um filtro, através do método *"phishing"*, das pessoas mais suscetíveis a "morder a isca de um falso amor", e então, entram em contato com essas pessoas, usando de jargões e palavras sedutoras, fazendo juras de amor, tudo isso para ganhar a confiança da vítima, obtendo seus dados pessoais, empréstimos e outras formas de golpe (DPE-DF; DPE-TO; PCMG; PCRS; PCSP, 2022).

2.1.2.10 – *Do Golpe do Nude*

Para obter vantagem econômica indevida, por meio do constrangimento e de grave ameaça, criminosos induzem a vítima a enviar fotos íntimas. De posse do material, passam a extorqui-las, ameaçando expor suas fotos (DPE-DF; PCRS; PCSP, 2022).

2.1.2.11 – *Do Golpe do Falso Delegado*

Em casos semelhantes ao golpe do Nude, criminoso se passando por um Delegado de Polícia, que dias após a troca do conteúdo íntimo, entra em contato com o homem abordado pelo *WhatsApp*, onde informa que a garota que "trocou nudes" se trata de uma menor de idade, e que os pais da suposta menor ficaram muito nervosos e abalados com o acontecido, e logo que ficaram sabendo compareceram à Delegacia. O falso Delegado ameaça abrir um inquérito policial pelo crime de pedofilia contra o homem, mas explica nas mensagens que caso o homem realize o pagamento de certa quantia, tudo isso com o objetivo de extorquir a vítima, para que esta realize a transferência de altos valores, com receio da responsabilização criminal (UOL SP; R7 MG, 2023).

2.2 – Dos Crimes de Estupro de Vulnerável, Aliciamento, Assédio e Pornografia Infantil praticados no ambiente virtual

O período de *lockdown* durante a pandemia propiciou o ambiente mais que perfeito para crimes virtuais, já que o lazer das famílias passou a ser preferencialmente pelo smartphone, computador e videogame, permitindo que os pequenos conversassem, jogassem e brincassem com seus amigos de forma online. Porém, esse ambiente virtual também é uma terra obscura e perigosa, ainda mais para menores que não foram bem instruídos por seus pais ou responsáveis acerca dos cuidados que devem ser tomados nesse ambiente (Santos, 2022).

Cada vez mais os pais têm usado os smartphones para manter as crianças entretidas e distraídas com jogos, vídeos, desenhos, músicas, e em alguns casos julgam serem necessários que crianças tenham o próprio aparelho celular, para se comunicarem com eles. Uma vez dentro do espaço virtual desacompanhados de seus pais e responsáveis, as crianças ficam extremamente vulneráveis a ações dos criminosos sexuais, por meio de assédio e aliciamento, puníveis com sanção de 1 (um) a 3 (três) anos de reclusão, segundo o art. 241-D da Lei nº 8.069/1990; além da prática de atos libidinosos, que configura o crime de estupro de vulnerável, punível com a sanção de 8 (oito) a 15 (quinze) anos de reclusão, e está previsto no art. 217-A, caput, do Código Penal (Brasil, 1940; 1990).

Quando os pais “postam” fotografias e vídeos de seus filhos, recém-nascidos, bebês e crianças, e o cibercriminoso tem acesso a esse tipo de conteúdo, este então posta isso na *Deep Web*, e realiza diversas montagens nas fotos, incluindo nelas a nudez ou cena de sexo explícito, e divulgam o produto final em sites e fóruns, onde outros indivíduos passam a ter acesso, ou ainda, comercializam vídeos e fotos de crianças nessas condições, cometendo assim, em ambos os casos o crime de pornografia infantil, com condutas típicas previstas nos art. 240; art. 241; art. 241-A; art. 241-B; art. 241-C do ECA (Brasil, 1990).

