FACULDADE EVANGÉLICA DE RUBIATABA
CURSO DE DIREITO
DANIEL FRANCISCO SOARES

UMA ANÁLISE SOB O CRESCIMENTO DOS CRIMES CIBERNÉTICOS NA PANDEMIA E O ACOMPANHAMENTO NO ÂMBITO DO DIREITO PENAL

RUBIATABA/GO

2022

DANIEL FRANCISCO SOARES

UMA ANÁLISE SOB O CRESCIMENTO DOS CRIMES CIBERNÉTICOS NA PANDEMIA E O ACOMPANHAMENTO NO ÂMBITO DO DIREITO PENAL.

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba, sob a orientação do professor Mestre em Ciências Ambientais Pedro Henrique Dutra.

RUBIATABA/GO

2022

DANIEL FRANCISCO SOARES

UMA ANÁLISE SOB O CRESCIMENTO DOS CRIMES CIBERNÉTICOS NA PANDEMIA E O ACOMPANHAMENTO NO ÂMBITO DO DIREITO PENAL.

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba, sob a orientação do professor Mestre em Ciências Ambientais Pedro Henrique Dutra.

MONOGRAFIA APROVADA PELA BANCA EXAMINADORA EM __ / ___ / ____

Orientador: Mestre em Ciências Ambientais Pedro Henrique Dutra

Professor da Faculdade Evangélica de Rubiataba

Escreva a titulação e o nome completo do Examinador 1

Examinador

Escreva a titulação e o nome completo do Examinador 2

Examinador

Quero dedicar esse trabalho primeiramente a Deus, por ter me dado a sabedoria e a capacidade para poder realizar este sonho de concluir esse curso, sem Deus nada seria possível. Devo isso tudo inteiramente a Deus. À minha mãe que sempre esteve presente comigo, me ajudando e me dando forças. À minha vó (Vovica) que sempre batalhou comigo pra que esse sonho se realiza-se, sem vocês eu não conseguiria. Não poderia deixar de dedicar ao meu orientador que me acompanhou desde o começo até o fim desta monografia, de alguma forma me auxiliando e me ajudando nos momentos de dificuldades.

AGRADECIMENTOS

Em primeiro lugar, a Deus, que fez com que meus objetivos fossem alcançados, durante todos os meus anos de estudos, por ter permitido que eu tivesse saúde e determinação para não desanimar durante a realização deste trabalho, pela minha vida, e por me permitir ultrapassar todos os obstáculos encontrados ao longo da realização deste trabalho.

Aos meus pais, avós e irmão, que me incentivaram nos momentos difíceis e compreenderam a minha ausência enquanto eu me dedicava à realização deste trabalho.

Aos familiares por todo o apoio e pela ajuda, que muito contribuíram para a realização deste trabalho.

Enfim, a todos aqueles que contribuíram, de alguma forma, para a realização deste trabalho. A todos que participaram, direta ou indiretamente do desenvolvimento deste trabalho de pesquisa, enriquecendo o meu processo de aprendizado.

Às pessoas com quem convivi ao longo desses anos de curso, que me incentivaram e que certamente tiveram impacto na minha formação acadêmica.

“Quem não luta pelos seus direitos não é digno deles”.

Ruy Barbosa

RESUMO

Este trabalho expõe os riscos inerentes ao desenvolvimento desta importante ferramenta, e demonstra o impacto da pandemia de COVID-19 no que tange ao cometimento de crimes cibernéticos. A pesquisa tem como objetivo geral averiguar o cenário de elevação na taxa de crimes cibernéticos, durante o isolamento social; também especificadamente visa: Apresentar o surgimento dos crimes cibernéticos; identificar crimes cibernéticos em período de pandemia; analisar a competência do Direito Penal referente aos cibercrimes; e propor metodologias para amenizar os crimes virtuais. Para isso foi utilizado ao procedimento metodológico, pesquisa bibliográfica bem como pesquisa de campo, onde obteve aplicação de questionário online a jovens entre 18 e 25 anos para obter um resultado mais característico, bem como, para obter Informações e ideias adicionais. Após breve realização da pesquisa, pode-se concluir que houve um aumento de crimes cibernéticos, ou seja, na época de pandemia aumentou bastante, e infelizmente as tipificações legislativas, principalmente no que concerne as leis penalistas, não conseguiram acompanhar de modo a penalizar da forma adequada, ficando nítido que o Direito Penal não conseguiu coibir os crimes cibernéticos entre os anos 2019 e 2021.

Palavras-chave: Covid-19. Crimes Cibernéticos. Direito Penal. Internet.

ABSTRACT

This research exposes the risks inherent in the development of this important tool, and demonstrates the impact of the COVID-19 pandemic on cybercrime. The research has as general objective to investigate the scenario of increase in the rate of cyber crimes, during social isolation; also specifically aims to: Present the emergence of cyber crimes; identify cyber crimes in a pandemic period; analyze the competence of Criminal Law regarding cybercrimes; and propose methodologies to mitigate cybercrime. For this, the methodological procedure was used, bibliographic research as well as field research, where an online questionnaire was applied to young people between 18 and 25 years old to obtain a more characteristic result, as well as to obtain additional information and ideas. After a brief survey, it can be concluded that there was an increase in cyber crimes, that is, at the time of the pandemic it increased a lot, and unfortunately the legislative typifications, especially with regard to criminal laws, were not able to follow in order to penalize the adequately, making it clear that Criminal Law was unable to curb cybercrimes between 2019 and 2021

Keywords: Covid-19. Cyber Crimes. Criminal Law. Internet

Traduzido por Marleides de Oliveira Mendes – Letras – FAFISP/Ceres.

LISTA DE ABREVIATURAS E SIGLAS

Art.	Artigo
CP	Código Penal Brasileiro
N°	Número

LISTA DE SÍMBOLOS

§ Parágrafo

SUMÁRIO

1. INTRODUÇÃO

Este trabalho tem como tema: Uma análise sob o crescimento dos crimes cibernéticos na pandemia e o acompanhamento no âmbito do direito penal. Partindo dessa temática é imprescindível a compreensão de que para chegar aos dias atuais passamos por uma grande evolução tecnológica, que marca o desenvolvimento da internet, a qual tem grande implicação na vida dos seres humanos haja vista que, a mesma está inserida de forma íntegra em seus cotidianos, por apresentar amplos recursos que proporcionam mais oportunidades e facilidade para a vivência dos cidadãos.

