PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO II

MONOGRAFIA

O AUMENTO DOS CRIMES CIBERNÉTICOS EM PERÍODO DE PANDEMIA E SEUS DESAFIOS NA SOCIEDADE BRASILEIRA

ORIENTANDO – NELSON DAVID SEVERINO NETO
ORIENTADOR - PROF. DR. RAFAEL ROCHA DE MACEDO

GOIÂNIA-GO
2023

NELSON DAVID SEVERINO NETO

O AUMENTO DOS CRIMES CIBERNÉTICOS EM PERÍODO DE PANDEMIA E SEUS DESAFIOS NA SOCIEDADE BRASILEIRA

Monografia Jurídica apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUC-GOIÁS). Prof. Orientador - Prof. Dr. Rafael Rocha Macedo.

GOIÂNIA-GO

2023

NELSON DAVID SEVERINO NETO

O AUMENTO DOS CRIMES CIBERNÉTICOS EM PERÍODO DE PANDEMIA E SEUS DESAFIOS NA SOCIEDADE BRASILEIRA

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador (a): Prof. Dr. Rafael Rocha De Macedo Nota

_____

Examinador Convidado : Prof. Dr. Andre Luiz Aidar Alves Nota

DEDICATÓRIA

Decido este trabalho a minha família que me apoiou durante toda a minha caminhada, me auxiliando, sendo para mim fonte de inspiração.

Aos meus amigos que, foram compassivos com o momento que eu precisava, mas sempre dispostos a discutir ideias, para aprimomarar o nosso conhecimento, e atraves disto a compreenção ampla sobre este determinado tema.

A Deus, por me permitir chegar até aqui, para que lá na frente eu esteja ainda mais próximo do meu propósito.

AGRADECIMENTOS

Agradeço a todos os professores do curso que, tiveram disposição e disponibilidade em transmitir seus conhecimentos, nos orientando para o melhor caminho profissional e pessoal.

Em especial, a minha familia e amigos que foram para mim combustivel para continuar firme e extraindo o conhecimento que toda essa fase nos proporciona, tanto profissional, como também no pessoal.

A Deus, por permitir que tudo fosse possível.

Honeste vivere, neminem laedere, suum cuique tribuere

(Preceitos do Direito Romano)

RESUMO

O presente trabalho de monografia pretede-se apresentar de forma genérica, breve e detalhada sobre o aumento significativo dos crimes cibernéticos em período de Pandemia 2019, apresentando os principais crimes ocorridos no período e visando ao longo do tempo a constante evolução tecnológica, o seu desenvolvimento e sua transformação, sendo fundamental para a sociedade e humanidade o uso de recursos tecnológicos diariamente devido a globalização. Algusn tópicos importantes serão apresentados como conceitos e histórico da Internet; conceitos e características dos crimes cibernéticas; a influência dos crimes cibernéticos na sociedade; o aumento dos crimes cibernéticos durante a pandemia do Covid-19 e formas de prevenir tais crimes. Diante disso, espera-se que após analisar tais informações possa-se ter mais conhecimento acerca do assunto Internet e os ataques criminosos e ainda, saber que no Brasil a Legislação, por mais que atuante, ainda é falha, devendo o governo capacitar ainda mais seus profissionais e criar Leis mais punitivas, garantindo a segurança de toda uma nação.

Palavras-chave: Internet; Crimes; Cibernéticos; Pandemia; Covid-19.

ABSTRACT

The present work of monograph intends to present in a generic, brief and detailed way about the significant increase in cyber crimes in the period of Pandemic 2019, presenting the main crimes that occurred in the period and aiming over time the constant technological evolution, its development and its transformation, being fundamental for society and humanity the use of technological resources daily due to globalization. Some important topics will be presented such as Internet concepts and history; concepts and characteristics of cyber crimes; the influence of cybercrime on society; the rise of cybercrime during the Covid-19 pandemic and ways to prevent such crimes. In view of this, it is expected that after analyzing such information, one can have more knowledge about the Internet and criminal attacks and also know that in Brazil the Legislation, however active, is still flawed, and the government must train even more its professionals and create more punitive laws, guaranteeing the safety of an entire nation.

Keywords: Internet; Crimes; Cybernetics; Pandemic; Covid-19.

SUMÁRIO

INTRODUÇÃO

O presente estudo visa abordar de forma clara e necessária a importância do tema devido ao aumento desenfreado das práticas de crimes cibernéticos, e o quanto os fatores externos sofridos pela sociedade influenciou nestas práticas. Diante a evolução destes crimes, no Brasil, os dados aumentaram durante a Pandemia, apontando um crescimento de mais de 175% nos números de golpes e crimes cometidos, sendo um alerta notório a sociedade e gerando diversas situações que sãodesencadeadas diante destas práticas cometidas pela Internet (GLOBO, 2022).

Os crimes cibernéticos são toda e qualquer ação que resulte em ato ilícito cometido através de rede mundial de computadores (Internet), tendo como o seu maior aliado aparelhos digitais como computadores, celulares, tablete e etc.

Com a junção desses dispositivos, torna-se possível estar “presente” em vários lugares, sem que seja necessário se deslocar de um só lugar, onde é possível que o infrator que comete práticas deste cunho, crie uma rede de proteção, onde eles se escondem, atrás da tela de um aparelho de tecnologia, sendo possível consumar o delito de diversas maneiras, desde crimes que ferem a honra a dignidade humana, até crimes que geram prejuízos econômicos as vítimas, crimes estes como invasão de contas bancárias, contas em lojas virtuais e realização de compras, golpe do pix via whattsapp, invasão de perfil em redes sociais com exposição das pessoas entre outros.

A identificação do infrator (criminoso) é uma das maiores dificuldades enfrentadas pelos policiais, dada a facilidade que é encontrada em criar perfis, redes sociais e sites, tornando-se o cenário ideal para aquele que usa deste meio de comunicação, para agir de má-fé. Como uma expressão utilizada no meio social e jurídico “à ocasião faz o ladrão”.

Cabe, portanto, analisar o quanto e de que forma os crimes cibernéticos sofreram este aumento desenfreado, buscando entender ainda a atuação da justiça quanto a encontrar os criminosos e o que pode ser feito para que tais crimes não aconteçam mais, pensando nos direitos dos cidadãos e garantindo a eles o acesso a informação, a busca de documentos, a execução de seus trabalhos e entre outros pontos favoráveis que a Internet traz para a sociedade.

Justifica-se a execução deste trabalho de monografia o aumento considerado explosivo do número de casos de crimes cibernéticos ocorridos em período de

pandemia do Covid-19, visto o aumento de pessoas conectadas a Internet.

Desta forma, tem-se por objetivo principal demonstrar este aumento significativo em números, não somente no Brasil mas como no mundo, bem como demonstrar que existem Leis que punem tais ações criminosas porém que podem e devem ser constantemente analisadas e atualizadas. Outros objetivos cabem a a apresentação das Leis existentes; os crimes cibernéticos e a sociedade; algumas formas de prevenção.

O método utilizado para o desenvolvimento desta monografia foi o de revisão bibliográfica, buscando na literatura já existente conceitos e características importantes para abordar o tema. Ainda, informações importates foram coletadas em artigos publicados recentemente, garantindo dados reais e atualizados podendo ter uma melhor análise crítica de toda a situação.

1. A HISTÓRIA DA *INTERNET* NO BRASIL

Após a chegada da *Internet* no país no ano de 1988, em uma iniciativa da FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo, em conjunto com a LNCC – Laboratório Nacional de Computação Científica e UFRJ – Universidade Federal do Rio de Janeiro. Com o apoio dessas entidades em desenvolver esse projeto de disponibilizar o acesso à *Internet* no Brasil, o ponto de partida iniciou com a criação de *banckbone RNP*, onde era possível interligar instituições educacionais à *Internet*.

Muitos são os conceitos existentes para a *Internet* e os dicionários o definem como “rede de computadores de âmbito mundial, sendo descentralizada e de acesso público tendo diversos serviços disponíveis como correio eletrônico e a Web” (CORREIA, 2002).

A Agência Nacional de Telecomunicações – ANATEL ao tentar regular o uso de serviços de conexão a *Internet*, editou uma norma n 004/95, conceituando a *Internet* como “nome genérico o qual designa o conjunto de redes , os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários para a comunicação entre os computadores, bem como software e dados contidos em tais computadores”.

Ainda, o Ministério da Ciência e Tecnologia, por meio da Rede Nacional de Pesquisa – RPN desenvolveu um Guia do usuário de *Internet*, trazendo certo conceito: A *Internet* é um conjunto de milhares de redes eletrônicas interconectadas, criando um meio global de comunicação. Tais redes acabam variando de tamanho bem como de natureza, e ainda, diferem as instituições mantenedoras e a tecnologia usada. O acaba unindo é a linguagem que utilizam para se comunicar (protocolos) e o conjunto de ferramentas usadas para se ter informações (correio eletrônico, FTP, *Telnet*, WAIS, *Gopher*, WWW). As informações podem ser encontradas em diferentes formatos e sistemas operacionais, que acaba rodando em todo o tipo de máquinas.

Em complemento, Correa (2002, p.11) cita a *Internet* sendo:

> um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina à outra qualquer, conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando com a criação de novos mecanismos de relacionamento.

Entretanto, somente no fim do ano de 1994 que a primeira empresa, a Embratel, começou a comercializar esse serviço para demais usuários, de modo que eles pudessem experimentar esse serviço. Foram escolhidas 5.000 pessoas para realizaresse teste, porém marcou o início de uma nova era. Foi necessário enfrentar diversasetapas, corrigir falhas na operação, dentre outras situações que precisaram ser desenvolvidas, para um melhor desempenho.

Já em meados do ano de 1995, através de uma Portaria Interministerial nro 147 de 31 de maio, criou-se o Ministério das Comunicações e Ministério da Ciência e Tecnologia, o Comitê Gestor da *Internet* no Brasil – CGI no intuito de garantir a qualidade e a eficiência dos serviços oferecidos, livre competição entre os provedores, manutenção de padrões de conduto de usuários bem como de provedores, levando em conta a necessidade de coordenar e integrar todas as iniciativas de serviços *Internet* no Brasil (BRASIL, 1995).

Em sequência, a portaria nro 148 tem por objetivo regular a Rede Pública de Telecomunicações para serviços de conexão à *Internet* (BRASIL, 1995). Os provedores privados de Internet seriam então os responsáveis de enviar Internet aos seus usuários finais, em contrapartida de pagamento de taxa para as empresas públicas de telecomunicações, que eram as responsáveis por garantir a infraestrutura.

Após o período experimental esse projeto passou por um momento de estagnação, sem que fosse desenvolvido e avançado. Em 1996, o projeto deu andamento, e logo o serviço de Internet se difundia pelo país, tendo um aumento de um milhão de usuários finais segundo afirmam Carvalho, Arita e Nunes (1999).

