PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
MONOGRAFIA JURÍDICA

CRIMES CIBERNÉTICOS

EVOLUÇÃO NO PERÍODO PANDÊMICO E COMBATE

ORIENTANDO: RODRIGO FERNANDES SOBRINHO

ORIENTADOR: PROF. DR. JOSÉ QUERINO TAVARES NETO

GOIÂNIA
2022

RODRIGO FERNANDES SOBRINHO

CRIMES CIBERNÉTICOS

EVOLUÇÃO NO PERÍODO PANDÊMICO E COMBATE

Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito, Comunicação e Negócios, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Professor Orientador: Dr. José Querino Tavares Neto.

GOIÂNIA
2022

RODRIGO FERNANDES SOBRINHO

CRIMES CIBERNÉTICOS
EVOLUÇÃO NO PERÍODO PANDÊMICO E COMBATE

Data Da Defesa: 28 de novembro de 2022

BANCA EXAMINADORA

_____

Orientador: Prof.: José Querino Tavares Neto Nota

_____

Examinador Convidado: Prof.: Dr. José Antonio Lobo Nota

AGRADECIMENTOS

Inicialmente, gostaria de agradecer a Deus, por todos esses anos vividos intensamente, e por Ele ter me concedido chegar até aqui.

Em especial, agradeço imensamente aos meus avós, Velma e Jaci, por todo o apoio e ajuda, e por terem proporcionado a realização do curso, além de contribuir para a realização deste trabalho.

Aos meus pais e irmãos, que estão sempre ao meu lado, me apoiando, incentivando, sendo meu pilar, me encorajando, me sustentando e me amparando nos momentos difíceis, sei que posso contar com vocês.

Agradeço e dedico esse trabalho aos meus finados avós, Clemente e Ruth, que infelizmente, não poderão me ver formar, porém, sei que estão felizes e orgulhosos de mim.

Aos amigos, que sempre estiveram ao meu lado, pela amizade incondicional e pelo apoio demonstrado ao longo de todo o período de tempo em que me dediquei a este trabalho.

Ao professor Jose Quirino, por ter sido meu orientador e ter desempenhado tal função com dedicação e amizade.

Aos professores, em especial ao professor Jose Lobo, pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo do curso.

SUMÁRIO

CRIMES CIBERNÉTICOS

RESUMO

Este trabalho tem como objetivo investigar os crimes cibernéticos na atual conjuntura do mundo moderno em meio a pandemia de Covid-19 visa expor o que são os crimes cibernéticos, quais são os crimes praticados atualmente, e algumas formas de preveni-los. Foi desenvolvida, por meio de pesquisa bibliográfica e documental, visando acrescentar algo a população e ao mundo jurídico de uma forma geral. Em um primeiro momento será abordado o início da internet num contexto global e no Brasil, como ela surgiu e se expandiu. Foi considerado incluir políticas de inclusão, devido a contribuição que esse fator tem na vida da população menos favorecida num país subdesenvolvido. Para apresentar a relevância desta pesquisa, os capítulos trarão uma análise de trabalhos correlatos ao tema de autores e doutrinadores renomados no meio acadêmico. Após a conclusão do presente trabalho, pela análise de todas as fases do processo, é concluído que diante do cenário atual, a população ainda tem uma grande batalha pela frente na luta contra o crime cibernético.

Palavras-chaves: Crime Cibernético, Crimes Virtuais,Internet, Inclusão Digital, Estelionato, Pornografia Infantil

LISTA DE SIGLAS

ARPA - Agência de Investigação de Projetos Avançados
ARPANET – Advanced Research Projects Agency Network
CERN - Centro Europeu de Investigação Nuclear
CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CETIC.br - Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CGI.br - Comitê Gestor da Internet no Brasil
EUA - Estados Unidos da América
ENIAC – Electronic Numerical Integratorand Computer
FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo
FERMILAB - Fermi National Accelerator Laboratory
HTML - Hyper Text Markup Language
HTTP - Hyper Text Transfer Protocol
IBASE - Instituto Brasileiro de Análises Sociais e Econômicas
IBGE - Instituto Brasileiro de Geografia e Estatística
LNCC - Laboratório Nacional de Computação Científica
MCT - Ministério da Ciência e Tecnologia
MIT - Massachusetts Instituteof Technology
NCP - Network Control Protocol
NSF - National Science Foundation
RNP - Rede Nacional de Pesquisas
ONG – Organização não Governamental
TCP/IP – Transmission Control Protocol/Internet Protocol
TIC - Tecnologia de Informação e Comunicação
UFRJ - Universidade Federal do Rio de Janeiro
URL – Uniform Resource Locator
WEP – Wired Equivalent Privacy
WPA - Wi-Fi protected access
WWW - World Wide Web

1. INTRODUÇÃO

Segundo o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, em pesquisa realizada em 2020, a proporção de domicílios com acesso à Internet chegou a 83%, o que representa aproximadamente 61,8 milhões de domicílios com algum tipo de conexão à rede. Estima-se que aproximadamente 152 milhões de brasileiros eram usuários da rede em 2020, o que representa 81% da população com dez anos ou mais. (CETIC.br, 2021, *online*). É notável que a ferramenta de Internet nos dias atuais, se tornou essencial na vida das pessoas. E grande parte disse se deve às políticas de inclusão digital.

A inclusão digital tem como objetivo garantir que os cidadãos e instituições disponham de meios e capacitação para acessar, utilizar, produzir e distribuir informações e conhecimento, por meio das tecnologias de informação e de comunicação, de forma que possam participar de maneira efetiva e crítica da sociedade da informação.

Atualmente, a circulação de informações é muito rápida por meio da rede de Internet, mas se formos fazer uma retrospectiva, o acesso a esse dispositivo era muito restrito. Segundo Wendt (2012, p.19), “a Internet no mundo, foi desenvolvida com a finalidade de automatizar o cálculo de tabelas balísticas, no ano de 1946 foi construído o primeiro computador digital, denominado ENIAC”.

“No ano de 1957 a União Soviética lançou o primeiro satélite espacial, o Sputnik. A contra ofensiva a esse fato foi que o então presidente dos Estados Unidos John Kennedy prometeu enviar um americano para a Lua e criar um sistema de defesa à prova de destruição.” (WENDT; JORGE, 2012). Em razão disso podemos concluir que a internet surgiu na corrida armamentista, a partir de pesquisas militares no auge da Guerra Fria, tornando o acesso restrito para o resto do mundo.

“Em agosto de 1969, foi criada a Advanced Research Projects Agency Network (ARPANET), primeiro conceito de rede que conectava três universidades e um centro de pesquisa. A ARPANET foi sendo aperfeiçoada e, por fim em 1991, o conceito do World Wide Web (WWW) foi criado no Centro Europeu de Investigação Nuclear (CERN), por Tim Berners-Lee”.(GUISSO, *apud,* 2017, p. 8.).

