O aumento dos crimes cibernéticos durante a pandemia da Covid-19 e as dificuldades para combatê-los

Amanda Carolina Gomes Lourenço[1]

Caroliny Estefane Pires Dos Santos[2]

Gustavo Henrique de Almeida[3]

Bernardo Vassalle de Castro[4]

Recebido em: 15.05.2023

Aprovado em: 13.07.2023

Resumo: Os avanços tecnológicos e o uso cada vez mais constante da internet, principalmente das redes socias, por meio de dispositivos portáteis, como tablets, smartphones, fez com que a prática de crimes cibernéticos se tornasse cada vez mais oportuna. Perante esse cenário em 2019 foi descoberta a SARS-CoV-2, uma infecção respiratória aguda causada pelo coronavírus, que desaguou em uma pandemia com necessidade de adoção de medidas como o isolamento social para diminuição da transmissão desse vírus, o que possibilitou que a população permanecesse mais tempo em casa e consequentemente mais conectada à internet, chamando a atenção dos criminosos virtuais que aproveitaram desse momento de fragilidade mundial para pratica de crimes cibernéticos. Nesse cenário, busca o presente estudo analisar o aumento dos crimes cibernéticos durante a pandemia da COVID 19, bem como, a eficácia os métodos utilizados no combate desses crimes. Este trabalho foi desenvolvido por meio de pesquisa bibliográfica e foi baseado em dados estáticos e textos legais que abordam o referido tema. Os quais possibilitaram a observação do surgimento de novos criminosos virtuais, bem com a adoção de um novo modus operandi por parte dos criminosos que praticavam anteriormente crimes no ambiente físico. Ao final foi possível constatar que apesar das medidas legislativas e investigativas implantadas, o ordenamento jurídico brasileiro e os investigadores não estão conseguindo acompanhar os avanços tecnológicos e os cibercriminosos que estão se mostrando ser mais bem preparados e mais velozes.

[1] Discente do curso de Direito da Faculdade Minas Gerais (FAMIG)

[2] Discente do curso de Direito da Faculdade Minas Gerais (FAMIG)

[3] Revisor. Doutor pela Pontifícia Universidade Católica de Minas Gerais. Mestre pela Universidade de Itaúna. Coordenador do Curso e Professor da Faculdade Minas Gerais –Famig. Consultor. Advogado.

[4] Revisor. Mestre em Direito pela Universidade Federal de Minas Gerais. Pós Graduado em Direito de Empresa pela Pontifícia Universidade Católica de Minas Gerais -IEC-Puc Minas. Graduado em Direito pela Universidade Federal de Minas Gerais.

Palavras-chave: crimes cibernéticos; aumento; covid 19; isolamento social; combate.

The increase in cybercrime during the Covid-19 pandemic and the difficulties in combating it

Abstract: Technological advances and the increasingly constant use of the internet, especially social networks, through portable devices such as tablets, smartphones, have made the practice of cybercrime increasingly timely. In view of this scenario, in 2019, SARS-CoV-2 was discovered, an acute respiratory infection caused by the coronavirus, which led to a pandemic with the need to adopt measures such as social isolation to reduce the transmission of this virus, which allowed the population to to stay at home longer and consequently more connected to the internet, drawing the attention of cyber criminals who took advantage of this moment of global fragility to practice cyber-crimes. In this scenario, this study seeks to analyze the increase in cybercrime during the COVID 19 pandemic, as well as the effectiveness of the methods used to combat these crimes. This work was developed through bibliographical research and was based on static data and legal texts that address the aforementioned theme. Which made it possible to observe the emergence of new cyber criminals, as well as the adoption of a new modus operandi by criminals who previously committed crimes in the physical environment. In the end, it was possible to verify that despite the legislative and investigative measures implemented, the Brazilian legal system and researchers are not managing to keep up with technological advances and cybercriminals who are proving to be better prepared and faster.

Keywords: cyber-crimes; increase; covid 19; social isolation; combat.

1 INTRODUÇÃO

O tema do presente trabalho de conclusão de curso refere-se à análise dos crimes cibernéticos durante a pandemia do Coronavírus (Covid-19), objetivando analisar se houve aumento desses crimes no período de isolamento social, bem como quais as dificuldades do Estado para combatê-los, esses crimes surgiram através dos avanços tecnológicos e evoluíram com o aumento do uso da internet, principalmente após a pandemia do COVID-19, a qual deu abertura para o fortalecimento dos cibercriminosos.

Em 2019, um vírus que até então não tinha sido identificado em humanos se espalhou por todo o mundo causando uma pandemia, que ficou conhecida como Covid-19, uma doença respiratória aguda, de alta transmissibilidade e de disseminação global.

A referida pandemia fez com que os países adotassem o lockdown, uma medida preventiva obrigatória que consistiu em total isolamento da população, como estratégia

que objetivou o desaceleramento da propagação da infecção causada por este vírus. Por sua vez, este confinamento e a adoção ampla de trabalho na modalidade home office, possibilitou um maior acesso da população a internet, o que ocasionou um aumento dos crimes cometidos por meio da rede de computadores, os denominados crimes cibernéticos.

O espaço virtual de comunicação instantânea entre pessoas, o seu distanciamento físico e principalmente sua proximidade virtual, fez com que essa realidade paralela se tornasse o lugar perfeito para prática de diversos tipos de delitos realizados através dos aparelhos informáticos.

Nesse contexto, o tema problema do presente trabalho é analisar os motivos do crescimento dos crimes cibernéticos durante a pandemia e a dificuldade enfrentada pelas autoridades competentes para solucionar e punir os referidos crimes.

O presente trabalho mostra-se bastante atual e relevante, pois retrata como os crimes virtuais, que vem crescendo e se diversificando na sociedade, tendo sido elaborados então cinco capítulos que buscaram definir e avaliar evolução dos crimes cibernéticos, determinar as espécies de crimes cibernéticos existentes e sua classificação, bem como o lugar e competência que podem abranger, analisar os métodos utilizados em seu combate, como ocorre a investigação policial e quais são as legislações vigentes contra esta infração, além da ressalva aos crimes cibernéticos na pandemia do Covid-19 e por fim um breve estudo da pandemia em si, sendo adotada como referencial teórico do presente trabalho a obra do autor Grégore Moreira de Moura intitulada Curso de Direito Penal Informático.

Utilizou-se o método estatístico, o qual permite a análise de determinados fatores através de dados estatísticos. O tipo de pesquisa a ser abordada será a pesquisa bibliográfica, a qual visa juntar informações que ajudarão na construção do trabalho através da coleta de dados de fontes secundarias, ou seja, por meio de informações sobre um determinado tema já trabalhado antes por outros autores. Os instrumentos e fontes escolhidos para a coleta de dados foram: livros, artigos, trabalhos acadêmicos, jornais, entrevistas, revistas, dadas estatísticas e legislações.

O procedimento utilizado para a coleta de dados foi a busca por informações que tenham ligação com o problema de pesquisa ou com o tema do trabalho. Para obter as referidas informações foram utilizadas palavras chaves e a leitura dos textos foi feita de forma objetiva visando reconhecer e avaliar informações. Portanto, houve o uso da leitura seletiva para concentrar somente nas informações necessárias, também foi utilizada a leitura crítica ou reflexiva onde foi possível avaliar e julgar as informações, intenções e propósitos dos autores das obras sendo possível separar a ideia central e a secundaria da pesquisa, por fim também foi usada a leitura analítica buscando uma leitura mais profunda e precisa do que foi pesquisado sendo possível obter uma melhor compreensão do que foi abordado.

2 CRIMES CIBERNÉTICOS

Os crimes previstos no ordenamento jurídico estão diretamente ligados as questões sociais e culturais da população, assim, com as mudanças culturais e sociais advindas do desenvolvimento tecnológico principalmente com o surgimento da internet que fez com que a população se tornasse cada vez mais globalizada, houve o surgimento dos crimes cibernéticos, os quais segundo Grégore de Moura:

> [...] estão diretamente ligados a questões de difusão da informação, aumento do número de usuários nas redes computacionais, o acesso indiscriminado à internet a partir dos anos 90, bem como aos efeitos da popularização dos smartphones e do crescimento da inclusão digital no mundo. (MOURA, 2021, p.16)

A internet se tornou uma ferramenta indispensável em nossas vidas, pois através dela a população consegue adquirir uma gama de benefícios, informações e facilidades, onde o que antes demorava dias ou horas para ser feito hoje pode ser feito em segundos tornando esse espaço altamente volátil. No entanto, apesar dos inúmeros benefícios trazidos pela internet juntamente com o seu crescimento e o aumento dos números de usuários também houve o surgimento dos cibercriminosos que se aproveitaram desse ambiente volátil, mutável e anônimo para a pratica de crimes que estão se tornando cada vez mais frequente possuindo um aumento assustadoramente acelerado à medida que a internet se expande.

Segundo Conte (2014), a popularização da Internet em rede mundial e o aumento da utilização deste meio de comunicação levaram também ao uso insensato dos recursos da

internet, criando assim os usuários que praticam novas modalidades de delito: os crimes virtuais.

2.1 Evolução

Por meio dos avanços tecnológicos, houve o surgimento de mecanismos que estão cada dia mais presentes no dia a dia da população como as redes sociais e a internet, por exemplo, os quais contribuem para o crescimento da globalização que de acordo com, Boaventura de Sousa Santos:“ é o processo no qual uma determinada condição ou entidade local consegue estender sua influência a todo o globo e, ao fazê-lo, desenvolve a capacidade de designar como local outra condição social ou entidade rival.”(SANTOS, 1997, p.108).

Dessa forma, através dos avanços tecnológicos se tem a disseminação de informações culturais, profissionais e interpessoais por diversas regiões do mundo, sendo possível a constituição de novas oportunidades e práticas comerciais e a criação de novas relações tanto pessoais quanto profissionais.

Mediante as significativas mudanças tecnológicas e por estar se tornando o epicentro de grandes avanços, a internet se transformou em um grande vetor de desenvolvimento virtual, a relação entre ela e os crimes digitais vem desde o seu surgimento na década de 60 pelo Departamento de Defesa dos Estados Unidos (ARPA – Advanced Research Projects Agency). Incialmente a internet era chamada de Arpanet e possuía a função de proteger de possíveis ataques as informações sigilosas do governo norte americano através da descentralização dessas informações que eram distribuídas para vários lugares de forma segura.

Após alguns anos a internet deixou de ser utilizada somente pela Força Aérea Americana e passou a ser utilizada pela população em geral, por governos, empresas, dentre outros. A partir desse desenvolvimento a internet se tornou um dos principais meios de comunicação da sociedade contemporânea, estando presente no mundo todo. (MACHADO,2019)

Diante disso, Zanellato (2002, p.173) afirma que: “A internet é um suporte (ou meio) que permite trocar correspondência, arquivo, ideias, comunicar em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos”.

No Brasil a internet chegou somente em 1991, com a RNP (Rede Nacional de Pesquisa) e desde então o número de pessoas conectadas à internet está se tornando cada vez maior, de acordo com a Pesquisa Nacional por Amostra de Domicílios (PNAD) de 2019, realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), a internet chega a oito em cada dez domicílios do País, estando presente em 82,7% dos domicílios brasileiros, havendo assim um aumento de 3,6 pontos percentuais em relação ao ano anterior. (IBGE,2019)

Embora o surgimento da internet e seu constante crescimento tragam muitos benefícios a população como a integração das pessoas por meio de diversos dispositivos que se conectam à internet, esse desenvolvimento tecnológico também criou novas ferramentas para a prática de atos ilícitos que passaram a ser cometidos não só no mundo real como também no mundo virtual.

Os primeiros casos de uso de computadores para cometimento de delitos informáticos foram relatados na década de 1960, nos Estados Unidos.

Assim, de acordo com Reginaldo César Pinheiro:

> Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente, se percebe que nem todos a utilizam de maneira sensata e, acreditando que a Internet é um espaço livre, acabam por exceder em suas condutas e criando novas modalidades de delito: os crimes virtuais. (PINHEIRO, 2001, p.18)

É inegável que com o passar do tempo os crimes cibernéticos foram se aprimorando à medida que novas tecnologias foram sendo disponibilizadas, assim, diante de um ambiente extremamente globalizado onde os dados de todos trafegam para o mundo inteiro, a disseminação indiscriminada desses dados pode causar efeitos. Segundo Paulo Roberto, “Dessas consequências específicas, podem surgir os delitos informáticos ou delitos comuns, praticados por meio do uso da tecnologia” (CARVALHO, 2014, p. 1).

Sendo assim, com o desenvolvimento tecnológico , as mudança em todos os meios de comunicação, serviços e rotina social, assim como a consequente evolução da internet estão amplamente ligados ao surgimento e adaptação dos crimes cibernéticos, fazendo

com que crimes comuns como o furto, a injúria e o estelionato migrem do ambiente real para o virtual, obrigando o poder legislativo a sempre se atentar ao surgimento de novas modalidades de ilícitos a fim de resguardar e proteger os direitos dos usuários do mundo virtual.

2.2 Definição de crimes cibernéticos

Antes de adentrar no conceito de cibercrimes é importante ressaltar que os crimes informáticos dividem-se em crimes contra o computador ,onde o computador é o alvo do crime, como é o caso do crime de invasão de dispositivo informático, previsto no artigo 154-A do Código Penal; e em crimes por meio do computador, em que este serve de instrumento para a prática do crime, ou seja, nos casos em que o cibercriminoso usa o computador como mecanismo para a execução da prática criminosa, como ocorre por exemplo , nos crimes contra a honra.