Em 1999, surgiu o Programa Sociedade da Informação (SocInfo) sendo ele coordenado pelo Ministério da Ciência e Tecnologia tendo o intuito de integrar, coordenar e fomentar ações para o uso de tecnologias de informação e comunicação, contribuindo para a inclusão social de todos os brasileiros na nova sociedade e ainda, contribuindo para que a economia nacional tenha condições de competir no mercado global. (MENEZES, SANTOS, 2002).

Ao passar de alguns anos, a *Internet* se popularizou, mas no início do ano 2000, com o aumento dessa comercialização, as pessoas começaram a instalar a *Internet* em suas residências, sendo ela de conexão discada, conectada a uma linha telefônica.

No ano de 2005, o Instituto Brasileiro de Geografia e Estatística – IBGE fez uma investigação quanto ao acesso a ìnternet através de pesquisa nacional por amostragem de domicílios resultando em que to total da população de 10 anos ou mais de idade, 21% das pessoas acessavam a *Internet*, por meio de um microcomputador, ao menos uma vez nos últimos três meses – daquele período (IBGE, 2005). Já no ano de 2011, a quantidade de pessoas que acessavam a *Internet* sendo elas no mesmo perfil subiu para aproximadamente 47% (IBGE, 2011).

Na sequência, no ano de 2014, o Centro de Estudos sobre as Tecnologias da Informação e da Comunicação – CETIC apresentou informações importantes sobre o uso de Tecnologias da Informação e Comunicação – TIC em residências, empresas, escolas, estabelecimentos públicos e de saúde bem como sobre o uso da Internet pelos jovens e crianças.

Nesta pesquisa foram apresentados informações com base ao acesso as TICs; uso de computadores, locais e frequência de uso; uso da *Internet*; governo eletrônico; comércio eletrônico; habilidades com o computador; uso de telefonia móvel; intenção de compra de novos aparelhos e serviços de TIC.

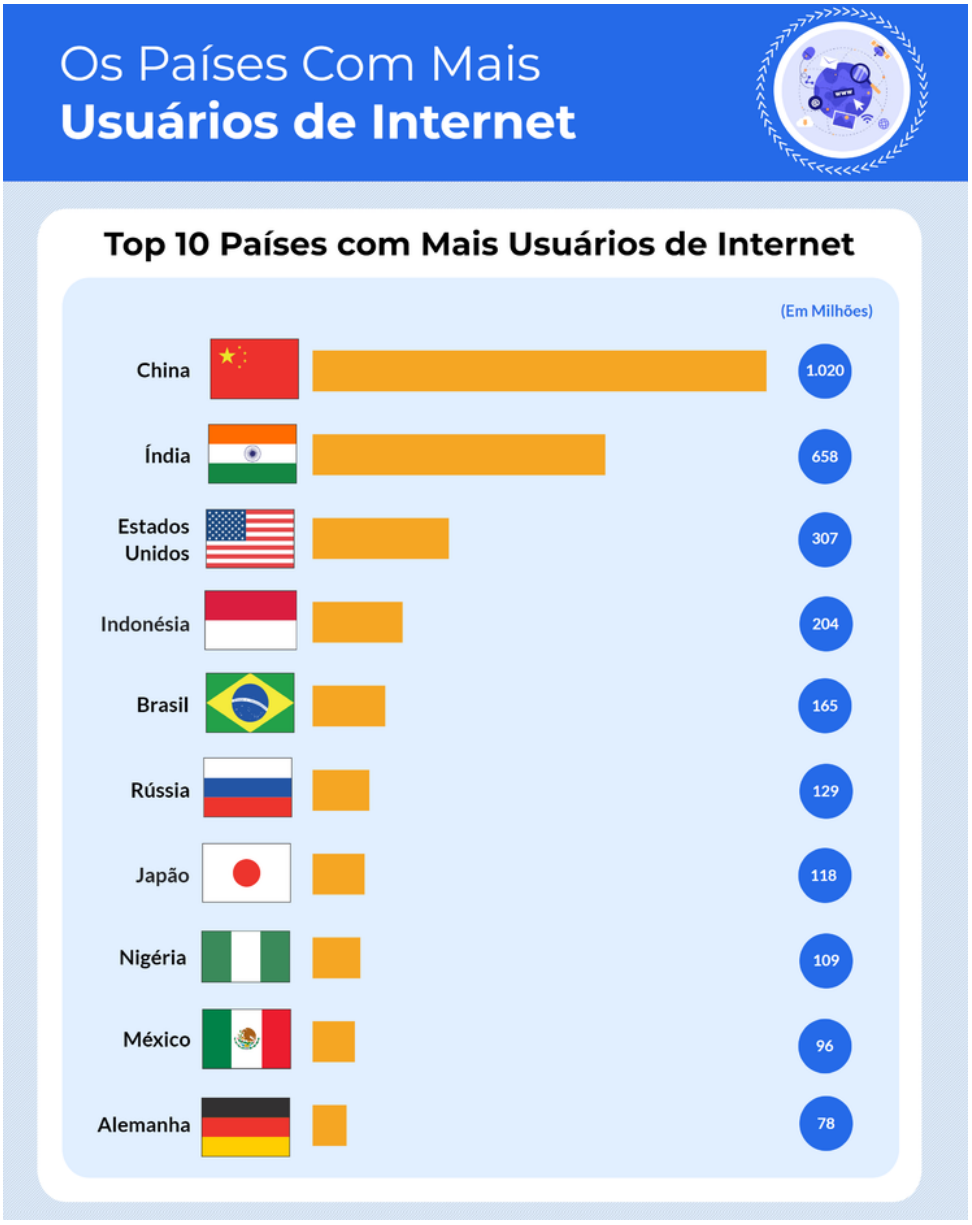
Desta forma as informações resultantes foram que aproximadamente 50% das residências possuíam computador onde o mais encontrado foi o de mesa; 45% das residências tinham acesso a *Internet*, e o acesso mais encontrado foi o via banda larga; 58% dos entrevistados já tiveram acesso a Internet e 71% usam ela diariamente onde aproximadamente 79% acessavam ela de casa; os principais acessos a rede sao uso de redes sociais, busca de informações e transações de produtos e serviços; videos e músicas online, educação, downloads entre outros; e por fim, cerca de 70% afirmaram que utilizaram o serviço eletrônico do governo como obtenção de documentos, cadastro de CPF, pagamento de taxas e impostos, informações de emprego e seguro desemprego, direitos do consumidor, bem como outros serviços demonstrando assim o quanto o acesso a *Internet* facilita o dia a dia das pessoas. (CETIC.BR).

Como pode ser visto, a Internet tem suma importância para toda a população no mundo todo pois informações fundamentais são disponibilizadas a todo momento sejam elas em sites públicos ou privados, garantindo agilidade a todos quanto a seu acesso. Documentos podem ser solicitados, compras efetuadas e problemas resolvidos pelo uso da Internet.

O Brasil ocupa o 5º lugar tendo o maior número de usuários entre os 10 mais

conforme figura 1 abaixo:

Figura 1. Os Países com Mais Usuários de *Internet*



Folhape.com.br, 18/10/2022

Neste sentido, ficou claro que com mais de 100 milhões de usuários, faltava um maior controle ou seja, uma lei a fim de regulamentar os direitos e deveres dos usuários, guiando as questões relativas a governança da *Internet*.

2. DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos são considerados atividades ilícitas por meio do uso de computadores, rede de *Internet* ou mesmo aparelhos eletrônicos e se classificam de acordo com a sua forma de comentimento afirmam Wendt, Jorge (2017). Portanto, são crimes praticados através de instrumento tecnológico conectados à *Internet*, como; computadores, tabletes, celulares e dentre outros meios que tipificam estes crimes.

> 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 (BRASIL, 2008 apud ALVES, 2018)

Segundo D'Urso (2017) foi em reunião do G-8 o que o combate as práticas ilícitas na *Internet* foi discutivo, na sua forma preventiva e punitiva, surgindo o termo "cibercrime". Termo este usado para mencionar as infrações penais praticadas na *Internet*.

Ainda, Jorge e Milagre (2016) afirmam que o crime cibernético ou virtual fala sobre as ações ilegais cometidas através do uso da tecnologia ou por meio de recursos informáticos. Trata-se de um comportamento ilegal onde o autor utiliza um computador, celular ou qualquer que seja o aparelho de informática que se conecta a *Internet*, acontecendo o ato ilícito virtualmente.

Segundo Azevedo e Cardoso (2021) os crimes ciberneticos são divididos em crimes próprios e impróprios. A qualificação própria acontece quando a ação do autor prejudica o sistema ou os dados de uma empresa, de um site, de uma pessoa. Ja o impróprio é quando se realiza o crime dentro e/ou fora da *Internet* como o estelionato.

Houve assim uma popularização da rede de *Internet* referente as mais variadas atividades, passando a existir certa preocupação diante da segurança de

seus usuários, baseados nas informações que eram compatilhadas online para todos que a utilizavam.

O desenvolvimento tecnológico tem dificultado o combate aos crimes que estão alinhados constantemente com as novas tecnologias. Desta forma, com o uso incontido da *Internet*, alguns indivíduos que possuem conhecimento em informática aprimoraram e usam tal conhecimento para roubar informações criptografadas para se ter vantagens econômicas, ou mesmo por diversão (JESUS E MILAGRE, 2016).

Tais indivíduos passaram a ser chamados de *Hackers* sendo designados indivíduos que sempre existiram. Este termo é inglês e utilizado para conceituar programadores habilitados e capacitados, seu alcança informações de forma secreta sobre o sistema informático de outra pessoa sem que a mesma saiba (JORGE E MILAGRE, 2016).

Santos, Martins e Tybucsh (2017) complementam que devido a falta de uma legislação específica no assunto, cabe ao ordenamento penal vigente julgar o cometedor do crime cibernético.

O desenvolvimento da *Internet*, a quebra de códigos bem como a invasão dos sistemas deixou de ser um instrumento de guerra tornando-se uma oportunidade de lucro ilícito bem como um passatempo. Os *hackers*, estelionatários viram então nas transações comerciais uma grande oportunidade de se aplicar golpes altamente lucrativos (JORGE E MILAGRE, 2016).

A *Internet* facilita claramente a vida do ser humano e tornou-se um meio gigantesco de comunicação, passando a ser expostos crimes cibernéticos ou ameaças do crime cibernético. Com o aumento grandioso de usuários, inúmeros grupos criminosos passaram a se formar na plataforma, prejudicando o domínio sem fronteiras dos espaços virtuais. Neste sentido, pode-se afirmar que sem a Internet e sem a tecnologia digital, os crimes não poderiam acontecer onde a tecnologia é o seu foco. Os crimes cometidos por meio da *Internet* acontecem facilmente devido a capacidade tecnológica (TOLEDO, 2017).

