PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

PRÓ-REITORIA DE GRADUAÇÃO

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

COORDENAÇÃO DO CURSO DE DIREITO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

PROJETO DE TRABALHO DE CURSO

CRIMES CIBERNÉTICOS:
DIFICULDADES PARA COMBATER E CONTER GOLPES NA INTERNET

ORIENTANDO: PAULO VICTOR VIEIRA MARQUES

ORIENTADORA: Mª. PAULA RAMOS NORA DE SANTIS

GOIÂNIA-GO
2023

PAULO VICTOR VIEIRA MARQUES

CRIMES CIBERNÉTICOS:

DIFICULDADES PARA COMBATER E CONTER GOLPES NA INTERNET

Artigo Científico apresentado à disciplina de Trabalho de Curso I, da Escola de Direito, Comunicação e Negócios, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).
Profª. Orientadora: Mª. Paula Ramos Nora de Santis.

GOIÂNIA-GO
2023

PAULO VICTOR VIEIRA MARQUES

CRIMES CIBERNÉTICOS:
DIFICULDADES PARA COMBATER E CONTER GOLPES NA INTERNET

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientadora: Prof.ª. Mª. Paula Ramos Nora de Santis. Nota

_____

Examinador Convidado: Prof. Titulação e Nome Completo Nota

DEDICATÓRIA

Dedico este trabalho a Deus, o maior orientador da minha vida, a minha família, em especial, minha querida mãe, pelo carinho, afeto, dedicação e cuidado. Quero agradecer também a professora Mª. Paula Ramos Nora de Santis por ser uma constante fonte de motivação e incentivo ao longo de todo o projeto.

Com muita satisfação, dedico aos amigos pelo apoio e suporte que me deram durante todo o curso, por fim, dedico também ao meu amor, sem ela por perto os resultados não seriam os mesmos. Grato pela sua compreensão e presença.

SUMÁRIO

CRIMES CIBERNÉTICOS:

DIFICULDADES PARA COMBATER E CONTER GOLPES NA INTERNET

PAULO VICTO VIEIRA MARQUES

RESUMO

O acesso dos criminosos à Internet facilita a prática de crimes cibernéticos. Isso ocorre porque a forma como a mídia digital evoluiu torna os usuários mais vulneráveis. Mais pessoas são vítimas devido à maior conveniência dos serviços baseados na Internet.

Este Trabalho de Conclusão de Curso utiliza diferentes capítulos para explorar vários aspectos dos crimes. Estes incluem declarações históricas sobre os eventos e pensamentos conceituais sobre o assunto. Além disso, abrange os principais tipos de crimes cibernéticos e terrorismo cibernético, este trabalho explica brevemente as leis brasileiras em meio à exploração de crimes virtuais.

A fim de enfatizar a relevância desta pesquisa, estudiosos profissionais e escritores da academia fornecem análises para seus trabalhos relacionados ao tema.

Muitos crimes online são constantemente aperfeiçoados, este trabalho analisa as principais características dos crimes mais comuns na internet. Também será analisado quais leis punem esses crimes.

Os usuários da Internet não podem viver sem confiar na Internet, então é por isso que muitas pessoas cometem crimes por meio dela. Embora não haja leis reais relativas a crimes cibernéticos no Brasil, a lei atualmente não é adequada para defender pessoas que cometem crimes online.

O principal problema enfrentado pelos usuários e profissionais do direito é a falta de normas uniformes para crimes na Internet. Isso resulta em interpretações ambíguas que não seguem o código penal.

Palavras-Chave: Crimes na internet, tipificações, documentos eletrônicos

INTRODUÇÃO

A mudança tecnológica continua a se expandir rapidamente. Como a internet vem se expandindo em um ritmo alarmante, pode ser considerada uma consequência disso. Considerar mudanças importantes na vida ajuda você a entender a maneira como você vive. Novos meios de comunicação estão criando mensagens profundas, significativas e únicas. onde todos acessam facilmente as informações com rapidez e frequência.

A informação digital torna possível conectar-se com muitas pessoas através de vários métodos. Gente do mundo todo não é só do Brasil. Nessa linha de pensamento, Telles (2015 apud Martins, 2010) afirma que:

> No presente século, tecnologia é tudo. Em uma casa ou em uma empresa, um computador ou qualquer outro dispositivo informático, eletrônico ou digital, podem ser utilizados para facilitar a consecução de uma variedade de tarefas do dia a dia, tais como administrar contas, estoques, informações de clientes, redigir documentos, fazer cálculos e muito mais; sendo que, para este autor, a essência de qualquer dispositivo tecnológico é o seu software.