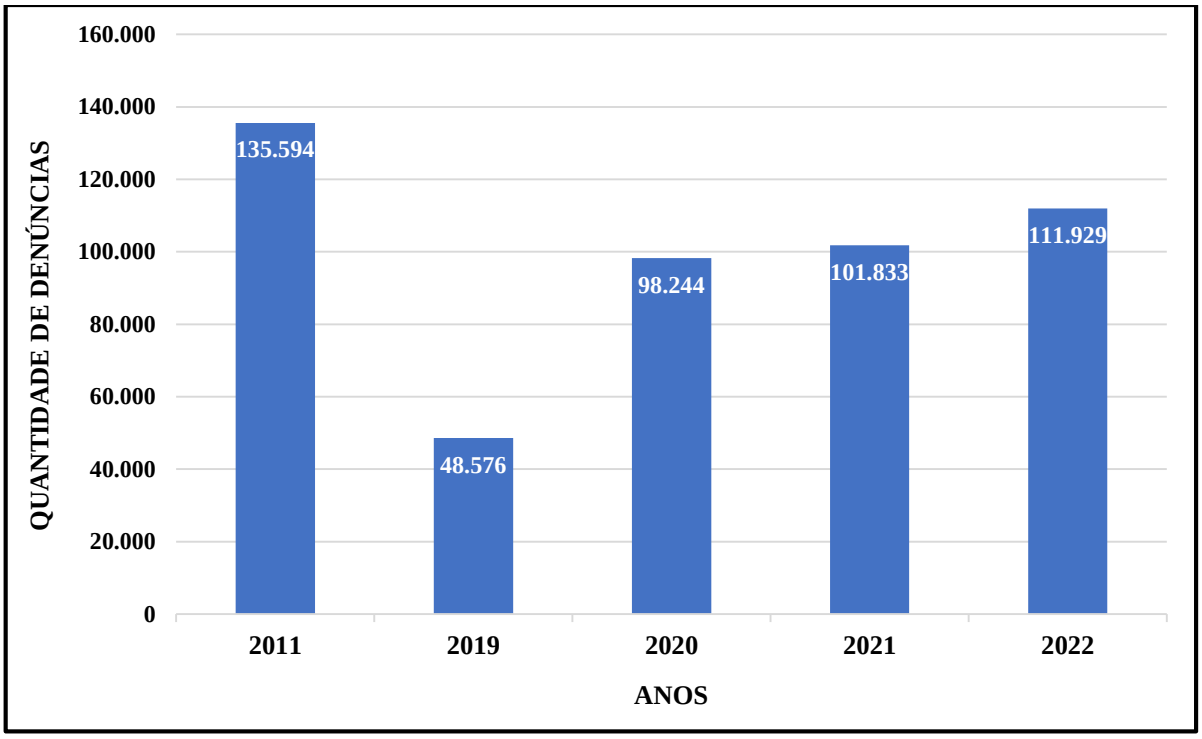
É arriscado expor crianças e adolescentes a esse risco, pois quando os pais se dão conta que seus filhos foram vítimas de um crime, já é tarde demais. Deve haver uma diligência maior dos adultos no tocante aos conteúdos que as crianças acessam diariamente, como forma de prevenção para que seus filhos não tenham sua inocência roubada ou desvirtuada por um criminoso sexual (Santos, 2022).

De acordo com o site BBC News Brasil (2023), dados apresentados pela organização britânica *Internet Watch Foundation* (*IWF*), demonstram que no ano de 2022, a *IWF* registrou mais de 63 mil páginas que mostram vídeos e imagens de abuso infantil, onde as próprias crianças tiram fotos e filmam a si mesmas enquanto são coagidas e ameaçadas pelos predadores da internet. A organização ainda pontuou que antes da pandemia do coronavírus, no ano de 2019 o registro era de 5 mil páginas com esse tipo de conteúdo, retratando um crescimento estrondoso desse tipo de conteúdo que vêm sendo publicado no ambiente virtual.

Conforme dados da ONG Safernet, do dia 1º de janeiro de 2023 ao dia 31 de abril de 2023 a plataforma recebeu 23.777 denúncias de imagens de abuso e exploração sexual infantil online, um aumento de 70% nesses meses, em relação a esse mesmo período no ano de 2022, onde a plataforma recebeu 14.005 denúncias deste gênero. No ano de 2022 o total de denúncias recebidas pela ONG foram de 111.929, uma média assustadora de 306 denúncias por dia. Esse problema assola o mundo desde os primórdios do uso da internet e, ao fazer uma análise da crescente quantidade de denúncias de pornografia infantil, do período inicial da pandemia do Covid-19, no ano de 2020 até os dias atuais, a análise do gráfico abaixo, com dados da ONG Safernet, faz notar o crescimento gradativo desse crime (Safernet, 2023).

GRÁFICO 1 – Denúncias de Pornografia Infantil na Internet

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1



Fonte: Elaborado pelo autor com base nas informações da ONG SaferNet (2023)

A esperança que se mostra iminente é a aprovação do Projeto de Lei nº 4319/20 que está em trâmite na Câmara dos Deputados, que têm dentre seus objetivos, alterar pontualmente o Estatuto da Criança e do Adolescente, em seus art. 240; art. 241; art. 241-A; art. 241-B, que tratam dos crimes de Produção, Armazenamento, Divulgação e Venda de Pornografia Infanto-Juvenil, sugerindo um aumento da pena atual para o patamar de 8 (oito) a 12 (doze) anos de reclusão. Além dos art. 241-C e art. 241-D, que tratam dos crimes de Simulação da participação de criança e adolescente em cena de sexo explícito ou pornográfica, e dos crimes de Aliciamento, Assédio e Pedofilia, sugerindo um aumento da pena atual para o patamar de 4 (quatro) a 8 (oito) anos de reclusão, esforçando-se para conter o aumento do índice de crianças e adolescentes vítimas desses crimes sexuais após a pandemia do coronavírus (Brasil, 1990).

2.3 – Dos Ataques em Escolas e Creches e sua relação com crimes cibernéticos

O isolamento social decorrente da pandemia do coronavírus facilitou a entrada de qualquer tipo de pessoa no ambiente virtual, sendo possível assumir outras identidades virtuais (perfis), e por meio deles expressar discursos de ódio contra pessoas e instituições nacionais, além de incitar a prática de delitos. As comunidades virtuais tornaram-se palcos para a exposição de ideias de práticas de massacres no ambiente escolar, onde os cibercriminosos buscam outros indivíduos que possuam um padrão ideológico semelhantes a eles, onde se inspiram em outros acontecimentos dessa natureza que tiveram grandes repercussões, como é o caso dos atentados na *Columbine High School* (1999), e *Virginia Polytechnic Institute and State University* (2007) nos Estados Unidos, além dos ocorridos no Brasil, como os massacres de Realengo (2011), e de Suzano (2019) (Barbosa; Guimarães, 2022).