Contudo, com a criação do mundo virtual, surgiram os conhecidos “crimes cibernéticos”, que consiste em delitos cometidos, utilizando ambientes de redes, que podem interferir e sensibilizar a vítima. Uma categoria destes crimes que são mais decorrentes é o *Phishing*, o qual corresponde a uma fraude de dados, onde o infrator objetiva obter informações pessoais do indivíduo e usá-las para seu benefício.

Compreende-se que a pandemia nos revelou uma realidade divergente da que vivíamos, visto que, trouxe um grande desafio e propiciou a necessidade instantaneamente de adaptação diante das novas condições de vida da população. Ademais, em consequência deste cenário, uma abundância de pessoas ficou desempregada, deste modo, mais flexíveis, adentraram com maior intensidade ao mundo virtual, em analogia, algumas até aderiram ao método de *Home Office* (trabalho remotamente).

Portanto, este período de isolamento social, tornou-se o meio ideal para a propagação dos crimes virtuais, o que é nítido, pois de acordo com o Jornal Nacional G1 (2020) obteve um aumento significativo de crimes virtuais durante a fase de isolamento social. É indispensável salientar, que se teve um avanço no Direito Penal, com a implantação da Lei n.º 12.737/2012, conhecida como “Lei Carolina Dieckman”, que simboliza o caso de uma atriz global, a qual teve suas fotos íntimas expostas nas redes sociais, após a invasão do seu computador.

Entretanto, lamentavelmente o Código Penal apresenta retrocesso diante da constante eclosão do estelionato de dados, em episódio de pandemia, já que é de extrema dificuldade identificar o infrator e as pessoas continuam desinformadas e ingênuas com relação aos crimes cibernéticos. Desse modo, será abordado aos

indivíduos, metodologias e técnicas, com objetivo de informar e propor práticas para se prevenirem e evitarem a propagação dos crimes virtuais. Nesse sentido, a problemática apresentada nesta pesquisa é: O Direito Penal foi capaz de coibir os crimes cibernéticos entre os anos de 2019 a 2021?

A pesquisa tem como objetivo geral averiguar o cenário de elevação na taxa de crimes cibernéticos durante o isolamento social; também especificadamente visa: Apresentar o surgimento dos crimes cibernéticos; identificar crimes cibernéticos em período de pandemia; analisar a competência do Direito Penal referente aos cibercrimes; e propor metodologias para amenizar os crimes virtuais.

O método a ser utilizado tem um caráter exploratório, visto que, tem como objetivo distinguir e fazer uma análise crítica sobre a elevação dos crimes cibernéticos durante a pandemia diante da verificação de leis sancionadas. Esta pesquisa apresenta três fases de embasamento, sendo elas: examinar o crescimento dos cibercrimes; explorar a legislação através de uma análise ampla e intensificada e propor aplicação para análise de resultados. O estudo foi desenvolvido com o suporte em materiais já elaborados, tendo destaques em artigos, livros, sites, e pesquisas científicas.

Além disso, é mister salientar que a pesquisa também se fundamenta no modelo de survey, onde foi adotada pesquisa de campo através da realização de um questionário online, permitindo portanto, corroborar com a situação investigada, contando com uma amostra de 152 participantes, sendo jovens entre 18 e 25 anos de idade, com a aplicação de questionário online mediante redes sociais.

Nesse sentido, afim de alcançar os objetivos supracitados, a pesquisa foi dividida em 4 (quatro) capítulos, sendo o primeiro acerca do crime cibernético, aduzindo sobre conceituação, surgimento, tipos de crimes e classificação. Em seguida o segundo capítulo trata sobre o crime cibernético e suas diretrizes no que tange a pandemia de covid-19. Logo vem o terceiro capitulo que faz uma abordagem jurídica sobre o crime cibernético bem como aduz sobre diretrizes penais sobre o feito.Com a objetividade de somar com toda a pesquisa o capitulo quarto traz consigo a metodologia aplicada para a solução da problemática e a seguir há o resultado de toda a pesquisa estudada onde pode-se absorver que as tipificações legislativas, principalmente no que se refere as leis penalistas, não conseguiram acompanhar de modo que penalize da forma adequada, sendo assim, não conseguindo coibir com os crimes cibernéticos entre os anos de 2019 a 2021.

2. ASPECTOS GERAIS DO CRIME CIBERNÉTICO

Falar sobre internet é ter em mente um meio de extrema valia que atua de modo a compartilhar dados diversos, com a objetividade de se conectar a meios globais, é de conhecimento geral que a mesma obtém benefícios diversos, porém é necessário aduzir que junto com os benefícios, surge consigo os malefícios, dentre eles destaca-se os crimes cibernéticos.

O crime cibernético por sua vez consiste no “cometimento de atividades ilícitas por meio do computador ou rede de internet e classificam-se de acordo com a sua forma de cometimento” (WENDT; JORGE, 2012), ou seja, é uma ação ilícita caracterizada através de meios tecnológicos sendo classificada conforme a forma que é realizada. Com efeito, podemos analisar que o crime cibernético ocorre de formas e métodos diversos.

2.1 DO SURGIMENTO

Com o avanço tecnológico, as pessoas introduziram em suas vidas a “internet”, que tem uma enorme função em seus cotidianos. Com a adesão do mundo virtual, tornou-se possível fazer tudo que necessitamos sem precisar sair de casa e em um piscar de olhos, visto que a sociedade passou a fazer praticamente tudo pelos meios tecnológicos cada vez mais.

A rede trouxe um vasto conhecimento à população, além disso, promoveu a possibilidade para manter a comunicação entre indivíduos que estão longe, trabalhar de casa, obter informações através de um simples clique e dentre várias outras vantagens.

Desse modo, essa virtualidade está presente continuamente no dia a dia das pessoas, facilitando as relações sociais e tornando o modo de vida mais prático e rápido. Portanto, esse universo digital trouxe tanta comodidade à vida das pessoas, que hoje em dia é impossível sobreviver sem, desse modo, tornou-se primordialmente um item de necessidade do dia a dia.

Os computadores foram criados inicialmente como o objetivo de garantir a comunicação entre pessoas, passar informações e aprendizagem. No entanto, com o crescimento da tecnologia, surgiram-se também os conhecidos crimes cibernéticos,

que equivale às fraudes cometidas usando um computador (tecnologias da informação) e conectados a uma rede

> [...] os primeiros casos de crimes cibernéticos foram na década de sessenta. Eram utilizados computadores como forma de cometimento do crime virtual, como o estelionato. Na referida década foi que começaram a ser relatados pela imprensa os primeiros casos de crimes cibernéticos. A partir da década de setenta, c começaram os primeiros estudos empíricos sobre a criminalidade cibernética (ALBUQUERQUE, 2006, p.35).