Segundo Vladimir Aras, os crimes de informática são conhecidos como:

> Delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, crimes telemáticos, crimes informacionais, ciberdelitos, cibercrimes.Não há um consenso quanto ao nomen juris genérico dos delitos que ofendem interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos (hardwares), redes de computadores e programas de computador (estes denominados softwares).
>
> Dentre essas designações, as mais comumente utilizadas têm sido as de crimes informáticos ou crimes de informática, sendo que as expressões "crimes telemáticos" ou "cibercrimes" são mais apropriadas para identificar infrações que atinjam redes de computadores ou a própria Internet ou que sejam praticados por essas vias. Estes são crimes à distância stricto sensu. Como quer que seja, a criminalidade informática, fenômeno surgido no final do século XX, designa todas as formas de conduta ilegais realizadas mediante a utilização de um computador, conectado ou não a uma rede, que vão desde a manipulação de caixas bancários à pirataria de programas de computador, passando por abusos nos sistemas de telecomunicação. (ARAS, 2015).

O aludido autor ainda se refere aos crimes informáticos como ato típico e antijurídico, cometido através da informática, ou contra um sistema, dispositivo informático ou rede de computadores, em que a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo direito penal.

Nesse contexto, o delito informático é gênero e abrange crimes e contravenções penais praticados no âmbito da Internet, como quaisquer condutas relacionadas aos sistemas informáticos, para crimes de meio ou de fim.

Os crimes informáticos podem ser divididos em crimes informáticos próprios: em que o bem jurídico ofendido é a tecnologia da informação em si e crimes informáticos impróprios: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Esses termos serão abordados de forma mais aprofundada no próximo capítulo.

Os referidos crimes possuem como principais características a imediatidade (por tudo acontecer em tempo real, ou seja, em questão de segundos), a desterritorialidade (por acontecerem e se espalharem por diversos países impossibilitando a identificação da jurisdição e da competência), o anonimato, a interatividade e a volatilidade.

Quanto as práticas de crimes realizados pela internet, esses possuem diversas denominações, são elas: como crime digital, crimes cibernéticos, cibercrimes, crime informático, crime informático-digital, high technology crimes, computer related crime, dentre outros.

No que diz respeito à nomenclatura relativa aos crimes cibernéticos Patrícia da Silva ensina que:

> [...] não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável. (SILVA, 2015, p.39).

Entende-se por crimes cibernéticos os atos criminosos praticados pela internet através do uso de dispositivos digitais como computadores ou quaisquer outros meios de tecnologia de informação e comunicação, os quais geram algum tipo de dano a vítima, seja ele patrimonial ou não. (LÍBANO MANZUR apud PINHEIRO,2001, p.18)[5]

Nessa mesma perspectiva, assevera Moisés de Oliveira Cassanti:

> Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime

5 LÍBANO MANZUR, Claudio. "Chile: Los Delictos de Hacking en sus Diversas Manifestaciones". Revista Electrónica de Derecho Informático, n. 21, abr. 2000. Disponível em: http://arquivo.ibccrim.org.br/site/boletim/pdfs/Boletim101.pdf. Acesso em: 29 set. 2021.

> informático, crimes eletrônicos, crime virtual ou crime digital. (CASSANTI, 2014, p. 3)

Assim, pode-se definir os crimes cibernéticos como condutas típicas, antijurídicas e culpáveis realizadas com o uso da informática, em ambiente de rede ou fora dele, os quais atingem dispositivos eletrônicos, como também, os seus usuários.

Nessa perspectiva, Augusto Rossini define os referidos crimes da seguinte forma:

> O conceito de delito informático poderia ser descrito como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou para a rede, e que ofenda, direta ou indiretamente, a segurança de informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p.110).

No âmbito jurisdicional do Direito Penal brasileiro, crime é toda conduta típica, antijurídica e culpável e o denominado crime cibernético associa-se ao fenômeno da criminalidade informacional de condutas que violam os direitos fundamentais da privacidade, da intimidade, da honra e da imagem das pessoas, os quais estão expressamente elencados no artigo 5°, X da Constituição Federal. Desse modo, os cibercriminosos ao utilizarem da tecnologia para a pratica de condutas que violam bem jurídicos tutelados pela Constituição Federal, bem como, os protegidos por outros ramos do direito estão praticando os chamados crimes informáticos.

Sendo assim, os crimes cibernéticos podem ser classificados como toda conduta típica, ilícita e culpável praticada com ou sem o uso da internet por meio de um computador ou de outros dispositivos eletrônicos.

3 ESPÉCIES DE CRIMES CIBERNÉTICOS

Segundo o doutrinador Luiz Flávio Gomes os crimes informáticos dividem-se em crimes contra o computador; e crimes por meio do computador, em que este serve de instrumento para atingimento da meta optada.

O Brasil ocupa um lugar de destaque na prática dos crimes cibernéticos, conforme destaca reportagem de Laura Pancini, da revista exame-tecnologia:

> A empresa de cibersegurança Norton divulgou recentemente os resultados de sua pesquisa, conduzida em parceria com o The Harris Poll, que destaca o Brasil como o terceiro país com mais dispositivos infectados por ameaças. De acordo

> com a análise, mais da metade (58%) dos brasileiros entrevistados afirma ter sofrido um crime cibernético em 2021.
>
> A pesquisa estima que cerca de 71 milhões de brasileiros sofreram ataques cibernéticos nos últimos 12 meses, e que mais de 828 milhões de horas foram gastas (uma média de 11,6 horas por pessoa) tentando resolver os problemas.
>
> Entre os entrevistados, 37% afirmam que detectaram software malicioso em um computador, rede Wi-Fi, smartphone, tablet, casa inteligente ou outro dispositivo conectado e 10% sabem que suas informações pessoais foram expostas em um vazamento de dados.
>
> A estimativa é que 32 bilhões de reais foram perdidos somente no ano passado, já que mais da metade das vítimas de crimes cibernéticos do último ano foi impactada financeiramente.
>
> Dentre os 10 países entrevistados (Austrália, Brasil, França, Alemanha, Índia, Itália, Japão, Nova Zelândia, Reino Unido e Estados Unidos), o Brasil é o terceiro com mais aparelhos eletrônicos infectados por stalkerware, que são aplicativos de espionagem, e ficou atrás apenas da Índia e dos EUA. (PANCINI,2022)

Na mesma perspectiva, a 'Internet Organised Crime Threat Assessment - IOCTA', da Europol, em um relatório feito em 2018, informou que “de modo semelhante aos EUA, o Brasil é um dos principais hospedeiros de sites de phishing[6], com alguns relatos colocando o Brasil como uma das dez maiores fontes mundiais de ataques cibernéticos.” (DECRETO n° 10.222/20)

A maioria dos crimes previstos no mundo real também estão presentes no mundo virtual. Sendo assim, os crimes cibernéticos correspondem de certo modo a todas as condutas tipificadas no ordenamento jurídico brasileiro, as quais são cometidas por intermédio do uso da tecnologia.

Nesse contexto, verifica-se os fatos que já possuem tipificação legal pelo ordenamento, com a internet, ficaram vistos apenas como uma nova instrumentalização da modalidade delitiva.

Segundo Grégore de Moura:

> O surgimento de novos aplicativos diariamente e a consequente criação de novas relações e bens jurídicos fazem surgir uma demanda por controle, visto que,

[6] Phishing, (pronunciado: fishing) é uma expressão originaria da língua inglesa, da palavra fishing (pescaria). Esse método de “pescar dados” é utilizado pelos cibercriminoso que coletam informações pessoais de suas vítimas por meio de ferramentas, como e-mails, aplicativos e sites enganosos, para que, dessa maneira, eles possam roubar o dinheiro ou a identidade dessas vítimas sendo possível, coletar dados pessoais, tais como, números de cartão de crédito e informações bancárias.

> ainda que facilite sobremaneira a vida do cidadão, geram conflitos que demandam a atuação jurídica. (MOURA, 2021, p.14)

O número desses crimes praticados por intermédio da tecnologia tem crescido a cada dia devido a expansão e acesso de mais usuários à rede de computadores e internet, em que criminosos infiltrados em redes sociais, jogos on-line e em outras plataformas da internet, intensificaram o uso no meio virtual para aplicar golpes, praticar ameaças, injúrias, furtos, pedofilia e até extorsões.

> Esta inovação também repercutiu no âmbito do Direito Penal e Processual Penal, haja vista que até o ano de 2012, a internet era isenta de qualquer regulamentação jurídica específica e em virtude disto, se tornou meio apto para a realização de crimes e condutas danosas. A internet/infomática se mostra um instrumento facilitador para a consecução de crimes, pois, em muitos casos, o agente delituoso não precisa utilizar de nenhum instrumento físico que seja ou violento ou ameaçador para realização daqueles, bastando apenas o computador e o conhecimento técnico, ou não, para concretizar as condutas delitivas. (ROCHA, 2012, p.2)

Diante disso, existem diversas espécies de crimes comuns que tem sido praticados por intermédio da tecnologias, configurando os denominados crimes cibernéticos, podendo-se citar os crimes contra a honra (art.138 a 140 do CP), apologia ao crime (art. 287, CP), incitação ao crime (art. 286, CP), estelionato (Art. 171, do CP), ameaça (art. 147, do CP), divulgação de segredo (Art. 153, do CP), invasão de dispositivo informático (Art. 154-A, do CP), furto (Art. 155), furto com abuso de confiança ou mediante fraude ou destreza (art. 155, § 4º, inciso II, do CP), pornografia infantil, racismo, entre outros.

3.1 Crimes cibernéticos quanto à classificação

Nas palavras de Fernando Capez (2020, p. 185) “O crime pode ser conceituado sob três enfoques, quais sejam, aspecto material, aspecto formal e aspecto analítico”.

Nesta linha de pensamento, Ricardo Antônio Andreucci, afirma que:

> O crime pode ser conceituado sob o aspecto material (considerando o conteúdo do fato punível), sob o aspecto formal e sob o aspecto analítico. Conceito material de crime. Violação de um bem penalmente protegido. Conceito formal de crime. Conduta proibida por lei, com ameaça de pena criminal. Conceito analítico de crime: fato típico, antijurídico e culpável. (ANDREUCCI. 2010, p. 71).

Desse modo, os crimes cibernéticos são classificados como toda conduta típica, ilícita e culpável praticada por meio de um computador ou dispositivos eletrônicos, os quais podem ou não estar conectados à internet.

À vista disso, Augusto Rossini colaciona que:

> O conceito de 'delito informático' poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade. (ROSSINI, 2004, p. 78)

A doutrina classifica os crimes cibernéticos de duas formas diferentes. Uma parte da doutrina classifica os referidos crimes como puros, mistos e comuns, em contrapartida, a outra parte da doutrina os classifica como próprios e impróprios.

Segundo Reginaldo César Pinheiro, os crimes cibernéticos puros, mistos e comuns são classificados da seguinte forma:

> Os crimes cibernéticos puros levam em consideração toda e qualquer conduta ilícita que utilize de forma exclusiva o sistema de computador, englobando o atentado físico ou técnico deste, inclusive dados e sistemas. Já os crimes mistos são aqueles o uso da internet ou do sistema é condição primordial para a efetivação da conduta. Por fim, os crimes cibernéticos comuns são aqueles em que a internet é utilizada para como meio para a realização de um crime já tipificado em lei (PINHEIRO, 2002, p. 85-87).

Os crimes cibernéticos próprios são condutas não tipificadas no ordenamento jurídico, as quais dependem da tecnologia da informação. A disseminação de vírus e a invasão de dispositivo informático (art. 154-A do CP), são exemplos de crimes cibernéticos próprios.

No que tange os crimes comuns e os próprios é importante frisar que eles não devem ser confundidos, pois conforme define Grégore de Moura:

> Crime comum é aquele que pode ser cometido por qualquer pessoa (exemplo: crime de homicídio previsto no artigo 121 do Código Penal), já o crime próprio exige um atributo ou qualidade especial do sujeito ativo (exemplo: condição de funcionário público no crime de peculato previsto no artigo 312 do Código Penal). (MOURA, 2021, p.23)

Os crimes cibernéticos impróprios podem ser classificados como condutas já tipificadas no ordenamento jurídico**,** as quais podem ser realizadas não somente no campo virtual, ou seja, podem se consumar em outro modus operandi. Sendo assim, nos crimes cibernéticos impróprios, a tecnologia da informação é utilizada como auxilio para o cometimento do ato ilícito. São exemplos de crimes cibernéticos impróprios, o estelionato, os crimes contra a honra, os crimes de invasão de privacidade e intimidade e os crimes contra a liberdade sexual.

Nesse sentido, Túlio Vianna e Felipe Machado alegam que:

> [...] os crimes próprios são considerados aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas. Já os crimes impróprios seriam aqueles que atingem um bem jurídico comum, como por exemplo, o patrimônio do indivíduo através de um sistema informático (VIANNA; MACHADO, 2013, p. 30- 32).

Humberto Martins estabelece que os crimes cibernéticos mais comuns são:

> Destaca-se os seguintes crimes contra a honra, "crime de difamação, crime de calúnia, crime de injúria" e também existem os crimes de:
>
> • Invasão de privacidade: ocorre o acesso ilegal as informações de usuários, com possibilidade de vazar informações;
>
> • Espionagem eletrônica: através dos softwares que espiam informações nos servidores de forma indevida;
>
> • Fraudes virtuais: a conduta refere-se à modificação, alteração ou adulteração de um sistema de processamento de dados ou programa eletrônico;
>
> • Pornografia infantil: tem-se a divulgação ou comercialização de material erótico envolvendo crianças ou adolescentes;
>
> • Contra a propriedade intelectual refere-se aos materiais com dados copiados que circulam livremente;
>
> • Estelionato: tem-se a intenção de adquirir para si ou para outras vantagens ilícitas;
>
> • E outros que aparecem em menor número. (MARTINS, 2017, p. 20)

Conforme exposto, percebe-se que os delitos praticados com maior frequência na internet são os denominados delitos cibernéticos impróprios os quais são praticados por meio do computador. Assim, com o advento da internet, a criação popularização e expansão das redes sociais promoveu uma grande interação entre as pessoas, contribuindo com a atuação de criminosos por meio da denominada engenharia social, a qual pode ser definida como o "conjunto de técnicas e subterfúgios utilizados pelos criminosos para atuar nas vulnerabilidades emotivas da vítima e não nas vulnerabilidades do computador." (MOURA, 2021, p.23).