No entanto, apesar de todos os seus benefícios, a Internet também traz as consequências, novas formas de cometer crimes, são amplamente conhecidas Como o cibercrime, que proliferou de forma avassaladora neste ambiente, torne o usuário-alvo vulnerável.

Além de amplo conhecimento em informática A maioria dos criminosos tem, e eles também se beneficiam da distância existente Entre eles e suas vítimas, infelizmente, as vítimas são alvos fáceis para seus crimes. e com base nesses acontecimentos, várias leis foram promulgadas para lidar com crimes virtuais, e ficam aqui neste trabalho, será abordada a validade dos dispositivos legais existentes

Primeiro, os princípios da Internet serão introduzidos Brasil, período estendido de uso restrito para uso comercial, evolução histórica, práticas iniciais e equipamentos informáticos, tipos de crime e por fim uma análise de algumas referências Leis existentes e se estão em vigor.

É muito importante ressaltar que este trabalho não esgotou todo material relacionados com o cibercrime e as leis específicas que os protegem, em vez de apontar, pois, a necessidade real da lei em questão e seu efeito no mundo jurídico.

1.1 CONCEITO DE CRIMES CIBERNÉTICOS

O cibercrime pode ser conceituado como crimes cometidos por qualquer pessoa, desde que cometidos com o auxílio de tecnologia da informação contra a segurança, imagem ou privacidade de terceiros.

Para caracterizar adequadamente os crimes virtuais, os crimes devem ocorrer em um ambiente de computador. A respeito dessa característica, Augusto Rossini a descreveu da seguinte forma:

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

Destaca-se que o referido "ambiente informático" se refere a todo e qualquer fato que, direta ou indiretamente, se utilize de meios tecnológicos, abrangendo também aquelas práticas que não tenham acesso à Internet, mostrando ser esta uma das principais características que tornam visível a materialização do crime, para além do auxílio das tecnologias de informação, o doutrinador Ramalho Terceira, na sua obra "Problemas na Classificação Criminal do Crime Virtual", conceitua o cibercrime Como:

> Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo; por isso, ficaram usualmente definidos como sendo crimes virtuais. Ou seja, os delitos praticados por meio da Internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas (Ramalho, 2012).

Ao longo de outras aspectos desse tipo de delito, salienta também a abstinência física do agressor, aspectos derivados do sentido literal do delito, uma vez que a palavra "virtual" implica uma simulação criada por meio eletrônico. O crime virtual recebe esse nome, sobretudo porque os criminosos não precisam

impreterivelmente estar na cena do crime. Esse fato torna os crimes mais difíceis de detectar, obrigando a polícia a fazer ajustes conforme necessário.

1.2.1 CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Os crimes podem ser categorizados de acordo com o uso da tecnologia da informação. Esses crimes de acordo com um quadro específico de procedimentos, as estruturas detalham como os crimes são avaliados e organizados em 3 grupos distintos.

Essas estruturas fornecem o nome “crimes cibernéticos”, que pode ser aplicado a qualquer crime que envolva um bem legalmente protegido.

Os computadores são utilizados em crimes informáticos mistos e inapropriados. envolvendo o uso da tecnologia da informação e a falta de segurança virtual, a fim de obter um resultado específico.

1.3 EVOLUÇÃO HISTÓRICA DOS CRIMES CIBERNÉTICOS

A internet tornou-se um componente essencial da vida moderna, mas, também ajudou a alimentar um aumento significativo na globalização para todos os envolvidos. Oferecendo muitos benefícios, mas também fornece anonimato aos seus usuários. Isso os leva a serem capazes de fazer o que quiserem sem se preocupar com as consequências. No entanto, isso também trouxe problemas que tiveram que ser tratados por sistemas instituídos pela lei.

Tem havido muitas discussões sobre a falta de leis relativas à internet. Isso ocorre porque o sistema jurídico não se adaptou à rápida evolução da tecnologia. O Brasil passou a usar a internet de forma mais lenta e metódica; eles foram alterados por várias ações governamentais.