O Brasil tem se deparado com uma onda de acontecimentos chocantes cometidos dentro do ambiente escolar, antes mesmo do período da pandemia do coronavírus. Segundo dados levantados pelo Instituto Sou da Paz (2023), do ano de

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

2002 até o mês de outubro do ano de 2023, o Brasil registrou cerca de 31 ataques a escolas e creches, ceifando a vida de dezenas de pessoas. Esses massacres trouxeram à baila discussões a respeito do tema, sobre como o Estado têm sido falho diante das orquestrações desses massacres, que se dão, ou na *Deep Web*, onde as atividades dos usuários não deixam rastros, ou por meio de aplicativos de conversas, como o *Discord*.

Esse aplicativo vem sendo alvo de duras críticas por não regular efetivamente conversas, fotos e vídeos com conteúdo forte ou proibido, e não realizar a exclusão dos perfis que compartilham tal conteúdo. Dentro do aplicativo, diversos usuários compartilham conteúdos ideológicos (apologia ao nazismo; ao racismo; à misoginia; à prática de automutilação; de atos cruéis contra animais; da exposição sexual; do estupro virtual; além de estimular a prática de ataques às pessoas dentro do ambiente escolar) com o objetivo de atrair outras pessoas que se identificam com os mesmos ideais criminosos. Muitos idolatram indivíduos que já cometeram crimes dessa natureza e até foram mortos, mas que deixaram um legado, um exemplo a ser seguido por seus admiradores. Esse fanatismo serve como combustível para criminosos agirem dolosamente contra a vida de brasileiros de todas as faixas etárias no interior das Instituições de Ensino (Iory; Mariano; Rodrigues, 2023).

O crime de invadir uma Instituição de Ensino e atentar contra a integridade física de pessoas que se encontram nesse ambiente, em regra não se tipifica como crime de Terrorismo, segundo o art. 2º da Lei nº 13.260/2016. Atualmente, existe uma grande lacuna no ordenamento jurídico brasileiro, por não existir uma tipificação específica para quem comete esse tipo de crime. Consequentemente, faz-se necessário que o Estado dê uma resposta à população brasileira, através da elaboração de uma Legislação Extravagante onde será regulado essa nova modalidade delituosa, preferencialmente com penas severas (Brasil, 2016).

2.4 – Da ineficácia e insuficiência atuação da legislação brasileiras para repressão de crimes cibernéticos

No que diz respeito as legislações pátrias que compõem o ordenamento jurídico brasileiro até o momento, e que regulamentam as condutas típicas dos crimes cibernéticos, é possível afirmar que estas por si só não são capazes de repreender as investidas dos cibercriminosos. Nesse sentido é vital ressaltar as disposições expressas dessas legislações que se apresentam como lacunas, falhas estruturais do sistema penal brasileiro (MARTINS, 2017).

2.4.1 – Da Lei nº 12.737/2012 (Lei Carolina Dieckmann)

No que tange à legislação que ficou popularmente conhecida como Lei Carolina Dieckmann, dada as circunstâncias do caso concreto vivido pela atriz brasileira, e pela ausência até aquele momento de uma norma que regulamentasse os crimes cibernéticos no Brasil, e que incluiu os Art. 154-A no Código Penal, porém, atualmente tal medida se mostra insuficiente, por tipificar apenas um dos vários *modus operandi* dos criminosos na prática desses crimes, qual seja a de Invasão de Dispositivo Informático, além de ter previsto sanções penais baixas, se levadas em consideração ao nível de exposição que as vítimas desse tipo de crime acaba sofrendo, e também incluiu o Art. 154-B que tem o objetivo de ressaltar a natureza da ação penal pública condicionada à representação da vítima nesses casos, exceto nos casos em que a vítima da invasão for a Administração Pública Direta ou Indireta,

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

qualquer dos Poderes dos entes federativos (União, Estados e Municípios), ou Empresas concessionárias de serviços públicos, conforme segue.

> 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 (Brasil, 2012).

2.4.2 – Da Lei nº 12.965/2014 (Marco Civil da Internet)

No ano de 2014 o governo brasileiro, com embasamento legal no princípio da governança e do uso da internet, vislumbrando a proteção da privacidade dos usuários na internet, através de um mecanismo que de certa forma assegurasse a inviolabilidade e o sigilo de informações e de comunicações privadas, seguindo a premissa de um dos direitos fundamentais individuais previsto no Art. 5º, X da CRFB/1988, o direito a intimidade, a vida privada, a honra e a imagem das pessoas, o qual assegura direito ao recebimento de indenização por dano material ou moral em decorrência de sua violação, concebeu a Lei nº 12.965, que ficou conhecida como marco regulatório da internet no Brasil (Brasil, 1988, 2014).