Várias são as formas delituosas praticadas na *Internet*, indo desde pedofilia, prostituição, tráfico de drogas, venda de produtos pirateados, sabotagens, terrorismo entre outros. A digitalização dos métodos de trabalho tem causado grandes transtornos provocados por uma nova onda de crimes ciberneticos. Este ano no Brasil, foram registrados inúmeros acessos indevidos a *sites* de empresas e hospitais, buscando solicitar dinheiro em prol de caridade (SANTOS; MARTINS;

TYBUCSH, 2017).

Um dos crimes que ocorrem também pelo meio digital é a pornografia infantil sendo visto como o ato de fotografar cenas de sexo explícito tendo a presença de crianças e adolescentes, nos moldes do artigo 241 do ECA. Injúria, difamação e calúnia sao vistos como crimes contra a honra e estão regulamentados nos artigos 138, 139 e 140 no Código Penal. Ainda, outros crimes muito comuns sao os de calúnia e difamação, sendo vistos como ofensas a honra objetiva e são considerados caso a ofensa seja enviada para grande público e não somente para a vítima, ja tratando-se de injúria, considerada ofensa à honra subjetiva, sendo a ofensa voltada para a própria vítima (SANTOS; MARTINS; TYBUCSH, 2017). As apologias ao crime, exaltar e ou elogiar criminosos ou atos criminosos de forma pública se caracteriza crime cibernético (TOLEDO, 2017)..

Os crimes cibernéticos podem ser configurados de diversas formas devido as diversas vertentes encontradas dentro dessa prática. A classificação pode ser vista da seguinte forma: os crimes própriamente cibernéticos os quais sao aqueles que ocorrem por meio do uso da *Internet*, onde com a sua ausência torna-se impossível a conclusão do ato ilicito, pois a configuração desse criem so pode ser feita por meios virtuais, e com o uso de computadores e outros recursos tecnológicos que permitem o acesso a *Internet*. Já os crimes cibernéticos abertos são aqueles que mesmo com a ausência destes meios pode ser realizada a ação, nao gerando nenhum impedimento aos criminosos (TOLEDO, 2017).

Colares (2022) complementa identificando várias espécies de crimes cibernéticos sendo:

> Dessa forma, são crimes que podem admitir sua consecução no meio cibernético: calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação ao direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, escrito ou objeto obsceno, incitação ao crime, apologia de crime ou criminoso, falsa identidade, inserção de dados falsos em sistema de informações, adulteração de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões, jogo de azar, crime contra a segurança nacional, preconceito ou discriminação de raça-cor-etnia-etc., pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software. (2002, online).

Além desses crimes, as ações prejudiciais atípicas não são configuradas como crimes, embora, são ações onde o indivíduo sem o objetivo de gerar para a vítima

transtornos e prejuízos, evade pastas e dentre outros documentos de cunho pessoal. Para o indivíduo que a comete não é previsto pelo Código Penal como crime, sendo ele responsabilizado apenas civilmente.

Tabela 1. Condutas Indevidas Praticadas por Computador

CONDUTAS INDEVIDAS PRATICADAS POR COMPUTADOR		
AÇÕES PREJUDICIAIS ATÍPICAS (Não é considerado crime)	**CRIMES CIBERNÉTICOS (Crime)**	
	CRIMES CIBERNÉTICOS ABERTOS **Forma tradicional ou por intermédio/contra computadores**	**CRIMES EXCLUSIVAMENTE CIBERNÉTICOS** **Somente por intermédio/ contra computadores**

Fonte: Próprio autor

2.1 CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Diante do aumento de atividades realizadas no âmbito virtual, logo é possível notar que os riscos aos usuários ficaram eminente, pela falta de conhecimento e cuidado necessário dos usuários. O fato da vítimas estar fisicamente em um ambiente seguro, não garante que não estejam sujeitas a riscos. Riscos esses que muitas das vezes não colocam a nossa integridade física em jogo, entretanto pode ocasionar diversos prejuízos emocionais, psíquicos e financeiros.

As apologias ao crime, exaltar e ou elogiar criminosos ou atos criminosos de forma pública se caracteriza crime cibernético (SANTOS; MARTINS; TYBUCSH, 2017).

Desta forma, os crimes propriamente cibernéticos são previstos no Código

Penal como: Invasão de Dispositivos Informáticos, art. 154-a; Divulgar total ou parcialmente, sem autorização devida, por meio de *Internet*, nome, ato ou documento de procedimento policial, administrativo ou judicial relativo a criança e adolescente a que se atribua ato infracional, art. 247, Lei n.° 8.069/90; Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por meio de sistema de informática, fotografia, vídeo ou outro registro que contenha qualquer situação envolvendo criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição de órgãos genitais de uma criança ou adolescente, para fins primordialmente sexuais, art. 241-A c/c 241-E da Lei n.° 8.069/90.

Já os crimes cibernéticos abertos, que fazem parte do índice de maioria, assim como os crimes próprios, estão previsto no Código Penal, compondo outros artigos, como: Crimes contra a honra, arts. 138, 139 e 140; Ameaça, art. 147; Furto, art. 155; Estelionato, art. 171; Estupro, art. 213; todos artigos previsto no CP. Injúria, difamação e calúnia sao vistos como crimes contra a honra e estão regulamentados nos artigos 138, 139 e 140 no Código Penal. Ainda, outros crimes muito comuns sao os de calúnia e difamação, sendo vistos como ofensas a honra objetiva e são considerados caso a ofensa seja enviada para grande público e não somente para a vítima, ja tratando-se de injúria, considerada ofensa à honra subjetiva, sendo a ofensa voltada para a própria vítima (SANTOS; MARTINS; TYBUCSH, 2017).

Tabela 2. de condutas indevidas praticadas por Computador

CONDUTAS INDEVIDAS PRATICADAS POR COMPUTADOR		
AÇÕES PREJUDICIAIS ATIPÍCAS	**CRIMES CIBERNÉTICOS ABERTOS**	**CRIMES EXCLUSIVAMENTE CIBERNÉTICOS**
• Invasão de computador sem a finalidade de obter, adulterar ou excluir dados e informações. • Difusão de *phishing scam*	• Crimes contra a honra • Ameaça • Pornografia infantil • Estelionato • Furto mediante fraude • Racismo • Apologia ao crime • Falsa identidade • Concorrência desleal • Tráfico de drogas	• Invasão de computador mediante violação de mecanismo de segurança, com a finalidade de obter, adulterar ou excluir dados e informações, sem autorização expressa ou tática do titular do dispositivo ou instalar vulnerabilidade para obter vantagens ilícita. • Interceptação telemática ilegal • Pornografia infantil por meio de sistema de informática • Corrupção de menores em sala de bate papo • Crimes contra urna eletrônica

Fonte: Próprio autor

3. AS VERTENTES DOS CIBERCRIMES

3.1 VÍRUS DE *BOOT*

No final da década de 80, iniciou-se a disseminação desse vírus em computadores, agindo através de um disco contaminado com a infecção desse vírus, se propagando também aos próximos discos; CDs, DVDs e *Pen drives* ali utilizados depois da instauração nos arquivos que ali contém. Exemplos desses vírus são o ping-pong, o jerusalém, etc (KOLLING, 2010).

3.2 VÍRUS *TIME BOMB*

Este tipo de vírus caracteriza-se por sua ativação ser feita em determinada data e horário estipulado pelo programador que o desenvolveu. O programador cria códigos malicioso, e no ato da criação desse vírus ele programa a data e horário que ele deve se instaurar, e ativado, gerando os seus respectivosefeitos, praticas essas ações, são conhecidas como o vírus sexta-feira 13, o michelangelo, o eros e o 1º de abril (WENDT; JORGE, 2017).

3.3 *WORM*

O fato do computador ou aparelho estar desatualizado, propicia a disseminação desse vírus, atuando na memória ativa da máquina, reproduzindo copias de pastas e arquivos sem a necessidade e consentimento da vítima. São exemplos que ocorrem quando são enviados e-mail para a lista de contatos, contendo esses vírus, se propagando nas redes sociais (facebook, orkut, google) ou no IRC - Internet Relay Chat.

Conforme previsto na Cartilha do CERT - BR,

> geralmente o worm não tem como consequência os mesmos danos gerados por um vírus, como por exemplo a infecção de programas e arquivos ou a destruição de informações. Isto não quer dizer que não represente uma ameaça à segurança de um computador. ou que não cause qualquer tipo de dano. *Worms* são notadamente responsáveis por consumir muitos recursos. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar. Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias*!

3.4 *BOTNETS*

A atuação desse vírus para à vítima é uma das mais perigosas, pois o programador, após a instauração do vírus no seu computador, ele obtém acesso total ao seu computador mesmo estando à distância. Conseguindo monitorar o seu acesso e ativando ferramentas disponíveis em seu equipamento, como microfone e câmera. Porém, determinas ações aplicadas de maneiras correta, podem ser positivo para utilizar contra os que às práticas, causando efeito reverso. Esse vírus passou a ser usual pela Polícia, com a finalidade de atacar os criminosos, obtendo acesso aos seus computadores.

De acordo com o autor Emerson Wendt (2017), o boetns obteve êxito em ataques contra sites do governo brasileiro:

> Os ataques praticados contra sites do governo brasileiro, em razão da parceria entre os grupos autodenominados Anonymous e LulzSec, que deflagraram a operação #AntiSec43 e Onslaught44 são exemplos deste tipo de ataque45. As ações conseguiram tornar indisponíveis os sites da Presidência da República, Agência Brasileira de Inteligência, Receita Federal, Marinha, dentre outros-6 (2017)

3.5 *DEFACE*

Esse tipo de ataque ocorrem em sites e redes sociais, com a finalidade desfigurar esses perfis, de modo que os criminosos se apropriam de perfil, *site*, *blog* e dentre outros meio, e a partir do momento da invasão ele identifica através da página qual grupo de ciberativista ele pertence. Esses ataques são praticados geralmente contra sites de grande circulação, sites de órgãos públicos, afetando o serviço público, de modo que impede o seu funcionamento, gerando diversos transtornos, entretanto o autor deste crime, poderá responder criminalmente pela ação, previsto no Código Penal de acordo com os arts. 153, § 1º-A; 163, ambos do CP:

> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
> Pena - detenção, de um a seis meses, ou multa, de trezentos mil réis a dois contos de réis. (Vide Lei nº 7.209, de 1984)
> § 1 o -A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: (Incluído pela Lei nº 9.983, de 2000)
> Pena - detenção, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela

> Lei nº 9.983, de 2000)
> Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia: Pena - detenção, de um a seis meses, ou multa.
> Dano qualificado
> Parágrafo único - Se o crime é cometido:
> - com violência à pessoa ou grave ameaça;
> - com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave
> - contra o patrimônio da União, de Estado, do Distrito Federal, de Município ou de autarquia, fundação pública, empresa pública, sociedade de economia mista ou empresa concessionária de serviços públicos;
> - por motivo egoístico ou com prejuízo considerável para a vítima:
> Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.