Ocasionando uma expressiva prática de crimes informáticos impróprios como os crimes contra a honra, por exemplo.

A prática dos ataques supracitados tem sido muito recorrente durante a pandemia da covid-19, tendo em vista a maior fragilidade das empresas e da população em geral que com o isolamento social passaram a ficar mais tempo conectados à internet.

3.2 Lugar do crime e competência

> O desafio no combate aos crimes informáticos é hercúleo, já que o "mundo virtual" se caracteriza pela imediatidade (tudo opera com rapidez e em tempo real), desterritorialidade (os crimes "atravessam" diversos países, o que dificulta a definição da jurisdição e da competência para julgamento, refletindo na apuração dos fatos), imaterialidade (as informações são líquidas) e interatividade (maior interação, mais possibilidade de ocorrência de crimes). (POLICARPO,2016, p.203)

Os limites fixados pelos critérios de territorialidade e de nacionalidade na prática de crimes cibernéticos foram ultrapassados, com o aumento das redes e acessos a meios eletrônicos a representatividade da internet se expandiu por todo o mundo, necessitando então de outras interpretações acerca da determinação do lugar do crime e de sua competência fazendo com que se dívida o iter criminis. Portanto, o fato de os crimes cibernéticos serem desterritorializados, dificulta a apuração e definição da jurisdição competente para julga esses crimes.

Em razão de tal dificuldade o Código Penal em seu art. 6°, por exemplo, utiliza a Teoria da Ubiquidade, a qual considera como lugar do crime, o local onde aconteceu a ação ou omissão, assim como, o local onde ocorreu ou deveria ocorrer o resultado (BRASIL,1940). Assim, essa teoria geralmente também é aplicada nos crimes cibernéticos pois, esses crimes podem ser praticados tanto em território nacional quanto internacional.

Ivette Ferreira aduz que:

> a mobilidade dos dados nos sistemas de informática, que facilita largamente que os delitos sejam cometidos à distância, usando-se um computador num determinado país e ocorrendo os resultados em outro, bem como os atentado às redes de telecomunicações internacionais, que atravessam vários países. (FERREIRA, 2001, p. 212-213)

De acordo com a doutrina a aplicação da Lei Penal no ciberespaço deve observar cinco princípios, os quais estão expressamente previstos nos artigos 5°, 6° e 7°, do Código Penal

Brasileiro, quais sejam os princípios da territorialidade, nacionalidade, proteção, da representação e da justiça universal.

O STJ e o artigo 70, do Código de Processo Penal afirmam que a determinação da competência do lugar em a infração foi consumada será estabelecida em razão do lugar onde a conduta criminosa foi consumada, ou se tratando de tentativa, no lugar em que for praticado o último ato de execução. (BRASIL,1940)

Por esse ângulo, Damásio de Jesus (2000, p. 117) entende que, "para casos relacionados à internet, deveria ser adotado algo semelhante à teoria da atividade que, como visto, determina como sendo o local do crime aquele em que o agente praticou o delito."

Portanto, a lei em si, não se refere como serão feitas a fixação de competência para julgar os delitos virtuais, no entanto, a doutrina e a jurisprudência utilizam como base para a verificação do lugar de consumação do crime ou lugar do último ato de execução, uma vez que tais crimes podem causar efeitos em territórios de outros países.

4 MÉTODOS UTILIZADOS NO COMBATE AOS CRIMES CIBERNÉTICOS

O filosofo e sociólogo polonês Zygmunt Bauman utiliza o termo modernidade líquida para definir a sociedade moderna, que vive em um mundo globalizado, o qual segundo ele é um mundo cercado de incertezas que por intermédio dos avanços tecnológicos e da criação das redes socias, resultou na quebra das relações sociais e das noções de tempo e espaço. Logo, o referido conceito pode ser definido da seguinte forma:

> A modernidade líquida gera a falta do sentimento de comunidade e esfacela a solidez das relações sociais o que, por consequência, faz com que o ator racional (o criminoso) se motive para a prática delituosa, não só por "valer mais a pena" (risco menor de ser pego e aumento desproporcional da lucratividade pelo proveito do crime), como também pela dificuldade em se investigar e punir esse tipo de criminalidade (a autoria, a materialidade, enfim, a prova deste tipo de crime é também "líquida").(MOURA, 2021, p.18)

Assim, por meio do desenvolvimento tecnológico e das mudanças socias advindas da modernidade líquida, a população se tornou mais vulnerável e propicia a ser vítimas dos chamados crimes cibernéticos, os quais estão cada vez mais difíceis de serem punidos e investigados, tendo em vista, a ruptura da noção de tempo e espaço existente, o que pode gerar um ambiente de impunidade e incertezas.

Portanto, as inovações tecnológicas originaram novos bens e relações jurídicas, o que resultou no surgimento de novos crimes como os crimes cibernéticos, os quais geraram a necessidade de criação de novos métodos de combate como a regulamentações de novas legislações e a criação de novas formas de investigação.

4.1 Investigação policial

Existem incontáveis maneiras de se praticar um crime cibernético, considerando o grande dinamismo das tecnologias disponíveis na internet. Um importante aspecto a ser considerado na investigação policial é identificar a ferramenta utilizada para cometimento do crime virtual.

Segundo o Ministério Público Federal (2015, p.35), os procedimentos administrativos e processuais usados para desvendar a conduta e autoria dos crimes cibernéticos são os seguintes: "identificação do meio empregado; preservação das provas, identificação dos responsáveis pelo serviço; quebra de sigilo de dados telemáticos (usuários); comprovação da autoria."

Alexandre Morais alega que:

> A revolução tecnológica e informacional exige a atitude de rever velhas práticas costumeiras, especialmente por quem se acha capaz de manter o antigo modo de decisão, mas que atualmente, com um pouco de realismo, encontra-se defasado. O tempo, a velocidade da informação, lançam novos desafios aos agentes da lei, cujo papel restou alterado. (MORAES, 2019, p.4)

Desse modo, para acompanhar os avanços tecnológicos e os cibercriminosos que estão em constante especialização, as autoridades policiais devem adotar rumos diferentes de acordo com a técnica empregada pelos criminosos. Cabe destacar a prática comum, por parte do criminoso, apagar e alterar dados, tentar ocultar vestígios e com isso dificultar o processo investigatório. Toda essa intenção de agravar a identificação do criminoso demanda maiores esforços na análise criminal. Existe grande complexidade na identificação dos crimes cibernéticos diante das inúmeras formas de cometimento de delitos (DA SILVA e DA SILVA, 2019; CAVALCANTI, 2021).

No Brasil a evolução e avanço dos primeiros passos no controle e combate desses crimes ocorreu com a criação de órgãos especializados como delegacias ou estruturas dentro das polícias com essa especificidade. Minas Gerais, por exemplo possui a Delegacia

Especializada – DEICC a qual é regulamentada pela Resolução 8004 de 14/3/2018 e tem a atribuições elencada no artigo 27 da referida resolução.

Diante das dificuldades enfrentadas durante a investigação dos crimes cibernéticos, em entrevista ao UOL, Rafael Alcadipani, professor da Fundação Getúlio Vargas e membro do Fórum Brasileiro de Segurança Público, disse o seguinte:

> Como as quadrilhas não precisam estar no mesmo local da vítima, há dificuldades extras para as polícias. "Um sujeito no Rio consegue aplicar um golpe em São Paulo, um sujeito no Acre consegue aplicar um golpe na Bahia. É preciso ter uma regulação muito maior da abertura de contas e uma desburocratização da investigação criminal." (ALCADIPANI, 2022)

Além da desterritorialidade e dos mecanismos que permitem ocultar a identidade dos criminosos pela capilaridade mundial da internet, as redes sociais capacitaram maior interação entre as pessoas, especialmente após a pandemia da Covid-19 que permitiu as pessoas a terem basicamente o mundo virtual como meio de comunicação durante o seu período de ocorrência, aumentando os crimes informáticos impróprios além de consistir em um ambiente propicio para a aplicação de técnicas de engenharia social por parte dos criminosos, neste meio há valiosa participação da vítima, uma vez que as informações por elas compartilhadas por meio das redes, muitas vezes facilitam para que se tornem alvos fáceis.

Diante disso, Gustavo Corrêa (2010, p. 87) afirma que o obstáculo para o combate dos crimes cibernéticos é "a quase ausência de evidências que provem contra o autor e a inexistência da arma no local do crime".

A obtenção de prova é de extrema importância desvendar o ato criminoso e encontrar o autor do delito. Porém, as autoridades competentes por investigar os crimes cibernéticos possuem dificuldade na obtenção de indícios da autoria e prova da materialidade, tendo em vista que os crimes cibernéticos geralmente não deixam traços nem evidências, sendo considerados "crimes perfeitos".

Nesse seguimento, o advogado criminalista, especialista em cibercrimes, D'URSO (2019), em entrevista ao Jornal Estadão afirmou que, a maior dificuldade com relação ao combate desses crimes está relacionada à dificuldade de se fazer prova e investigar a origem do delito, a materialidade e a autoria, bem como a falta de conhecimento técnico dos

usuários, as supostas vítimas, tornando alvos fáceis do cibercriminoso e a variedade de delitos, que é quase ilimitada.

Um importante aspecto a ser analisado é o Log File (processo de registro de eventos relevantes num sistema computacional). Ao utilizar a internet ou realizar acessos pacotes são trocados entre cliente e servidor e o endereço da máquina de acesso é registrado nos logs. Tudo que for realizado na troca de informações é armazenado no Log de forma que isso pode ser acessado pela equipe investigadora contribuindo para identificação do delito.

O log traz consigo inúmeras informações que permitem ao investigador verificar a consistência das informações e traçar caminhos que permitam identificar o criminoso (VALENTE, 2012; CAVALCANTI, 2021). Como mencionado acima o endereço da máquina de acesso é de muita relevância no que tange a localização da máquina invasora. De posse desse endereço chamado de IP (internet protocol) pode-se chegar ao exato local que iniciou o ato criminoso, podendo assim identificar, inclusive o criminoso (VALENTE, 2012; CAVALCANTI, 2021).

Alguns crimes são cometidos por meio de websites na internet. Os sites podem coletar informações e disseminá-las na grande rede mundial. Alguns criminosos criam sites idênticos aos originais com o intento de obter informações pessoais dos usuários. Mas para isso o site precisa ser colocado em um servidor e precisa ter um endereço web válido para que o acesso seja feito. A investigação nesses casos coleta tudo que for possível desse website falso para que haja profunda investigação nesses dados, buscando assim identificar aspectos que possam levar ao criminoso (DA SILVA e DA SILVA, 2019; CAVALCANTI, 2021).

A investigação policial também pode ser realizada por interceptação telemática, mas esse processo não é tão simples por esbarrar em uma série de gargalos tecnológicos dificultando a padronização da investigação. Essa investigação faz a análise de pacotes transmitido via internet, acontece que não é possível formar um arquivo completo em pacotes interceptados de forma incompleta o que gera dados faltantes dificultando o entendimento da autoridade policial (VALENTE, 2012; CAVALCANTI, 2021).

> Pelo desenvolvimento e evolução da tecnologia da informação, a investigação passa a outro nível, pois os ocultadores de IP, as criptografias e diversas outras técnicas para manutenção do anonimato, tornam necessárias outras formas investigativas, como a investigação *undercover,* a infiltração e o incentivo a delações de membros das quadrilhas especializadas na pratica de crimes informáticos , a vigilância ostensiva e o monitoramento diário por agência executivas, a próprio estado, instalação de programas em aparelhos de prisioneiro, uso de GPS, análise de aparelhos relacionados à internet das coisas (lOt), entre outros elementos. (MOURA, 2021, p. 286).

Diante disso, foram adotadas no Brasil medidas para ajudar na investigação dos crimes cibernéticos como a como a cadeia de custódia e a infiltração policial a qual foi aderida ao Brasil em 1995 e revogada em 2013 por meio do artigo 10 da Lei 12.850/2013, onde até então não havia menção em lei quanto a sua utilização da investigação undercover (infiltração policial) em crimes cibernéticos, a qual veio a ser reconhecida após as alterações promovidas pelo Pacote Anticrime (Lei 13.964/2019), mais especificamente em seu artigo 10 que possui a seguinte redação:

> Art. 10-A. Será admitida a ação de agentes de polícia infiltrados virtuais, obedecidos os requisitos do caput do art. 10, na internet, com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas. (BRASIL, 2019)

Outro importante meio de investigação trazido pelo Pacote Anticrime foi a alteração ao Capítulo II (Do exame de Corpo de Delito, da Cadeia de Custodia e da Perícias em Geral) trazendo a aplicação da Cadeia de Custódia aos crimes virtuais, sendo de grande importância na apuração dos crimes informáticos, conforme afirma Grégore de Moura:

> Como a prova pericial assume papel de relevância na apuração dos crimes informáticos, pela sua natureza e modo de execução, faz-se mister tratar da cadeia de custódia e sua aplicação a este tipo de criminalidade, o qual exige transparência, preservação de dados e segurança na análise probatória, em virtude da volatilidade dos dados informáticos e a possibilidade de sua alteração em frações de segundos. (MOURA, 2021, p.302)

No que diz respeito a adoção de medidas, como as citadas anteriormente para o combate aos crimes cibernéticos Ricardo Uberto Rodrigues, afirma o seguinte:

> A proliferação dos denominados “crimes cibernéticos” tem exigido dos agentes envolvidos em sua repressão a adoção de medidas compatíveis com a instantaneidade e com a peculiar característica nômade destes delitos, as quais, muitas vezes, não se demonstram suficientemente previstas no arcabouço das medidas processuais penais típicas, vazadas na legislação vigente. A atual quadra de desenvolvimento tecnológico da humanidade impõe aos órgãos de repressão

> penal das condutas veiculadas pela rede mundial de computadores que sejam dotados de instrumentos eficazes ao combate dos "crimes cibernéticos". Hodiernamente, constitui-se em desafio aos órgãos de repressão penal a obtenção de informações e dados existentes em provedores, em tempo mínimo, para que possam ser adotadas providências no sentido de identificar os autores do delito e colher provas atinentes à sua "materialidade". (RODRIGUES, 2018, p. 153)

Apesar das medidas adotadas e inclusas recentemente como os órgãos especializados e o pacote anticrime, entende-se que a principal demanda apontada frente ao combate dos crimes cibernéticos com foco no avanço e evolução da tecnologia que ocorre progressivamente é a necessidade crucial de aperfeiçoamento mútuo dos agentes que atuam diretamente contra as infrações virtuais, o que tornará o enfrentamento a essas condutas mais eficaz.