Esta recente legislação tentou trazer uma noção geral e abstrata em relação à internet, e também ficou popularmente conhecida como a “Constituição da Internet”, onde passaram a serem previstos direitos e deveres individuais dos brasileiros no momento em que estes usam os meios digitais, evitando ser mais uma legislação que apenas criminaliza as condutas criminosas no ambiente virtual. Essa ideia ampla de direitos e responsabilidades, pauta-se em princípios que devem ser respeitados, dentre eles os que merecem destaque estão dispostos no Art. 3º, I, II, III, IV, VI, da Lei nº 12.965/2014, sendo a garantia da liberdade de expressão, comunicação e manifestação de pensamento; a proteção à privacidade; a proteção de dados pessoais; a preservação e garantia da neutralidade da internet; e a responsabilização dos agentes de acordo com suas atividades delituosas (Brasil, 2014).

Da mesma forma, os direitos individuais dos usuários, partindo do pressuposto que o acesso à internet em si é uma atividade indispensável ao exercício pleno da cidadania, devendo ser resguardados esses direitos também no ambiente virtual, enfatizando-se os previstos no Art. 7º, I, II, III; e Art. 8º da referida Lei. No entanto, conforme dados e informações já abordados nesse trabalho, em referência ao crescimento assombroso dos crimes cibernéticos no Brasil, logo após o período da pandemia do Covid-19, percebe-se que a privacidade, o sigilo e a inviolabilidade das informações, dados e conversas privadas dos brasileiros no ambiente virtual não vem sendo cumprida efetivamente, seja pela dificuldade do rastreamento eficaz dos criminosos pelo Estado, e/ou pelo fato do Estado não conseguir a real concretização

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

da neutralidade da rede, por não existir um monitoramento para aferir o descumprimento de tal norma (BRASIL, 2014).

2.4.3 – Da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais)

Outra tentativa do ordenamento jurídico brasileiro em regulamentar a segurança de dados dos brasileiros no interior do ambiente virtual em seu acesso diário, manifestou-se a partir da promulgação da Lei Geral de Proteção de Dados Pessoais no ano de 2018, sendo esta inspirada na Lei implementada pela União Europeia também em 2018, denominada "*General Data Protection Regulation (GDPR)*". A LGPD buscou ser mais específica no sentido de abranger meramente a proteção de dados de pessoas físicas armazenados no banco de dados online das pessoas jurídicas de direito público e privado (Corrêa, 2022).

A Lei nº 13.709/2018 prevê a responsabilização por meio de indenizações a serem pagas pelas pessoas jurídicas que possuem armazenadas em seu banco de dados, informações e dados de pessoas físicas, que acabam sendo irregularmente divulgados, por não os protegerem de forma eficaz, segundo o Art. 42 da citada legislação. Essa inovação legislativa tornou-se ainda mais relevante após a ocorrência da Pandemia de Covid-19, em virtude da maior interação virtual dos brasileiros ocasionada pelo afastamento social imposto pela OMS. Com o aumento de casos de crimes virtuais relacionado a este novo contexto social, mais relevante se torna a proteção de dados dos usuários por *big techs*, redes sociais e empresas que realizam atividades eletrônicas e administram esses dados (Brasil, 2018).

Tal legislação incluiu em seu bojo requisitos para o tratamento de dados pessoais, inclusive aqueles considerados sensíveis, os pertencentes a crianças e adolescentes, regulamentando tal manejo por entidades públicas e privadas, estabelecendo responsabilidade aos entes que descumprirem os preceitos legais. Também tratou da transferência internacional de dados, da segurança e governança relativas aos dados pessoais, da penalização e responsabilidade dos gestores encarregados pelo vazamento de tais dados e da fiscalização dessas atividades (Brasil, 2018).

2.4.4 – Da Lei nº 13.964/2019 (Pacote Anticrime)

A parcela de contribuição que o Pacote Anticrime trouxe em relação aos crimes cibernéticos se resumiu apenas a inclusão do § 5º no Art. 171 do Código Penal, tipo penal do crime de estelionato, no qual passou a definir a natureza da ação penal pública (sem a necessidade de representação da vítima), quando determinados tipos de pessoas forem vítimas do crime de estelionato, em especial das crianças (até 12 anos incompletos), dos adolescentes (com idade entre 12 e 18 anos), das pessoas portadoras de deficiência mental, dos idosos (com mais de 70 anos de idade), e demais incapazes, bem como da própria Administração Pública Direta e Indireta, segundo a nítida disposição na norma penal brasileira (Brasil, 2019).

2.4.5 – Da Lei nº 14.155/2021

A mais recente legislação que trouxe uma certa reformulação ao ordenamento jurídico pátrio, no que diz respeito a norma penal dotada de caráter sancionador, consiste na Lei nº 14.155/2021, a qual se preocupou em reanalisar alguns tipos penais, mais precisamente no *quantum* de pena aplicável no caso de sua infração. O primeiro tipo penal que sofreu alteração por essa legislação foi o Art. 154-A, caput, §

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

2º e § 3º do Código Penal, onde alargou-se “significativamente” as sanções desses citados pontos.