3.6 CAVALO DE TROIA

Esse tipo de ataque é semelhante ao botnets, pois ambos possibilita que o programador obtenha acesso a máquina à distância, conseguindo realizar ações como se fosse o verdadeiro usuário. De acordo com o conhecimento de Symantec, o cavalo de troia:

> Um programa que se apresenta como um programa desejável, mas que é malicioso. Uma distinção muito importante dos vírus verdadeiros é que esses arquivos não se replicam, como os vírus fazem. Os Cavalos de Troia contêm um código malicioso que causa a perda ou o roubo dos dados. Para que ele se espalhe, basta convidar esses programas a entrarem em seu computador como, por exemplo, abrindo um anexo de e-mail (CASSANTI, 2014, p. 34)

Os Cavalos de Troia também são conhecidos por criar uma porta dos fundos em um computador. A porta dos fundos dá a outro usuário acesso a um sistema e possivelmente permite o comprometimento de informações confidenciais ou pessoais. Diferentemente de vírus e worms, Cavalos de Troia não se reproduzem infectando outros arquivos, nem se autorreplicam.”

Segundo Kolling (2010) É um tipo de vírus que permite total acesso remoto à máquina após a infecção. Pode também ter outras funções como roubar dados do usuário e executar instruções de *scripts*. Entre essas instruções, podem surgir ordens de deletação de arquivos, destruição de aplicativos, etc.

Complementando o raciocínio acima, a Cartilha do CERT diz que:

> é um programa, normalmente recebido como um "presente (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo etc.), que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e

> sem o conhecimento do usuário. Algumas das funções maliciosas que podem ser executadas por um cavalo de Troia são: instalação de keyloggers ou screenloggers: furto de senhas e outras informações sensíveis, como números de cartões de crédito: inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador: alteração ou destruição de arquivos.

3.7 *KEYLOGGER*

A atuação desse vírus acontece com o intuito de monitorar todas as informações digitadas e acessos, feitos pelo usuário. Permitindo que durante a ação o criminoso acesse o computador totalmente, ficando gravadas as ações realizadas durante o uso, desde a tela, mouse, teclado e arquivos. A disseminação desse vírus conta com a ajuda de outros infecteis, exemplo disso são os casos de *phishing scms* que são aplicadosem conjunto (CASSANTI, 2014, p. 34).

Logo, é um aplicativo que captura tudo que o usuário digita. É muito usado para conseguir senhas de acesso a contas e, geralmente está embutido em vírus, spywares ou softwares de procedência duvidosa (ALECRIM, 2011).

3.8 *HIJACKER*

A disseminação dessa infecção tecnológica ocorre através de anúncios indesejados, que ficam aparecendo durante buscas no seu navegador, geralmente anúncios esses contendo conteúdos pornográficos ou ligação com sites ilícitos.

Diante do conteúdo encontrado no livro Crimes Cibernéticos: Ameaças e procedimentos de Investigação, do autor Emerson Wendt e Jorge (2017), esses criminosos usam o nome de órgãos públicos, para obter êxito na ação:

> Para convencer o usuário a executar este tipo de arquivo existem diversos meios fraudulentos, dentre eles temos visto *e-mails* de criminosos digitais que se passam por determinados órgãos, como SERASA, Polícia Federal, Ministério Público, amigo da vítima, instituições bancárias, lojas de comércio virtual (phishing) etc. Estes arquivos maliciosos, além de muitas vezes serem imperceptíveis, também são capazes de produzir inúmeros problemas, como por exemplo podem ter propriedades de Keylogger (arquivo que registra todas as teclas digitadas no computador), vírus (arquivo que contamina e se espalha por arquivos de computador e pode produzir danos contra seus programas, hardware e arquivos), scanner (programa utilizado para localizar as vulnerabilidades dos computadores da vítima), etc. (2017).

3.9 *SNIFFER*

A finalidade de monitorar todo o tráfego que ocorreu na rede, podendo o programador interceptar e averiguar as ações realizadas pelo o usuário. Esse vírus tem uma utilização usual no meio corporativo, para que possa ser detectadas atividade suspeitas realizadas por funcionários, e também costuma ser utilizada por Cibercriminosos (WENDT; JORGE, 2017).

3.10 *BACKDOOR*

O modo de ataque dessa ferramenta, geralmente ocorre a partir da vulnerabilidade do sistema, havendo a possibilidade do programador a ter acessos a dados, que nem mesmo o usuário possui. Há alguns exemplos de como esse ataque pode ocorre, de modo que navegações não seguras, podem gerar riscos, propiciando aos *hackers*, acessos a dados e informações pessoais, que ali contém (WENDT; JORGE, 2017).

Sendo assim, é uma falha de segurança, conhecida como porta dos fundos, onde um programa ou sistema operacional permite a invasão de um cracker no sistema, que obtém acesso total da máquina, podendo instalar vírus e programas maliciosos (KOLLING, [2010]b).

3.11 *HOAX*

Esse método é utilizado para chamar a atenção da vítima, através de imagens contendo Fake News, em redes sociais, sites e *e-mails*. Usando de modo apelativo falsas informações, como; falecimento de pessoas famosas, traições, promoções, dentre outros. Para a propagação desse vírus, eles convencem o usuário a compartilhar aquela “mentira”, sensibilizando à vítima com mensagens emocionalmente apelativas, como por exemplo “Cada pessoa que compartilhar esse post , o *Facebook* doará 10 centavos para o tratamento de câncer” (WENDT; JORGE, 2017).

3.12 *PISHING SCAM*

A aplicação desse golpe, ocorrer através de *links*, mensagem de texto, *e-mails* e arquivos contaminados, com a finalidade de obter dados confidenciais,

bancários, senhas e números de cartões de credito, afim de gerar danos as vítimas, seja ele de dados ou financeiros. No Brasil esse ataque virtual faz parte dos crimes cibernéticos que mais ocorre. É considerado uma fraude que ocorre através do envio de mensagens não solicitadas. Estas mensagens levam o usuário a acessar páginas falsas pensando ser de uma empresa, banco, ou organizações conhecidas. Ao acessar a página, o usuário tem seus dados pessoais e/ou financeiros capturados (KOLLING, 2010b).

3.13 ADWARES E SPYWARES

Os *adwares* têm a função de projetar propagandas através de um *browser* ou programa instalado no computador de forma muitas vezes invasivas e perigosas, podendo minar as configurações de segurança para rastrear suas atividades. De maneira semelhante, os spywares captam informações como dados do usuário e repassam para terceiros, sem autorização (KOLLING, 2010b).

4. OS IMPACTOS DOS CRIMES CIBERNÉTICOS NA SOCIEDADE

O mundo nos últimos tempo obteve avanços, principalmente no mundo tecnológico, passando a proporcionar a sociedade a possibilidade de um desenvolvimento tecnológico avançado. A era digital obteve crescimento significativo nesses anos. Diante desse crescimento tecnológico que gerou à sociedade uma determinada dependência e necessidade dos meios digitais, sendo de certa maneira "obrigado" a inserir nesta era digital. A transformação veio caminhando para a evolução, facilitando à vida daqueles que optam e necessitam da utilização destes meios, tornando-se essencial no meio social e profissional.

No meio social, houveram diversas mudanças e inovações. As criações de novas redes sociais, possibilitou o usuário a se conectar, interagir e estar "presente", sem que seja necessária a presença física de fato, estando presente de um modo virtual, e se conectando de forma instantânea com usuários de todo mundo, através de um simples *click*. Porém, essa facilidade acarretou consequências negativas, diante da facilidade e o aumento descontrolado de usuários sem a devida orientação e cautela necessária.

Segundo um grande sociólogo Bauman (2010), o mundo atual vive um momento de frouxidão nas suas relações sociais onde com o avanço tecnológico no século XXI, as pessoas tendem a se relacionar mais por meio de aparelhos eletrônicos do que pessoalmente, sendo um grande fato gerador para o oportunismo dos grandes criminosos cibernéticos.

Aproveitando da fragilidade humana e tecnológica os criminosos passaram a agir a partir desta falha, sendo oportuno diante da facilidade encontrada em aplicar golpes através de meios digitais, disseminando vírus, e *links*. Além de golpes aplicados por intermédio de redes sociais de mensagens instantâneas, onde os criminosos passam por familiares, amigos e conhecidos, das vítimas.

Muito ainda acontece nas redes sociais, onde hoje as pessoas vivem um "amor descartável!" afirma Bauman (2010) onde relacionamentos estão mais frágeis e descartáveis tendo a relação das pessoas baseadas em redes sociais como o *Facebook*, Instagram, entre outros aplicativos que permitem facilmente adicionar novos amigos e novos amores a qualquer momento e com isso vem os acessos indesejdos, pessoas desconhecidas entrando na vida das pessoas, podendo a qualquer momento buscar seus dados e efetivar um crime cibernético.

Quando se é falado de redes sociais, o estudo da E.life afirma que mais da metade dos brasileiros que utilizam a *Internet* tem parte do seu tempo designado as redes sociais, onde até mesmo serviços como SAC – Serviço de Atendimento ao Consumidor são utilizados pelo Facebook. (FERNANDES, 2020)

As empresas tem utilizado os canais das redes sociais no intuito de melhorarem seus serviços e produtos pois conseguem monitorar o que as pessoas dizem, percebendo seus gostos, desejos e ainda pontuando aquilo que não estão gostando. As empresas precisam se atentar para nao prometer algo que não poderá cumprir podendo afetar a confiança do cliente.

Quando uma empresa recebe uma denúncia ou uma reclamação via rede social, ela deve ver a situação nao como um problema mas sim como uma oportunidade de consertar uma falha, ganhando mais um cliente e demonstrando ser de confiança para todos os demais que, nas redes sociais, acompanham tal reclamação. Para a sociedade, é um grande ponto favorável pois não somente as redes sociais possuem tais links, mas sites como o Reclame Aqui demonstram as satisfações e insatisfações quanto a uma empresa, podendo até mesmo identificar situações de fraudes entre outras situações consideradas crimes cibernéticos.

Tudo é feito pela *Internet* atualmente desde pequenos acessos a informações básicas, soluções de problemas, solicitações de documentos, grandes negociações e permitindo até mesmo que as pessoas estudem virtualmente, sendo assim a Internet a grande aliada da sociedade. Porém, devido ao crescente número de crimes cibernéticos ocorridos no período de pandemia e que vem acontecendo aos dias de hoje, torna a sociedade mais frágil e tantos acessos e facilidades trazidas pela *Internet* pode se tornar um grande problema para as pessoas.

Neste sentido, tal avanço tecnológico demostra a importância da informação, se tornando um bem jurídico de grande importância. Um direito fundamental do homem, que se encontra descrito no artigo 5º da Constituição Federal é:

> "Art. 5 – Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: IV – é livre a manifestação de pensamento, sendo vedado o anonimato; V – é assegurado o direito de resposta, proporcional ao agravo, além de indenização por dano material, moral ou à imagem; IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; XIV – é

> assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício ao exercício profissional; XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade de do Estado; LXXII – conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constante de registros ou banco de dados de entidades governamentais ou de caráter público; b) para retificação de dados, quando não se prefira fazêlo por processo sigiloso, judicial ou administrativo;" (Constituição Federal de 1988)

Tais garantias acima estão diretamente relacionadas a liberdade da informática a qual tem o intuito de ligar as pessoas a informação e podendo tambem transmití-las a outras pessoas. Tal transmissão de informações não se pode ser realizado de forma desordenada, devido aos variados meios de propagação.