De acordo com Chagas (2003), surge no Brasil em 1992 a primeira rede conectada à Internet nas principais universidades, não existia interface gráfica, o

monitor, monocromático, era uma tela preta com letras e números verdes, acessível a um grupo restrito de interessados. A única possibilidade era trocar *e-mails.* Em 1995, o Ministério da Ciência e Tecnologia libera o uso comercial da internet no Brasil.

No mesmo ano, foi criado o Comitê Gestor da Internet no Brasil (CGI.br), criado com a finalidade de coordenar e integrar iniciativas de serviços de internet no país, promovendo a inovação, qualidade técnica, e o acesso dos serviços ofertados para o resto da população. (WENDT; JORGE, 2012).

É notório que a Internet trouxe inúmeros benefícios para o mundo atual. Sendo possível ver nitidamente a influência que a rede de Internet possui sobre o comportamento humano. Sabemos que a *Web*, nos proporciona vários pontos positivos, entre eles, a facilidade de comunicação e informação.

Por outro lado, existem os pontos negativos, e dentre eles, os mais prejudiciais são os crimes cibernéticos que utilizam computadores, redes de computadores ou dispositivos eletrônicos conectados para praticar ações criminosas, as quais geram danos a indivíduos ou patrimônios, por meio de extorsão de recursos financeiros, estresse emocional ou danos à reputação de vítimas expostas na Internet.

Neste trabalho, serão abordadas algumas questões que envolvem o uso da Internet, as ameaças mais frequentes na atualidade as quais as pessoas são expostas, bem como as formas de prevenção e boas práticas de utilização desses recursos.

2. JUSTIFICATIVA

A Internet teve um papel importantíssimo no processo de fortalecimento na globalização, visto que, influenciou diretamente na relação entre as pessoas, diminuindo a distância entre elas. (MACHADO, 2021). A pandemia chegou assolando o mundo todo, acentuando ainda mais essa relação e fomos obrigados a nos adaptar ao mundo virtual.

O isolamento pela Covid-19 modificou a forma como estávamos acostumados a viver. As pessoas em sua maioria foram forçadas a se relacionar por meio dos computadores, *smartphones, tablets* e demais dispositivos conectados à rede. O impacto foi nos mais variados segmentos. Um exemplo, talvez o mais expressivo, foi no ambiente de trabalho onde as empresas precisaram se adaptar e

buscar a mesma produtividade do ambiente presencial, agora, com trabalhadores em casa. E isto só tem sido possível graças à Internet.

> Segundo o Diretor de Soluções de Identidade e Prevenção a Fraudes da Serasa Experian, Jaison Reis, o aumento das tentativas de fraude ocorrido em 2021 é um reflexo da aceleração da digitalização por conta da pandemia de Covid-19. Houve uma mudança no comportamento dos brasileiros, que passaram a adquirir bens e serviços online, graças às regras de distanciamento social impostas pela pandemia. Portanto, os oportunistas tinham mais transações para tentar acessar dados e recursos. Por isso a importância de ter plataformas robustas que identifiquem essas tentativas e impeçam a ação dos fraudadores. (SERASA EXPERIAN BRASIL, 2022).

Afirma-se que, com todo o avanço tecnológico sabemos que “são infinitos os benefícios que a *web* nos proporciona, porém junto a eles há também os riscos de segurança digital aos quais os usuários são expostos. Os ataques cibernéticos contra a honra, injúria, difamação e *bullying* são cada vez mais comuns e um dos principais facilitadores é a ‘falta de conhecimento’ dos usuários”. (GUISSO, *apud*, 2017, p. 11).

A falta de conhecimento e a desinformação são as principais causas de danos as vítimas? Sim, o presente trabalho, visa trazer conhecimento para o público em geral, para que estes estejam a par dos delitos que podem ser cometidos por meios dos sistemas informáticos. A fim de orientá-los, para que não caiam em armadilhas usadas pelos denominados *crackers.*

Conforme Crespo (2011, p. 95-98) conceitua: Crackers:

> Considerados os verdadeiros criminosos da rede, ocupam-se de invadir e destruir sites, nesta categoria estão presentes também ladrões, valendo-se da Internet para subtrair dinheiro e informações, sendo o termo *Cracker*, a expressão consagrada para denominar os criminosos que utilizam os computadores como armas.

Este se justifica pela necessidade do autor em passar o devido conhecimento e nutrir a falta de informação das pessoas no âmbito virtual, para que estes identifiquem com mais facilidade os riscos que estão expostos no dia-a-dia, fazendo com que os mesmos estejam aptos para prevenir os ataques.

3. HISTÓRIA DA INTERNET

Define-se “Internet” como “Rede de computadores que, pela troca virtual de dados e mensagens, une esses computadores particulares, organizações de pesquisa, institutos de cultura, institutos militares, bibliotecas, corporações de todos os tamanhos; rede mundial de computadores.” (INTERNET, 2022).

No ano de 1957, a União Soviética lançou seu primeiro satélite espacial, o Sputinik. A controvérsia a esse fato foi que o então presidente dos EUA, Jonh Kennedy prometeu enviar um americano a lua e criar um sistema de defesa a prova de destruição. Com essa última finalidade e, também para acelerar o desenvolvimento do país foi criada a Agência de Investigação de Projetos Avançados (ARPA). (WENDT; JORGE, 2012).

No ano seguinte a ARPA se enfraqueceu, com a criação do National Aeronaltics & Space Administration (NASA), no qual possuía a mesma finalidade. A saída da ARPA foi modificar a perspectiva de pesquisa. Com o passar dos anos, o objetivo era criar uma rede capaz de integrar computadores que estivessem distantes e que, por intermédio dela, fosse permitida a comunicação de dados, a ARPANET foi criada em 1969,uma rede com tecnologia chamada de troca de pacotes para o transporte de informações. Essa mesma tecnologia é à base da Internet de hoje. (WENDT; JORGE, 2013).

Inicialmente, a ARPANET interligou a Universidade da Califórnia (Los Angeles e Santa Bárbara), a Universidade de Stanford (Santa Cruz) e a Universidade de Utah (Salt Lake City). Em 1972, foi organizada a primeira demonstração pública da rede, onde já era possível utilizar serviços como *login* remoto e correio eletrônico. Já no ano de 1973, foi possível realizar a primeira conexão internacional, que interligou a Inglaterra e a Noruega. Também no final dessa década, foi substituído seu protocolo de comunicação de pacotes, de Network Control Protocol (NCP) para Transmission Control Protocol/Internet Protocol (TCP/IP). A alteração de protocolo foi necessária para que se pudesse ter um padrão de comunicação, tornando a interligação de redes independentes mais fáceis. (GUISSO, *apud*, 2017, p. 14).