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
> § 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 2 (dois) a 5 (cinco) anos, e multa (Brasil, 2021).

A segunda alteração executada por tal lei diz respeito à inclusão dos § 4º-B e § 4º-C, I, II no Art. 155 do Código Penal, onde passou a reprimir outra modalidade de furto cometido no ambiente virtual, no caso, o furto mediante fraude por meio de dispositivo eletrônico ou informático, além de passar a prever duas causas de aumento de pena em situações especiais em que este tipo de crime for praticado, com base no pensamento de uma reprimenda com um nível superior que se mostra necessária, para auxiliar no melhor rastreamento e responsabilização criminal dos criminosos que lesam esses grupos de pessoas, por estes infelizmente se mostrarem como mais propensos a serem vítimas desse tipo de furto.

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável (Brasil, 2021).

Por último, mas não menos importante, a Lei nº 14.1555/2021 também teve o cuidado de incluir os § 2º-A e § 2º-B, no Art. 171 do Código Penal, onde passou a prever sobre outra modalidade de estelionato cometido no ambiente virtual, nesse caso, o estelionato cometido por meio de fraude eletrônica, bem como inovou ao seguir o Art. 155, § 4º-C, I do Código Penal, em relação à causa de aumento de que para o criminosos praticarem determinada conduta necessariamente recorrem a utilizar servidores (computadores com um grande poder de armazenamento e processamento, que possibilita a conexão entre milhões de computadores através de uma única rede) com o domínio externo, que não se limita ao território nacional, dificultando ainda mais o seu rastreamento e sua responsabilização.

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> (...)
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

> por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional (Brasil, 2021).

Além de alterar a causa de aumento da pena, prevista no § 4º do Art. 171 do Código Penal que anteriormente se restringia apenas a figura da vítima idosa, acrescentando a figura do vulnerável, e seguiu o Art. 155, § 4º-C, II do Código Penal, ao aumentar o *quantum* de pena que antes era do dobro da pena do caput, e passou a ser de 1/3 até o dobro da pena: "§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso" (BRASIL, 2021).

3 – CONSIDERAÇÕES FINAIS

Imperioso remeter que o presente artigo visou abordar a inexistência de normas concretas que regulem de forma eficaz a culpabilidade dos criminosos diante da prática dos crimes cibernéticos citados no Brasil, principalmente após o período da pandemia do Covid-19. Da mesma forma, buscou-se estabelecer uma relação entre o isolamento social imposto à população brasileira na tentativa de frear o acelerado avanço de contágio do coronavírus (*SARS-CoV-2*) durante os anos de 2020 e 2021, e o aumento demasiado de ocorrências envolvendo os crimes cibernéticos, dada a vulnerabilidade digital de grande parte da sociedade.

A pesquisa desenvolvida buscou expor as principais modalidades de Golpes Virtuais, que continuam fazendo milhares de vítimas no Brasil, apresentando-se o *modus* dos criminosos em cada uma dessas modalidades, como forma de ser mais um a contribuir para a conscientização do maior número de brasileiros possíveis, acerca das precauções que se fazem necessárias para evitar que caiam em algum golpe dessa natureza.

Além disso, foi abordado de forma breve a respeito do crescimento dos crimes contra a dignidade sexual de crianças e adolescentes cometidos no ambiente virtual durante a pandemia do Covid-19, onde foi possível apresentar dados de ONGs e plataformas de controle da internet, responsáveis por receberem notificações e denúncias de compartilhamento de imagens que caracterizam pornografia infantil.

Por meio de dados concretos sobre o aumento da ocorrência desse tipo de crime tanto nos anos de 2020 e 2021, quanto nos anos de 2022 e 2023, retratam que infortunadamente as crianças e adolescentes brasileiros estão à mercê apenas do cuidado e da vigilância dos pais para não o exporem a tais riscos, e desamparados pela legislação brasileira responsável em garantir seus direitos e por não prever penas à altura do nível de reprovação desse tipo de crime.

Acerca das práticas criminosas de organização e execução de ataques a escolas e creches no Brasil, que se mostra como um grande problema nos últimos anos, faz-se necessária a análise fria e minuciosa, de um outro ponto de vista pelos legisladores brasileiros, com vista na prevenção e precaução, pelo fato da preparação desses tipos de ataques se dar através do ambiente virtual, onde alguns dos homicidas até postam manifestos, pensamentos, e diários macabros na internet, como forma de justificar seus atos criminosos.

Da mesma forma, a pesquisa discutiu sobre como o isolamento social exigido pela pandemia do Covid-19 contribuiu para a organização e planejamento no espaço

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

virtual dos ataques à escolas e creches brasileiras, que fez centenas de vítimas nos últimos anos, frente à inexistência de uma norma específica que puna com rigor esse tipo de crime, demonstrando-se uma desatenção ou passividade estatal em seu dever constitucional de punir os indivíduos que cometem crimes dessa natureza, nos termos do art. 144, caput, da CRFB/1988.