Desta forma, com tanto acesso a informação, surge a necessidade do Estado intervir, atuando como um fiscalizador a fim de prevenir práticas que podem ser nocivas a sociedade. Sendo assim, a fim de resguardar a eficiência das informações ora divulgadas:

> “A sociedade da informação surgiu a partir da facilitação no desempenho de atividades cotidianas proporcionadas pelo uso de ferramentas informatizadas. Mais do que isso: esses mecanismos eletrônicos guarnecem inúmeros bens jurídicos de suma importância para o ser humano, a exemplo da saúde, intimidade, segurança, liberdade entre muitos outros. Desse modo, a sociedade se vê vinculada às tecnologias da informação, tendo, a criminalidade, passado por esse mesmo processo. Aparecem os crimes virtuais e, com eles, novos bens jurídicos, aos quais a ordem constitucional precisa proteger. Há um impacto da sociedade da informação na ordem constitucional, o que gera consequências na esfera penal.” (MONTEIRO NETO, 2008, p. 6; OLIVEIRA, 2013, p. 11).

No meio profissional, o *home-office* foi desenvolvido e adotado por empresas privadas, e órgãos públicos. Diante desta inovação no mercado de trabalho, sendo interessante para o profissional, como para a empresa ou órgão competente, a comodidade e economia tornou um dos grandes atrativos para esta modalidade. Porém, não sendo diferente do meio social, a facilidade que veio acompanhando de uma fragilidade no sistema e desencadeando a prática de furto de dados, invasões deacessos, dentre outras ações executadas por esses *Hackers*.

Os impactos que podem ser causados às vítimas são os mais diversos, desde a prejuízos econômicos, emocionais, psíquicos e social, gerando muita das vezes

prejuízos irreparáveis, exemplo disso são os traumas psicológicos ocasionados diante de fatos como esse, que ocorrem no Brasil e no mundo de forma corriqueira. Às vítimas são colocadas em situações em que o seu emocional fica totalmente abalado, desencadeando e propiciando a vítima o afloramento de sentimentos ruins, o que reflete na sociedade em que vivemos, e qual a percepção da vítima após ser aplicada em um golpe.

5. DAS LEIS ENTRE 1996 A 2023 DESIGNADAS PARA A PROTEÇÃO CONTRA O CIBERCRIME

Com a grande incidência dos crimes cibernéticos no Brasil e no mundo, os Estados Unidos foram os pinoeiros a criarem bem como a editarem legislações a fim de se evitar e punir tais crimes. Logo após os EUA, teve a Alemanha, a França, a Espanha, Europa e na sequência o Brasil entre outros países menores tendo todos os mesmos objetivos, amenizar os ataques cibernéticos, sabendo que eliminá-los de vez, neste andar da carrugaem, será impossível.

Os Estados Unidos iniciaram com a criação de legislação nos anos 80, citando-se alguns exemplos como a ECPA “Lei de Privacidade de Comunicação Eletrônica” ; a CFAA “Lei de Fraude e Abuso de Computadores”. Já na Europa acontecceu a convenção de Budapeste e no Brasil, uma das Leis mais conhecidas é a “Lei Carolina Dieckman” sendo a Lei nº 12.737/2012 a qual surgiu devido ao fato acontecido com a atriz brasileira Carolina Dieckman, onde algumas fotos íntimas foram expostas e divulgadas sem a sua autorização, sendo ela ameaçada, com crime de extorsão.

A Lei 11.829/2008 fala sobre a proteção da criança e do adolescente, alterando a Lei 8.069 de 13 de julho de 1990, aprimorando o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na *Internet*.

Já a Lei 12.735/2012 altera o Decreto-Lei 2.848/1940 do Código Penal, o Decreto Lei de 1.001 /1969 e na Lei 7.716 de 1989.

> Sobre a lei nº 12.735/12, enquanto projeto foi apelidada de “AI-5 digital” por conta dos pontos polêmicos que continha, em especial, os referentes à guarda dos logs de acesso dos usuários pelos provedores. Em face disso o projeto foi esvaziado e se tornou uma lei com poucas e frágeis disposições. Em resumo, o texto aprovado determina que os órgãos da polícia judiciária deverão criar delegacias especializadas no combate a crimes digitais (art. 4º). A medida é salutar, mas depende do Poder Público a ela prover a concretude necessária, investindo na especialização da Polícia com treinamentos e equipamentos.

A Lei 12.737/2012 fez com que algumas alterações no Código Penal ocorressem, tendo assim um melhor amparo legal a qual se adequou a realidade

digital. A LGPD, possui alcance extraterritorial com efeitos internacionais, ao fato que se aplica aos dados que sejam tratados fora do país, desde que a coleta tenha acontecido em território nacional, ou mesmo com a oferta de produtos e serviços aos consumidores em espaço nacional. Sendo assim, o dado pessoal tratado por uma empresa de serviço de cloud computing que armazene o dado fora do país precisará seguir as exigências da LGPD afirma Pinheiro (2018).

Neste sentido, a LGPD – Lei Geral de Proteção de Dados teve um papel fundamental para os usuários digitais, sendo pessoas físicas ou jurídicas, obtendo assim grandes avanços a sua proteção de dados.

Antes da criação da lei 12.737/2012, não existia como combater as práticas lesivas cibernéticas. O direito atual proíbe fazer analogia para prejudicar o réu. Logo,

> "O artigo 5º, inciso II, da Constituição Federal dispõe que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei". Reforçando essa garantia, o artigo 5º, XXXIX da carta magna (com idêntica redação do artigo 1º do CP) anuncia que "não há crime sem lei anterior que o defina nem pena sem prévia cominação legal". Trata-se de real limitação ao poder estatal de interferir na esfera de liberdades individuais, daí sua inclusão na Constituição entre os direitos e garantias fundamentais" (Manual de direito Penal, p.94)

Sem essa norma não se pode punir os criminosos que tentam lesar a sociedade. Em complemento, o artigo 1º do CP e o 5º da CF afirmam,

> "Pelo princípio da anterioridade, a criação de tipos e a combinação de sanções exige lei anterior, proibindo se a retroatividade maléfica. "Paulo Queiroz, citando Hobbes, esclarece que, se apenas supõe um fato considerado como transgressão à lei, o dano praticado antes de existir a lei que não o proibia não é uma pena, mas um ato de hostilidade, pois antes da lei não existe transgressão à lei. Por isso que a CF (e o CP) dispõe que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal", de sorte que a formulação completa do princípio da legalidade compreende, necessariamente, a anterioridade da lei e sua irretroatividade. " (Manual de direito Penal, p.94)

Deve-se ainda levar em consideração o princípio da territorialidade que por mais que a *Internet* permite acessos fora do país, tendo alcance global, o Código Penal afirma que os crimes praticados em território brasileiro ou nacional será

punido e julgado pelas leis brasileiras, podendo ainda ser julgado pelo principio da extraterritorialidade, quando os crimes cometidos fora do país sao julgados pelas leis nacionais.

Portanto, as leis penais não acompanham as mudanças e o desenvolvimento constante da tecnologia, porém algumas mudanças já estão expressas na constituição que busca a prevenção e a proteção dos direitos essenciais. A necessidade de regulamentação penal a fim de prevenir e combater ainda mais os crimes cibernéticos é algo considerado fundamental e urgente, visto que falta norma regulamentadora para uma nova realidade social.

5.1 A *INTERNET* E A GOVERNANÇA – MARCO CIVIL

No ano de 2003, aconteceu em Genebra a Cúpula Mundial das Nações Unidas sobre a sociedade da informação sendo criado o WGIG contendo 40 membros sendo eles representantes de governos, do setor público e privado, e sociedade civil. Aconteceram no total 4 encontros, tendo assim resultados alcançados a serem aqui citados.

Em uma de suas quatro reuniões, os Chefes de Estado e o Governo conseguiram identificar a importância da *Internet* como sendo um elemento central de infraestrutura de uma sociedade de informação emergente (WGIG, 2005).

O relatório gerado por ele demonstrou a definição de governança da *Internet*: “governança da *Internet* é o desenvolvimento e execução, usado pelos Governos, setores privados e sociedades civis, de princípios compartilhados, normas e regras, procedimentos de tomada de decisão, e programas que figuram a evolução e uso da *Internet*” (WGIG, 2005).

No Brasil, o CGI.br aprovou a resolução Princípios para a governança e uso da *Internet* no Brasil. Este documento demonstra que a “governança da *Internet* deve ser realizada de forma clara e concisa, multilateral e democrática, tendo vários setores incorporados na participação, preservando e estimulando o seu caráter de criação coletiva. Esta governança da *Internet* deve promover a evolução contínua bem como a grande difusão de novas tecnologias e modelos de uso e acesso (COMITÊ GESTOR DA *INTERNET* NO BRASIL, 2009).

O Marco Civil da *Internet* foi então apresentado como um conjunto de normas a fim de regulamentar o uso da Internet, tendo como princípios a neutralidade da

rede, a privacidade do usuário e a liberadade de expressão. Ele é encontrado como Lei nro. 12.965 de 23 de abril de 2014 (ARAGÃO, 2014).

Em seu primeiro artigo demonstra que ela determina princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil, determinando as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios frente a matéria.

Em seu 3º artigo são citados 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.

A lei ainda determina que o acesso a *Internet* é fundamental para que o cidadão exerça a sua cidadania, e ao usuário, são assegurados diversos direitos como:

> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela *Internet*, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à *Internet*, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à *Internet*;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de Internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de *Internet*, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso,

> armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de *Internet*;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de Internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à *Internet* e de aplicações de *Internet*;
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na *Internet*.

Esta lei, segundo Oliveira (2014) busca guardar e cuidar da disponibilização dos registros de conexão e de acesso a aplicações de *Internet* bem como dos dados pessoais e as comunicações privadas, atendendo à preservação da intimidade, da vida privada, da honra e da imagem das partes de forma direta ou indiretamente envolvidas.

A lei também aborda atuação do Poder Público, apresentando as diretrizes para a atuação da União, dos Estados, dos Municípios e do Distrito Federal a fim de garantir o desenvolvimento da Internet e as aplicações dela usadas pelo próprio Poder Público. Ainda, fala sobre a função do Estado no âmbito educacional e o uso da Internet como uma ferramenta importante para o exercício da cidadania, promoção da cultura e do desenvolvimento tecnológico. Certo disso, demonstra quais os deveres das iniciativas públicas de fomento à cultura digital sendo a *Internet* vista como uma grande ferramenta social afirma Oliveira (2014).