Outro ponto marcante da história foi a criação do WWW, no final da década de 1980, por Tim Berners-Lee, que também criou o protocolo Hyper Text Transfer Protocol (HTTP) e a linguagem Hyper Text Markup Language (HTML). Preocupados com a segurança da rede, em 1984 a National Science Foundation (NSF) montou sua própria rede de comunicação, chamada NSFNET. Em 1990 a ARPANET foi

desativada por ser considerada obsoleta. Nesse período, a NSFNET tentou comercializar sua tecnologia financiando fabricantes de computadores dos Estados Unidos da América (EUA), porém a maioria dos computadores já possuía capacidade de acesso à Internet e com isso em 1995 a NSFNET foi desativada dando origem à Internet privada comercializada por diversos provedores que montavam suas próprias redes. (GUISSO, *apud*, 2017, p. 15).

4. A INTERNET NO BRASIL

O primeiro contato do Brasil com a internet ocorreu em 1988, quando a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), ligada a Secretaria Estadual Ciência e Tecnologia, realizou a primeira conexão à rede através de uma parceria com o *Fermi National Accelerator Laboratory* (FERMILAB), um dos mais importantes centros de pesquisa científica dos Estados Unidos. (VIEIRA, 2003, p. 08).

A Universidade Federal do Rio de Janeiro (UFRJ) e o Laboratório Nacional de Computação Científica (LNCC) também se conectaram logo em seguida, através de *links*, com universidades americanas. O governo federal entrou na onda em 1992, com a criação da Rede Nacional de Pesquisas (RNP) através do Ministério de Ciência e Tecnologia (MCT). Surgindo uma imensa infra-estrutura de cabos, chamada de espinha dorsal, para suportar a rede mundial de computadores que recebia o *link* internacional e o espalharia pelas principais capitais do país. (VIEIRA, 2003).

Paralelamente ao início das pesquisas (RNP), surgiu no Rio de Janeiro uma organização não-governamental (ONG), chamada Instituto Brasileiro de Análises Sociais e Econômicas (Ibase), e no futuro se tornaria a primeira instituição brasileira fora do ambiente acadêmico a utilizar a Internet através do Alternex. A Web, finalmente, ganhava o Brasil. (VIEIRA, 2003).

No decorrer dos anos seguintes, o que se viu, além do crescimento na utilização da Internet, foi uma disputa entre a iniciativa privada e as estatais pelos direitos de acesso à rede no Brasil. Em 1994 o governo federal teve interesse em investir e promover o desenvolvimento da Internet no país. Ao que tudo indicava, a Embratel teria o monopólio da Internet, porém em 1995,no governo privatizador do então presidente Fernando Henrique Cardoso assim que assumiu o cargo declarou que as operadoras estatais não poderiam oferecer o serviço de Internet ao

consumidor final, pois isso ficaria sob responsabilidade da iniciativa privada. As operadoras estatais, por sua vez, ficariam limitadas a proporcionar a infraestrutura necessária para o mercado corporativo. (VIEIRA, 2003).

Segundo Vieira (2003, p.11), o ano de 1995 pode ser considerado o marco-zero da Internet comercial no Brasil e no mundo.

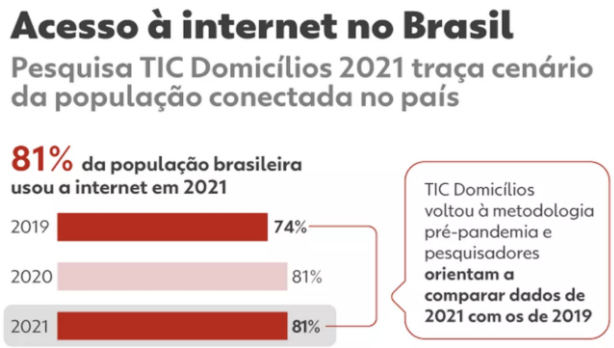
A última medida do governo federal nessa alçada foi à criação do Comitê Gestor de internet (CGI), em 1996, formado por representantes do Ministério da Ciência e Tecnologia, Universidades, ONGs e provedores de acesso, sendo o principal órgão do governo até hoje, quando se fala em rede mundial de computadores. (VIEIRA, 2003).

4.1. ESTATÍSTICAS

No Brasil é realizada anualmente pesquisas sobre a disponibilidade das TICs (Tecnologia da Informação e Comunicação), sendo o órgão responsável o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br).

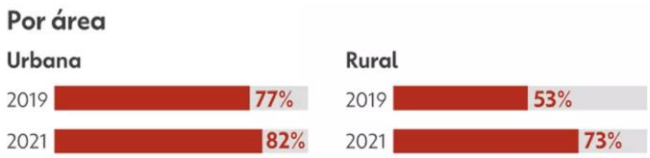
Segundo Silva (2022), a pesquisa TIC Domicílios 2021 a internet foi acessada por 81% da população brasileira. Podemos observar que esses números estão diretamente ligados à evolução tecnológica vivenciada ao longo do tempo no mundo.

Na Figura 1, é possível identificar o crescimento da proporção de indivíduos que já acessaram a Internet entre os anos de 2019 e 2021. “A faixa etária mais conectada é a pessoas que estão entre os 16 e 24 anos onde 94% declararam ter usado a internet. Em seguida, estão as faixas de 25 a 34 anos (91%); 10 a 15 anos (90%); 35 a 44 anos (89%); 45 a 59 anos (78%) e 60 anos ou mais (48%)”. (SILVA, g1, 2022, *online*).



Fonte: Cetic.br, (imagem g1.com.br)

Vale ressaltar que, o acesso à Internet na zona rural passou de 53% (antes da pandemia) para 73% em 2021:

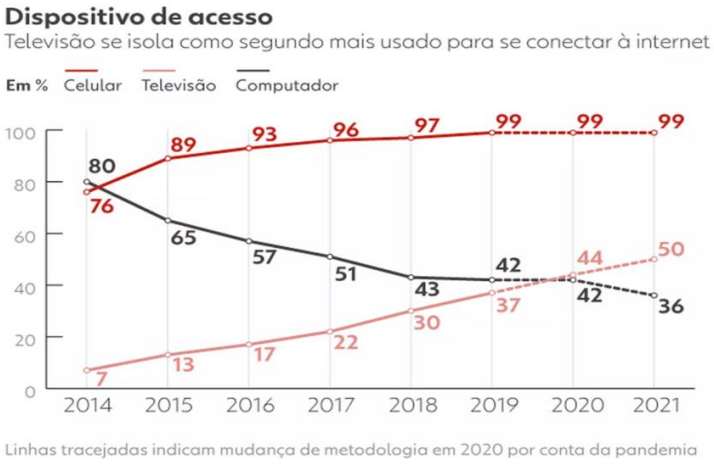


Fonte: Cetic.br, (imagem g1.com.br)

O Brasil já superou a marca de mais da metade da população sendo usuário de Internet como mostra os estudos e o gráfico anterior. É nítida a evolução e estamos em constante desenvolvimento tecnológico, o que inclui por exemplo a disseminação dos dispositivos móveis e as novas possibilidades de acesso à rede.