4.2 Legislações vigentes

Os crimes cibernéticos não possuem uma legislação específica no Brasil, eles são abordados em alguns artigos e legislações do ordenamento jurídico brasileiro, também é aplicada a analogia para a punição e identificação dos referido crimes. Porém, tal conduta não pode ser aplicada no direito penal, pois o princípio da analogia fere o princípio da taxatividade e também vai contra ao que estabelece o princípio da legalidade, pois de acordo com esse princípio previsto no artigo 1º do Código Penal, bem no artigo 5º, XXXIX da Constituição Federal, "não há crime sem lei anterior que o defina e não há pena sem prévia cominação legal" (BRASIL, 1940). Dessa forma, uma conduta não prevista em lei não pode ser considerada crime.

Á vista disso, Justiniano determina que:

> Como a jurisprudência atual denota que não há o que falar em crime sem observar tal princípio, é de suma importância que o ordenamento jurídico observe práticas que não tenham consagração legal, como no caso de delitos cibernéticos." (JUSTINIANO, 2017, p. 35).

Atualmente as legislações que tratam sobre os crimes cibernéticos são, a Lei nº 12.737/2012, a lei do Marco Civil da Internet (Lei 12.965/2014), A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18) e a lei 14.155/21 e recentemente o Brasil aprovou a adesão à Convenção de Budapeste.

De acordo com Grégore Moura, "no caso dos crimes informáticos, a política criminal até a Lei Carolina Dieckmann era praticamente inexistente, ao menos em relação aos crimes informáticos próprios." (MOURA,2021, p.174)

A Lei nº 12.737/2012, também conhecida como "Lei Carolina Dickmann", foi a primeira lei brasileira que abordou de modo específico os crimes cibernéticos. A referida lei alterou o Decreto-Lei nº 2.848/40(Código Penal), acrescentando a ele os artigos 154-A e 154-B os quais discorrem sobre o delito de invasão de disposto informático.

No ano de 2011 a atriz Carolina Dieckmann teve sua privacidade violada e sua intimidade exposta por um infrator que invadiu o computador pessoal da atriz e através disso conseguiu acessar e expor fotos pessoais de cunho intimo da mesma. O infrator foi julgado pelo crime de extorsão previsto no artigo 158 do Código Penal, tendo em vista que, após o furto das imagens ele exigiu que a atriz pagasse um determinado valor para que as fotos dela não fossem divulgadas.

Dois anos após a criação da "Lei Carolina Dickmann", foi sancionada a lei do Marco Civil da Internet (Lei 12.965/2014) também apelidada como Constituição da Internet Brasileira por ter como objetivar a garantia dos direitos constitucionais no meio virtual, bem com assegurar o uso da internet de forma segura. Sendo assim, a Lei 12.965/2014 visa instituir princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Desse modo, Moisés de Oliveira Cassanti afirma que:

> Remoção de conteúdo: Segundo o Marco Civil, os provedores de conexão à internet não serão civilmente responsáveis por danos relacionados ao conteúdo gerado por terceiros (essas empresas não responderão na Justiça pelo conteúdo publicado por seus usuários. Isso só acontecerá, após ordem judicial, a empresa não tome as providências para tornar o conteúdo indisponível. Dados pessoais: O Marco Civil assegura ao internauta o direito ao sigilo de suas comunicações via internet (salvo por ordem judicial); informações claras e completas dos contratos de prestação de serviço; não fornecimento a terceiros de seus registros (...) Neutralidade da rede: Este item propõe que o responsável pela transmissão do conteúdo deve tratar de forma igual quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino. É a chamada neutralidade da rede. (CASSANTI, 2014, p. 91-92)

Com base no artigo 3º da referida lei, devem ser respeitados os seguintes princípios:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção

> dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (BRASIL, 2014).

A lei do Marco Civil da internet determina que os registros de conexão e de acesso devem ser preservados, sob sigilo, por um determinado período, o qual pode ser prorrogado por autoridade competente, sendo assim, com base nos artigos 13 e 15 da referida lei:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput. (BRASIL, 2014). Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13. (BRASIL, 2014).

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709, de 14 de agosto de 2018) entrou em vigor em 2020 e possui como inspiração a GDPR (General Data Protection Regulation), que entrou em vigor na União Europeia em 2018. A LGPD complementa a lei do marco civil da internet no que diz respeito ao tratamento de dados pessoais e dispõe sobre o tratamento de dados pessoais, tanto das pessoas físicas quanto das jurídicas, inclusive nos meios digitais, buscando salvaguardar os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018)

A supracitada lei visa garantir a proteção dos dados das empresas e de seus clientes evitando prejuízos e garantindo credibilidade. A referida lei busca assegurar que as empresas lidem com as informações de seus clientes com seriedade, segurança e transparência deixando claro o objetivo para sua coleta, armazenamento e processamento de dados. Portanto, as empresas ou órgãos públicos só poderão guardar

ou usar dados pessoais de seus clientes se houver o consentimento expresso dos mesmos, seja no mundo virtual ou no físico.

Conforme estabelece o artigo 7º, inciso I, da Lei nº 13.709/18 o fornecimento de dados pessoais apenas poderá ocorrer mediante o consentimento do titular e nas demais hipóteses elencadas no referido artigo. (BRASIL, 2018). Portanto, através da Lei nº 13.709/18 o cidadão passou a ter um maior controle sobre a coleta e a utilização dos seus dados.

Diante do aumento dos crimes cibernéticos e da gravidade dos danos causados por eles entrou em vigor recentemente a Lei 14.155/21, a qual altera o Código Penal e no Código de Processo Penal estabelecendo penas mais rígidas aos crimes de violação de dispositivo informático, furto e estelionato realizados de forma eletrônica ou pela internet.

A referida lei preenche a lacuna existente no artigo 154-A do Código Penal que antes determinava que a invasão de dispositivo devia ocorrer através da violação indevida de mecanismo de segurança, ou seja, para configurar invasão de dispositivo informático era necessário que o infrator ultrapassasse um dispositivo de segurança como senha, antivírus, firewall ou qualquer outro meio que torne o dispositivo eletrônico mais seguro. Agora em detrimento da Lei 14.155/21 não é mais necessário que a invasão de dispositivo informático aconteça por meio de violação indevida de dispositivo de segurança.

As legislações abordadas anteriormente possuem como objetivo estabelecer, identificar, reformular e atualizar as legislações que discorrem sobre os crimes cibernéticos, os quais estão em sua maioria tipificados no ordenamento jurídico brasileiro, no entanto, os cibercriminosos não praticam somente as condutas já tipificadas, pois existem condutas que ocorrem somente no meio virtual e as mesmas não se encontram tipificadas e estão cada dia mais evoluídas. Desse modo, a política criminal brasileira no que se refere aos crimes cibernéticos ainda necessita de muita evolução.

Nesse prisma, conforme relatório, de 2018, da IOCTA, da Agência da União Europeia para a Cooperação Policial – Europol:

> a falta de legislação adequada sobre crimes cibernéticos fez com que o Brasil fosse o alvo número um e a principal fonte de ataques online na América Latina;

> 54% dos ataques cibernéticos reportados no Brasil supostamente são originários de dentro do país. (DECRETO Nº 10.222/20)

Diante desse fator, surgem questionamentos no meio jurídico a respeito da eficácia e suficiência das legislações vigentes, exigindo do legislador uma análise minuciosa das condutas e das tecnologias usadas pelos cibercriminosos para estabelecer punições eficazes às práticas delituosas cometidas no meio digital.

O Ministério Público Federal, através da Cartilha de Atuação do MPF no combate aos crimes cibernéticos, elencou os seguintes problemas no que concerne a deficiência da legislação brasileira:

> Necessidade de violação de dispositivo de segurança para configurar o crime, o texto não protege igualmente os dispositivos que têm ou não senha. O crime não pode ficar condicionado à presença de barreira de segurança; - O indevido acesso por si só, ainda que com violação de mecanismos de segurança, não é punido, porque essa lei prevê a invasão como ocupação ou conquista pela força e de modo abusivo. - O uso do termo "dispositivo informático" também é criticado porque deveria ter sido usado "dispositivo eletrônico" justamente para abranger a grande quantidade de celulares, televisores etc., que permitem acesso à Internet; - Ausência de definição de termos técnicos; - Ínfima quantidade de pena a ser aplicada, enquadrando a conduta no âmbito dos crimes de pequeno potencial lesivo. (MINISTÉRIO PÚBLICO FEDERAL, 2015, p.32)

Assim, Barbosa (2020), estabelece que o aprimoramento do legislativo é importante para que sociedade não fique refém de leis complexas ou ineficientes. O autor ainda destaca a necessidade de constante evolução dos mecanismos digitais de combate e proteção aos dados dos usuários, confirmando o considerável desconhecimento dos usuários acerca de formas de proteção e esquiva de golpes e ataques virtuais.

Por último a adesão do Brasil à Convenção sobre o Crime Cibernético, conhecida como Convenção de Budapeste assinada por mais de 60 países e utilizada em outros 160 como orientação para legislações locais.

O Projeto de Decreto Legislativo (PDL) 255/2021 foi aprovado pela Câmara dos deputados e aguarda promulgação pelo Congresso Nacional, este tem por objetivo a cooperação internacional para o cibercrime e também da criminalização de condutas, normas para investigação e produção de provas eletrônica, dessa forma irá agilizar o acesso das autoridades brasileiras a provas eletrônicas sob jurisdição estrangeira.

O pedido para tal adesão foi feito pelo procurador da República George Lodder, que integra o Grupo de Apoio sobre Criminalidade Cibernética da Câmara Criminal do MPF (2CCR/MPF).

> (...) atualmente, muitas das informações sobre crimes de pedofilia e outros praticados no Brasil por meio da internet chegam ao conhecimento das autoridades nacionais por meio do National Center for Missing & Exploited Children (NCMEC), entidade privada sem fins lucrativos que atua nos Estados Unidos, onde a legislação estabelece que essa comunicação é obrigatória. (MINISTÉRIO PÚBLICO FEDERAL,2021)

A PDL 255/2021 abrange todos os crimes classificados como “próprios” e “impróprios”, incluindo no texto disposições adicionais sobre a tentativa, auxílio e incitação ao cometimento das infrações descritas, e trata também de sanções e medidas quanto à responsabilidade das pessoas jurídicas.

Contem no texto determinação à articulação de uma rede que funcione a qualquer momento, e que cada Estado-membro poderá designar um ponto de contato disponível todo o tempo a fim de assegurar a prestação de assistência imediata a investigações ou procedimentos relativos a infrações penais ou mesmo para recolher provas eletrônicas de uma infração penal.

Apesar de tardia, a adesão a Convenção de Budapeste é de extrema relevância, tendo em vista que a internet é uma ‘terra sem fronteiras’ onde pode acontecer de o autor e a vítima dos crimes cibernéticos serem de países diferentes e esse é justamente o problema, pois cada país tem sua própria legislação o que dificulta a definição de competência para apuração do crime e até mesmo a busca pelos dados, investigação e punição desses crimes.

5 CRIMES CIBERNÉTICOS NA PANDEMIA DA COVID-19

O uso global da internet vem se expandindo gradualmente desde o seu surgimento em 1969, e através deste crescimento foi possível estabelecer uma integração cultural e econômica com todos os outros países do mundo, o que faz com ela esteja diretamente ligada a globalização e a evolução tecnológica, a comunicação com outros países se tornou cada vez mais fácil e eficiente.

Apesar de todos os benefícios que se acentuaram ao longo dos anos, o mundo virtual proporcionou também o início das práticas de crimes virtuais, os quais são praticados pelos cibercriminosos que aproveitam o anonimato decorrente desse mundo virtual para a prática de atos ilícitos que podem ser cometidos contra o computador ou por meio do dele.

O século XXI é marcado pelo uso indiscriminado da tecnologia, no primeiro semestre de 2021 em uma pesquisa divulgada pelo CUPONATION foi apontado que "existem cerca de 4,66 bilhões de usuários ativos na internet em todo o mundo, o que equivale a 59,5% da população mundial" (CUPONATION, 2021), o que quer dizer que mais da metade da população mundial tem acesso ao universo virtual, o fácil acesso a este meio permite cada vez mais consulta a informações, comunicação, atividades que não precisam de se locomover para que sejam realizadas como compras, serviços bancários, e trabalho remoto com grande satisfação, tornando o mundo virtual um ambiente cada vez mais propício a pratica de crimes cibernéticos .