Caso haja infrações as normas dispostas nesta Lei ficam assim sujeitas a algumas sanções, aplicadas isoladamente e de forma cumulativa.

Abaixo um quadro analítico sobre o impacto do Marco Civil nas atividades executadas pelos senhores usuários.

Quadro 1. Impacto do Marco Civil nas Atividades Realizadas pelos Usuários

Caracterização das ações	Antes do Marco Civil	O que muda com o Marco Civil
Redes Sociais digitais	Os dados dos usuários poderiam ser coletados e vendidos a terceiros, para fins comerciais.	Os dados fornecidos aos provedores de aplicações não poderão ser repassados a terceiros, o que mantém o princípio da privacidade. Ao se desligar de um serviço, o provedor de aplicações não poderá guardar os dados do usuário.
Criação de conteúdos (sites, blogs, wikis etc.)	O provedor de aplicações podia ser responsabilizado por conteúdo publicado pelos usuários.	O provedor de aplicações não poderá ser responsabilizado por conteúdo publicado por seus usuários e esse conteúdo só poderá ser retirado do ar mediante ordem judicial.
Formas de comunicação na internet: • em tempo real; • correio eletrônico; • grupos e fóruns de discussão.	Os provedores de conexão alteravam a velocidade da conexão conforme o serviço utilizado sem restrição alguma.	A neutralidade de rede obriga os provedores de conexão a tratarem de maneira igual toda informação que trafega na rede; são proibidas distinções em razão do tipo, origem ou destino dos pacotes de dados.

Fonte: Lei 12.965/14

Como pode ser notado, o Marco Civil demonstra as normas as quais acabam impactando ao falar das atividades realizadas pelos usuários na *Internet*. Os princípios, garantias, direitos e deveres estão sendo reanalisados de forma democrática, buscando a especificação clara do que poderá ser feito ou não com o decreto de regulamentação da Lei 12.965. Existem alguns pontos que acabam gerando questionamentos e indagações, carecendo de especificação detalhada, sendo eles a neutralidade da rede e da privacidade dos dados pessoais e comuncações privadas. Tudo isso garantindo a segurança pública ou telemedicina.

Portanto, regulamentar o uso da *Internet*, controlar, gerir e aperfeiçoar o controle sao pontos fundamentais para garantir o direito do cidadão, a segurança pública, e o acesso de todos a informação.

As penas variam de 3 meses a 5 anos de prisão, indo de acordo com o tipo de crime cometido pelo criminoso virtual.

6. O CIBERCRIME E O PERÍODO PANDÊMICO COVID-19

Os crimes cibernéticos cresceram de forma preocupante e significativa durante a pandemia do Covid 2019. Constantemente as pessoas físicas, jurídicas, instituições bancárias e governamentais foram vítimas de crimes digitais.

Com o início da pandemia e o isolamento social o uso de aparelhos eletrônicos, para a realização de negocios, trabalho, acesso a bancos e sites de compras aumentaram tornando o cenário vulneravel e mais favorável para a prática de crimes digitais.

Se as pessoas estão passando muito mais tempo alienados ao computador, aos seus celulares é natural que estejam mais sujeitas a serem vítimas de crimes ciberneticos, visto que o consumo de conteúdo digital na Internet é maior.

Vários são os motivos que instigaram os criminosos a agirem virtualmente onde eles encontraram no cenário pandêmico, na instabilidade emocional de toda uma população, na sociedade e na crise economica uma grande oportunidade de atuação e aumentando assim os crimes virtuais.

Alguns crimes cibernéticos se destacaram durante o longo período de pandemia que o mundo tem vivenciado.

A clonagem de *WhatsApp* é quando o criminoso enviar um código de aesso pelo aplicativo para o celular da vítiam, entrando em contato com a vítima e se passando ser de alguma empresa. Com este código, o criminoso consegue acessar o WhatsApp da vítima com seus contatos e conversas no aplicativo. Desta forma, o criminoso consegue enviar mensagem aos seus contatos pedindo depósitos em dinheiro (SOUZA, 2002).

Os *Malwares*, considerados sequestradores de dados, é um vírus de resgate que sequestra os dados dos usuários ou o controle de algum sistema. Logo, o criminoso chantageia a vítima, exigindo pagamentos em troca dos dados sequestrados.

Os *Pishings* acontecem quando o criminoso manda um e-mail ou SMS –

Serviço de Mensagens Curtas para a vítima. O e-mail ou SMS possui links ou arquivos contaminados com vírus, levando o usuário a um site. Tem por objetivo enganar a vítima, fazendo com que ela dê informações pessoais como dados bancários entre outros acessos. Este é um dos crimes virtuais mais executados onde o criminoso desenvolve sites, aplicativos digitais e engana muitos usuários de formas variadas (SOUZA, 2002). Um grande exemplo é no e-commerce onde sites são criados e desenvolvidos contendo produtos em grandes promoções, atraindo diversos clientes que efetuarão o pagamento de compras de produtos que nunca receberão e ainda, fornece os dados financeiros e pessoais permitindo ao criminoso realizar novas compras em seu nome.

Outras formas de pishing sao as doações para fundos de instituição de caridade, e para beneficiários do auxílio emergencial, sendo pago pelo governo durante o período da pandemia.

Crimes como falsidade ideológica, calúnia, difamação, ameaça e injúria são considerados crimes cibernéticos porém ja existiam antes mesmo da pandemia.

Desta forma, a sociedade como um todo, além de ter que se preocupar com o Covid-19, com a crise econômica, política e financeira no país, a instabilidade econômica e emocional, passou a ter que se preocupar com seus dados e informações pessoais por meio dos crimes cibernéticos.

Dentre os crimes cibernéticos acometidos no ano de 2017, temos serviços falsos, prêmios falsos, páginas de *Internet* falsas e golpes de WhatsApp, conforme segue na figura abaixo:

Figura 2. Ataques Cibernéticos Mais Comuns no Brasil

Fonte: https://www.psafe.com/blog/ataques-ciberneticos-como-se-proteger/, em 07/04/2023.

Com toda a situação caótica vivenciada por toda uma nação, os criminosos encontraram uma grande oportunidade de realizarem seus crimes, aumentando os dados consideravelmente.

Segundo dados apresentados por meio de relatórios do FortiGuard Labs, durante o ano de 2020 o Brasil teve aproximadamente 8,5 bilhões de tentativas de ataques cibernéticos, onde 5 bilhões aconteceram apenas nos meses de outubro, novembro e dezembro.

Ja no ano de 2021, o Brasil passou de 88 bilhões de tentativas de ataques ciberneticos, sendo um aumento de mais de 950% diante do ano de 2020, ocupando o segunda lugar em número de ataques na América Latina e Caribe, ficando atrás do México.

A grande alta nos números foi constatado durante todo o ano, ocorrendo em toda a região, que chegou a registrar 289 bilhões de ataques no total, portanto 600% diante do ano anterior.

Quadro 2. Número de ataques cibernéticos

México	156.000.000.000
Brasil	88.500.000.000
Peru	11.500.000.000
Colômbia	11.200.000.000

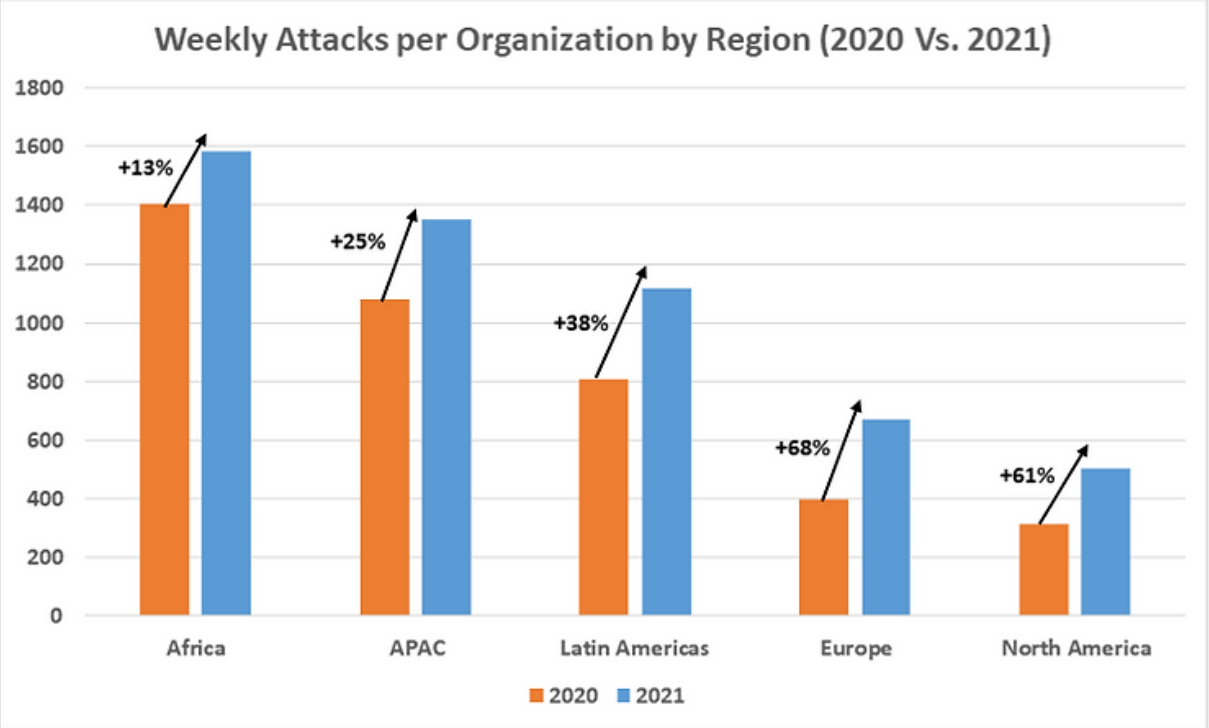
Chile	9.400.000.000
Argentina	3.200.000.000
Panamá	3.200.000.000
Costa Rica	2.500.000.000
República Dominicana	2.200.000.000
Porto Rico	926.000.000
LATAM	289.000.000.000

Fonte: fortinet.com São Paulo - 08/02/2022

Ainda pelo mundo pode-se analisar que a África sofreu o maior número de ataques no ano de 2021, tendo uma média de 1582 ataques semanais por empresa, representando um aumento de aproximadamente 13% diante do ano de 2020.

No segundo lugar, vem a Ásia – Pacífico – APAC tendo uma média de 1380 ataques durante a semana por empresa (aumento de aproximadamente 25%) seguidos da América Latina com 1120 ataques semanais (aumento de aproximadamente 38%). A Europa tem 670 ataques semanais (com aumento de 68%) e a América do Norte com cerca de 500 ataques semanais por empresa (aumento de 61%).