É um fato que a internet tem e vem colaborando de forma sublime na vida do ser humano, mas sempre há algumas pessoas que invertem essa situação para um lado negativo e tiram proveito dela, já que, existem indivíduos que veem a tecnologia como uma oportunidade de conseguir aplicar atos ilícitos para gerar o seu próprio benefício

Em 1960 o termo *hacker* surgiu com a finalidade de nomear os indivíduos que pretendiam fazer programação, porém, com o avanço da internet, mudou-se essa definição para os invasores de computadores alheios.

> [...] os transgressores da lei penal logo viram no computador e na Internet formidáveis instrumentos à consecução de vários delitos. Como se não bastasse, essa revolução tecnológica também deu azo à criatividade delituosa, gerando comportamentos inéditos que, não obstante o alto grau de reprovabilidade social, ainda permanecem atípicos (FURLANETO; GUIMARÃES, 2003, p.264).

Vale evidenciar que nem sempre os criminosos cometiam as fraudes eletrônicas com o objetivo financeiro, mas na maioria das vezes faziam apenas por prazer, para demonstração de habilidades informáticas e curiosidade, já que os *hackers* sabem que todo Sistema de Segurança há algum defeito que lhe dá abertura para invadir os computadores alheios e comandá-los à distância.

Haja vista que esses comportamentos já eram considerados como atos ilícitos, que consequentemente provocava a danificação, deterioração e podendo gerar grandes prejuízos, pois alguns programas ou dados do computador não teriam a possibilidade de serem utilizados novamente pelo dono.

2.2 TIPOS DE CRIMES CIBERNÉTICOS

Segundo o Departamento de Justiça dos Estados Unidos (2021, p. 2), os crimes cibernéticos podem ser divididos em três categorias principais, sendo eles: cibercrimes puros, cibercrimes mistos e cibercrimes comuns.

Em se tratando do cibercrime puro o mesmo é definido como: “Toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes inclusive dados e sistemas”.

Nesse caso, o crime cibernético puro trata das transgressões em que o computador torna-se o alvo dos delituosos, ou seja, é o momento em que tanto o sistema pessoal ou corporativo recebe algum ataque, o agente que irá cometer o delito aqui, tem como principal objetivo atingir o computador de forma intensificada.

Podendo fazer um destaque às condutas realizadas pelos hackers, que são pessoas que detém um poder de forma intensificada acerca dos dados de modo que possuem um conhecimento elevado e que o utiliza para invadir ou prejudicar servidores ou sistemas informáticos.

Os Cibercrimes mistos ocorrem quando o sistema de computador é utilizado como “arma” para a execução dessas ações. Os Cibercrimes comuns referem-se àqueles delitos em que o computador é manuseado como um instrumento, apenas com a finalidade de armazenar informações ilegais e roubadas.

No cenário tecnológico existe uma variedade de crimes eletrônicos, sendo eles: pedofilia, *phishing,* crimes contra a honra, *cyberbulling* e *sextortion*.

Inicialmente convém salientar acerca da pedofilia, também considerada um crime virtual, a pedofilia é um crime gravíssimo, que consiste em um transtorno psiquiátrico crônico, onde o indivíduo tem desejos e fantasias de modo sexual por crianças, sendo muito praticado de forma virtual com a venda de pornografia infantil. Ademais, para este crime especifico foi implementada a Lei nº 8.069/1990, mais especificamente no art 240 “produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa”.

Cabe ressaltar que existem diversos sites que produzem conteúdos que expõem de forma explicita atos sexuais que sucedem entre menores de idade, por

meio de fotos de nudez e que contém cenas para satisfazer o desejo sexual dos criminosos.

Nessa categoria de crime, o bem jurídico tem como objetivo principal garantir a proteção da criança que sofre tanto do abuso físico, quanto do abuso virtual, onde tem sua foto, vídeo, ou até mesmo sua imagem de forma integra publicada nos sites e mídias criadas de modo ilícito.

O *Pishing* é o crime virtual mais eficaz, pois, ele tem a possibilidade de modificar-se, dado que, consegue alterar os objetivos e temáticas, acerca do momento e situação condizente. A intenção deste cibercrime é fazer com que os indivíduos exponham todos os seus dados de maneira manipulada. Esses criminosos aplicam táticas arquitetadas e planejadas com a principal finalidade de ludibriar as vítimas e conseguir enganá-las.

As estratégias mais frequentes são: recriar ambientes virtuais falsos, fazendo com que as pessoas informem seus dados, bem como, enviar links e e-mails com vírus, ou até mesmo com propostas incríveis que chame a atenção da vítima, em que é incentivada a passar suas informações particulares para ganhar o prêmio ou comprar um objeto com desconto extremo, além disso, tem como alternativa invadir os sistemas.

Os crimes contra a honra, também considerados como crimes virtuais, caracterizam-se por fazer calúnia e difamação a um indivíduo nas redes sociais. Assim aduz o artigo 138 e 139 do CP:

> Art. 138 – Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena – detenção de 06 meses a 02 anos, e multa; Art. 139 – Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena – detenção de 03 meses a 01 ano, e multa (BRASIL, 1940)

Em se tratando da calúnia, a mesma é um crime que acontece no presencial porém como já foi abordado anteriormente é considerada um crime virtual, uma vez que consiste em espalhar comentários, acusações falsas referente a um tipo de crime sobre uma pessoa, e esta situação só é considerada crime se a calúnia chegar a um terceiro. Já a difamação equivale ao ato de difamar, em que, faz insultos e prejudica a carreira e reputação da pessoa, podendo ser verdade ou não a difamação.

2.3 CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Com o advento da Internet, a tecnologia percorreu um longo caminho. Essa expansão fica evidente quando observamos que os meios de comunicação se tornaram mais desenvolvidos e acessíveis a uma maior proporção da população. Fazer compras online, conversar com amigos e até namorar, hoje isso é absolutamente normal e possível.

A internet veio para ficar, mas diante de toda essa facilidade, o crime nesse caso tomou uma forma mais sutil e está se tornando bastante comum, crescendo a cada dia causando mais vítimas e fazendo do virtual um ambiente cheio de perigos e armadilhas. Não há nomenclatura adequada para esse tipo de crime, pois também é um aspecto novo no mundo jurídico. Sendo assim, esses delitos são denominados também de Crimes Virtuais, Crimes Digitais, Crimes Computacionais dentre vários outros tipos.