Durante o desenvolvimento do presente artigo foram encontradas algumas dificuldades no tocante à escassez de material bibliográfico contemporâneo que discorram estritamente sobre os temas abordados. A forma encontrada para superar esse problema consistiu na leitura minuciosa de artigos acadêmicos publicados na internet onde os autores abordam separadamente as questões argumentadas no referencial teórico, sendo necessária realizar uma fusão entre os conteúdos destes, para uma abordagem coerente e exata.

Embora não abordados na presente pesquisa por estarem fora de seu escopo, outros temas correlatos, cuja a pesquisa se mostra relevante e atraente diretamente ligados ao ambiente virtual são: I – A relação entre o aumento do índice de crianças vítimas de abusos sexuais e estupros durante o período da pandemia e o momento de isolamento social que impossibilitou o convívio social das crianças, o que foi notado apenas no ano subsequente; II –A ampliação de ocorrências dos crimes contra Honra (Calúnia, Difamação, Injúria) e dos crimes de Ameaça e Perseguição (“*stalking”*) cometidos no ambiente virtual durante o período pandêmico.

A resposta ao problema proposto é que a falta de legislações pertinentes e eficazes possibilitam no Brasil, o aumento da quantidade de crimes virtuais, que são, por sua vez, impulsionados por fatores como a pandemia do Covid-19, que influenciou no aumento dos crimes cibernéticos no Brasil, uma vez que o isolamento social vivido pelos brasileiros durante esse período tornou as pessoas mais suscetíveis a caírem em golpes e fraudes virtuais, além da ingenuidade, credulidade e falta de condições financeiras da população brasileira, cumulada com seu despreparo e desatenção em decorrência de sua vulnerabilidade tecnológica, além da dificuldade do rastreamento dos cibercriminosos pelas forças policias ante a ausência de contingente, bem como de recursos financeiros e aparatos tecnológicos que favoreceria a eficaz aplicação do ordenamento jurídico em seu poder-dever de punir tais condutas.

REFERÊNCIAS:

AO KASPERSKY LAB. **Brasil é o país com mais ataques de *phishing* por *WhatsApp* no mundo em 2022, aponta Kaspersky**. 2023. Disponível em: https://www.kaspersky.com.br/about/press-releases/2023_brasil-e-o-pais-com-mais-ataques-de-phishing-por-*WhatsApp*-no-mundo-em-2022-aponta-kaspersky. Acesso em: 15 de julho de 2023.

AO KASPERSKY LAB. **O número de ataques de phishing dobrou para atingir mais de 500 milhões em 2022**. 2023. Disponível em: https://www.kaspersky.com/about/press-releases/2023_the-number-of-phishing-attacks-doubled-to-reach-over-500-million-in-2022. Acesso em: 15 de julho de 2023.

ARAÚJO, Eduardo. CHICRE, Bruno. REBELLO, Gabriel. **PHISHING**. Trabalho acadêmico desenvolvido pelos docentes da Universidade Federal do Rio de Janeiro (UFRJ). Redes de computadores I – 2016.1. Departamento de Engenharia Eletrônica e de Computação (DEL). Publicado em 2016. Disponível em: https://www.gta.ufrj.br/ensino/eel878/redes1-2016-1/16_1/phishing/referencias.html. Acesso em 14 de julho de 2023.

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Diário Oficial da União. Brasília, 05 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 27 de setembro de 2022.

BRASIL. **Decreto-Lei nº 2.848 de 07 de dezembro de 1940**. Código Penal. Diário Oficial da União. Rio de Janeiro, 31 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 28 de setembro de 2022.

BRASIL. **Lei nº 12.737 de 30 de novembro de 2012**. Diário Oficial da União. Brasília, 03 de dezembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 29 de setembro de 2022.

BRASIL**. Lei nº 12.850 de 2 de agosto de 2013**. Diário Oficial da União. Brasília, 05 de agosto de 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 18 de julho de 2022.

BRASIL. **Lei nº 12.965 de abril de 2014**. Diário Oficial da União. Brasília, 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 de setembro de 2022.

BRASIL. **Lei nº 13.260 de 16 de março de 2016**.. Diário Oficial da União. Brasília, 17 de março de 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em: 28 de setembro de 2022.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Diário Oficial da União. Brasília, 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 de setembro de 2022.

BRASIL. **Lei nº 13.964 de 24 de dezembro de 2019**. Diário Oficial da União. Brasília, 29 de abril de 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 29 de setembro de 2022.

BRASIL. **Lei nº 14.155 de 27 de maio de 2021**. Diário Oficial da União. Brasília, 28 de maio de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 29 de setembro de 2022.

BRASIL. **Lei nº 8.069 de 13 de julho de 1990**. Estatuto da Criança e do Adolescente. Diário Oficial da União. Brasília, 16 de julho de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 26 de setembro de 2022.

BRASIL. **Lei nº 8.072 de 25 de julho de 1990**. Diário Oficial da União. Brasília, 26 de julho de 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8072.htm. Acesso em: 28 de setembro de 2022.