Gráfico 1. Ataques Semanais por Organização pela Região – 2020 x 2021

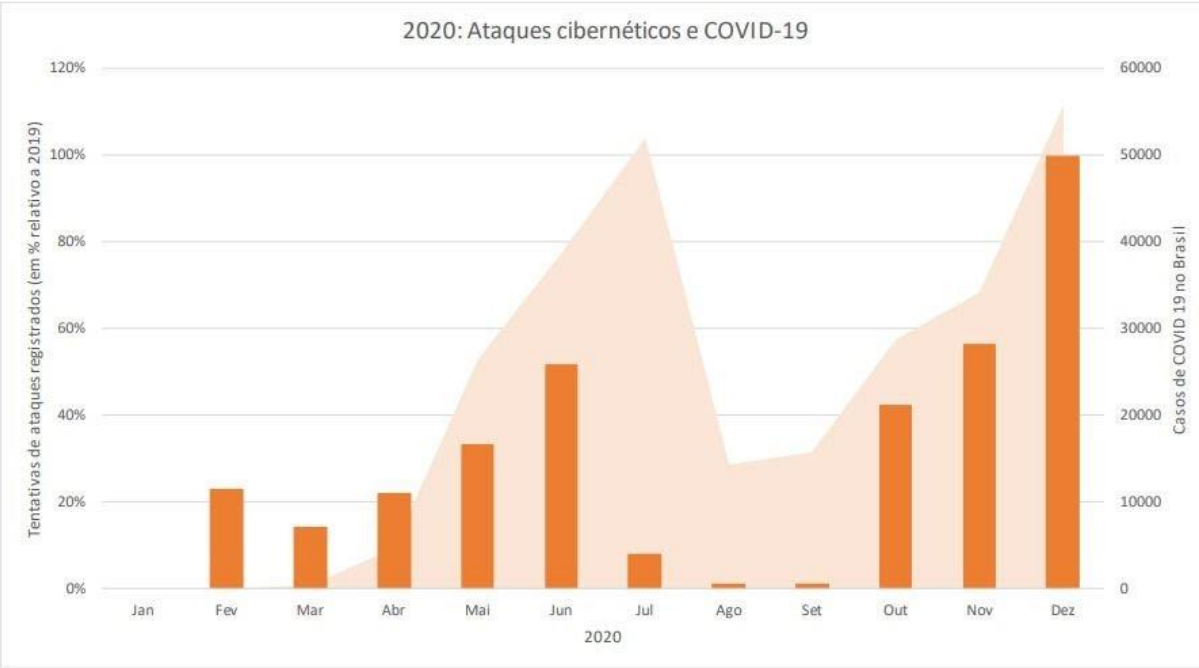


Fonte: Internationalit.com (2022)

Ao se falar em Brasil, em levantamento realizado por uma empresa de segurança cibernética industrial, chamada TI Safe, apontou um aumento de 460% de tentativas de ataques cibernéticos em organizações industriais, entre os meses de março e junho de 2020. Entre os meses de julho a setembro o padrão voltou ao seu normal, mas já em dezembro foi observado um crescimento de 860% de tentativa de invasões.

Os dados demonstram uma grande coincidência entre os períodos de novas ondas da Covid-19 e as ocorrências. Muitas empresas aderiram ao trabalho remoto porém nao se precaveram quanto a segurança cibernética, deixando suas redes de TIC – tecnologia da informação e comunicações em risco.

Gráfico 2. Ataques cibernéticos e Covid-19

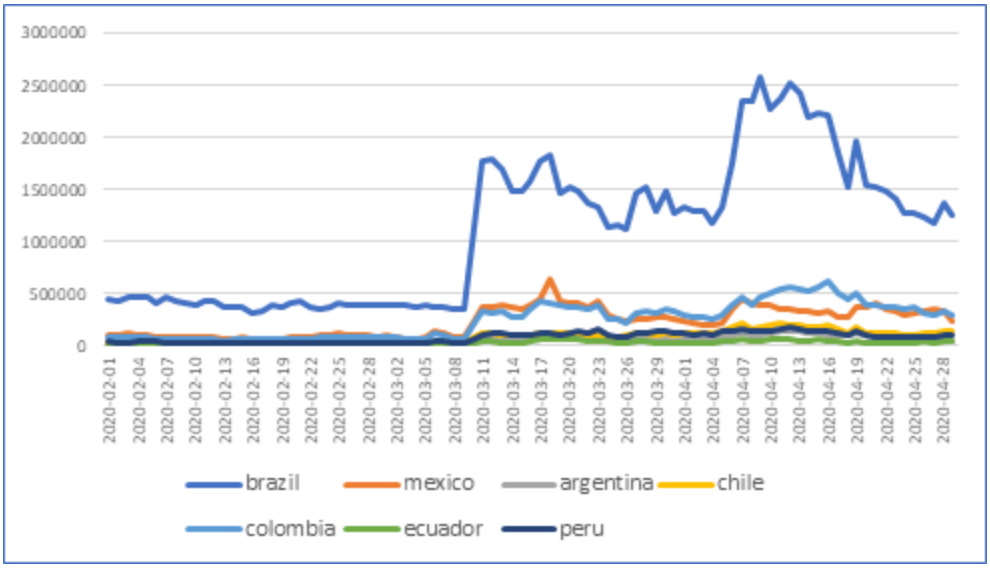


Fonte: Internationalit.com (2022)

Já no gráfico 3 abaixo verifica-se ataques que aumentaram a partir do início de março em toda a América Latina. O crescimento mais significativo, no Brasil, ocorreu entre os dias 9 e 10 quando o número de ataques triplicou em apenas um dia. Logo, a média diária manteve-se acima de 1 milhão até o final do mês de abril. Já em fevereiro, foram identificados aproximadamente 12 milhões de ataques de força no país, em abril, mais de 50 milhoes, sendo assim um crescimento de 330% em apenas dois meses.

Além do Brasil o segundo país mais atingido foi a Colômbia com 12 milhões de ataques e seguidos pelo México (9 milhões), Chile (4,3 milhões) Perú (3,6 milhões) e Argentina (2,6 milhões).

Gráfico 3. Ataques cibernéticos em período de pandemia do Covid-19



Fonte: Internationalit.com (2022)

No momento de pandemia, segundo afirma Kaspersky (2021):

> "Muitas empresas foram forçadas a transferir seus funcionários muito rapidamente para o trabalho à distância, sem terem tempo para garantir a existência de medidas de segurança adequadas. Isto deixou-as mais suscetíveis a este tipo de ataque, porque seus colaboradores precisam acessar os recursos da empresa a partir dos seus computadores domésticos, que, muitas vezes, estão ligados a redes com pouca proteção. À medida que o trabalho remoto continua, os funcionários devem tomar precauções adicionais de segurança, como a criação de uma senha forte para as ferramentas de acesso remoto"

Sabe-se que muitas empresas mantiveram seus colaboradores em *home-office* até os dias de hoje e que o estado de pandemia ainda não finalizaou, causando ainda certas restrições.

7 PREVENÇÃO AOS CRIMES CIBERNÉTICOS

Existem muitas formas de se precaver quanto ao acesso a *Internet* e o uso de dispositivos eletrônicos, sendo cuidados básicos, simples que auxiliam os usuários a evitar a ocorrência de crimes digitais.

Podem ser citados abaixo alguns deles afirma Souza (2002):

- não acessar links enviados por *e-mails* que não tenha solicitado, nao acessando tambem os seus anexos;

- não acessar links recebidos por mensagens, sejam de SMS ou *WhatsApp*, não conhecendo a origem ou a certeza de que os sites sao reais e de pessoas confiáveis;

- confirmar os sites relacionados a arquivos antes de fazer download;

- não realizar doações sem que saiba a autenticidade da instituição;

- ter cuidade ao usar um *QR Code*, verificando se o mesmo é original do site em questão;

- usar senhas fortes em aplicativos, sites, não as repetindo em plataformas diferentes, devendo alterar as senhas com certa frequência;

- manter os dados e informações pessoais na consideração de privadas;

- manter as atualizações de antivírus e *firewalls*;

- lembrar que nenhum banco, instituição financeira ou empresa de cobrança entra em contato com o cliente para solicitar número de cartao de crédito, senha, muito menos solicita transferência de valores.

Como suporte, qualquer vítima de crime digital pode realizar uma denúncia dentro de uma Delegacia Especializada em Crimes Digitais existentes no Brasil. A denúncia poderá ser realizada em qualquer outra delegacia, caso ela não tenha no município onde a vítima mora.

Ainda, o projeto ‘Ministério Público pela Educação Digital nas Escolas’, que através da atuação do Ministério Público Federal, tem como público-alvo educadores de escolas da rede pública e privada, oferecendo incentivo para a realização de atividades que ensinem crianças e adolescentes sobre o uso seguro e responsável da *Internet*, evitando assim que sejam vítimas ou pratiquem crimes virtuais (MINISTÉRIO PÚBLICO FEDERAL, 2018).

Com isso, educa-se os jovens e adolescentes para que tenham consciência da importância de saber utilizar a *Internet*, incentivando ao bom uso da mesma, evitando que pratiquem crimes virtuais.

Quando encontrado ou denunciado um crime virtual, a delegacia a qual foi realizada a denúnica investigará tudo sobre o fato e ao findar o Inquérito Policial, os autos serão enviados ao Ministério Público para que seja iniciado o Processo Judicial.

Ainda este processo é falho e vago por falta até mesmo de investimento e capacitação dos envolvidos mas fica aqui um ponto a ser fortemente analisado pelo Ministério Público e pelo governo.

CONSIDERAÇÕES FINAIS

O objetivo principal deste trabalho de monografia foi o de relatar o grande aumento dos crimes cibernéticos acontecido no Brasil e no mundo diante do momento de pandemia do Covid-19, de como este momento caótico na vida de toda uma nação serviu de base e de oportunidade para que os criminosos deixar suas técnicas de invasão e de criminalidade ainda mais sofisticadas e desenvolvidas.

Diante desta total dependência do ser humano pelos sistemas informatizados, computadores e pela *Internet*, a adoção de legislação nesta área se justifica tanto pelo caráter patrimonial quanto pela sua preservação da integridade do sistema de computador, bem como ofertar bens e serviços para a população. As mudanças tecnológicas acabam refletindo neste acontecimento jurídico, afetando assim as relações humanas. Neste sentido, torna-se necessária uma proteção jurídica maior, viável e aplicável, não devendo a Lei ter um papel passivo nesta revolução e evolução sem retorno.

Quando falamos em crime cibernético, pensamos em *hackers* utilizando um computador e invandindo contas bancárias mas não, atualmente, o acesso a informação está muito difundida, existe muita tecnologia no mercado e pessoas muito capacitadas a não somente acessarem contas bancárias mas a praticarem crimes cibernéticos dos mais simples e variados como injúria, difamação entre outros como pode ser visto no desenvolvimeto desta monografia.

Contudo, uma legislação adequada não é o suficiente o bastante. Aperfeiçoar os meios de investigação, o progresso técnico dos profissionais ligados à área da persecução penal, a melhor formação e treinamento de auxiliares da Justiça bem como a conscientização dos usuários são vistos como elementos fundamentais para coibir práticas desonestas no mundo virtual.