Não obstante esse aumento nos números de usuários da internet, em 2020, ocorreu um fenômeno mundial, que ocasionou o isolamento de pessoas ao redor do mundo, a pandemia da Covid-19, fenômeno que ocasionou o isolamento social ou medidas mais restritivas como o lockdown que promoveram um expressivo e prolongado uso da internet acentuando ainda mais a prática de crimes de natureza virtual.

5.1 A Pandemia da COVID-19

A COVID-19 é uma infecção respiratória aguda causada pelo coronavírus SARS-CoV-2, com grave e elevado potencial de transmissibilidade, além de ser de distribuição global, foi descoberta em amostras obtidas de pacientes na cidade de Wuhan, província de Hubei, China em dezembro de 2019.

Segundo a Organização Pan-Americana da Saúde:

> Em 31 de dezembro de 2019, a Organização Mundial da Saúde (OMS) foi alertada sobre vários casos de pneumonia na cidade de Wuhan, província de Hubei, na República Popular da China. Tratava-se de uma nova cepa (tipo) de coronavírus que não havia sido identificada antes em seres humanos (...) e em 11 de fevereiro de 2020, recebeu o nome de SARS-CoV-2). Esse novo coronavírus é responsável por causar a doença COVID-19. (OPAS, 2021)

Em 30 de janeiro de 2020, a OMS (Organização Mundial da Saúde) declarou o novo coronavírus como uma Emergência de Saúde Pública de Importância Internacional (o mais alto nível de alerta da Organização), buscando interromper a propagação do vírus por meio da coordenação, cooperação e solidariedade global, o que não deu muito certo, pois ele se espalhou- rapidamente pelo mundo todo passando, assim, a ser denominado como uma pandemia em março do mesmo ano. (OPAS, 2021)

O primeiro caso de contaminação registrado no Brasil foi em 26 de fevereiro de 2020 e após mais de dois anos no 1° de novembro de 2022, o Conselho Nacional dos Secretários de Saúde informou que o Brasil possui "34.837.035 casos confirmados e 688.219 mortes" pela Covid-19. (CONASS,2022). E até o presente momento de acordo dados do Worldometers, o Brasil se encontra no ranking mundial como o segundo país em número de óbitos e o terceiro em número de casos confirmados de infectados pelo vírus. (WORLDOMETERS,2022)

O primeiro caso de contaminação de fevereiro 2020 e desde de então os números de casos cresceram de forma acelerada fazendo com que fossem adotadas medidas como o uso de máscara, álcool em gel e o isolamento social onde a população ficou um grande período em casa isolada do convívio com outros indivíduos ou com um grupo de indivíduos para evitar a propagação da doença, ficando consequentemente mais vulnerável, pois sem ter nada para fazer ou trabalhando de forma remota a internet se tornou um grande aliado para a população e junto com ela também vieram os cibercriminosos que se aproveitaram desse momento de fragilidade para cometer crimes virtuais.

5.2 A pandemia e o aumento dos crimes cibernéticos

Frente a pandemia causada pela COVID 19 em que o mundo inteiro acompanha, o avanço da tecnologia nos últimos anos teve relevante evolução e durante o período de isolamento as pessoas e organizações foram instruídas a utilizar deste meio o tornado fundamental tanto em casa quanto no trabalho, conforme mostra a pesquisa realizada pela FIA Employee Experience (2020), 90% das empresas brasileiras aderiram alguma modalidade de home office. Logo, durante esse período as pessoas passaram a ficar cada vez mais conectadas e em decorrência de tal fato a internet teve um crescimento inigualável se comparado a períodos anteriores.

Diante deste cenário, oportuno fora também o crescimento para a prática de crimes virtuais, a Europol afirma o seguinte:

> Como de costume, os cibercriminosos foram particularmente rápidos em se adaptar à crise da COVID-19, aproveitando os eventos atuais e as notícias para aumentar a probabilidade de infectar vítimas que procuram informações relacionadas. Eles têm explorado a ansiedade crescente dos indivíduos, a demanda por informações e o fornecimento de certos produtos, bem como a confiança em soluções digitais ao trabalhar em casa e oferecer educação em casa para as crianças. (EUROPOL, 2020)

Como assevera Grégore de moura (2021, p.26), "computadores pessoais, tablets, smartwatch, smartphones e outros objetos, armazenam dados mais privados do que aqueles que estão em nossa própria residência, uma vez que o que era materializado tornou-se virtualizado." Assim aproveitando esse cenário onde o mundo virtual está se tornando cada vez mais vital e diante do aumento do número de usuários da internet durante a pandemia principalmente no período de isolamento social onde esse recurso se tornou essencial para o dia a dia da população, os crimes virtuais avançaram muito durante esse período conforme afirma Alvim Júnior, em uma entrevista ao UOL, na qual segundo ele:

> (...) já que mais pessoas passaram a recorrer a soluções digitais. Os criminosos, então, seguiram esse movimento e sofisticaram as ferramentas. "A partir do momento em que o smartphone ficou bem mais popularizado, que se consolidou a rede 4G e os aplicativos de banco permitiram mais ações dos usuários, os golpes passaram a se propagar." (JÚNIOR, 2022).

Dados coletados pela Kaspersky Lab evidenciaram que no mês de março de 2020 houve um aumento significativo de 124% de ataques a dispositivos móveis, mostrando que o Brasil veio a ser a região mais afetada com ataques de malware diários na América Latina, tendo 64,4% em proporção a sua população e esse aumento nos ataques cibernéticos, a maioria deles utilizando o a crise pandêmica como tema. (KASPERSKY LAB,2020)

A COVID-19 trouxe ao Brasil um alcance dos maiores índices jamais vistos. De acordo com a Fortinet Threat Intelligence Insider Latin America, de janeiro a setembro de 2020, o país sofreu mais de 3,4 bilhões de tentativas de ataques virtuais.

A migração repentina e despreparada da população para o ambiente virtual durante a pandemia contribuiu para esse cenário, pois a população necessitou da internet como instrumento para estudo, bem como para trabalho("home office"), sendo esse

instrumento implementado na grande maioria dos casos de forma rápida e sem muito planejamento, tornando a população vulnerável e o ambiente virtual propício para a prática de crimes virtuais, tendo em vista que, conforme afirmou Luis Corrons em uma entrevista à CNN Brasil, "A segurança, em muitos casos, ficou comprometida. A rede usada em casa, por exemplo, não é igual à da empresa – e isso abre brechas" (CORRONS,2021)

A tabela a seguir mostra os dados referentes a ocorrência de crimes cibernéticos correspondente aos anos de 2018 a 2021 sendo possível observar um claro e expressivo aumento desses crimes durante o período de auge da pandemia da COVID-19 que foi entre os anos de 2020,2021 e 2022.

Tabela 1 - Crimes cibernéticos correspondente aos anos de 2018 a 2021

Crimes cibernéticos	Mês / Fato												
Ano / tipo natureza	1	2	3	4	5	6	7	8	9	10	11	12	Total geral
2018													
Consumado	2406	2064	2516	2243	2062	2171	2255	2494	2324	2898	2499	2189	28121
Tentado	37	29	31	36	48	34	46	56	36	59	49	44	505
2019													
Consumado	2743	2633	2779	3054	3153	2688	2957	3112	3314	3620	3449	3139	36641
Tentado	59	55	57	73	101	90	86	106	111	119	120	110	1087
2020													
Consumo	3769	3513	3376	3571	4281	5207	5508	5161	5511	5852	5923	4649	56321
Tentado	145	125	105	121	171	194	243	243	224	215	226	173	2185
2021													
Consumado	5206												5206
Tentado	238												238
Total Geral	14603	8419	8864	9098	9816	10384	11095	11172	11520	12763	12266	10304	130304

Fonte: MOURA, Grégore Moreira de. **Curso de Direito Penal Informático**. Ed. D'Plácido. Minas Gerais. 2021. Anexo 6, p.451

De acordo com a CEACrim (Coordenadoria de Estatística e Análise Criminal), da Secretaria de Segurança Pública estadual de São Paulo, no ano de 2020, houve um aumento de 265% nos crimes praticados no ambiente virtual no estado de São Paulo. Já no Rio de Janeiro o ISP (Instituto de Segurança Pública) afirmou que houve um aumento de 11,8% nos casos

de golpe na internet. Em Minas Gerais, conforme os dados da polícia civil os crimes virtuais tiveram um aumento de 50% em 2020. (REDAÇÃO DC, 2021).

Em contrapartida durante esse mesmo período houve uma queda significativa nos índices de crimes violentos e de roubo no estado de Minas Gerais, conforme pode ser observado nas tabelas a seguir:

Tabela 2 – Registros de criminalidade

Ano	1	2	3	4	5	6	7	8	9	10	11	12	Total Geral
2012	6.512	6.417	7.001	7.115	6.964	6.667	6.550	6.755	6.492	7.198	7.117	7.735	82.523
2013	7.817	7.392	8.561	8.681	8.251	7.879	8.530	8.782	8.082	8.490	9.357	9.465	101.287
2014	10.059	9.590	10.451	9.870	10.344	8.821	8.853	9.712	9.837	10.277	10.093	10.198	118.105
2015	10.672	9.961	11.529	11.358	11.780	11.292	11.054	11.628	11.646	12.358	12.694	12.272	138.244
2016	13.403	12.763	13.514	13.368	13.285	12.354	12.605	12.517	12.570	13.487	13.651	13.233	156.750
2017	14.277	12.318	12.962	11.572	11.769	10.297	10.589	11.000	10.166	10.641	10.765	10.233	136.589
2018	10.132	8.969	8.956	8.264	7.403	7.210	7.334	7.482	7.088	7.920	7.298	7.033	95.089
2019	7.122	6.339	6.598	6.172	6.072	5.072	5.398	5.207	4.872	5.385	5.384	5.474	69.095
2020	5.545	5.481	4.615	3.577	3.198	3.260	3.144	3.076	3.186	3.686	3.753	3.996	46.517
2021	3.773	3.252	3.180	3.190	3.133	2.960	2.730	2.910	2.857	2.918	3.001	3.104	37.008
2022	2.898	2.574	3.659	3.500	3.052	2.861	2.890	2.881					24.315
Total Geral	**92.210**	**85.056**	**91.026**	**86.667**	**85.251**	**78.673**	**79.677**	**81.950**	**76.796**	**82.360**	**83.113**	**82.743**	**1.005.522**

Registros de Criminalidade Violenta
Todos os Municípios

Fonte: Sejusp MG- Secretaria de Estado de Justiça e Segurança Pública de Minas Gerais

Tabela 3 –Alvos de roubo

	Mês												
Ano	1	2	3	4	5	6	7	8	9	10	11	12	Total Ge
2015	6.219	6.042	7.083	7.148	7.523	7.310	7.028	7.516	7.277	7.781	7.988	7.690	86.
2016	8.489	8.293	8.609	8.581	8.525	7.918	8.284	8.137	8.004	8.631	8.735	8.179	100.
2017	9.025	7.864	8.242	7.259	7.353	6.333	6.693	6.722	6.148	6.434	6.507	5.928	84.
2018	5.920	5.286	5.217	4.810	4.334	4.102	4.275	4.408	4.119	4.635	4.238	3.864	55.
2019	4.070	3.733	3.810	3.603	3.511	2.923	3.157	2.984	2.671	2.952	2.896	2.962	39.
2020	3.111	3.096	2.529	1.851	1.567	1.643	1.469	1.428	1.534	1.789	1.857	1.933	23.
2021	1.857	1.627	1.496	1.487	1.428	1.440	1.305	1.368	1.321	1.366	1.491	1.513	17.
2022	1.442	1.274	1.799	1.711	1.478	1.399	1.356	1.366					11.
Total Geral	**40.133**	**37.215**	**38.785**	**36.450**	**35.719**	**33.068**	**33.567**	**33.929**	**31.074**	**33.588**	**33.712**	**32.069**	**419.**

Alvos de Roubo - Variação Percentual
Todos os Municípios

Fonte: Sejusp MG- Secretaria de Estado de Justiça e Segurança Pública de Minas Gerais

Essa queda se deve aos efeitos da política de isolamento social, período em que se teve uma baixa circulação de pessoas, assim como a crise econômica mundial advinda desse isolamento, levando em conta que muitas pessoas perderam o emprego durante esse período. Diante desse cenário muitos criminosos passaram a ver as vantagens advindas do ambiente virtual como desterritorialidade, anonimato, rapidez e sensação de impunidade, as quais provavelmente fizeram com que

os criminosos do mundo físico migrassem para o mundo virtual, bem como o surgimento de novos criminosos.

À vista disso, no seminário virtual "Criminalidade em tempos de Covid-19: atuação do sistema de justiça", o ministro Humberto Martins, afirmou o seguinte:

> O isolamento social decorrente da pandemia de Covid-19 fez cair significativamente o número de roubos e furtos nas cidades brasileiras, devido à baixa circulação das pessoas, mas abriu espaço para o desenvolvimento de outras práticas criminosas, como os crimes cibernéticos. (MARTINS, 2020)

No que se refere ao estelionato virtual, Guilherme Caetano do Jornal o Globo, forneceu os seguintes dados:

> Em meio à simplificação de transferências bancárias no Brasil, o número de crimes de estelionato digital disparou quase 500% entre 2018 e 2021 no país. Em números absolutos, passou de 7.591 para 60.590 no período. Em 2020, houve 34,713 casos, ante 14.677 no ano anterior. (CAETANO,2021)

Assim, com a migração dos bancos do ambiente físico para o digital onde as transações e depósitos bancários então sendo feitos por meio de dispositivos eletrônicos como os celulares, algo que se intensificou durante esse período de pandemia principalmente durante o isolamento social e o lockdown(bloqueio total de circulação de pessoas) em que sem poder sair de casa muitas pessoas optaram por essa forma de serviço online atraindo não somente os criminosos que já operavam nesse ambiente digitam , como também, os antigos criminosos que praticavam os crimes de estelionato fisicamente e passaram a adotar um novo modus operandi diante as dificuldades advindas da pandemia da COVID-19 e a atratividade do mundo virtual como a desterritorialidade em que esses crimes podem ser praticados em qualquer lugar e o anonimato.