A Internet comercial do Brasil não chegou até 1996, o que causou problemas para os usuários e provedores do país. A razão para isso foi o Código Integral do país, que foi implantado em 1964 (DIAS 2004). Este código estabeleceu o Ministério das Comunicações e criou a EMBRATEL Corporation para implementar a rede nacional do Brasil. No entanto, o uso comercial da Internet não foi imposto até 1994; a essa altura, os usuários tinham que pagar uma taxa para acessar o serviço. A criação do CGI — Comitê Gestor da Internet

— em 1994 envolveu academia, empresas ligadas a conexões, provedores e usuários.

Esse comitê foi formado para regulamentar usuários e provedores da rede e estimular o desenvolvimento de novos serviços a ela conectados (OLIVEIRA 2011; p. 22).

Apesar desse comitê ter sido formado em 1994, o uso comercial da Internet só foi disponibilizado em 1996. Em 2021, foi publicada no Diário Oficial a lei 14.155 daquele ano. Isso foi escrito pelo presidente Jair Bolsonaro e atualmente é uma das muitas leis nesse cenário específico.

2. ANÁLISE SISTEMATICA DOS INDÍCIOS APRESENTADOS NOS CRIMES CIBERNÉTICOS

Uma análise sistemática dos indícios apresentados nos crimes cibernéticos é fundamental para investigar e identificar os responsáveis por esses crimes. Alguns dos indícios mais comuns encontrados nos crimes cibernéticos incluem:

Logs de servidores: Esses registros fornecem informações sobre o acesso, o tráfego de rede e as atividades realizadas em um servidor. Eles podem ser usados para identificar a origem de um ataque ou para rastrear um invasor.

Endereços IP: Os endereços IP são usados para identificar a origem de um ataque ou para rastrear um invasor. Eles podem ser encontrados em registros de servidor, logs de firewall, ou nos dados coletados durante uma investigação.

Malware: Malware é um software malicioso que pode ser usado para roubar informações, espionar usuários, danificar sistemas ou para outros fins maliciosos. A presença de malware em um sistema pode indicar que um ataque foi realizado.

Registros de transações financeiras: Quando um crime cibernético envolve atividades financeiras, como roubo de informações bancárias, registros de transações financeiras podem ser usados para rastrear o fluxo de dinheiro e identificar os responsáveis pelo crime.

Registros de comunicações: Quando os criminosos cibernéticos usam ferramentas de comunicação, como e-mail, mensagens instantâneas ou fóruns on-line para planejar ou executar um ataque, essas comunicações podem ser registradas e analisadas para identificar os envolvidos.

Análise comportamental: A análise comportamental pode ser usada para identificar comportamentos incomuns ou anormais em um sistema ou em uma rede, o que pode indicar a presença de um invasor.

Esses são apenas alguns dos indícios que podem ser usados para analisar e investigar crimes cibernéticos. É importante lembrar que a investigação de crimes cibernéticos pode ser complexa e exigir conhecimentos específicos de tecnologia da informação e segurança cibernética

2.1 METODOS UTILIZADOS

Existem diversos métodos utilizados pelos criminosos cibernéticos para cometer crimes na internet. Aqui estão alguns dos principais métodos:

Malware: o malware é um software malicioso que é projetado para se infiltrar em sistemas de computador sem o consentimento do usuário. Os tipos mais comuns de malware incluem vírus, cavalos de Troia, worms e ransomware. Esses programas podem ser usados para roubar informações, controlar computadores remotamente, danificar arquivos ou criptografar dados.

Ataques de negação de serviço (DDoS): os ataques de negação de serviço (DDoS) são usados para sobrecarregar um site ou servidor com um grande volume de tráfego, impedindo que os usuários legítimos acessem o sistema. Esses ataques são frequentemente usados como uma forma de extorsão ou sabotagem.

Sniffing: o sniffing é uma técnica que permite aos criminosos interceptar e capturar dados que estão sendo transmitidos pela rede. Isso inclui informações como senhas, informações bancárias e outras informações confidenciais.

Exploração de vulnerabilidades: os criminosos cibernéticos podem explorar vulnerabilidades em softwares e sistemas para obter acesso não autorizado a informações confidenciais. Isso pode incluir a instalação de malware, roubo de informações ou o controle remoto de sistemas.