Para que haja uma melhor compreensão acerca desse assunto, é necessário compreendermos o conceito de crime. Conforme aduz Carvalho (2008, não paginado), crime é:

> [...] material, como “todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para a existência da coletividade da paz social”. E, formal, onde o “crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo”

Já no conceito mais minucioso, o crime informático (sendo também um crime cibernético) é “toda ação típica, antijurídica e culpável, cometida contra ou pela utilização do processamento automático de dados ou transmissão”. (VELLOSO, 2015 apud FERREIRA, 2000, p. 210).

Conforme aduzido anteriormente, uma grande parcela dos doutrinadores não possui um consenso no que tange este instituto, contudo existe uma classificação que atua de forma evidente nas literaturas atuais. Conforme leciona Velloso (2015 apud CORRÊA, 2000b, p. 43), os crimes cibernéticos, são “todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar”.

É importante ressaltar que, conforme o parágrafo anterior, o crime será cometido contra a máquina, o próprio computador, ou seja, contra os dados presentes no aparelho. Destruição de software e dados, roubo de informações, etc. são exemplos de alguns dos danos que seu PC pode sofrer. Portanto, para classificar de forma mais instrutiva, a classificação mais aceita da doutrina é a divisão entre crimes cibernéticos puros, impuros ou mistos.

2.3.1 Crimes cibernéticos puros

Crime cibernético puro é quando um agente precisa absolutamente de um computador para atacar remotamente, ou diretamente usando um sistema de computador, e todos os interesses legítimos já estão protegidos. Nesse caso, envolve não apenas a invasão e captura de dados em massa armazenados, mas também a intenção de alterar, inserir, adulterar ou destruir dados existentes no computador.

Nessa perspectiva Viana (2003, p. 13-26), destaca que “são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)”. Ainda nesse sentido, Damásio de Jesus (2003) trás consigo o posicionamento de que os crimes eletrônicos puros ou próprios são crimes cometidos por computador e cometidos ou consumidos em meio eletrônico. Dentre eles, a tecnologia da informação (segurança do sistema, propriedade da informação e integridade dos dados, máquinas e periféricos) é o objeto jurídico protegido.

É imprescindível destacar também a presença de duas figuras, sendo elas: Os *hackers* e os *crackers. Hackers* por sua vez são pessoas que usa de seu conhecimento técnico para ganhar acesso a sistemas consideravelmente privados. Analisando esse contexto, podemos concluir que os *hackers* possuem um conhecimento único sobre o assunto e não necessariamente o utiliza para fins de ato ilícito, pois a partir desse discernimento pode-se concluir que o campo pode ser visto como algo positivo ou não

Os *crackers*, por outro lado, são aqueles que focam em vantagens ilegais. Eles invadem e comprometem sites, sejam eles quais forem, quebram senhas e desenvolvem *software* que pode comprometer várias máquinas ao mesmo tempo.

2.3.2 Crimes cibernéticos impuros

Os crimes cibernéticos impuro ou impróprio é um crime cometido usando computadores. Ao contrário do crime cibernético puro, essa forma de crime usa apenas computadores como ferramenta para realizar o crime. No entanto, os crimes cometidos no âmbito desse “auxílio” já são representados pelo Código Penal Brasileiro, o que mostra que o uso de computador pessoal não é o fator principal, mas uma das diversas formas de se atingir os crimes já tutelados. Desta forma, aduz Damásio de Jesus (2003) aduz que o crime eletrônico impuro ou impróprio é quando um agente usa um computador como meio de produzir um resultado natural que ofende o mundo físico ou o espaço "real" e ameaça ou prejudica outros ativos não computacionais.

Através disso, fica mais fácil entender o que são crimes cibernéticos puros e crimes cibernéticos não puros, sempre enfatizando que em um a pessoa precisa necessariamente de um computador, enquanto o outro modelo precisa apenas de um PC como ferramenta para realizar o crime.

3. EVOLUÇÃO DO CRIME CIBERNÉTICO E O SEU AUMENTO DURANTE A PANDEMIA DE COVID 19

É imprescindível a compreensão de que no que se refere crime e internet, ambos obtêm uma relação desde o ano de 1960, justamente quando também nasceu a internet, conforme aduz Guimarães (2003, p.68):

> Segundo Ferreira, o surgimento dos crimes informáticos remonta, no entender de Ulrich Sieber, da Universidade de Wurzburg, à década de 1960, época em que apareceram na imprensa e na literatura científica os primeiros casos de uso do computador para a prática de delitos, constituídos, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo do de computadores e sistemas, denunciados em matéria jornalística. Somente na década seguinte é que se iniciaram os estudos sistemáticos e científicos sobre essa matéria, com emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial.

Quando a Internet surgiu, no momento em que se desenvolvia e se movia em direção à poderosa ferramenta que se tornara, ajudando nas tarefas do dia a dia, no lazer e em outras escolhas, eles não previam que ela também poderia ser uma "arma" poderosa. Para se envolver em atividades criminosas, infelizmente, todo esse conhecimento maravilhoso sobre a mente humana é desenvolvido não apenas para o bem, mas também para os caminhos do crime. Assim, com o passar dos anos, o comportamento criminoso começou a se manifestar e tomar a forma que tem hoje, conforme institui Guimarães (2003, p. 68):

> A partir de 1980, ressalta a autora o aumento de ações criminosas que passaram a incidir em manipulações de caixas bancárias, pirataria de programas de computador, abusos nas telecomunicações etc., revelando a vulnerabilidade que os criadores de processo não haviam previsto. Acrescente-se, ainda, o delito de pornografia infantil na rede, igualmente difundido na época.

Ou seja, a relação de crimes que podem ser praticados através da internet é extensa e vem sendo alargada há cerca de vários anos.

Em relação a isso é necessário fazer uma breve análise acerca da nossa realidade, e nada é tão mais real do que a fase difícil que todos estão enfrentando que é a chamada pandemia em razão da Covid-19. Em razão disso surge o seguinte

questionamento: Com a propagação da Covid-19 e a entrada na fase de pandemia houve um aumento e uma dificuldade em coibir os crimes cibernéticos?

É de conhecimento geral que a pandemia trouxe consigo desafios diversos de modo que fez que o mundo se juntasse para tentar acabar com seu avanço, nota-se portanto que esta é uma doença de fácil contágio, sintomas diversos e sem obtenção de meios que acabem de vez com a mesma.

Em razão disso, que a sociedade em questão teve que se adaptar de modo a criar mecanismos que ao menos inibem a possibilidade de contagio, dentre esses mecanismo convém fazer destaque do isolamento social. Isolamento social consiste justamente em se afastar de outras pessoas de forma voluntaria ou involuntária, e foi justamente isso que as pessoas tiveram que fazer, ficar em suas casas, evitar qualquer contato, para então, poder objetivar um futuro mais seguro e garantidor.