No passado a conexão era limitada ao “computador de mesa (Desktop)”, mas agora é comum a utilização de Smartphones, notebooks, tablets e até mesmo televisões e aparelhos de videogame.

Em 2021, a televisão se isola como segundo dispositivo mais usado para acesso à internet no país, perdendo posição só para o celular como demonstra o gráfico, a seguir:



Fonte: Cetic.br (imagem g1.com.br)

Essa pesquisa foi realizada em mais de 20 (vinte) mil domicílios em 2021:

> A pesquisa foi produzida pelo Cetic.br a partir de entrevistas feitas em 23.950 domicílios entre outubro de 2021 e março de 2022. A TIC Domicílios considerou dados de 21.011 dessas entrevistas (o restante foi destinado para uma pesquisa do Cetic.br sobre uso de internet por crianças e adolescentes).
> O que a pesquisa de 2021 mostra claramente é o aumento da conectividade nos domicílios e de usuários de internet em relação ao período pré-pandemia. (SILVA, 2022).

Diante das pesquisas, foi possível concluir que houve, num contexto pandêmico um grande salto, e uma constante evolução na utilização da Internet, isso se deve à grande variedade de dispositivos com acesso a Internet, e as regras de distanciamento, juntamente com as políticas do fique em casa, medidas imposta pelo governo federal durante o período pandêmico.

4.2. A INTERNET NA ATUALIDADE E SEUS RISCOS

Segundo Wendt (2013, p.27), a internet tem sido utilizada para inúmeras finalidades, seja para realizar negociações comerciais, conhecer pessoas, manter relacionamentos, produzir atividades de marketing, buscar diversão, e em alguns casos, promover transtornos para outras pessoas, incluindo prejuízo financeiro as vítimas.

O uso da Internet tornou-se uma ferramenta indispensável no cotidiano das pessoas, e muitas das vezes não notamos que algumas atividades são realizadas através dela. A sua adesão é percebida em todas as faixas etárias, algo que não era capaz de ser imaginado, como idosos utilizando serviços de Internet banking e interagindo em redes sociais. E do lado oposto vem a era dos nascidos digitais, parecem ter habilidades natas para lidar com a comunicação online e com as diversas ferramentas que a tecnologia traz para o nosso cotidiano. (GUISSO, *apud*, 2017, p.22).

Atualmente, as pessoas estão cada vez mais dependente da internet, e cada dia que passa, esse número cresce exponencialmente, devido a facilidade que o avanço tecnológico vem trazendo e o barateamento dos computadores e as redes móveis de acesso à rede mundial. (WENDT; JORGE, 2013).

No entanto, devido à facilidade de acesso, é certo que a Internet tem facilitado a informação, mas acabou restringindo a capacidade de reflexão das pessoas. A circulação instantânea de informações e o imediatismo são prejudiciais. Muitas vezes se obtém um informação aparentemente correta, e na correria do dia a dia muitos não param pra raciocinar se o que está sendo transmitido tem veracidade e acabam por não selecionar as mesmas. E é nesse momento que distribuem informações *fakes*.

São as famosas *Fake News* (Notícias Falsas). Basicamente são notícias falsas publicadas por veículos de comunicação como se fossem informações reais.

5. SURGIMENTO DOS CRIMES CIBERNÉTICOS

Como tudo possui seu lado bom e ruim a evolução dos recursos tecnológicos não poderia ser diferente, as ameaças praticadas via computador se aprimoraram com o passar dos anos. Antes mesmo do aparecimento dos primeiros códigos maliciosos, no final da década de 50, foi desenvolvido por um grupo de programadores um jogo chamado Core Wars, que era capaz de se reproduzir a cada vez que era executado, sobrecarregando a memória da máquina do oponente. Os mesmos criadores também inventaram um antivírus capaz de destruir as cópias geradas pelo jogo. Essas informações somente vieram a público em 1983, através de um artigo escrito e publicado por uma conceituada revista científica da época, escrito por um de seus criadores. (WENDT; JORGE, 2013).

Richard Skrenta, em 1982, com apenas quinze anos, criou o ElkCloner. Sendo considerado por muitos estudiosos como o primeiro vírus desenvolvido para infectar computador. Mas esse termo “vírus de computador” surgiu somente em 1984 por Fred Cohen. Em 1986 dois irmãos paquistaneses criaram o vírus chamado *Brain*, que atingia o setor de inicialização de disco e tinha por finalidade detectar o uso não autorizado de um software médico de monitoramento cardíaco que haviam desenvolvido. O código sofreu modificações maliciosas as quais o transformou em vírus e passou a espalhar causando lentidão nas operações de sistemas e ocupando espaço na memória dos computadores. Tem relatos de que os primeiros cavalos de Troia surgiram também em 1986. (WENDT; JORGE, 2013).

Segundo Wendt (2013, p.26), primeiro antivírus foi criado no ano de 1988 por Denny Yanuar Ramdhani, em Bandung, Indonésia, e tinha funcionalidade de imunizar o sistema do computador contra o vírus *Brain.*

Surgiram também novos meios para a difusão de ameaças, utilizando o celular, em 2004 foi criado o primeiro vírus para infectar aparelhos móveis, oriundo das Filipinas, foi apelidado de Cabir, criado para infectar sistemas operacionais Symbian, com o objetivo de descarregar toda a bateria de celulares que eram infectados através do Bluetooth. (WENDT; JORGE, 2013).

> O Brasil sempre teve altos índices de criminalidade digital e, no ano de 2002, chegou a ganhar o título de maior “exportador” de criminalidade via internet. Embora houvesse altos índices de delitos, a primeira condenação efetiva ocorreu somente em janeiro de 2004, onde um jovem de dezenove anos que aplicava golpes pela Internet

> no Brasil e Estados Unidos teve condenação de seis anos e quatro meses. (GUISSO, *apud*, 2017, p. 24).

No mesmo ano o vírus foi aprimorado por um brasileiro, chamado Marcos Velasco, especialista em malware e dono de uma empresa de segurança, ele decidiu aprimorar o vírus para telefones móveis. Este vírus éconhecido como Lasco ou Symbos_ Vlasco.A de auto instalação. (WENDT; JORGE, 2013).