Esses são apenas alguns dos métodos mais comuns usados pelos criminosos cibernéticos. É importante ressaltar que a lista de técnicas é extensa e está em constante evolução, devido à rápida evolução tecnológica e novas formas de ataque sendo desenvolvidas

2.2 ANÁLISE GERAL DOS PERFIS DOS CRIMINOSOS QUE PRATICAM CRIMES VIRTUAIS

É difícil descrever com precisão os cibercriminosos porque eles variam muito em idade, sexo, histórico educacional, motivação e comportamento. No entanto, com base em pesquisas e pesquisas sobre o **tema**, algumas características comuns podem ser identificadas.

Um dos principais fatores que levam as pessoas a se envolverem em atividades delituosas é a motivação financeira. Isso significa que muitos cibercriminosos são motivados pelo dinheiro para ganhar dinheiro por meio de roubo de informações, fraude financeira, extorsão e outras atividades ilegais e criminosas que podem ser realizadas online.

Além disso, a maioria dos criminosos cibernéticos possui habilidades técnicas e experiência em tecnologia da informação e sistemas de computador, o que lhes permite desenvolver e executar ataques cibernéticos sofisticados. No entanto, alguns cibercriminosos usam ferramentas prontamente disponíveis na Internet para realizar ataques mais simples.

Em termos de idade, muitos criminosos virtuais são jovens, geralmente com idades entre 18 e 35 anos. Isso pode ser atribuído em parte à facilidade de acesso à tecnologia e à internet para essa faixa etária. No entanto, também há criminosos virtuais mais velhos e experientes, muitas vezes com histórico de crime convencional.

Em relação à formação educacional, os criminosos virtuais variam amplamente. Muitos deles possuem formação em tecnologia da informação ou em áreas relacionadas à segurança cibernética, enquanto outros têm experiência prática adquirida em fóruns e comunidades de hackers.

Por fim, é importante notar que os perfis dos criminosos virtuais estão em constante evolução e mudança. À medida que a tecnologia e as ameaças

cibernéticas evoluem, os perfis dos criminosos virtuais também mudam, o que torna difícil identificá-los e combatê-los.

3. APLICAÇÃO DAS SANÇÕES

A aplicação das sanções em casos de crimes cibernéticos varia de acordo com a legislação de cada país. No Brasil, por exemplo, os crimes cibernéticos estão previstos na Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, e na Lei nº 13.964/2019, Pacote Anticrime.

De acordo com a Lei nº 12.737/2012, são considerados crimes cibernéticos a invasão de dispositivos informáticos alheios, a obtenção, transferência ou comercialização de dados pessoais sem autorização, a interrupção ou perturbação de serviços de informática, e a distribuição de vírus e outros programas maliciosos.

As sanções para esses crimes podem incluir penas de reclusão e multas, dependendo da gravidade do crime e das circunstâncias específicas do caso. Além disso, a lei prevê a possibilidade de indenização às vítimas dos crimes cibernéticos.

Já a Lei nº 13.964/2019, que alterou o Código Penal Brasileiro, prevê a inclusão de novos tipos penais para os crimes cibernéticos, como a divulgação de informações sigilosas, o ataque a sistemas eletrônicos de controle de tráfego aéreo e o uso de informações obtidas por meio de phishing.

As sanções para esses crimes podem incluir pena de reclusão, multa e outras medidas restritivas de direitos, dependendo da gravidade do crime e das circunstâncias específicas do caso.

Em geral, a aplicação das sanções em casos de crimes cibernéticos envolve a colaboração entre autoridades policiais, judiciais e técnicas, bem como a utilização de ferramentas e tecnologias especializadas para investigação e rastreamento dos crimes na internet

3.1 MOTIVADORES DA CONDUTA CRIMINOSA

Os motivadores da conduta criminosa em crimes online são diversos e podem variar de acordo com o tipo de crime cometido e o perfil do criminoso. Algumas das principais motivações incluem:

Ganho financeiro: uma das principais motivações para os crimes online é o ganho financeiro. Os criminosos podem roubar informações pessoais, como dados bancários e de cartões de crédito, ou extorquir vítimas em troca de desbloqueio de arquivos ou de acesso a informações.

Diversão ou desafio: alguns criminosos cometem crimes online simplesmente pela diversão ou pelo desafio. Eles podem se sentir atraídos pelo anonimato da internet e pelas possibilidades de causar danos sem serem identificados.

Vingança: alguns crimes online são cometidos por motivos de vingança, como a divulgação de informações pessoais ou imagens íntimas sem autorização da vítima.

Ideologia ou ativismo: alguns grupos de criminosos online têm motivações ideológicas ou políticas. Eles podem realizar ataques para demonstrar sua insatisfação com determinadas empresas ou governos, por exemplo.