3.1 DO AUMENTO DO CRIME CIBERNÉTICO EM MEIO A PANDEMIA DE COVID-19

De fato, o isolamento social é um método de extrema valia, conforme já foi aludido, porém convém salientar que com o advento do isolamento social houve também um crescente número de crime cibernético, conforme aduz Martins (2020, p. 02):

> Criminosos percebendo o uso massivo da rede mundial de computadores por grande parte da população mundial procuraram, rapidamente, adaptar-se à nova realidade para cometer fraudes eletrônicas, aproveitando-se do estado de medo e ansiedade que a pandemia e a necessidade de isolamento causam as pessoas.

Conforme o site Toxicologia Pardini, esse cenário de Covid-19, colaborou para que o mundo virtual se transformasse em um ambiente extremamente propício para os *hackers* e os criminosos digitais, já que, com tal condição de cessar as relações sociais, as pessoas adentraram mais neste universo tecnológico, acessando modalidade virtual para estudar, trabalhar (*Home Office*), serviços *streaming* filmes, *delivery* e compras *online*, onde há uma grande vulnerabilidade, cedendo uma abertura para roubo de dados, invasão de redes particulares e ataques contra empresas e usuários.

No decorrer da pandemia, a empresa Akamai Technologies conhecida por ser líder em serviços CDN (Rede de Entrega de Conteúdo), detectou 1,6 bilhão de

tentativas de roubo de credenciais somente no Brasil, sendo que em apenas um dia teve o recorde de 55 milhões de tentativas de delitos.

Cabe ressaltar, conforme o site Canal Tech que em Fevereiro de 2020 foi emitido um alerta com relação ao primeiro trojan criado no Brasil com finalidade de roubo de informações bancárias de usuários do país, onde usaram como estratégia, imagens da construção do hospital provisório de Wuhan em sete dias, na China, para tratar a Covid-19.

O vídeo possui uma proposta chamativa que faria qualquer pessoa clicar, sendo que a interface do vídeo possui um formato semelhante ao do YouTube, porém ao clicar no botão de play, a vítima é redirecionada a uma outra página, a qual é de acesso do *hacker*, enquanto a pessoa assiste ao vídeo, é instalado um arquivo executável no navegador, e consequentemente o *hacker* ganha acesso remoto ao computador, sendo possível obter e roubar as credenciais bancárias do indivíduo

4. ABORDAGEM JURÍDICA ACERCA DOS CRIMES CIBERNÉTICOS

É importante salientar acerca de algumas normas que tratam sobre proteção de dados no que tange aos crimes cibernéticos, sendo: Lei nº 12.735/2012 (Lei Azeredo); Lei nº 12.737/2012 (Lei Carolina Dieckmann); Lei nº 12.965/2014 (Lei do Marco Civil), as quais serão tratadas de forma mais específica abaixo.

4.1 LEI Nº 12.735 /2012 (LEI AZEREDO)

A Lei Azeredo vem definindo os crimes que por sua vez são cometidos no âmbito digital bem como em meios que que possuem acesso às tecnologias da informação, a mesma vem atuando de modo que estabelece meios como por exemplo, delegacia virtual, que devem ser criados com a objetividade de interromper atividades consideravelmente delituosas no âmbito virtual; desta forma aduz em seu artigo 4°:

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. Art. 5º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação: II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

Ou seja, a atuação das equipes especializadas deve ser imediata, e deve vigorar sempre combate às ações delituosas

4.2 LEI Nº 12.737/2012 (LEI CAROLINA DIECKMANN)

No que tange a Lei Carolina Dieckmann, a mesma define os crimes cometidos pela internet como por exemplo, invasão de computadores, o roubo de senhas e de conteúdos de e-mails, a derrubada proposital de sites, entre outros, assim reza o art. 1º e seguintes da referida lei.

> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B: “Invasão de dispositivo informático. Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação

> indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Em outras palavras tal lei atua de forma intensificada de modo que visa uma garantia de direitos no que tange aos dados das pessoas. Não diferente da legislação penal, porém, possuindo consigo a necessidade de um melhor reajuste para uma melhor aplicabilidade e eficácia legal.

4.3 LEI Nº 12.965/ 2014 (LEI DO MARCO CIVIL)

A Lei nº 12.965/2014, conhecida como “Marco Civil da Internet”, consiste em designar conceitos, vantagens, direitos e obrigações para a utilização da Internet no Brasil, e contempla em seu art. 3º sobre as concepções que carecem ser analisadas em sua utilização:

> [...]Art. 3 A disciplina do uso da internet no Brasil tem os seguintes princípios: garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; proteção da privacidade; Art. 7 O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

Contudo, nesta lei não existe qualquer providência, que lide com a divulgação e compartilhamento de dados tipos de imagens ou vídeos, que tenha cunho íntimo ou sexual, conseguidos de maneira ilícita.

4.4 ACOMPANAHMENTO LEGISLATIVO AOS CRIMES CIBERNÉTICOS

Como foi aludido anteriormente, há normas que tipificam os crimes cibernéticos, porém após breve análises, pode-se observar que elas são insuficientes para cobrir crimes cometidos virtualmente. Portanto, por se tratar de um tipo de crime penal, e no Direito Penal ter a obrigatoriedade de respeitar o princípio da reserva legal bem como o princípio da legalidade do crime, torna-se difícil para pesquisadores e profissionais do direito punir os infratores.

Isso ficou claro, quando foi aplicado o formulário, onde 94,1% de uma quantidade de 152 pessoas jovens, aduziram que não houve uma aplicabilidade de punição aos infratores que praticam esses delitos, isso só comprova a tamanha falta de leis adequadas para garantir uma melhor segurança a todas as pessoas.

5. PERCURSO METODOLOGICO

Para a realização deste trabalho de pesquisa, inicialmente foi adotado a pesquisa de cunho bibliográfico. Para a obtenção de êxito, fez-se um levantamento de livros e artigos, tanto físicos como virtuais no sentido de se coletar material para a construção do embasamento teórico. A pesquisa bibliográfica, por sua vez, conforme Gil (2002), tem como base material já elaborado, como os livros e artigos. Ainda, de acordo com Gil (1999, p. 71): “a principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente”.

No intuito de se obter uma pesquisa mais clara, a pesquisa de cunho bibliográfico atua de modo que não altera a realidade pesquisada, sendo portanto, de extrema valia. Com o propósito de coletar dados foi então realizada a pesquisa de campo, onde foi aplicado um questionário a 256 pessoas via *Google Forms,* composto por 5 perguntas fechadas.