6. O QUE SÃO OS CRIMES CIBERNÉTICOS

Os crimes cibernéticos geralmente são praticados por indivíduos ou organizações, denominados por cibercriminosos ou *crackers*. Pode ser definido como uma atividade criminosa que tem como alvo ou faz uso de um computador ou uma rede de computadores, celulares ou qualquer outro aparelho eletrônico que passa vir a se conectar na internet.

> Ao contrário do que se imagina, os crimes virtuais não são praticados apenas por atacantes com conhecimento sofisticado em informática, a cada dia é mais comum os crimes através de e-mails e redes sociais. Os atacantes são estimulados pela falsa ideia de que ficarão impunes aos delitos por eles terem sido realizados pela internet, mas como qualquer outro crime, as penas são as mesmas independentes do meio utilizado para a prática. (GUISSO, *apud*, 2017, p. 34).

As práticas envolvem desde a disseminação de vírus por meio de links enviados por e-mail até invasões de sistemas operacionais de empresas ou mesmo privados.

Os infratores podem roubar informações e dados confidenciais, sendo capazes de aplicar golpes como os de estelionato e falsidade ideológica, por exemplo. Os crimes cibernéticos envolvem, de um lado, um ou mais criminosos e, do outro, uma ou mais vítimas.

Com o passar dos anos os dispositivos evoluíram nas últimas décadas, com isso, desenvolveram-se a forma como os delitos são cometidos. E infelizmente qualquer pessoa está sujeita a ser atacada.

6.1. OS CRIMES DIGITAIS MAIS COMUNS NA INTERNET ATUALMENTE

Os crimes praticados virtualmente não possuem apenas efeitos em seu meio virtual, como já foi dito, mas também na esfera moral e material. Alguns dos tipos mais comuns de cibercrimes incluem os seguintes:

6.1.1. ESTELIONATO VIRTUAL

Com a tecnologia avançando cada vez mais, é comum que os crimes antes cometidos pelo telefone agora sejam facilmente executados na internet, mais especificamente nas redes sociais. O Whatsapp e o Facebook são sem dúvidas os preferidos quando o assunto é crime de estelionato, por serem gratuitos e de fácil acesso. “Esse fator levou o Senado Federal a aprovar no dia 05 de maio de 2021, um projeto de lei que aumenta a pena para o crime de estelionato mediante o uso da internet e aparelhos digitais como computadores e celulares.” (AGÊNCIA SENADO, 2021, *online*).

> A figura do estelionato executado em ambiente virtual ainda é algo recente dentro do estado e dos tribunais brasileiros, no entanto, merece atenção especial, data vênia a popularização e modernização da internet, atingindo e adquirindo milhares de novos usuários a cada dia. (FEITOZA, *apud*, 2012, p. 43).

Tipos de estelionato:

- GOLPE DO BOLETO FALSO

Esse vem sendo o tipo mais comum de fraude no Brasil. Normalmente, os criminosos elaboram um boleto falso contendo todos os dados da vítima, onde se passam por uma empresa de cobrança real. Eles enviam o boleto via WhatsApp solicitando pagamento. A conta pode ser um financiamento, contas de serviços como telefone, ou pagamentos de compras de produtos.

- GOLPE VIA SMS

O SMS é um dos golpes favoritos dos criminosos. Nas mensagens, eles pedem que a vítima atualize cadastros de bancos, enviando links que direcionam para páginas falsas. O objetivo final desse golpe é conseguir os dados pessoais para acessar os canais oficiais.

Esses golpistas estão se especializando cada vez mais e contratando sistemas de disparos de mensagens em massa, no qual conseguem atingir um número maior de vítimas. O SMS é semelhante com os recebidos de instituições financeiras, já que ele aparece com o número pequeno no identificador.

- GOLPE DO PERFIL FALSO

Nesse golpe, os criminosos usam contas com perfis falsos nas redes sociais. Ele se divide em duas situações:

- Golpistas se passando por contas de lojas, onde vendem os produtos que não são entregues. Nesse caso, a vítima fica no prejuízo e não recebe as compras;
- Quando se passam por pessoas e simulam relacionamentos virtuais, conhecido como Catfish. Eles encontram um alvo e começam a ganhar confiança da vítima. Após estreitarem relações, começam a relatar problemas e dificuldades financeiras, pedindo dinheiro para cobrir despesas. Na maioria das vezes, as mulheres são as grandes vítimas desse tipo de golpe.

- GOLPE DO INVESTIMENTO

Se tratando de golpes, os criminosos não perdem tempo. Devido ao crescimento de investidores no Brasil, esse tipo de golpe vem aumentando e se especializando. O fraudador promete retorno de investimentos em determinada criptomoeda. E claro, esse investimento não existe.

- GOLPE DO MARKETING MULTINÍVEL

Parecido com o golpe do investimento, o golpe do marketing multinível promete retorno financeiro com uma condição: a vítima deve realizar um depósito inicial e, após, indicar outras pessoas para fazerem parte do negócio. Um esquema parecido com as pirâmides financeiras. Os golpistas pagam as pessoas que entraram antes com o dinheiro do novo entrante. Infelizmente, no Brasil essa prática é bastante comum.

- GOLPE DO EMPREGO

No golpe do emprego, o fraudador cria páginas falsas anunciando empregos, mas solicita que a vítima realize um cadastro e que pague um valor para acessar às oportunidades. Com isso, além deles terem acesso aos dados pessoais das vítimas, ainda tiram dinheiro com falsas promessas de trabalho.

- GOLPE DO SUPORTE TÉCNICO

É possível que 70% dos brasileiros já tenham sofrido essa tentativa de golpe, de acordo com a Microsoft. Os criminosos criam pop-ups (aquelas janelas que abrem na tela), alertando que seu computador ou celular está com vírus e precisa ser protegido. Quando a vítima clica no link, abre um falso site de antivírus, e assim, a pessoa paga por um produto que não irá proteger seu celular ou computador.

- GOLPE DO WHATSAPP

Com certeza você conhece alguém ou já ouviu falar no golpe do WhatsApp. Os bandidos clonam seu WhatsApp, e mandam mensagens para seus contatos, como familiares ou amigos e solicitam um Pix com urgência, alegando que seu limite diário acabou. Muitas pessoas acabam caindo no golpe e fazem a transferência sem desconfiar. Muitas vezes, os golpistas encontram as fotos em perfis de redes sociais. Por isso, é necessário confirmar sempre as informações em duas etapas, com os códigos de segurança.

- GOLPE VIA PÁGINAS FALSAS

A empresa de segurança Avast realizou uma pesquisa que 71% dos golpes de páginas falsas são realizados por e-mails, e quase metade das vítimas caem. Essa prática é comum na rede e é conhecida como Phishing. Com o golpe, os criminosos conseguem roubar dados pessoais das vítimas, dinheiro ou até mesmo instalar um malware (software malicioso) nos dispositivos.