Acesso a informações: alguns criminosos podem realizar ataques online com o objetivo de acessar informações confidenciais de empresas ou governos, para posteriormente utilizá-las em benefício próprio ou para divulgar publicamente.

Psicopatia: em alguns casos, criminosos online podem apresentar traços de psicopatia, como a falta de empatia e a impulsividade, que os levam a cometer crimes sem preocupação com as consequências.

Esses são apenas alguns exemplos de motivações para a conduta criminosa em crimes online. É importante ressaltar que muitas vezes esses motivadores se entrelaçam e se combinam de maneiras complexas, o que torna a investigação e a prevenção desses crimes ainda mais desafiadoras

3.2 A COMPREENSÃO DA EXECUÇÃO DO FATO DELITUOSO.

Compreender como os crimes são executados no cibercrime é um aspecto importante da detecção e prevenção desses crimes. O cibercrime pode ser realizado de diferentes formas, dependendo do tipo de crime e das técnicas

utilizadas pelos criminosos. Uma das formas mais comuns de cometer crimes cibernéticos é através da invasão de um sistema ou rede de computadores.

Os criminosos podem usar técnicas para obter acesso não autorizado a sistemas e redes para roubar informações pessoais ou comerciais, instalar malware ou conduzir ataques de negação de serviço.

Neste mesmo sentindo, na obra "Crimes Cibernéticos: Análise da Legislação Brasileira e dos Desafios à Investigação e à Punibilidade", existe um trecho que relata:

> "A execução do fato delituoso nos crimes cibernéticos pode apresentar desafios distintos em relação aos crimes convencionais, uma vez que muitas vezes envolvem ações realizadas por meio de sistemas computacionais e redes de comunicação. No entanto, para que haja a caracterização do delito, é necessário que a conduta seja executada de acordo com o previsto na legislação brasileira. Dessa forma, a compreensão da execução do fato delituoso nos crimes cibernéticos deve levar em consideração não apenas as especificidades técnicas envolvidas, mas também as normas e jurisprudências relacionadas ao tema, garantindo a aplicação da lei de forma justa e eficaz."

Outra maneira pela qual o cibercrime é realizado é por meio da engenharia social, que envolve manipular ou enganar as vítimas para que forneçam informações confidenciais ou tomem ações que beneficiem o criminoso.

O cibercrime também pode ser cometido por meio de fraude online, como a venda de produtos ou serviços falsificados ou inexistentes.

Além disso, o cibercrime também pode ser realizado por meio da disseminação de conteúdos ilegais na Internet, como pornografia infantil, discurso de ódio, incitação à violência e terrorismo.

Em geral, a execução de um ato criminoso dentro do cibercrime envolve o uso de tecnologias e técnicas avançadas, o que torna esses crimes mais complexos e mais difíceis de investigar e prevenir. É, por isso, importante que as autoridades e as empresas invistam em medidas de cibersegurança e em equipas especializadas na investigação destes crimes.

3.3 MELHOR MANEIRA DE PUNI-LOS PELA PRÁTICA DE CONDUTAS CRIMINOSAS

A melhor forma de punir os criminosos que cometem crimes relacionados com o cibercrime depende do tipo de crime cometido e das leis e regulamentos do país onde o crime ocorre. Algumas opções comuns de penalidade incluem:

Prisão: Em muitos casos, a punição mais comum para crimes cibernéticos é a prisão. Dependendo da gravidade do crime, o criminoso pode ser condenado a uma pena de prisão de curto ou longo prazo.

Multa: As multas são outra forma comum de punição para crimes cibernéticos. As multas podem ser aplicadas em casos de violação de leis de privacidade, quebra de direitos autorais, fraudes online, entre outros.

Restituição: Em alguns casos, a vítima do crime pode ter direito a uma restituição pelos danos causados pelo crime cibernético. O criminoso pode ser obrigado a pagar uma quantia para cobrir os custos do dano causado.

Proibição de acesso à internet: Em alguns casos, os criminosos podem ser proibidos de usar a internet ou outros dispositivos eletrônicos como parte de sua sentença.

Serviço comunitário: Em alguns casos, os criminosos podem ser condenados a realizar serviço comunitário como parte de sua sentença.