A pesquisa de campo por sua vez, é a etapa do trabalho onde há a aplicação de instrumentos elaborados com a objetividade de coletar dados, para Lakatos e Marconi (2002, p.83) a:

> Pesquisa de campo é aquela utilizada com o objetivo de conseguir informações e/ou conhecimentos acerca de um problema para o qual se procura uma resposta, ou de uma hipótese que se queira comprovar, ou, ainda, descobrir novos fenômenos ou as relações entre eles.

Por conseguinte, nota-se que a mesma tem por objetivo familiarizar-se com o assunto pouco conhecido de modo objetivo e direto, em razão disso que foi usado no trabalho tal modalidade, de modo que houve a aplicação de formulários online com a objetividade de averiguar de forma mais intensificada o estudo.

A pesquisa em questão foi direcionada de forma aleatória a uma parcela da população jovem, sendo entre 18 a 25 anos de idade, onde 152 pessoas tiveram interesse em estar respondendo o questionário.

Nota-se, contudo, que a pesquisa foi realizada através de estimativas e opiniões pessoais, sendo utilizado questionário digital, o qual foi aplicado no dia 23 de janeiro de 2022, sendo, portanto, partilhado, através de redes sociais, como por exemplo, Instagram e WhatsApp. Vindo alcançar, deveras, o resultado esperado.

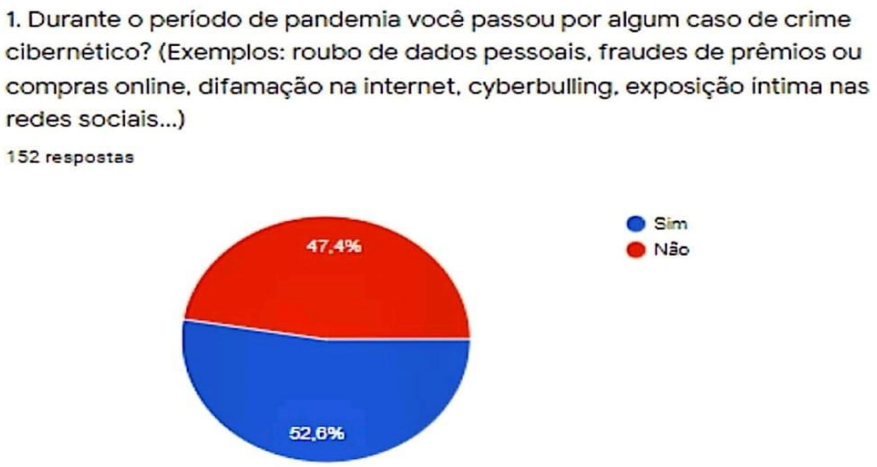
5.1 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Nesse tópico, por sua vez, são apresentadas as análises bem como as discussões dos resultados alcançados através da aplicação do formulário online, com a objetivo de responder a problemática da pesquisa que consiste no seguinte: “O Direito Penal foi capaz de coibir os crimes cibernéticos entre os anos de 2019 a 2021?”

5.1.1 Análise e Discussão da questão 1

A questão número 1 indaga se a pessoa passou por algum crime cibernético nesse período de pandemia, a pergunta foi fechada, onde obteve participação de 152 pessoas, conforme gráfico abaixo:

Gráfico 1- Crime cibernético no período de pandemia.



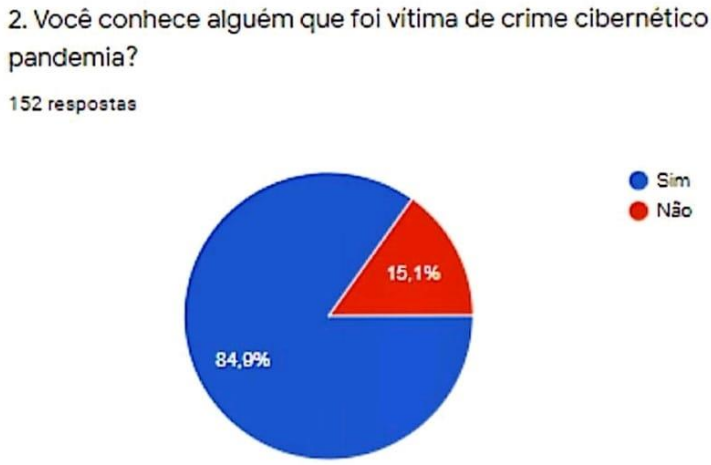
Fonte: próprio autor

Em relação à pergunta 1, relativa ao crime cibernético no período de pandemia, ficou evidente a partir das respostas dos informantes, que uma boa parcela dos jovens sofreu crime cibernético na época da pandemia, onde 52,6% disseram que sim e 47,4 % responderam que não**.**

5.1.2 Análise e discussão da questão 2

A seguir traz dados referentes a pergunta 2, onde pergunta se o entrevistado conhece alguém que foi vítima do crime cibernético durante a pandemia, a seguir:

Gráfico 2- Vítimas de crime cibernético durante pandemia



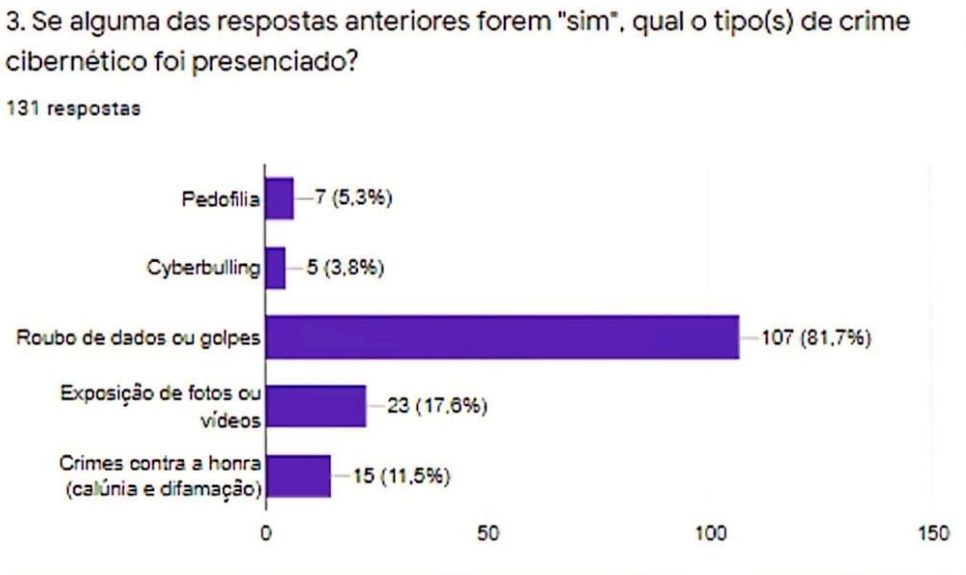
. **Fonte**: próprio autor.