Nessa perspectiva, em entrevista ao UOL notícias o promotor de Justiça, do Ministério Público de Minas Gerais, Mauro Ellovitch, afirmou o seguinte:

> Muitos dos crimes de estelionato, que dobraram no Estado em três anos, afirmou Ellovitch, são feitos por organizações criminosas estruturadas, algumas delas ligadas a grandes facções. "A gente já identificou quadrilhas ligadas ao PCC (Primeiro Comando da Capital), ao Comando Vermelho. Os crimes cibernéticos são crimes de baixo risco, grande lucro e para os quais o Estado ainda não se estruturou adequadamente para reprimir. O criminoso vê isso como oportunidade, como um mercado a ser explorado."(ELLOVITCH, 2022)

Destaca-se também a dark web, camada mais profunda e obscura da web, onde criminosos possuem muito conhecimento e são extremamente bem preparados e organizados. A agência europeia diz que está tem sido usada para a comercialização de produtos falsificados relacionados à COVID-19, como máscaras, produtos farmacêuticos e kits de testes, mencionada o relatório da Europol que casos e tentativas de exploração sexual infantil têm sido uma ameaça constante durante a pandemia, a agência diz, inclusive, que houve um aumentou na incidência de referências a sites ilegais envolvendo exploração sexual infantil (GATEFY, 2020).

A TransUnion em um estudo global feito em 2020, constatou que:

> a porcentagem de transações digitais suspeitas de fraude aumentou 5% quando se comparam os períodos de 1 de janeiro a 10 de março e 11 de março (quando o contágio dacovid-19 foi declarado uma pandemia pela Organização Mundial de Saúde) a 28 de abril deste ano. Identificamos mais de 100 milhões de transações suspeitas de fraude entre 11 de março e 28 de abril. Além disso, desde o início do ano foram descobertos mais de 40 mil domínios de altíssimo risco com as palavras-chave 'covid' ou 'corona'. Nesse contexto, duas grandes plataformas de e-commerce removeram 250 mil anúncios e 15 milhões de produtos por serem de procedência ou identificação duvidosa. Na Alemanha, mais de 10 milhões de máscaras, em um montante de €15 milhões foram vendidas e nunca chegaram. (TRANSUNION,2020)

Levando em conta a constante evolução tecnológica e o consequente aprimoramento de técnicas e mecanismos utilizados pelos criminosos virtuais para a realização de crimes cibernéticos, juntamente com o evidente aumento da pratica desses crimes durante a pandemia. A junção de todos esses fatores acendeu ainda mais o alerta das autoridades responsáveis por combate-los, impulsionando mudanças na legislação brasileira como a promulgação das leis 14.155 de 2021 e a Lei 14.132 de 2021, as quais possibilitaram a alteração de pontos importantes do Código Penal e Processual Penal brasileiro no que diz respeito ao ambiente virtual.

A promulgação das referidas legislações trouxe sensíveis mudanças na tipificação e tratamento de alguns crimes virtuais , como o aumento das penas dos crimes de violação de dispositivo informático, furto e estelionato cometidos com ou sem o uso de internet, trazido pela Lei 14.132/21, bem como , a criação de um novo tipo penal **,** denominado crime de perseguição ou stalking, o qual foi inserido pela Lei 14.132/21 ao artigo 147-A do Código Penal e pode ser definido da seguinte como o ato de: “Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica,

restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade."(BRASIL,2021)

O cenário de insegurança virtual já existente, o qual foi intensificado pela pandemia e o crescimento dos crimes virtuais durante esse período também impulsionou a adoção de medidas como o primeiro Plano Tático de Combate a Crimes Cibernéticos, criado em março de 2022, pelo Governo Federal, por meio do Ministério da Justiça e Segurança Pública , com o propósito de prevenir e reprimir os crimes virtuais no país, por meio de um acordos como o de compartilhamento de informações que será feito entre a Polícia Federal e a Federação Brasileira de Bancos (Febraban).

Em dezembro de 2021 a Comissão de Ciência, Tecnologia e Comunicações da Câmara dos Deputados fez um seminário, o qual teve como proposito discutir sobre o papel do Parlamento frente ao aumento dos crimes cibernéticos durante a pandemia. O evento contou com a presença de autoridades como Arthur Pereira Sabbat, representante da ANPD (Autoridade Nacional de Proteção de Dados), a qual visa educar a sociedade sobre os assuntos referentes à Lei Geral de Proteção de Dados Pessoais, buscando zelar os dados dos cidadãos, através de medidas como guias com matérias educativos.

Nota-se que as autoridades competentes por investigar e julgar os crimes cibernéticos adotaram medidas para tentar impedir o constante crescimento desses crimes principalmente após perceber o expressivo aumento dos crimes virtuais durante a pandemia, tendo em vista que os cibercriminosos aproveitaram do ambiente de fragilidade emocional causado durante esse período para praticar crimes virtuais, considerando a sensação de anonimato e impunidade sentida por quem está por trás da tela de um computador.

Portanto, os avanços tecnológicos e o surto da COVID-19 fizeram com que o mundo inteiro tivesse que se adaptar com um novo cenário onde a tecnologia e as redes socias se tornaram ferramentas fundamentais para todos.

Assim, considerando a fragilidade da população e as vantagens advindas do mundo virtual, os crimes virtuais acabaram ganhando espaço, perante os navegadores, ampliando os riscos de cybercrimes. Do mesmo modo, pode ter ocorrido uma possível

migração de criminosos que antes não atuavam no mundo virtual para esse ambiente, bem como a de novos criminosos que nunca praticaram outra modalidade de delitos, considerando a vulnerabilidade da população durante esse período pandêmico, como também, as vantagens advindas do mundo virtual e a dificuldade de investigação e punição desses crimes. Desse modo, a junção de todos esses fatores ocasionou um expressivo aumento dos crimes cibernéticos durante a pandemia.

6 CONSIDERAÇÕES FINAIS

Este trabalho teve como foco estudar o aumento dos crimes cibernéticos durante a pandemia da COVID-19 e as dificuldades para combatê-los. Para a realização desta pesquisa, procurou-se entender os aspectos envolvidos no cometimento dos crimes cibernéticos e as ferramentas ou formas mais utilizadas no combate a esta modalidade de crimes.

Foi possível verificar que existem inúmeras maneiras de prática desses crimes haja vista a evolução tecnológica e o dinamismo tecnológico trazido pela internet que contribuíram para as mais diversas práticas de crimes virtuais, os quais podem ser cometidos contra o computador ou por meio dele.

Diante desse cenário, de desenvolvimento tecnológico e a consequente evolução desses crimes, a qual a pandemia causada pela COVID-19 serviu para agrava-la ainda mais, pois os crimes cibernéticos tiveram um claro e expressivo crescimento esse período, o qual se deu em função do isolamento social e a quarentena, medidas de contenção da proliferação do novo coronavírus, que fez eram com que as pessoas ficassem confinadas em casa, passando consequentemente mais tempo na internet.

O referido cenário atraiu a atenção dos cibercriminosos que viram nesse momento de fragilidade mundial uma oportunidade para a pratica de crimes virtuais. Além dessa questão também foi possível observar uma possível migração dos criminosos do mundo físico para o mundo virtual, bem como o surgimento de novos criminosos. Tendo em vista, a baixa circulação de pessoas, a crise econômica mundial decorrente do isolamento social e as vantagens advindas do ambiente virtual como desterritorialidade, anonimato, rapidez e sensação de impunidade.

A presente pesquisa permitiu a verificação de um cenário preocupante que é a constante evolução dos criminosos em que pese às táticas de cometimento do crime cibernético, sendo necessária uma maior disseminação de informações e boas práticas de segurança para a população como um todo.

No tocante às formas de combate aos crimes cibernéticos, é possível identificar um crescimento de políticas públicas fomentando a formação policial mais especializada e o consequente subsídio de tecnologia, considerando que os cibercriminosos conseguem acompanhar acompanham as evoluções tecnológicas estando à frente desses profissionais.

Além disso, o poder público está atuante em fortalecer a legislação existente tornando-a mais austera com o intuito de combater e inibir os criminosos. Assim, é importante que seja dada uma maior atenção legislativa a para os crimes cibernéticos, tendo vista que a legislação brasileira começou a tratar desses crimes de maneira efetiva tardiamente, somente em 2012, por meio da Lei 12.737/2012. Logo, apesar dos esforços para a punição e investigação desses crimes ainda há muito a ser feito.

REFERÊNCIAS

ABES. Câmara dos Deputados aprova adesão do Brasil à Convenção sobre Crime Cibernético. Associação brasileira das empresas de software. 2021. Disponível em https://abes.com.br/camara-dos-deputados-aprova-adesao-do-brasil-a-convencao-sobre-crime-cibernetico/. Acesso em: 01 out. 2022

ALBRECHT, Evandro Carlos. PEREIRA, Tacieli. PITON, Vinícius. QUAL A INFLUÊNCIA DA PANDEMIA DO COVID-19 AOS CRIMES CIBERNÉTICOS? 2021.Disponível em: https://portalperiodicos.unoesc.edu.br/apeusmo/article/view/27783. Acesso em: 09 out. 2021

ALVES, Castro. Navio negreiro: Virtual Books, 2000. Disponível em: http://www.terra.com.br/virtualbooks/freebook/port/l_port2/navionegreiro.html. Acesso em 01 out. 2021

ALVES, R, F, L e SILVA, S, A. Crimes Virtuais: Uma análise sobre crimes cibernéticos e a dificuldade na aplicação da legislação. 2019. Disponível em: https://bdtcc.unipe.edu.br/wp-content/uploads/2019/09/CRIMES-DIGITAIS-1.pdf. Acesso em 17nov. 2021, Acesso em 17nov. 2021

ANDRADE, Camila Barreto. Crimes virtuais: As inovações jurídicas decorrentes da evolução tecnológica que atingem a produção de provas no processo penal,

2014.Disponível em: https://repositorio.uniceub.br/jspui/bitstream/235/5977/1/20888860.pdf. Acesso em: 28 set. 2021.

ANDREUCCI, Ricardo Antonio. Manual de Direito Penal. 6. ed. rev. e atual. São Paulo: Saraiva, 2010.

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade.2015 Disponível em https://www.informatica-juridica.com/trabajos/crimes-de-informatica-uma-nova-criminalidade/#_ftn18. Acesso em 20 out.2022

ASSUNÇÃO, Ana Paula Souza. CRIMES VIRTUAIS ,2018. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/538/1/Monografia%20-%20Ana%20Paula%20Souza.pdf. Acesso em: 29 set. 2021.

AZEVEDO, L.S; CARDOSO, T.M. CRIMES CIBERNÉTICOS: EVOLUÇÃO E DIFICULDADES NA COLHEITA DE ELEMENTOS DE AUTORIA DELITIVA. 2020. Uma Bom Despacho Faculdade de Direito. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/14146/1/TCC%20Crimes%20Cibern%C3%A9ticos.pdfa%20atualizado.pdf Acesso em: 29 set. 2021

ALPACINI, Ricardo Antônio. Em alta, golpes virtuais entram na mira do crime organizado.2022. Disponível em: https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2022/08/08/em-alta-golpes-virtuais-entram-na-mira-do-crime-organizado.amp.htm. Acesso em: 2 nov. 2022

BARBOSA, Juliana Souza. SILVA, Danihanne Borges. OLIVEIRA Daniela Cabral. JESUS Dilça Cabral. MIRANDA Wesley Flávio. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional,2021. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/12557 Acesso em: 10 out. 2021.

BARBOSA, M. I. A. C. CRIMES VIRTUAIS: A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E OS DESAFIOS NO COMBATE. 2020. Trabalho de Conclusão de Curso (Bacharel em Direito) - PUC Goiás, [S. l.], 2020. Disponível em:https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/105/1/MATEUS%20ISRAEL%20ALVES%20CRUVINEL%20BARBOSA%20-%20TC%20PDF.pdf. Acesso em: 29 set. 2021.

BES, Pablo Rodrigo. MÉTODO DA PESQUISA CIENTÍFICA EM CIÊNCIAS DA RELIGIÃO. Fundamentos da metodologia científica. Disponível em: https://cesmig.grupoa.education/sagah/object/default/14518156. Acesso em 30 out. de 2021

BOUSSO, A. Lei 14.155/2021 reforça ideia de que ambiente virtual não é esfera à parte,2021. Disponível em: https://www.conjur.com.br/2021-jun-29/alan-bousso-consideracoes-lei-141552021.Acesso em: 28 out. 2021.

BRASIL, Decreto n º 10.222, de 5 fevereiro de 2020. Estratégia nacional de segurança cibernética. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 20.out.2022

BRASIL. Código Penal Brasileiro de 1940. Decreto-Lei nº 2.848/1940.Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.Acesso em: 28 out. 2021.

BRASIL. Constituição Federal de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 out. 2021.

BRASIL. Lei 13.964 DE 24 de dezembro de 2019.Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 01 nov. 2022

BRASIL. Lei 14.132 de 31 de março de 2021. 2021.Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.132-de-31-de-marco-de-2021-311668732. Acesso em: 02 nov. 2022

BRASIL. Lei Geral de Proteção de Dados Pessoais -Lei 13.709, de 14 de agosto de 2018.Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 out. 2021.