- GOLPE DO FGTS E MAIS

O Ministério da Justiça e Segurança Pública relatou que é comum os golpistas usarem o nome do órgão para enviarem falsas mensagens em nome de serviços como o FGTS, recadastramento do Auxílio Emergencial, ou agendamento de vacinas, isso para roubar dados. O contato geralmente é feito por telefone, email ou SMS. Também é necessário cuidar dos aplicativos nos quais são instalados no

celular e que não sejam conhecidos, pois eles podem instalar spywares (softwares espiões) para se apropriar dos dados de seu smartphone.

6.1.2. PORNOGRAFIA INFANTIL

O crime de pornografia infantil existe há décadas, antes registradas em fitas, fotografias, DVD 's e em computadores sem conexão com a internet, hoje circula pelo ciberespaço em sites adultos disfarçados ou habilitados apenas para quem fizer a assinatura e pagar pelo conteúdo. Segundo o Estatuto da Criança e do Adolescente (Lei n.8069 de 13 de julho de 1990) consta em seu artigo 241-A até o artigo 241-C, assim como em seus parágrafos e respectivos incisos que:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008).
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> § 1 o Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; (Incluído pela Lei nº 11.829, de 2008)
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
> § 2 o As condutas tipificadas nos incisos I e II do § 1 o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> § 1 o A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
> § 2 o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por: (Incluído pela Lei nº 11.829, de 2008)
> I – agente público no exercício de suas funções; (Incluído pela Lei nº 11.829, de 2008)
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o

> encaminhamento de notícia dos crimes referidos neste parágrafo; (Incluído pela Lei nº 11.829, de 2008)
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. (Incluído pela Lei nº 11.829, de 2008)
> § 3o As pessoas referidas no § 2 o deste artigo deverão manter sob sigilo o material ilícito referido. (Incluído pela Lei nº 11.829, de 2008)
> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: (Incluído pela Lei nº 11.829, de 2008).

Sendo assim, as únicas menções em legislações brasileiras até o momento. A pessoa que comete um crime tão banal deve ser punida de maneira mais severa, como por exemplo a perda da guarda de seus filhos. Caso o conteúdo encontrado não seja referente à criança no qual o adulto possui parentesco, há de se haver restrições para entrar em locais destinados ao público infantil, como escolas e creches.

7. COMO EVITAR OS CRIMES CIBERNÉTICOS

Cada vez mais, esses crimes são cometidos por grupos organizados que operam em um país e cujas vítimas estão em outro. A natureza transfronteiriça do crime cibernético complica a aplicação das leis, e os marcos legais inadequados em alguns países criam refúgios seguros para os criminosos cibernéticos.

O impacto financeiro de todos esses crimes é grande e crescente. Além desses custos econômicos, há impactos menos tangíveis, incluindo a confiança perdida no comércio online, a erosão da privacidade individual e a redução da confiança nos serviços on-line.

Cada um destes efeitos ameaça retardarem a adoção da inovação baseada em nuvem e reduzir os benefícios das novas e promissoras tecnologias.

Prevenção de crimes cibernéticos vem com a recomendação de políticas públicas e a harmonização das leis de crimes cibernéticos em todo o mundo, combinada com iniciativas privadas para facilitar uma coordenação mais rápida e eficaz entre os órgãos responsáveis pela aplicação das leis, é essencial. Esses esforços podem ser envidados em um ambiente onde cada país respeita a

soberania das outras nações, e onde os direitos e liberdades fundamentais dos cidadãos sejam plenamente respeitados. Para reforçar a aplicação das leis de uma forma equilibrada, os governos devem considerar as seguintes etapas:

7.1. FORTE APLICAÇÃO DAS LEIS E REGRAS EQUILIBRADAS

Para lutar contra a criminalidade cibernética de forma eficaz, os órgãos responsáveis pela aplicação das leis e a indústria devem ter as ferramentas legais necessárias para perseguir os criminosos cibernéticos onde quer que estejam. Os governos devem trabalhar para atualizar suas leis penais de modo que eles sejam capazes de tratar das ameaças existentes e emergentes feitas pelos criminosos on-line. Ao mesmo tempo, essas leis devem tomar cuidado para não prejudicar a inovação ou a adoção de novas tecnologias. Eles também devem apoiar as iniciativas de autorregularão da indústria.

7.2. ADOÇÃO DE LEIS CONSISTENTES COM AS CONVENÇÕES INTERNACIONAIS AMPLAMENTE ACEITAS

A Convenção de Budapeste do Conselho da Europa oferece um bom modelo de legislação sobre crimes cibernéticos que pode ajudar a harmonizar as leis e melhorar a cooperação além das fronteiras. Essa coordenação e cooperação internacionais ajudarão a eliminar os refúgios para os agentes criminosos e minimizar os riscos que surgem quando intermediários e outras partes inocentes estão sujeitos a obrigações ou responsabilidades conflitantes.

> O Senado aprovou, nesta quarta-feira (15), a adesão do Brasil à Convenção sobre o Crime Cibernético, celebrada em Budapeste, na Hungria, em novembro de 2001 (Projeto de Decreto Legislativo 255/2021). A matéria, que teve como relator o senador Nelsinho Trad (PSD-MS), será encaminhada à promulgação.
>
> A Convenção de Budapeste visa facilitar a cooperação internacional para o combate ao crime na internet. O documento lista os principais crimes cometidos por meio da rede mundial de computadores. Elaborado pelo Comitê Europeu para os Problemas Criminais, com o apoio de uma comissão de especialistas, foi o primeiro tratado internacional sobre os chamados "cibercrimes". A Convenção já foi assinada por 66 países e é usada por outros 158 como orientação para suas legislações nacionais. (Agência Senado, 2021, *online*).

7.3. DESENVOLVIMENTO DE NOVAS FORMAS DE PREVENIR OS CRIMES CIBERNÉTICOS

Os atuais esforços para fazer cumprir as leis contra o crime cibernético são totalmente inadequados, dada a grandeza do problema. Novas abordagens para perseguir os criminosos são necessárias. Um exemplo pode ser um programa-piloto lançado pela polícia da cidade de Londres, em parceria com escritórios de advocacia, que utiliza os tribunais civis para apreender os bens dos criminosos cibernéticos. Encontrar outras maneiras de dimensionar os esforços de aplicação é crítico.

7.4. TRABALHAR COM A INDÚSTRIA NAS MELHORES PRÁTICAS E QUESTÕES EMERGENTES

Os governos podem tirar proveito da experiência e dos recursos do setor privado na luta contra a criminalidade cibernética. Oportunidades incluem trabalhar com a indústria para treinar as autoridades responsáveis pela aplicação das leis sobre as novas e emergentes ameaças que os fornecedores de tecnologia sofrem no mundo real e que seus clientes vêem como prioridades. Os governos muitas vezes não dispõem de recursos suficientes para lidar efetivamente com a criminalidade cibernética. Trabalhar com o setor privado pode ajudá-los a obter maior sucesso, o que aumentará a confiança na computação online.