A resposta no que tange a pergunta n° 2 teve participação de 152 pessoas, onde 84,9 % disseram que sim, que tinham conhecimento de pessoas que foram vítimas de crime cibernético no período de pandemia, tendo apenas 15,1% respondendo não. Esses dados demonstram uma preocupação enorme, haja vista, deixar claro, que juntamente com o período consideravelmente difícil, cheio de desafios a serem enfrentados, obteve ainda mais um desafio, o chamado crime cibernético.

5.1.3 Análise e discussão da questão 3

A seguir foi realizado a pergunta n° 3, onde questiona acerca dos tipos de crimes cibernéticos que as pessoas que deram como positiva a resposta anterior presenciaram, nessa pergunta obteve participação de 131 pessoas em razão dessa questão se referir apenas àqueles que disseram o sim na pergunta anterior, conforme gráfico abaixo:

Gráfico 3- Tipos de crimes



. **Fonte**: próprio autor

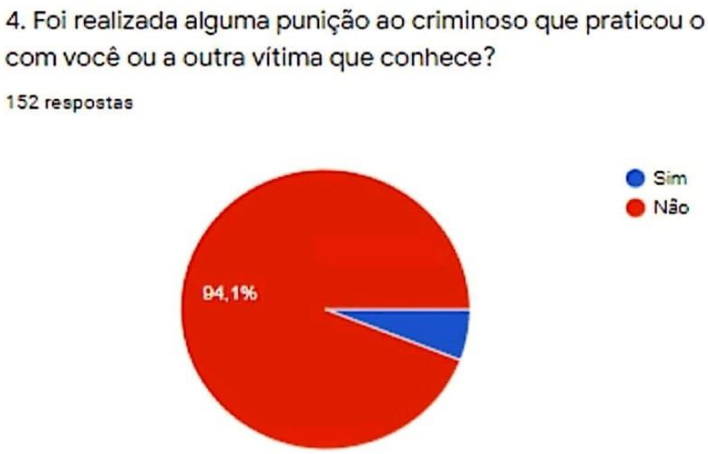
Conforme aludido anteriormente, foram expostos os seguintes crimes: pedofilia com uma quantidade de votos de 5,3% totalizando 7 votos; *cyberbulling* com um percentual de 3,8% equivalente a 5 votos; roubo de dados ou golpes com 81,7 % sendo 107 votos; exposição de fotos ou vídeos com 17,6% com 23 votos e por fim crimes contra a honra com 11,5% com 15 votos.

Através desses dados pode-se concluir que roubo de dados e golpes pegou a liderança, o que por óbvio, deixa as pessoas muito assustadas, haja vista a maioria desses golpes trazer consigo prejuízos financeiros diversos e irreparáveis.

5.1.4 Análise e discussão da questão 4

Posteriormente foi feita a pergunta número 4, onde questionou se houve alguma punição delitiva aos criminosos que praticaram o delito virtual, da qual se obteve 152 respostas, conforme gráfico a baixo:

Gráfico 4- Punição ao criminoso.



Fonte: próprio autor

Após análise desses dados restou comprovada uma preocupação ainda mais intensa, pois obteve 94,1 % de votos como não, expondo que os criminosos não sofreram punição, e apenas 5,9 % disseram que houve punição. Isso demonstra de forma preocupante que além de o crime acontecer de forma intensificada e rotineira, quando se fala em punições o mesmo não obtém um mesmo retorno.

5.1.5 Análise e discussão da questão 5

Por fim, foi feita a última pergunta, acerca de que durante o período de pandemia o entrevistado percebeu alguma atividade suspeita na internet, sendo também uma pergunta fechada, onde 152 pessoas responderam, conforme abaixo:

Gráfico 5- Atividade suspeita durante a pandemia

. **Fonte**: próprio autor.

Conforme demonstrado no gráfico acima, obteve-se um percentual altíssimo com 94,1 % mencionando que sim e 5,9% declarando que não. Ou seja, diariamente a maioria das pessoas estão se deparando com atividades suspeitas na internet, e como na pandemia o número de pessoas em casa aumentaram, consequentemente, pode-se notar um aumento no que tange a possibilidade de crimes cibernéticos. Esse aumento de forma gradativa pode trazer consigo dificuldades diversas principalmente no que se refere a uma melhor aplicabilidade da lei penal nos casos em concreto.

6. CONSIDERAÇÕES FINAIS

Há um paradoxo que está sempre permeando no que tange a internet atualmente, nota-se que a mesma atua de forma diversa e está presente em quase todos os momentos de nossas vidas, é notório que ela traz consigo benefícios diversos, porém é de suma importância analisar os pontos negativos em que a mesma permeia.

Internet é uma poderosa ferramenta de comunicação, porém, quando usada de forma incorreta, de modo que afeta de forma intensificada outras pessoas, é exigindo a intervenção do Estado, em sentimentos sobre práticas restritivas que podem estar além do escopo da liberdade. Nesse sentido, é necessário tipificar esses comportamentos para que assim o Estado possa exercer suas funções, o que infelizmente não está acontecendo.

Após a realização da pesquisa de campo pode-se chegar a uma resposta no que já se ponderava no início da pesquisa, o aumento de crimes cibernéticos na época de pandemia aumentou bastante, e infelizmente as tipificações legislativas, principalmente no que concerne as leis penalistas, não conseguiram acompanhar de modo a penalizar da forma adequada, ficando nítido que o Direito Penal não conseguiu coibir os crimes cibernéticos entre os anos de 2019 a 2021; há inúmeras lacunas legislativas, e enquanto elas permanecerem, não se logrará êxito no que tange a banalização e amenização dos crimes cibernéticos.

Nota-se que a grande quantidade de pessoas que caíram em golpes durante a pandemia, consiste em pessoas desenformadas, que não tomaram devida proteção, bem como não são instruídas e não possuem discernimento para identificar tais golpes. Portanto, há a necessidade de adotar alguns cuidados e estar cientes de situações, para evitar que uma grande massa da população seja ludibriada pelos criminosos.