BRASIL. Lei Geral de Proteção de Dados Pessoais -Lei 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.Acesso em: 28 out. 2021.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 28 out. 2021.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm.Acesso em 28 out. 2021.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em 2 nov. 2022

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. Crimes Cibernéticos. 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília: MPF, 2018. 275 p. – (Coletânea de artigos; v. 3). Disponível em: http: //www.mpf. mp.br/atuacaotematica/ccr2/publicações. Acesso em: 28 out. 2021.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 29 set. 2021.

BRITO, Auriney Uchôa de. O bem jurídico-penal dos delitos informático.2009. Disponível em https://www.ibccrim.org.br/noticias/exibir/4800/. Acesso em: 20 out.2022

CAETANO, Guilherme. Estelionato digital explode no Brasil e cresce 500% em quatro anos.2021. Disponível em: https://oglobo.globo.com/brasil/noticia/2022/06/estelionato-digital-explode-no-brasil-e-cresce-500percent-em-4-anos.ghtml. Acesso em: 26 out.2022

CAMPANHOLA, Nadine Finoti. Crimes Virtuais Contra a Honra, 2018.Disponível em: http://www.conteudojuridico.com.br/consulta/Artigos/51558/crimes-virtuais-contra-a-honra/. Acesso em 18 out. de 2021

CAPEZ, Fernando. Curso de processo penal. 27. ed. São Paulo: Saraiva Educação, 2020

CAPEZ, Fernando. Curso de direito penal, volume 2, parte especial: dos crimes contra a pessoa a dos crimes contra o sentimento religioso e contra o respeito aos mortos .10. ed. São Paulo: Saraiva, 2010.

CARDOSO, Oscar Valente. Novas disposições sobre crimes cibernéticos. 2022. Disponível em: https://jus.com.br/amp/artigos/98006/as-novas-disposicoes-sobre-os-crimes-ciberneticos. Acesso em: 02 nov. 2022

CARDOSO, Nágila Magalhães. A pandemia do cibercrime. 2020.Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/88. Acesso em: 10 out. 2021

CARDOZO, Alexandro Gianes. *Competência nos crimes cibernéticos*. 2017. Disponivel em: https://agianes.jusbrasil.com.br/artigos/514359859/competencia-nos-crimes-ciberneticos. Acesso em: 25 out. 2022

CASSANTI, M. O. *Crimes Virtuais*: vítimas reais. 1. ed. Rio de Janeiro: Brasport, 2014.

CAVALCANTI, W. F. *Crimes cibernéticos*: noções básicas de investigação e ameaças na internet. 27 out. 2021. Disponível em: https://www.conteudojuridico.com.br/open-pdf/cj054548.pdf/consult/cj054548.pdf. Acesso em: 27 out. 2021.

CAVAZZINI, L. S., Cavalcanti, L. de L., Machado, A. R., Denny, D. M. T. & Saleme, E. R. Aplicabilidade da indústria 4.0 na cadeia produtiva agroindustrial: sonho ou realidade? VIII Congresso Brasileiro de Engenharia de Produção.2018. Disponível em:https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwja0Iu3wJz7AhXgLbkGHcEBCiYQFnoECBkQAQ&url=http%3A%2F%2Fanteriores.aprepro.org.br%2Fconbrepro%2F2018%2Fdown.php%3Fid%3D5132%26q%3D1&usg=AOvVaw1z3KYy2rzzKfLnoFmzgaPD. Acesso em: 27 out. 2021.

COELHO, F. E.S., Araújo, L. G. S. ,2013. Gestão da Segurança da Informação NBR 27001 e 27002. Escola Superior de Redes.Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwil1uyewZz7AhWYGrkGHR5pDNQQFnoECC4QAQ&url=https%3A%2F%2Fwww.kgay4all.com%2Fseioqueseiporleroqueleio%2FBooks%2FSecurity%2FGesta%25CC%2583o%2520de%2520Seguranc%25CC%25A7a%2520da%2520Informac%25CC%25A7a%25CC%2583o%2520ABR%252027001%2520e%2520ABR%252027002.pdf.gz&usg=AOvVaw0Ed4OMQOheikugfBTWJ6PY. Acesso em: 27 out. 2021.

CONASS. Painel nacional: COVID -19.2022. Disponível em: https://www.conass.org.br/painelconasscovid19/. Acesso em 1 nov. 2022

CONTE, Christiany Pegorari. Jurisdição e competência nos crimes informáticos. RBMAD, São Paulo, v. 1, n. 1, p. 49-208, jan./jun. 2014. Disponível em: www.revistaseletronicas.fmu.br/index.php/rbmad/article/download/359/522. Acesso em: 20 out.2022

CORREA, Gustavo Testa. Aspectos Jurídicos da Internet. 5. ed. São Paulo, Saraiva,2010.

CORREIO BRAZILIENSE. O ataque de crimes cibernéticos durante a pandemia. 2021. Disponível em:https://www.correiodopovo.com.br/podcasts/direto-ao-ponto/o-aumento-de-ataques-cibern%C3%A9ticos-durante-a-pandemia-1.643164#:~:text=O%20trabalho%20remoto%20e%20o,triplicassem%20na%20pandemia%2C%20apontam%20pesquisas. Acesso em 10 out. 2021.

CORREIO BRAZILIENSE. Registros de golpes na internet crescem 310% no DF durante a pandemia. 2020. Disponível em: https://www.correiobraziliense.com.br/cidadesdf/2020/08/4868977-mais-golpes-na-pandemia.html. Acesso em: 10 out. 2021.

COSTA, Rafaela Seles da. Evolução dos Crimes Cibernéticos e a Violência Contra Mulher. 2019. Disponível em:https://ambitojuridico.com.br/cadernos/internet-e-informatica/evolucao-dos-crimes-ciberneticos-e-a-violencia-contra-mulher/. Acesso em: 17 nov. 2021.

COSTA, Taís Barros Trajano Ribeiro. O aumento do crime cibernético durante a pandemia do Covid-19.2020. Disponível em:https://jus.com.br/artigos/84536/o-aumento-do-crime-cibernetico-durante-a-pandemia-do-covid-19. Acesso em:09 out. 2021.

CORRONS, Luiz. Por que o Brasil é um dos principais alvos de ataques cibernéticos do mundo.2021. Disponível em: https://www.cnnbrasil.com.br/tecnologia/por-que-o-brasil-e-um-dos-principais-alvos-de-ataques-ciberneticos-do-mundo/?amp. . Acesso em: 20.out.2022

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. 1 ed. 2º tirada, Saraiva. 2011: São Paulo. P. 117.

CUNHA, Lílian. Por que o Brasil é um dos principais alvos de ataques cibernéticos do mundo.2021. Disponível em: https://www.cnnbrasil.com.br/tecnologia/por-que-o-brasil-e-um-dos-principais-alvos-de-ataques-ciberneticos-do-mundo/?amp. Acesso em: 20. out.2022

CUPONATION. Internet 2021 Veja quantos usuários usam a internet ao redor do mundo.2021. Disponível em: https://www.cuponation.com.br/insights/internet-2021. Acesso em: 02 nov. 2022

D'URSO, Luiz Augusto Filizzola. Em tempos de cibercrimes. 2019. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/em-tempos-de-cibercrimes/. Acesso em: 10 out. 2021.

SILVA, K. R.; SILVA, R. A. Crimes cibernéticos: necessidade de novas ferramentas de investigação com encargos no ônus da prova. Revista Artigos.Com, v. 12, p. 1-10, 2019. Disponível em: https://acervomais.com.br/index.php/artigos/article/view/2480. Acesso em: 27 out. 2021.

SILVA, Patrícia Santos da. Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

DAMASCENO, Mônica Maria Siqueira; DUARTE, Antônia Edileusa Carvalho. Escola, família e aprendizagem: uma articulação possível. 2008.Dispoivel em: https://idonline.emnuvens.com.br/id/article/viewFile/140/140. Acesso em 30 out. de 2021

EGEWART, A. B. OS Crimes cibernéticos e a ineficácia da lei "Carolina Dieckmann". 2019. Monografia (Bacharel em Direito) – UNIJUÍ, 2019. Disponível em: https://bibliodigital.unijui.edu.br:8443/xmlui/bitstream/handle/123456789/6497/Arthur%20Egewarth.pdf?sequence=1&isAllowed=y. Acesso em: 20 out. 2021.

ELLOVITCH. Em alta, golpes virtuais entram na mira do crime organizado. 2022. Disponível em: https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2022/08/08/em-alta-golpes-virtuais-entram-na-mira-do-crime organizado.amp.htm. Acesso em: 20 out.2022

FEBRABAN. Conheça as tentativas de golpes financeiros mais comuns na pandemia e saiba como evitá-los. 2020. Disponível em: https://portal.febraban.org.br/noticia/3522/pt-br/. Acesso em: 04 nov. de 2021

FERREIRA, Ivette Senise. A Criminalidade Informática. In: LUCCA, Newton De; SIMÃO FILHO, Adalberto (Coord.). Direito & Internet: Aspectos Jurídicos Relevantes. São Paulo: Edipro, 2001. p. 212-213

FERREIRA, Sarah Pereira, Crimes cibernéticos: a ineficácia da legislação brasileira, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1709/1/Artigo%20Cientif%c3%adco-%20Sarah%20Pereira%20Ferreira.pdf. Acesso em: 28 out. 2021.

FIA EMPLOYEE EXPERIENCE (FEEx). Crimes cibernéticos: o que são, tipos, como detectar e se proteger. 2021. Disponível em: https://fia.com.br/blog/crimes-ciberneticos/. Acesso em: 20 out. 2021

FORTINET. Threat Intelligence Insider. 2021. Disponível em: https://www.fortiguardthreatinsider.com/pt/bulletin/Q1-2021. Acesso em 04 nov. de 2021.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. Anuário Brasileiro de Segurança Pública. 2020. Disponível em: https://forumseguranca.org.br/wp-

content/uploads/2020/10/anuario-14-2020-v1-interativo.pdf. Acesso em 05 nov. de 2021.

FROTA, Jessica Olívia Dias; PAIVA, Maria de Fátima Sampaio. Crimes virtuais e as dificuldades para combatê-los. 2017. Disponível em: https://flucianofeijao.com.br/novoo/wp-content/uploads/2018/11/ARTIGOS_CRIMES_VIRTUAIS\nDIFICULDADE. Acesso em: 10 out. 2021.

GARIBE, A. Direito digital - Crimes cibernéticos. Migalhas. 2022. Disponível em:https://www.migalhas.com.br/depeso/373904/direito-digital--crimes-ciberneticos. Acesso em 01 out. 2022

GASTAL, M. Crimes Cibernéticos E A Pandemia De Covid-19. 2021. Disponível em: https://wlm.org.br/crimes-ciberneticos-e-a-pandemia-de-covid-19/. Acesso em 04 nov. de 2021.

GATEFY. Como a COVID-19 impactou os crimes cibernéticos, segundo a Europol. Blog Cibersegurança. 2021. Disponível em https://gatefy.com/pt-br/blog/covid19-crimes-ciberneticos-relatorio-europol/. Acesso em 04 nov. de 2021.

GIANNETTI, Eduardo da Fonseca. Globalização, transição econômica e infraestrutura no Brasil. Texto preparado para o Seminário "Competitividade na infraestrutura para o Século XXI", promovido pelo Instituto de Engenharia, São Paulo, realizado em 24/09/96, reproduzido em Ideias Liberais, Ano IV, N° 62, 1996.

GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais.2013. Disponível em https://revistadoutrina.trf4.jus.br/index.htm?https://revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Acesso em: 20 out.2022

GIMENES, Emanuel Alberto Sperandio Garcia. JUSTIÇA E SEGURANÇA: Crimes Virtuais e condutas criminosas cometida via rede mundial de computadores – Brasil. Revista de Doutrina da 4ª Região, Porto Alegre.2013. Disponível em https://www.topsulnoticias.com.br/news/justi%C3%A7a-e-seguran%C3%A7a%3A-crimes-virtuais-e-condutas-criminosas-cometidas-via-rede-mundial-de-computadores-brasil/. Acesso em 20 out.2022

GOMES, Luiz Flávio. Atualidades Criminais. 2012.Disponível em: Atualidades Criminais (1). In: www.direitocriminal.com.br. Acesso em: 20 out.2022

GOVERNO FEDERAL. ANPD participa de Seminário que discute o combate aos crimes cibernéticos.2021 Disponível em: Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos — Português (Brasil) (www.gov.br). Acesso em 2 nov. 2022

GOVERNO FEDERAL. Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos. 2022.Disponível em:Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos — Português (Brasil) (www.gov.br). Acesso em 2 nov. 2022

GRECO, Rogério. Curso de Direito Penal: parte especial/volume II: introdução à teoria geral da parte especial: crimes contra a pessoa. 4.ed. Niterói, RJ: Impetus, 2007.

IBGE, 2019. Uso de internet, televisão e celular no Brasil.2020. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html. Acesso em: 28 set. 2021.

INELLAS, Gabriel César Zaccaria de. Crimes na Internet. 2. ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009

JESUS, Damásio de. Manual de crimes informáticos, 1.ed. São Paulo: Saraiva, 2015.

JORNAL DAQUI. Crimes Cibernéticos Crescem Durante a Pandemia da Covid-19, 2020.Disponível em: https://www.daquibh.com.br/crimes-ciberneticos-crescem-durante-apandemia-da-covid-19/. Acesso em 10 out. 2021.

JUSTINIANO, Nara Fernanda. Terminologia e Tecnologia: um estudo de termos de crimes cibernéticos. 2017. 106 f., il. Dissertação (Mestrado em Linguística) —Universidade de Brasília, Brasília, 2017.