CÂMARA DOS DEPUTADOS. **Projeto altera Código Penal para aumentar tempo de prisão por crimes de estupro. Proposta também agrava as penas para**

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

crimes de pedofilia virtual. 2021. Disponível em: https://www.camara.leg.br/noticias/722355-projeto-altera-codigo-penal-para-aumentar-tempo-de-prisao-por-crimes-de-estupro/. Acesso em: 09 de março de 2023.

CARDOSO, Bruna. **Núcleo do Consumidor cria material informativo com dicas para não cair em golpes virtuais**. Site da Defensoria Pública do Estado do Tocantins. Comunicação DPE-TO. Nossas Publicações. Cartilha Guia sobre golpes virtuais. Disponível em: https://www.defensoria.to.def.br/pagina/22639/. Acesso em: 18 de julho de 2022.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro – RJ: Editora Brasport Livros e Multimídia Ltda. 2014.

CORRÊA, Bruna Marques. **A Importância da Lei Geral de Proteção de Dados em Combate aos Crimes Cibernéticos**. Universidade Presbiteriana Mackenzie, São Paulo. 2022. Disponível em: https://adelpha-api.mackenzie.br/server/api/core/bitstreams/472ca665-d2c6-4e8d-9181-6b9bf152060c/content. Acesso em: 20 de julho de 2023.

DIAS, Rodrigo. **Criminosos usam foto de delegado para aplicar "golpe do nudes"**. Site R7 Minas Gerais. 2022. Disponível em: https://noticias.r7.com/minas-gerais/criminosos-usam-foto-de-delegado-para-aplicar-golpe-do-nudes-12042022. Acesso em: 23 de fevereiro de 2023.

GONÇALVES, Dayane Maciel. **O Canto da sereia – da captação de vítimas de estelionato virtual por meio das redes sociais**. 2022. Disponível em: http://repositorio.aee.edu.br/jspui/handle/aee/20162. Acesso em: 20 de julho de 2023.

GUIMARÃES, Augustto de Paula; BARBOSA, Beatriz da Silva Queiroz. **A Escola como palco de Massacres e Atentados Armados**. 2022. Disponível em: https://www.usf.edu.br/galeria/getImage/768/607340100344074.pdf. Acesso em: 20 de julho de 2023.

INSTITUTO SOUDAPAZ. **Ataques em Escolas: Casos com uso de armas de fogo foram três vezes mais letais que os com armas brancas**. 2023. Disponível em: https://soudapaz.org/noticias/ataques-em-escolas-casos-com-uso-de-armas-de-fogo-foram-tres-vezes-mais-letais-que-os-com-armas-brancas/. Acesso em: 22 de julho de 2023.

IORY, Nicolas; MARIANO, Laura. **Ataques em escolas: antes restrito à 'deep web', conteúdo extremista contribui para aumento de casos**. Site do Jornal O Globo. São Paulo. 2023. Disponível em: https://oglobo.globo.com/brasil/noticia/2023/04/ataques-em-escolas-antes-restrito-a-deep-web-conteudo-extremista-contribui-para-aumento-de-casos.ghtml. Acesso em: 09 de junho de 2023.

JESUS, Bruna Souza de. **Crimes Virtuais**. 2022. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/20152/1/2022%20-%20TCC%20-%20BRUNA%20SOUZA%20DE%20JESUS.pdf. Acesso em: 20 de julho de 2023.

MARTINS, Aislan Bruno da Silva. **Crimes Virtuais**. Curso de Direito da Faculdade de Sabará. 2017. Disponível em: https:

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

https://faculdadedesabara.com.br/media/attachments/monografias/Monografia_Crimes-Virtuais_Aluno-Aislan.pdf. Acesso em: 15 de julho de 2023.

POLÍCIA CIVIL/DF. **Cartilhas e Folders**. 2023. Disponível em: https://www.pcdf.df.gov.br/informacoes/cartilhas-e-folders. Acesso em: 16 de julho de 2023.

POLÍCIA CIVIL/MG. **Golpe, só se for nos criminosos**. Cartilhas da PCMG. Disponível em: https://www.policiacivil.mg.gov.br/pagina/servico-cartilhas-pcmg. Acesso em: 18 de julho de 2022.

POLÍCIA CIVIL/RS. **Polícia Civil deflagra Operação Alfarrábio com objetivo de combater o "Golpe dos Nudes"**. Comunicação. Notícias. 2021. Disponível em: https://www.pc.rs.gov.br/policia-civil-deflagra-operacao-alfarrabio-com-objetivo-de-combater-o-golpe-dos-nudes. Acesso em: 22 de março de 2023.

POLÍCIA CIVIL/RS. **Polícia Civil lança nova versão do aplicativo "PC Alerta" e inclui usuários do sistema iOS**. Comunicação. Notícias. 2021. Disponível em: https://www.pc.rs.gov.br/policia-civil-lanca-nova-versao-do-aplicativo-pc-alerta-e-inclui-usuarios-do-sistema-ios. Acesso em: 22 de março de 2023.