Dentre alguns cuidados pode-se citar: nunca abrir um link ou arquivo desconhecido; sempre desconfiar de propostas incríveis e tentadoras de descontos ou prêmios; verificar a reputação da empresa antes de comprar produtos online; não informar dados pessoais aos sites que não sabe a autenticidade do sítio; procurar utilizar senhas e login diferentes para cada site, para ficarem protegidos e alterar senhas caso haja vazamento de dados.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A Criminalidade Informática**. São Paulo: Editora Juarez de Oliveira, 2006. AMBITO JURIDICO. Crimes Cibernéticos: Phishing. Disponível em: https://ambitojuridico.com.br/edicoes/revista-191/crimes-ciberneticos-phishing/.htm. Acesso em: 8 set. 2021.

BRASIL. **Código Civil**. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/2002/l10406.htm. Acesso em: 8 set. 2021. BRASIL. Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689Compilado.htm. Acesso em: 8 set. 2021.

BRASIL. **Código Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm. Acesso em 8 set. 2021. BRASIL. Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 8 set. 2021.

_____. **Lei 12.737/2012.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 20 set. 2021.

CANAL TECH. **Hackers usam mensagens sobre corona vírus para roubar dados no Brasil.** Disponível em: https://canaltech.com.br/seguranca/hackers-usam-mensagens-sobre-coronaviruspara-roubar-dados-bancarios-no-brasil-160465/.htm. Acesso em: 8 set. 2021.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em: 05 mar. 2022.

CORREIO BRASILIENSE. **Estudo aponta 1,6 bilhão de casos de roubo de dados pessoais na internet.** Disponível em: https://www.correiobraziliense.com.br/brasil/2021/06/4928596-estudo-aponta-16- bilhao-de-casos-de-roubo-de-dados-pessoais-na-internet.html. Acesso em: 8 set. 2021.

CRYPTO ID. **Crescimento de crimes cibernéticos na pandemia: como não ser uma vítima.** Disponível em: https://cryptoid.com.br/identidade-digital-destaques/crescimento-de-crimesciberneticos-na-pandemia-como-nao-ser-uma-vitima/.htm. Acesso em: 8 set. 2021. BRASIL. Lei 12.735/2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em 20 set. 2021.

FAC. DOM BOSCO. **Crimes virtuais: ciberbullying, revenge porn, sextortion, estupro virtual.** Disponível em: https://facdombosco.edu.br/wp-content/uploads/2018/12/%C3%82ngela-TerezaLucchesi-Erika-Fernanda-Tangerino-Hernandez-crimes-virtuais-Copia.pdf. Acesso em: 20 set. 2021.

FERREIRA, Ivete Senise**. A Criminalidade Informática**. In: LUCCA, Newton. SIMÃO FILHO, Adalberto (Coord.). Direito e internet. Bauru: Edipro, 2001.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. **Crimes Na Internet: elementos para uma reflexão sobre a ética informacional** - R. CEJ,

JORNAL NACIONAL G1. Crimes virtuais crescem durante o isolamento social. Disponível em: Https://g1.globo.com/jornal-nacional/noticia/2020/07/10/crimes-virtuais-crescem-durante-o-isolamento-social.ghtml. Acesso em: 20 de mar. 2022.

JUS BRASIL. **Falta de lei sobre crimes virtuais leva à impunidade, diz especialista**. Disponível em: https://alexandre-atheniense.jusbrasil.com.br/noticias /2530003/falta-de-lei-sobrecrimes-virtuais-leva-a-impunidade-diz-especialista.htm. Acesso em: 20 set. 2021.

LIMA CARVALHO, Paulo Roberto de. **Crimes cibernéticos: uma nova roupagem para a criminalidade.** Disponível em: <https://jus.com.br/artigos /31282/crimesciberneticos-uma-nova-roupagem-para-a-criminalidade>. Acesso em 20 set. de 2021.

SECURITY REPORT. **Ataques de phishing aumentaram 70% durante a pandemia**. Disponível em: https://www.securityreport.com.br/overview/ataques-de-phishing-aumentaram-em70-das-organizacoes-durante-a-pandemia/#.YVHbZ7hKjIU.htm. Acesso em: 20 set. 2021.

TILT UOL. **Google alerta para ataques de hackers usando o covid-19 como isca**. Disponível em: https://www.uol.com.br/tilt/noticias/afp/2020/04/22/google-alerta-para-ataques-dehackers-usando-a-covid-19-como-isca.htm. Acesso em: 20 set. 2021.

TOXICOLOGIA PARDINI. **Ataques de phishing na pandemia-Veja os 5 ataques mais explorados.** Disponível em: https://www.toxicologiapardini.com.br/ataques-phishing-pandemia-covid/.htm. Acesso em: 20 set. 2021.

VIANA, Marco Túlio apud CARNEIRO, Adeneele Garcia. **Fundamentos de direito penal informático.** Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003, p. 13-26

APÊNDICE A

1) Durante o período de pandemia você passou por algum caso de crime cibernético? (Exemplos: roubo de dados pessoais; fraudes de prêmios ou compras online; difamação na internet; cyberbulling; exposição intima nas redes sociais)

2) Você conhece alguém que foi vítima de crime cibernético durante a pandemia?

3) Se alguma das respostas anteriores forem “sim”, qual o(s) tipo(s) de crime cibernético foi presenciado?

4) Foi realizada alguma punição ao criminoso que praticou o delito virtual com você ou com a outra vítima que conhece?

5) Durante o período de pandemia, você percebeu alguma atividade suspeita na internet? (Exemplos: links suspeitos; propagandas de produtos com baixíssimos valores para realizar golpes; fotos ou vídeos íntimos expostos)

ANEXOS

1. Durante o período de pandemia você passou por algum caso de crime cibernético? (Exemplos: roubo de dados pessoais, fraudes de prêmios ou compras online, difamação na internet, cyberbulling, exposição íntima nas redes sociais...) *

- ◯ Sim
- ◯ Não

2. Você conhece alguém que foi vítima de crime cibernético durante a pandemia? *

- ◯ Sim
- ◯ Não

3. Se alguma das respostas anteriores forem "sim", qual o tipo(s) de crime cibernético foi presenciado?

- ☐ Pedofilia
- ☐ Cyberbulling
- ☐ Roubo de dados ou golpes
- ☐ Exposição de fotos ou vídeos
- ☐ Crimes contra a honra (calúnia e difamação)

4. Foi realizada alguma punição ao criminoso que praticou o delito virtual com você ou a outra vítima que conhece? *

- ◯ Sim
- ◯ Não

5. Durante o período de pandemia, você percebeu alguma atividade suspeita na internet? (Exemplos: links suspeitos, propagandas de produtos com baixíssimos valores para realizar golpes, fotos ou vídeos íntimos expostos...) *

- ◯ Sim
- ◯ Não

Enviar

Limpar formulário