Reabilitação: Alguns criminosos cibernéticos podem ser encaminhados para programas de reabilitação ou tratamento para ajudá-los a superar seus comportamentos criminosos e evitar futuras violações da lei.

É importante ressaltar que a punição não deve ser vista como a única solução para combater os crimes cibernéticos. É necessário investir em medidas preventivas, como a educação digital e a segurança cibernética, além de melhorar as leis e regulamentações para combater de forma mais eficaz os crimes cibernéticos.

A respeito, no livro, *"Aspectos Penais da Lei Carolina Dieckmann"*, de Guilherme Magalhães Martins e André Guilherme Tavares de Freitas (2015), diz que:

> "A melhor maneira de punir a prática de condutas criminosas em ciber crimes de acordo com a legislação brasileira é garantir a

> aplicação das leis existentes, adaptando-as aos novos desafios trazidos pelo ambiente virtual. A Lei Carolina Dieckmann, por exemplo, trouxe importantes alterações ao Código Penal brasileiro para criminalizar condutas como invasão de dispositivos informáticos e divulgação de conteúdos privados sem autorização. Além disso, é preciso fortalecer as instituições responsáveis pela investigação e punição desses crimes, de modo a garantir que os responsáveis sejam identificados e levados à justiça."

No Brasil, os crimes cibernéticos são regulamentados pela Lei nº 12.735/2012, conhecida como "Lei Carolina Dieckmann", que alterou o Código Penal Brasileiro para incluir novos tipos penais relacionados à internet e às tecnologias da informação e comunicação.

As formas de punição para os crimes cibernéticos no Brasil podem incluir:

Prisão: A pena de prisão pode variar de acordo com a gravidade do crime, podendo chegar até a 10 anos de reclusão em casos de invasão de dispositivo informático.

Multa: A multa pode ser aplicada em casos de crimes cibernéticos que envolvem violação de direitos autorais, por exemplo, e pode chegar a valores elevados.

Perda de bens e valores: Em alguns casos, o criminoso pode ser obrigado a devolver o valor obtido com o crime ou a perder bens adquiridos ilegalmente.

Suspensão ou interdição de atividades: O criminoso pode ser impedido de exercer determinada atividade relacionada ao crime cibernético praticado.

Proibição de acesso à internet: Em alguns casos, o juiz pode proibir o criminoso de acessar a internet ou outros dispositivos eletrônicos.

Trabalhos comunitários: Em alguns casos, o criminoso pode ser condenado a prestar serviços à comunidade.

Reclusão em regime semiaberto ou aberto: Em casos de menor gravidade, o juiz pode determinar o cumprimento da pena em regime semiaberto ou aberto.

Vale ressaltar que a escolha da pena vai depender do tipo de crime cibernético cometido e das circunstâncias em que ocorreu. Além disso, o Juiz pode levar em consideração a reincidência do criminoso, sua conduta social, personalidade, entre outros fatores, para determinar a punição adequada.

4. CONCLUSÃO

A ascensão da tecnologia e da conectividade abriu caminho para um aumento alarmante do crime cibernético. Do ganho financeiro à vingança ou espionagem, os cibercriminosos empregam uma variedade de táticas para perpetrar seus crimes, conforme revelado pelos perfis dos criminosos. Além disso, as motivações por trás desses ataques cibernéticos são diversas e vão da ganância ao terrorismo.

É crucial enfatizar que existem regulamentos e penalidades estritos para dissuadir e penalizar a prática de crimes cibernéticos. A Lei Carolina Dieckmann e o Marco Civil da Internet do Brasil exemplificam medidas legais implementadas para proteger os cidadãos de crimes online. Além disso, as autoridades alocaram recursos significativos para a implementação de tecnologias e táticas para conter e combater o cibercrime.

Aumentar a conscientização sobre a importância da segurança digital e promover boas práticas online é crucial. Isso inclui o uso de senhas fortes e atualizadas, instalação de software de segurança confiável, verificação de informações antes de clicar em links e denúncia de atividades suspeitas. Os esforços combinados do governo, empresas e sociedade civil são essenciais para diminuir a prevalência do cibercrime e estabelecer um ambiente digital seguro para todos.

REFERÊNCIAS

ADAMI, Andreia C.; TONINI, Rafael; CARVALHO, Aury Lopes de. Crime Eletrônico. São Paulo: Saraiva Educação, 2021.

BRASIL. CF/1988. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

CALVACANTI, E. C. (2021). Inteligência cibernética e investigação criminal. Editora Fórum.