8. INVESTIGAÇÃO E PRODUÇÃO DE PROVAS

As investigações dos crimes virtuais são feitas por meio de uma análise técnica, na qual irá verificar tanto a autoria quanto a materialidade dos crimes praticados por meio de uma rede que interliga os computadores.

Porém, ao analisarmos casos de crimes cibernéticos, fica nítido a dificuldade na obtenção de provas em investigações relacionadas aos crimes virtuais, uma vez que as infrações praticadas no ambiente cibernético não deixam rastros, facilita-se o anonimato de quem pratica tal ato, além de que a proporção que algo pode atingir na rede de internet é ilimitada.

Outro ponto no qual deve ser observado, é a identificação do meio onde ocorreu o ato ilícito, sendo primeiramente o local - facebook, whatsapp, instagrametc- e em segundo momento o endereço de IP, para que assim ocorra uma investigação na qual irá determinar quais ações deverão ser adotadas. No entanto, ainda nos falta tecnologia e mão de obra especializada para combater tais crimes.

Vale ressaltar que a obtenção de provas ilícitas decorrentes de investigações realizadas sem que haja a devida autorização, violam o artigo 5º, da Constituição Federal e o artigo 157 do Código de Processo penal, sendo consideradas inaceitáveis no processo penal por estarem em desacordo com as normas do direito material.

Uma maneira para que se possa realizar a investigação desses crimes é a identificação do endereço de IP do computador onde foi realizado o delito. Todavia, em alguns casos a identificação do criminoso pode ser de difícil descoberta.

8.1. INVESTIGAÇÃO DO CRIMINOSO

O anonimato é o maior problema quando se trata de identificar o autor do delito, tendo em vista que o ambiente virtual fornece a possibilidade de criar perfis falsos, fazendo com que a identidade do indivíduo mude conforme ele queira. Os usuários aproveitam das leis escassas sobre o assunto para invadir computadores e praticarem atos ilícitos. Conforme preceitua BRASIL (p. 23,2008):

> Crime virtual ou crime digital pode ser definido como sendo termos utilizados para se referir a toda a atividade onde um computador ou uma rede de computadores são utilizados como uma ferramenta, uma base de ataque ou como meio de crime. Infelizmente, esta prática tem crescido muito já que esses criminosos virtuais têm a errada impressão que o **anonimato é possível na Web e que a Internet é um "mundo sem lei". (grifamos).**

9. QUAL É A PUNIÇÃO PARA OS CRIMES CIBERNÉTICOS

No Código Penal brasileiro até pouco tempo atrás não existiam artigos sobre crimes virtuais. Há que se considerar que o Código Penal é de 1940, e na época não existia sequer a Internet.

O Direito Penal já tipificava como crimes atos como invadir, violar dados pessoais e divulgá-los, além de demais atos criminosos. A sociedade precisou evoluir diante do avanço da tecnologia, tornando de extrema importância a análise e a tipificação dos atos cometidos pelos meios informáticos e telemáticos.

No Brasil, as questões envolvendo o Direito sobre crimes cibernéticos só foram tipificadas em 2012, alterando o Código Penal, acrescentando os artigos 154-A, 154-B, e modificando os artigos 266 e 298; a primeira Lei dos Crimes Cibernéticos (LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.), conhecida como Lei

Carolina Dieckmann, nome dado em homenagem à atriz brasileira que teve o seu celular invadido e fotos pessoais divulgadas na rede por um cracker. Dispondo sobre a tipificação criminal de delitos informáticos.

Os artigos 154-A e 154-B, que fora acrescido no Código Penal brasileiro, *in verbis*:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: **Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.**
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Dessa forma, a lei tipifica como crime a invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Complementando a legislação acima, foi sancionada a LEI 12.735, DE 30 DE NOVEMBRO DE 2012, conhecida como a primeira lei a tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989 – Lei do Racismo.

Em 2018, foi aprovada pelo então presidente Michel Temer, a Lei Geral de Proteção de Dados (LGPD). Lei Nº 13.709, de 14 de agosto de 2018.Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Em 28/05/2021, o Senado Federal sanciona Lei com penas mais duras contra crimes cibernéticos os crimes digitais como fraude, furto e estelionato

praticados com o uso de dispositivos eletrônicos como celulares, computadores e tablets, passarão a ser punidos com penas mais duras. Foi publicada no Diário Oficial da União a Lei 14.155, de 2021, sancionada na quinta-feira (27) pelo Presidente Jair Bolsonaro.

A lei, que tem origem no Projeto de Lei (PL) 4.554/2020, do Senador Izalci Lucas (PSDB-DF), foi aprovada pelo Senado no início do mês. O texto altera o Código Penal (Decreto-Lei 2.848, de 1940) para agravar penas como invasão de dispositivo, furto qualificado e estelionato ocorrido em meio digital, conectado ou não à internet. (Agência Senado, 2022, *online*).

Hoje, com a alteração imposta pela nova lei, dita o seguinte:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
>
> **Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.**

Segundo o Ministério da Justiça e Segurança Pública, o Brasil foi o 5º país do mundo que mais sofreu com crimes cibernéticos, em 2021. Para intensificar a repressão a esses delitos, a Polícia Federal inaugurou, a Unidade Especial de Investigação de Crimes Cibernéticos (UEICC). A iniciativa é um dos pontos da parceria público/privada proposta pelo Ministério da Justiça e Segurança Pública (MJSP), com apoio da Federação Brasileira de Bancos (Febraban), para promover a troca de informações em busca de resoluções mais rápidas e prevenção contra crimes cibernéticos. (gov.br, 2022, *online*).

Além de crimes cibernéticos relacionados a instituições bancárias, a UEICC irá intensificar a repressão a diversos outros crimes praticados no ambiente virtual, como a pornografia infantil, contra instituições públicas, setor varejista, operadoras de telefonia, telecomunicações, entre outros. De acordo com o Diretor-Geral da PF, Márcio Nunes, o órgão já vem combatendo esses crimes por meio dos rastros que os criminosos deixam e procedido com a responsabilização dos autores a partir de investigações. (gov.br, 2022, *online*).

10. METODOLOGIA

O método de pesquisa utilizado neste trabalho é o qualitativo, dando sustentação ao tema e apoiando-se em técnicas de coleta de dados. De acordo com Neves (1996, p.01, Apud, SILVA, 2021, p.07), “a pesquisa qualitativa não busca enumerar ou medir eventos. Ela serve para obter dados descritivos que expressam os sentidos dos fenômenos.”