O anonimato que ocorre na *Internet* é um grande fator para a prática dos crimes cibernéticos devido a falta de identificação dos criminosos, muitos dos crimes nao podem ser solucionados, tornando a lei fraca e ineficaz nestas situações. A livre liberdade de expressão que está contido na Constituição Federal fala sobre a livre expressão de pensamento, tendo o anonimato vedado.

Considera-se que, de forma positiva, o Código Penal tem servido como base para punir grande parte dos crimes virtuais ocorridos e cometidos no Brasil. Porém, apesar desta positividade, a legislação brasileira ainda carece de legislações

específicas, gerando lacunas ao falar sobre a criminalização de certas condutas ainda carentes de tipificação. Espera-se que o avanço nas questões legislativas ocorridas nos últimos anos continuem e contribuam para a punição daqueles que cometem crimes cibernéticos, não deixando lacunas para impunidades.

Finalizando, é de grande importância que haja um avanço tanto normativamente quanto a existência de uma polícia especializada investigativa para o combate a esses crimes. Atualmente, não se tem segurança plena contra as práticas criminosas realizadas pela Internet, precisando de mudanças em caráter de urgência.

Para estudos futuros, cabe analisar os crimes cibernéticos envolvendo jovens adolescentes, entender o que desperta nos jovens o interesse em realizar crimes, quais motivos os fazem se tornar especialistas em ataques cibernéticos, indo para o caminho do crime. Ainda, analisar a fundo como estão os projetos de lei que envolvem a proteção aos cidadãos diante dos ataques diários e de situações mais sérias, envolvendo nao somente dinheiro mas a imagem e a moral das pessoas.

REFERÊNCIAS BIBLIOGRÁFICAS

ALECRIM, Emerson. **Vírus de computador e outros malwares: o que são e como agem. Infowester.** 2011. Disponível em: . Acesso em: 20 de março de 2023.

ARAGÃO, A. (2014). **Dilma sanciona Marco Civil na abertura do NETMundial**. Folha de S. Paulo. Recuperado em http://www1.folha.uol.com.br/tec/2014/04/1444200-dilma-sanciona-marco-civil-na-abertura-do-netmundial.shtml

AZEVEDO, Letícia; CARDOSO, Thais. **Crimes Cibernéticos**. Artigo científico. Anima Educação. 2021.

BAUMAN, Zygmunt. **A sociedade líquida: entrevistado por Maria Lúcia Garcia Palhares-Burke**. São Paulo: Folha de São Paulo, 2003.

BRASIL (1995a). **Portaria Interministerial n° 147,** de 31 de maio de 1995. Brasília, 1995. Recuperado em <http://www.cgi.br/portarias/numero/147>

_____ (1995b). **Portaria Interministerial n° 148,** de 31 de maio de 1995. Aprova a Norma n° 004/95 - Uso da Rede Pública de Telecomunicações para acesso à Internet. Brasília, 1995. Recuperado em <http://legislacao.anatel.gov.br/normas-do-mc/78-portaria-148>

_____. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm;

_____, **Lei nº. 8.069/1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 30 março. 23.

_____, **Lei 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 05 de maio de 2022.

_____, **Lei 12.965 de 23 de Abril de 2014.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 05 de maio de 2022.

_____, **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 10 de maio de 2022.

_____, **Lei 14.155 27 de Maio de 2021**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em 10 de maio de 2021.

CARVALHO, J.M.; ARITA, C.H.; NUNES, A.F. **A política de implantação da Internet no Brasil**. Intercom, São Paulo, 1999.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais.** Rio de Janeiro: Brasport, 2014. Disponível em: . Acesso em: 07 maio. 2023.

Central Nacional de Denúncias de Crimes Cibernéticos. Disponível em: https://indicadores.safernet.org.br/. Acessado em 12 de março de 2023.

Centro de Estudos sobre as Tecnologias de Informação e Comunicação. (2014). **TIC domicílios e empresas 2013:** pesquisa sobre o uso das tecnologias da informação e comunicação no Brasil. São Paulo: Comitê Gestor da Internet no Brasil.

COLARES, R.G. **Cibercrimes: os crimes na era da informática**. Conjur. Disponível em: https://www.conjur.com.br/2002-jul-26/crimes_informatica, acessado em 11 de abril de 2023.

Comitê Gestor da Internet no Brasil (2009). Resolução CGI.br/RES/003. **Princípios para a Governança e uso da Internet no Brasil** (CGI.br/ RES/2009/003/P). Recuperado em <http://www.cgi.br/resolucoes/documento/2009/003> Acessado em 12 de março de 2023.

Comitê Gestor da Internet no Brasil (2014). **Resolução CGI.br/RES/2014/009. Grupo de Trabalho sobre Governança da Internet.** Recuperado em <http://www.cgi.br/resolucoes/documento/2014/009>Acessado em 12 de março de 2023.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** 2 ed. rev. São Paulo: Saraiva, 2002.

D'URSO, Luiz Augusto Filizzola. **Cibercrime: perigo na internet**. Publicado em 2017. Disponível em http://politica.estadao.com.br/blogs/fausto-macedo/cibercrime-perigo-na-internet/. Acesso em 28 de Agosto de 2017.

E-LIFE Social Mix **A mídia tradicional e as oportunidades de negócios do social TV** http://www.elife.com.br/ Acessado em 11/02/2023

FORTIGUARD **Labs apresenta relatório sobre ciberataques no Brasil.** Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021. .Acesso em 15 de março de 2023.

BANDEIRA, K. **O Brasil é o quinto país com mais usuários de internet do mundo. Folha de Pernambuco.** Outubro de 2022. Disponível em: https://www.folhape.com.br/colunistas/tecnologia-e-games/brasil-e-o-quinto-pais-com-mais-usuarios-de-internet-no-mundo/33765/, acessado em 12 de abril de 2023.

FERNANDES, P. Time da Elife lista dicas para criar uma operação de CRM em Home Office. E.life. 2020. Disponível em: https://elife.com.br/index.php/category/newsletter/page/2/

GLOBO. **Crimes virtuais crescem no Brasil; veja flagrante e histórias de vítimas com o Profissão Repórter.** Disponível em: https://g1.globo.com/profissao-reporter/noticia/2022/07/27/crimes-virtuais-crescem-no-brasil-veja-flagrante-e-historias-de-vitimas-com-o-profissao-reporter.ghtml, acessado em 11 de abril de 2023.

GLOBO, **Crimes Virtuais**. Disponível em: https://g1.globo.com/profissao-reporter/noticia/2022/07/25/crimes-virtuais-no-auge-da-pandemia-fraudes-cometidas-no-mundo-digital-aumentaram-175percent.ghtml, acessado em 15 de março de 2023.

IBGE - Instituto Brasileiro de Geografia e Estatística (2005). **Acesso à Internet e uso pessoal de telefone móvel celular para uso pessoal.** Recuperado em <http://www.ibge.gov.br/home/estatistica/populacao/acessoaInternet/> acessado em 10 de abril de 2023.

INFORCHANNEL. **Ataques cibernéticos crescem no Brasil.** https://inforchannel.com.br/2021/03/03/ataques-ciberneticos-no-brasil-crescem-860-na-pandemia/, Acessado em 07 de abril de 2023.

JESUS, Damásio de; MILAGRE, José Antônio**. Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

KASPERSKY. **Home-office motiva aumento de mais de 330 em ataques usando o sistema de acesso remoto**. Disponível em: https://www.kaspersky.com.br/about/press-releases/2020_home-office-motiva-aumento-de-mais-de-330-em-ataques-usando-sistemas-de-acesso-remoto-no-brasil, Acessado em 05 de abril de 2023

KOLLING, Gabriella S. **Segurança da informação**. [2010]a. Disponível em: . Acesso em: 20 de março de 2023.

LEITE, Oliveira Henrique, **Crimes Cibernéticos – No mundo durante a pandemiacovid-19 e seus impactos,.** Disponível em> https://conteudojuridico.com.br/consulta/Artigos/58541/crimes-cibernticos-no-mundo-durante-a-pandemia-covid-19-seusimpactos#:~:text=Os%20Crimes%20Cibern%C3%A9ticos%20trazem%20consigo,a%20pr%C3%A1tica%20de%20viol%C3%AAncias%20cibern%C3%A9ticas. Acessado em 28 de março de 2023.

Marco Civil. (2014). **Marco civil da Internet: seus direitos e deveres em discussão.** Recuperado em http://culturadigital.br/marcocivil/. Acessado em 25 de março de 2023.

MENEZES, E. T. de e SANTOS, T. H. dos. (2014). **SocInfo (Programa Sociedade da Informação). Dicionário Interativo da Educação Brasileira.** Recuperado em http://www.educabrasil.com.br/eb/dic/dicionario.asp?id=470 [Acesso em: 9 jun. 2014]

OLIVEIRA, C. E. E. de (2014). **Aspectos Principais da Lei n° 12.965, de 2014, o**

Marco Civil da Internet: subsídios à comunidade jurídica. Núcleo de Estudos e Pesquisas/CONLEG/ Senado, 2014 (Texto para Discussão n° 148). Recuperado em http://www12.senado.gov.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-148-aspectos-principais-da-lei-no-12.965-de-2014-o-marco-civil-da-internet-subsidios-a-comunidade-juridica.

OLIVEIRA, Ana Sofia Schmidt de. **A vítima e o direito penal.** Uma abordagem do movimento vitimológico e de seu impacto no direito penal. São Paulo: Revista dos Tribunais, 2013.

PINHEIRO, Patrícia Peeck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD),** São Paulo: Saraiva Educação, 2018.

SANTOS, L.R; MARTINS, L.B; TYBUSCH, F.B.A. **Os Crimes Cibernéticos E O Direito A Segurança Jurídica:** Uma Análise Da Legislação Vigente No Cenário Brasileiro Contemporâneo. 4º Congresso Internacional de Direito e Contemporaneidade, 8 a 10 de novembro de 2017, Santa Maria/RS.

SOUZA, Celina. **Políticas Públicas:** Tipologias e Sub-Áreas. 2002. Disponível em: http://professor.pucgoias.edu.br/SiteDocente/admin/arquivosUpload/3843/material/001-%20A-%20POLITICAS%20PUBLICAS.pdf. Acesso em: 12 de março de 2023.

TOLEDO, Marcelo. **Hackers invadem sistema do Hospital do Câncer de Barretos e pedem regaste.** Publicado em 2017. Disponível em https://www.em.com.br/app/noticia/internacional/2017/05/12/interna_internacion Acesso em: 02 de março de 2023.

http://repositorio.aee.edu.br/bitstream/aee/18725/1/2021%20-%20TCC%20-%20Matheus%20Rabelo%20Barros.pdf;

WENDT, Emerson e JORGE, Higor Vinicius Nogueira: **Crimes Cibernéticos – Ameaças e Procedimentos de Investigação** – 2º Ed. Rio de Janeiro: Brasport, 2017.