CASTRO, Bruno Bioni. Proteção de Dados Pessoais: A Função e os Limites do Consentimento. Disponível em: https://www.conjur.com.br/2018-dez-20/opiniao-protecao-dados-pessoais-funcao-limites-consentimento. Acesso em: 01 mar. 2023.

DECKER, C. R., & Decker, K. T. (2020). Cibercrime no Brasil: análise de casos e tendências. Revista Brasileira de Polícia Federal, 3(1), 1-18.

FERREIRA, Guto. Segurança cibernética: ameaças e desafios. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/14143/1/Tcc%20definitiv o%20enviado%20RUNA.pdf. Acesso em 15 de março de 2022.

FERNANDES T. (2017). Cibercrime e segurança informática. Escola da Magistratura do Estado do Rio de Janeiro.

GOMES, Luiz Flávio; BIANCHINI, Alice; ALMEIDA, Daniel D'Ávila. Crimes Eletrônicos. São Paulo: Editora Revista dos Tribunais, 2019.

HOFFMANN, Diogo Rais. Direito Digital. São Paulo: Editora Juspodivm, 2020.

JARDIM, L. A. F., & Costa, E. G. (2021). Cibercrime e cyberlaw: a interface entre o direito e a tecnologia. Editora Atlas.

KOLLMANN, Cristiane. A Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados. Disponível em: https://www.conjur.com.br/2020-nov-30/opiniao-protecao-dados-pessoais-lei-geral-protecao-dados. Acesso em: 15 mar. 2023.

Lei 14.155, de 2021, Diário Oficial da União. Disponível em https://www.in.gov.br/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em 28 de novembro de 2021.

LOPES, E. A., & Figueiredo, A. D. (2016). A face oculta dos crimes cibernéticos. Revista Internacional de Ciências Humanas, 9(1), 34-47.

LIMA, Renato Opice Blum. A Responsabilidade Civil dos Provedores de Internet. Disponível em: https://www.conjur.com.br/2016-ago-31/opiniao-responsabilidade-civil-provedores-internet. Acesso em: 15 fev. 2023.

MACHADO, D. M. (2020). Crimes cibernéticos: legislação, jurisprudência e doutrina. Editora Juspodivm.

MONTALVAO, T. C. (2020). Cibercrime e proteção de dados pessoais: desafios e perspectivas. Editora Revista dos Tribunais.

MONTEIRO, Douglas de Castro. Crimes Cibernéticos: Comentários à Lei 12.737/2012. São Paulo: Saraiva Educação, 2021.

PINHEIRO, L. B. (2018). Cybercrime: conceito e classificação. Revista Eletrônica de Direito Penal e Política Criminal, 2(2),

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

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. Jus Navigandi, Teresina, a. 6, n. 58, ago. 2002.

RIBEIRO, Fabio Augusto. A Investigação Criminal de Crimes Cibernéticos. Disponível em: https://www.conjur.com.br/2018-ago-28/opiniao-investigacao-criminal-crimes-ciberneticos. Acesso em: 01 jan. 2023.

RODRIGUES, Geórgia Z. B.; SOUZA, Felipe P. de. Crimes Digitais: Desafios para a Aplicação da Lei. Disponível em: https://www.conjur.com.br/2022-fev-14/opiniao-crimes-digitais-desafios-aplicacao-lei. Acesso em: 22 mar. 2023.

SILVA, P. H., & Lobo, P. (2017). Crime cibernético: análise de casos concretos. Revista Internacional de Direito e Cidadania, 2(2),

SOUZA, M. C. F. (2017). Análise dos tipos penais previstos na lei 12.737/12 frente à evolução do cibercrime. Revista da Escola Superior de Advocacia, 12(23),

STÁBILE, L. P., & Fragoso, G. (2016). Crime organizado e crime cibernético: novas ameaças e desafios. Revista Brasileira de Ciências Criminais, 127(1),

SANTOS, Anderson de Jesus. Crimes Cibernéticos: Uma Análise Jurídica. 2ª ed. São Paulo: Saraiva Educação, 2020.

TELLES (2015 apud Martins, 2010). TCC, CRIMES CIBERNÉTICOS: Análise das leis 12.735 e 12.737 no que tange a sua real necessidade de existência.

Disponível em https://www.facem.edu.br/aluno/arquivos/monografias/luis_carlos.pdf. Acesso em 07 de março de 2022