ALEXANDRE JUNIOR, Edilson Campelo; NASCIMENTO, Volny Costa. Mecanismos de prevenção.2020. Disponível em: https://semanaacademica.org.br/system/files/artigos/artigo-_crimes_virtuais_-_edilson_campelo_alexandre_junior_e_volny_costa_do_nascimento.pdf Acesso em 29 set. 2021

LEMOS, Edson Paulo. Crimes virtuais: a prática dos crimes cibernéticos.2021. Disponível emhttps://conteudojuridico.com.br/consulta/Artigos/56376/crimes-virtuais-a-prtica-dos-crimes-cibernticos. Acesso em 20 out.2022

LÍBANO MANZUR, Claudio. "Chile: Los Delictos de Hacking en sus Diversas Manifestaciones", in Revista Electrónica de Derecho Informático, nº 21, abril de 2000. Site: http:// publicaciones.derecho.org/redi. Disponível em: http://arquivo.ibccrim.org.br/site/boletim/pdfs/Boletim101.pdf. Acesso em: 29 set. 2021.

MACHADO, Luiz Alberto. Revoluções industriais: do vapor à Internet das coisas,2016. Disponível em: https://www.cofecon.org.br/2016/10/13/revolucoes-industriais-do-vapor-a-internet-das-coisas/. Acesso em 10 out. de 2021

MANSUIDO, Mariane. Violência de gênero na internet: o que é e como se defender .2020. Disponível em: https://www.saopaulo.sp.leg.br/mulheres/violencia-de-genero-na-internet-o-que-e-e-como-se-defender/. Acesso em 17nov. 2021

MARTINS, A. B. da S. Crimes virtuais. Curso de Direito da Faculdade de Sabará. 2017.Disponível em: http://faculdadesabara.com.br/media/attachments/monografias/Monografia_Crime. Acesso em:09 out. 2021

MARTINS, Humberto. Crime cibernético tomou lugar de roubos e furtos na pandemia, diz ministro Humberto Martins. 2020. Disponível em: 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: 1 nov.2022

MARTINS, Humberto. Seminário virtual: Criminalidade em tempo de Covid. Atuação do Sistema de Justiça. p. 02. junho de 2020.Disponível em: https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/18062020. Acesso em: 10 out. 2021

MAZZONI, Cesar Augustus et al. Crimes virtuais: evolução no combate.2017. Disponível em https://jus.com.br/artigos/59468/crimes-virtuais-evolucao-no-combate. Acesso em 31 out 2022

MEDINA. José Miguel Garcia. Constituição Federal comentada. 3. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2014.

MEIRELES, J. Crimes Virtuais e as Dificuldades de Combatê-los,2020. Disponível em: https://juapmeireles.jusbrasil.com.br/artigos/876548834/crimes-virtuais-e-as-dificuldades-de-combate-los. Acesso em: 10 out. 2021.

MINISTÉRIO DA SAÚDE. O que é a Covid-19? 2021. Disponível em: https://www.gov.br/saude/pt-br/coronavirus/o-que-e-o-coronavirus. Acesso em: 28 set. 2021.

MINISTÉRIO PÚBLICO FEDERAL. Brasil aprova adesão à Convenção de Budapeste que facilita cooperação internacional para combate ao cibercrime. Procuradoria Geral da República. 2021. Disponível em https://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-de-budapeste-que-facilita-cooperacao-internacional-para-combate-ao-cibercrime. Acesso em 04 out. 2022

MINISTÉRIO PÚBLICO FEDERAL. Grupos de Combate aos Crimes Cibernéticos da PR/SP e PR/RJ. Cartilha de Atuação do MPF no combate aos crimes cibernéticos. São Paulo: MPF, 2015. Disponível em: https: //www.cnmp.mp.br/portal/images/Palestras/Atua%C3%A7%C3%A3o_do_MP_no_combate_aos_crimes_cibern%C3%A9ticosINFANCIA_E_JUVENTUDE.pd. Acesso em: 28 out. 2021.

MIRANDA, S. L. L. ADOLESCENTES COMO VÍTIMAS POTENCIAIS PARA CRIMES CIBERNÉTICOS. BIBLIOTECA DIGITAL DO SUSP, 2018. Disponível em: https://dspace.mj.gov.br/handle/1/5166. Acesso em: 20 out. 2021.

MORAIS DA ROSA, Alexandre. A questão digital: o impacto da inteligência artificial no Direito. Revista de Direito da Faculdade Guanambi, Guanambi, v. 6, n. 02, e 259, jul./dez. 2019. Disponível em: https://doi.org/10.29293/rdfg.v6i02.259. Acesso em: 28 out. 2021.

MORAIS, Lucas Andrade de. Ciberpedofilia: os crimes de pedofília praticados através da internet. Conteúdo Jurídico, Brasília-DF: 06 maio 2021. Disponível em: . Acesso em: 20 out. 2021.

MOURA, Grégore Moreira de. Curso de Direito Penal Informático. Ed. D'Plácido. Minas Gerais. 2021.

NADELLA, Satya. 2 anos de transformação digital em 2 meses, Nascimento, Talles Leandro Ramos. Crimes Cibernéticos, 2018.Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em 19 out. de 2021

NASCIMENTO, Talles Leandro Ramos. Crimes Cibernéticos, 2018.Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em 19 out. de 2021

NOVAIS, L. C. CRIMES CIBERNÉTICOS E SUA EVOLUÇÃO. 2021. Trabalho de Conclusão de Curso (Bacharel em Direito) - Faculdade do Vale do Cricaré. 2020. Disponível em: https://repositorio.ivc.br/handle/123456789/265. Acesso em: 29 set. 2021.
NUCCI, Guilherme de Souza. Manual de Direito Penal. 11. Ed. Rio de Janeiro: Forense, 2015.

NUNES, Beatriz Zuqui et al. Os crimes cibernéticos no contexto da pandemia do Covid-19. 2022.Disponível em: https://www.jornaljurid.com.br/doutrina/penal/os-crimes-ciberneticos-no-contexto-da-pandemia-do-covid-19. Acesso em 02 nov. 2022

NUNES. Karina da Silva. METODOLOGIA CIENTÍFICA. Disponível em: https://cesmig.grupoa.education/sagah/object/default/14682257. Acesso em 30 out. de 2021

OLIVEIRA, Fernando. Crimes Virtuais: Dos crimes contra a honra, 2018.Disponível em: https://fernandodeoliveira01.jusbrasil.com.br/artigos/586245962/crimes-virtuais-dos-crimes-contra-a-honra. Acesso em 19 out. de 2021

OPAS. Histórico de pandemia de COVID-19. 2022. Disponível em: https://www.paho.org/pt/covid19/historico-da-pandemia-covid-19#:~:text=Em%2031%20de%20dezembro%20de,identificada%20antes%20em%20seres%20humanos. Acesso em 02 nov 2022

PAIZ, R. B. revolução 4.0. Uma Discussão acerca do papel do Esatdo e sua relação com os princípios constitucionais dentro do contexto jurídico trabalhista conteporâneo. Universidade de Passo Fundo Faculdade De Direito. Disponível em: http://repositorio.upf.br/bitstream/riupf/1762/1/PF2019Rodrigo%20Paiz%20Basso.pdf. Acesso em 10 out. de 2021

PARANÁPORTAL. Crimes virtuais contra mulher têm crescimento de 1.640%. Mar. 2019. Disponível em: https://paranaportal.uol.com.br /geral/crimes-virtuais-contra-mulher-tem-crescimento-de-1-640/. Acesso em 17 nov. 2021.

PEIXOTO, Andrea Stefani. Lei de Proteção de Dados: entenda em 13 pontos!.2020. Disponível em: https://www.politize.com.br/lei-de-protecao-de-dados/. Acesso em 17nov. 2021

PINHEIRO, E. P. Crimes virtuais: uma análise da criminalidade informática e da resposta estatal. Porto Alegre: PUCRS, 2006. Disponível em:http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2006_1/emeline.pdf. Acesso em: 20 out. 2021.

PINHEIRO, Reginaldo Cesar. Os crimes virtuais na esfera jurídica brasileira. Boletim IBCCrim, 2001, n.101, p.18. Disponível em: http://arquivo.ibccrim.org.br/site/boletim/pdfs/Boletim101.pdf. . Acesso em: 29 set. 2021.

POLICARPO, Poliana e outra. Cibercrimes na E-Democracia. Belo Horizonte: Editora D'Plácido, 2016.

REDAÇÃO DC. ACSP cria conselho de cibersegurança e proteção de dados. 2021. Disponível em: https://dcomercio.com.br/categoria/inovacao/acsp-cria-conselho-de-ciberseguranca-e-protecao-de-dados. Acesso em: 8 nov. 2021.

REVISTA JURIDICA FACULDADE DE DIREITO. CIBERCRIME: UM ESTUDO ACERCA DO CONCEITO DE CRIMES INFORMÁTICOS. 2019. Discorre acerca do conceito de crimes cibernéticos ou cibercrimes sob o viés do Código Penal Brasileiro. v. 14, n. 1 (2019). Universidade Estadual de Londrina (UEL), Londrina/PR. Disponível em:https://www.revista.direitofranca.br/index.php/refdf/article/view/602.Acesso em 29 set. 2021

ROCHA, A. A. Cibercriminalidade: os crimes cibernéticos e os limites da liberdade de expressão na internet. Faculdade de Ensino Superior e Formação Integral. Curso de Direito. São Paulo, 2017. Disponível em: https://www.faef.br/userfiles/files/23%20%20CIBERCRIMINALIDADE%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20N%2ITERNET.pdf. Acesso em 29 set. 2021

ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004.

SANTOS, Boaventura de Sousa. Por uma concepção multicultural de direitos humanos. São Paulo: Revista Lua Nova. Vol. 39, 1997.

SANTOS, Gabrielly Daianne Alves dos. CRIMES VIRTUAIS: tratamento legal e limitações no combate aos crimes cibernéticos. Disponível em: http://repositorio.aee.edu.br/bitstream/aee/18227/1/Gabrielly%20Daianne.pdf. Acesso em: 29 set. 2021.

SCHAUN, Guilherme. Uma lista com 24 crimes virtuais, 2018.Disponível em: https://guilhermebsschaun.jusbrasil.com.br/artigos/686948017/uma-lista-com-24-crimes-virtuais. Acesso em 19 out. de 2021

SCHWAB, K. A Quarta Revolução Industrial, 2016.Editora Edipro. Edições Profissionais Ltda.

SILEVIRA, Wesley P. Como se define o local do crime nos crimes plurilocais e nos crimes à distância? 2017. Disponível em https://wesl.jusbrasil.com.br/artigos/566936270/como-se-define-o-local-do-crime-nos-crimes-plurilocais-e-nos-crimes-a-distancia. Acesso em 31 out. 2022

SILVA, Hugo Hayran Bezerra. Crimes Cibernéticos: uma análise sobre a eficácia da lei brasileira em face das políticas de segurança pública e política criminal,2020. Disponível em: https://conteudojuridico.com.br/consulta/artigos/55020/crimes-cibernticos-uma-anlise-sobre-a-eficcia-da-lei-brasileira-em-face-das-polticas-de-segurana-pblica-e-poltica-criminal/. Acesso em 18 out. de 2021

SOUZA, A. D. G. O avanço dos crimes Cibernéticos: Um estudo sobre os crimes previstos nas leis 12.737/2012 E 12.735/2012 e a importância da materialidade da prova e seus reflexos no ataque cibernético na rede de informática do Superior Tribunal de Justiça em 2020. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/13241/1/ARTIGO%20TCC%20II. .pdf. Acesso em: 28 out. 2021.

TAFNER, Andre. A origem e evolução da internet. 2021.Disponível em https://www.blog.tafner.net.br/post/a-origem-e-evolução-da-internet. Acesso em 31 out. 2022

TERRON, L, L, S. CORREA, R,A. CORREIA, T, M. Cibercrimes: aspectos panorâmicos dos crimes informáticos mais praticados e as condutas de prevenção. 2020. Revista cientifica do Curso de Direito do UNIBH. Disponível em: https://unibh.emnuvens.com.br. Acesso em: 20 out. 2021

TRANSUNION. Como a gestão de dados desempenha um papel vital contra os crimes cibernéticos. 2020. Disponível em:https://newsroom.transunion.com.br/ como-a-gesto-de-dados-desempenha-um-papel-vital-contra-os-crimes-ciberneticos/. Acesso em:01.ago.2021

TRUJ TRUJILLO, F, A. Metodologia da Ciência. 3. ed. Rio de janeiro: Kennedy, 1974. Cap. 8.

UOL, Notícias. Em alta, golpes virtuais entram na mira do crime organizado.2022. Disponível em: https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2022/08/08/em-alta-golpes-virtuais-entram-na-mira-do-crime-organizado.amp.htm. Acesso em: 2 nov. 2022

VALENTE, M. M. G. Teoria Geral do Direito Policial. 3. ed. Coimbra: Almedina, 2012.

VIANNA, E. W. & Fernandes, J. H. (2015). C. O Gestor da Segurança da Informação no Espaço Cibernético Governamental: Grandes Desafios, Novos Perfis e Procedimentos. 2021. Disponível em: https://brapci.inf.br/index.php/res/download/48809. Acesso em: 20 out. 2021

VIANNA, Túlio; MACHADO, Felipe. Crimes informáticos. Belo Horizonte: Fórum, 2013.

WALTRICK, R. CRIMES VIRTUAIS TRAZEM PREJUÍZO BILIONÁRIO PARA BRASILEIROS. Norton Cybersecurity Insights Report. Infografia: Gazeta do Povo, 2016. Disponível em: https://www.gazetadopovo.com.br/economia/inteligencia-artificial/crimes-virtuais-trazem-prejuizo-bilionario-para-brasileiros-c50g4ta0o4u4dwvt7l9ippivh/. Acesso em: 19 nov. 2021.

WORLDOMETERS. COVID-19 Coronavirus Pandemic.2022. Disponível em: https://www.worldometers.info/pt//. Acesso em 1 nov. 2022

ZANELLATO, Marco Antônio. Condutas Ilícitas na sociedade digital, Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet, julho de 2002.