A pesquisa em tela se classifica como sendo exploratória proporcionando maiores informações sobre o referido tema, além de ser qualificada como sendo uma cadeia de raciocínio pelo método hipotético-dedutivo, que a partir de teorias e leis gerais pode-se chegar à determinação ou previsão de fenômenos particulares.

O estudo foi realizado a partir de um levantamento bibliográfico e documental, com o uso de leis, doutrinas, jurisprudências e demais legislações que regulamentem acerca da relação entre os Crimes Cibernéticos.

11. CONCLUSÃO

Diante de todo o exposto e ao fim da pesquisa, conclui-se a importância de saber como os Cibercrimes estão presente no dia a dia das pessoas, verificamos que todos com acesso a Internet estão expostos e possivelmente poderão se tornar vítima algum dia, às vezes por um pequeno descuido ou simplesmente por estar conectado a rede.O aumento explosivo dos dispositivos conectados, e da rápida expansão de serviços inovadores baseados em nuvem, percebe-se que está criando muitas oportunidades econômicas e sociais para os consumidores, governos e empresas.Porém observamos que o desafio, consiste nos governos lutando para enfrentar a crescente ameaça, a sofisticação e a prevalência de crimes cibernéticos.

A Internet, desde a sua criação sofreu transformações e evoluções ao longo do tempo e é inegável que os Crimes Virtuais também acompanharam essa evolução, talvez até ultrapassando e se aperfeiçoando cada vez mais. Os criminosos não descansam, e estão sempre um passo à frente, e a cada dia que passa surgem novas modalidades de crimes, fazendo com que a legislação seja constantemente alterada para suprir e tipificar essas modalidades criminosas.

Ao longo do trabalho, foram expostas algumas modalidades de crimes e como podemos combatê-los. Alcançando o seu objetivo que é expor a prática dos Crimes Virtuais e a maneira como ocorrem, para que os “internautas” possam saber como se prevenir, caso vierem a se tornar vítimas, foi demonstrado como recorrer ao

judiciário e ser amparado pela legislação vigente, pois medidas estão sendo tomadas pelo governo em parceria com instituições privadas, na busca de novas formas para trazer mais segurança aos usuários, criando leis e fiscalizando o uso.

12. REFERÇÊNCIAS BIBLIOGRÁFICAS

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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 12. Nov. 2021.

BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à Luz do Marco Civil da Internet**. Editora Brasport. Rio de Janeiro. 2016.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014. Disponível em:<https://play.google.com/books/reader?id=ribyAgAAQBAJ&pg=GBS.PA5&printsec=frontcover&output=reader.> Acesso em: 21/03/2022.

CETIC.br. **Cresce o uso de Internet durante a pandemia e número de usuários no Brasil chega a 152 milhões, é o que aponta pesquisa do Cetic.br**. Disponível em: <https://cetic.br/pt/noticia/cresce-o-uso-de-internet-durante-a-pandemia-e-numero-de-usuarios-no-brasil-chega-a-152-milhoes-e-o-que-aponta-pesquisa-do-cetic-br/> Acesso em 06/11/2022.

FEITOZA, Luis Guilherme de Matos. **Crimes cibernéticos: estelionato virtual**. 2012.
70 p. Monografia de Conclusão (Bacharel em Direito) - Universidade Católica de Brasília, Brasília, 2012.

INTERNET. *In*: DICIO, **Dicionário Online de Português**. Porto: 7Graus, 2022. Disponível em: <https://www.dicio.com.br/internet/>. Acesso em: 06/11/2022.

GUISSO, Leonardo. **Segurança Digital: Avaliação Do Nível De Conhecimento DaPopulação Sobre Os Riscos De Segurança Atrelados Ao Uso DaInternet Na Região De Bento Gonçalves**. 2017. 84 p. Relatório de Conclusão (Bacharelado em Sistemas de Informação) - Universidade De Caxias Do Sul, Rio Grande do Sul, 2017.

GOV.BR. **Polícia Federal cria Unidade Especial para intensificar a repressão a crimes cibernéticos**. <Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-

crimesciberneticos#:~:text=Bras%C3%ADlia%2C%2028%2F6%2F2022,de%20Crimes%20Cibern%C3%A9ticos%20(UEICC)> Acesso em 10/11/2022.

MACHADO, Thiago José Ximenes**. Cibercrime e o Crime no Mundo Informático: a especial vulnerabilidade das crianças e dos adolescentes**, Belo Horizonte: Editora Dialética, 2021. Disponível em: <https://play.google.com/store/books/details/Thiago_Jos%C3%A9_Ximenes_Machado_Cibercrime_e_o_Crime_n?id=_fUvEAAAQBAJ>. Acesso em: 22/03/2022.

PLANALTO.GOV.BR. **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: 09/05/2022.

SAFERNET.ORG.BR. **[Site institucional]**.
Disponível em: <https://new.safernet.org.br/content/delegacias-cibercrimes> Acesso em: 21/03/2022.

SENADO NOTÍCIAS. **Senado aprova aumento de punições para fraudes eletrônicas; texto vai a sanção**. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/05/05/senado-aprova-aumento-de-punicoes-para-fraudes-eletronicas-texto-vai-a-sancao> Acesso em: 06/11/2022.

SENADO NOTÍCIAS**. Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético**. Disponivél em: <https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico> Acesso em 09/11/2022.

SERASAEXPERIANBRASIL. **Fraudes de identidade: conheça o perfil de quem mais sofre tentativas de uso de dados no Brasil**. Disponível em: <https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2021/09/Indicadores-Economicos-Estudo-de-Fraude.pdf> Acesso em: 06/11/2022.

SILVA,Ayume da Silva Assunção. **A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impactoda Lei nº 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos.** 2021. 16 p. Artigo Científico (Bacharel em Direito) -Centro Universitário Faculdade Guanambi, Bahia, 2021.

SILVA, Vitor. **81% da população brasileira acessou a internet em 2021, diz pesquisa; TV supera computador como meio**. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/06/21/81percent-da-populacao-brasileira-acessou-a-internet-em-2021-diz-pesquisa.ghtml> Acesso em 06/11/2022.

VIEIRA, Eduardo. Os **Bastidores da Internet no Brasil**. 1. ed. Barueri, São Paulo: Manole, 2003. Disponível em: <https://books.google.com.br/books?id=tR4t1Lg2uCcC&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false> Acesso em: 09/05/2022.

WENDT, Emerson; JORGE, Higor Vinicius Nogueria. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação**. 2. ed. Rio de Janeiro: Brasport, 2013. Disponível em: <https://play.google.com/books/reader?id=iGY-AgAAQBAJ&pg=GBS.PP1&printsec=frontcover&output=reader>Acesso em: 22/03/2022.