POLÍCIA CIVIL/RS. **Polícia Civil mira em organizações criminosas e realiza operação de 5 dias contra estelionato no Estado**. Comunicação. Notícias. 2021. Disponível em: https://www.pc.rs.gov.br/policia-civil-mira-em-organizacoes-criminosas-e-realiza-operacao-de-4-dias-contra-estelionato-no-estado. Acesso em: 22 de março de 2023.

POMPEU, Ana Luiza Brandão Calil et al. **Crimes Cibernéticos: A Ineficácia da Lei Carolina Dieckmann**. 2022. Disponível em: http://65.108.49.104/bitstream/123456789/509/2/Template%20de%20TCC%20Direito%202021%20%281%29.docx.pdf. Acesso em: 20 de julho de 2023.

RODRIGUES, Henrique. **O que é o "desafio do Discord" que estaria por trás de ataques a escolas**. Revista Fórum. 2023. Disponível em: https://revistaforum.com.br/brasil/2023/4/12/que-desafio-do-discord-que-estaria-por-tras-de-ataques-escolas-134212.html. Acesso em: 09 de junho de 2023.

SAFERNET. **Denúncias de imagens de abuso e exploração sexual infantil online compartilhadas pela SaferNet com as autoridades têm aumento de 70% em 2023**. 2023. Disponível em: https://new.safernet.org.br/content/denuncias-de-imagens-de-abuso-e-exploracao-sexual-infantil-online-compartilhadas-pela. Acesso em: 22 de julho de 2023.

SANTOS, Isabela Cardoso dos. **Crimes cibernéticos-ciberpedofilia: o aumento da atividade do pedófilo virtual em tempos de pandemia**. Publicado em: 2022. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/4546. Acesso em: 22 de julho de 2023.

SECRETARIA DE SEGURANÇA PÚBLICA/SP. **Aprenda a se proteger de golpes digitais e a fazer o uso seguro da internet**. Cartilha Crimes Digitais. 2022. Disponível em: https://drive.google.com/file/d/1I13hvAc24lfieHngWAKqiAL19vM85I5a/view. Acesso em: 20 de julho de 2022.

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1

SECRETARIA DE SEGURANÇA PÚBLICA/SP. **Crimes virtuais: aprenda a reconhecer quais os tipos de golpes e como se proteger**. Cartilha Delitos praticados por meios eletrônicos. 2021. Disponível em: https://www.policiacivil.sp.gov.br/portal/imagens/CRIMES%20CIBERN%C3%89TICOS%20-%20PERGUNTAS%20E%20RESPOSTAS%20V2.pdf. Acesso em: 19 de julho de 2022.

SECRETARIA DE SEGURANÇA PÚBLICA/SP. **Polícia Civil lança aplicativo para prevenir golpes de estelionato**. Cartilha GOLPE? TÔ FORA!. 2020. Disponível em: https://www.ssp.sp.gov.br/midia/Midia/00000349.pdf. Acesso em: 19 de julho de 2022.

SECRETARIA DE SEGURANÇA PÚBLICA/SP. **Secretaria da Segurança Pública na proteção da criança e do adolescente**. Cartilha Violência Sexual contra crianças e adolescentes. 2021. Disponível em: https://www.policiacivil.sp.gov.br/portal/imagens/Cartilha%20Violencia%20Sexual.pdf . Acesso em: 17 de julho de 2022.

STJ. **Crime cibernético tomou lugar de roubos e furtos na pandemia, diz ministro Humberto Martins**. Site do STJ. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Crime-cibernetico-tomou-lugar-de-roubos-e-furtos-na-pandemia--diz-o-ministro-Humberto-Martins.aspx. Acesso em: 14 de julho de 2023.

TIDY, Joe. **Pedofilia: Imagens de vítimas de violência sexual explodiram na internet após lockdowns, diz estudo**. Site BBC News Brasil. 2023. Disponível em: https://www.bbc.com/portuguese/geral-64420807. Acesso em: 30 de janeiro de 2023.

UOL/SP. **Golpe dos Nudes: Vídeos usavam delegacia, clínica, velório e família falsas**. Publicado em: 29 de maio de 2023. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2023/05/29/golpe-nudes-encenacao-videos-delegacia-falsa-clinica.htm. Acesso em: 23 de fevereiro de 2023.

VIDAL, Daniella Thaysa Neves. **Internet, uma terra sem lei?**. 2018. Disponível em: http://repositorio.asces.edu.br/bitstream/123456789/1604/1/Artigo%20Daniella%20Vidal%2027022018.pdf. Acesso em: 20 de julho de 2023.

WANDERLEY, Carlos Alberto Cardoso; DA COSTA, Rodrigo Silva; RIBEIRO, Lara de Paula. **Crimes Cibernéticos Em Tempos De Pandemia: O Isolamento Social Como Propulsor Da Vulnerabilidade Da População E Do Aumento Dos Casos**. Facit Business and Technology Journal, Ed. 37, v. 1, Págs.166-184. 2022. Disponível em: https://jnt1.websiteseguro.com/index.php/JNT/article/view/1619/1106. Acesso em: 18 de julho de 2023.

Ano 10, vol. 3, n. 1 - ISSN: 2594-9624 - jun./set. 2024.
http://doi.org/10.53426/unicad-2024.v3n1