PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

CRIMES CIBERNÉTICOS:
DIFICULDADE PARA OBTER INDÍCIOS DE AUTORIA E MATERIALIDADE

ORIENTANDO: BRUNO PEREIRA BARROS

ORIENTADOR: Prof. GIL CÉSAR COSTA DE PAULA

GOIÂNIA
2023

BRUNO PEREIRA BARROS

CRIMES CIBERNÉTICOS:
DIFICULDADE PARA OBTER INDÍCIOS DE AUTORIA E MATERIALIDADE

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof. Orientador: Gil César Costa De Paula.

GOIÂNIA
2023

BRUNO PEREIRA BARROS

CRIMES CIBERNÉTICOS:
DIFICULDADE PARA OBTER INDÍCIOS DE AUTORIA E MATERIALIDADE

Data da Defesa: 29 de novembro de 2023.

BANCA EXAMINADORA

_____
Orientadora: Prof. GIL CÉSAR COSTA DE PAULA Nota

_____
Examinador Convidado: Prof. Gaspar Alexandre M. de Sousa Nota

SUMÁRIO

CRIMES CIBERNÉTICOS:

DIFICULDADE PARA OBTER INDÍCIOS DE AUTORIA E MATERIALIDADE

BRUNO PEREIRA BARROS[1]

Resumo

Os crimes cibernéticos referem-se a atividades criminosas que envolvem o uso de computadores, redes e sistemas de informação. Esses tipos de crimes podem variar em gravidade e escopo, e geralmente são realizados por indivíduos ou grupos que exploram vulnerabilidades tecnológicas para obter ganhos financeiros, roubar informações pessoais, prejudicar sistemas ou causar perturbações. Entender a autoria e a materialidade de crimes cibernéticos pode ser desafiador devido à natureza digital e muitas vezes anônima dessas atividades. No entanto, as autoridades e especialistas em segurança cibernética utilizam diversas técnicas e abordagens para coletar indícios e identificar os responsáveis por esses crimes. Algumas das estratégias comuns incluem: registro de logs e metadados; análise de malware; rastreamento de transações financeiras etc. Para combater crimes cibernéticos, governos, empresas e indivíduos adotam medidas de segurança cibernética, como a utilização de firewalls, antivírus, autenticação de dois fatores, educação sobre segurança online e leis específicas para punir os infratores. É importante ressaltar que a investigação de crimes cibernéticos exige expertise técnica e legal.

Palavras-chave: Crimes cibernéticos. Crimes digitais. Cibe criminalidade.

---

[1]Qualificação do autor.

INTRODUÇÃO

A crescente integração da tecnologia digital em nossas vidas tem trago inúmeros benefícios, mas também tem dado origem a novos desafios, um deles é o cibercrime.

O cibercrime refere-se a atividades criminosas que ocorrem no espaço virtual, envolvendo o uso de tecnologia da informação e comunicação para cometer uma ampla gama de infrações. Essas atividades vão desde ataques cibernéticos a sistemas de computador até fraudes online, roubo de dados pessoais e empresariais, disseminação de malware, phishing, entre outros.

O cibercrime é alimentado pela acessibilidade e conectividade que a internet proporciona, permitindo que criminosos operem de maneira global e maioria das vezes anônima. Eles podem atacar indivíduos, empresas, instituições governamentais e até infraestruturas críticas, causando danos financeiros e comprometendo a privacidade e segurança das pessoas.

Para combater o cibercrime, governos, empresas e indivíduos têm adotado medidas de segurança cibernética, leis mais rigorosas e cooperação internacional, a conscientização sobre práticas seguras na internet, a utilização de software de segurança atualizado e a educação sobre os riscos do cibercrime são passos importantes para se proteger contra essas ameaças em constante evolução.

A conscientização é fundamental. Quanto mais as pessoas compreenderem os riscos associados ao uso da tecnologia e os métodos empregados pelos criminosos cibernéticos, mais capazes estarão de proteger suas informações pessoais e financeiras. A batalha contra o cibercrime é uma jornada contínua, pois as ameaças continuarão a evoluir com o progresso tecnológico.

1. DO CRIME VIRTUAL - CIBERCRIME

Crime virtual é um termo utilizado para descrever atividades criminosas que ocorrem no ambiente virtual, também conhecido como ciberespaço. Esses crimes envolvem o uso de computadores, redes de computadores e a internet para cometer atividades ilegais.

Os crimes virtuais podem incluir atividades como hacking, phishing, roubo de identidade, fraudes online, disseminação de malware, ataques cibernéticos a sistemas e redes, pornografia infantil, cyberbullying, entre outros. Essas atividades visam obter informações pessoais e financeiras, causar danos a sistemas e infraestruturas, extorquir dinheiro, espalhar desinformação, entre outros objetivos. (NOVELINO, 2016).

A obtenção de indícios de autoria e materialidade no cibercrime pode ser desafiadora devido à natureza complexa e evasiva das atividades criminosas online. No entanto, as autoridades e especialistas em segurança cibernética têm desenvolvido técnicas e estratégias para lidar com esses desafios.

Os criminosos cibernéticos muitas vezes usam técnicas para ocultar sua identidade real, como o uso de redes virtuais privadas (VPNs), proxies e serviços de anonimato. Para lidar com isso, as investigações podem envolver a rastreamento de endereços IP, análise de logs de servidores, cooperação internacional e monitoramento de fóruns e comunidades online onde os criminosos podem se comunicar. (CORREIA, 2020)

Sua atividade podendo ser escondida utilizando malware que se modifica constantemente ou criptografia. Para superar isso, os investigadores precisam de especialização em análise de malware e forense digital para identificar e decifrar essas ameaças.

Jurisdição Transnacional o crime muitas vezes atravessa fronteiras, o que torna difícil a aplicação das leis em diferentes jurisdições. A cooperação internacional e

acordos de compartilhamento de informações entre agências de aplicação da lei de diferentes países são fundamentais para resolver esse problema. (TEIXEIRA.2014).

As evidências digitais podem ser facilmente manipuladas ou apagadas. Portanto, é crucial coletar e preservar evidências de forma adequada desde o início da investigação. Isso inclui a utilização de técnicas de coleta de dados forenses e o armazenamento seguro das evidências.

As equipes de investigação e aplicação da lei precisam de treinamento especializado e recursos adequados para lidar com casos de cibercrime. Manter-se atualizado com as técnicas de ataque em constante evolução é essencial. (CRESPO/2016).

Roubo de identidade, os criminosos obtêm informações pessoais, como números de cartão de crédito, senhas e dados bancários, de forma ilícita. Eles podem usar essas informações para fazer compras online, acessar contas bancárias ou cometer fraudes em nome de outras pessoas.

> Cibercrime é compreendido como a prática de uma conduta ilícita manifestada por meio eletrônico, em que se é utilizado o recurso de Internet como meio para prática delituosa, assim como no envolvimento de arquivos e/ou sistemas digitais. Podem ser cometidos somente em ambiente tecnológico, ocorridos, por exemplo, na manipulação de caixas eletrônicos, ou até mesmo nos crimes convencionais executados na forma digital ou que incluam alguma ação tecnológica para praticar o crime, tendo os crimes contra a honra como exemplificação. (CORREIA, 2020)

Os criminosos utilizam a internet para atrair vítimas e enganá-las, muitas vezes resultando em perdas financeiras significativas. Os ataques cibernéticos envolvem a invasão de sistemas de computadores ou redes para roubar informações.

No Brasil, a legislação também trata dos crimes virtuais, como é o caso da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que criminaliza práticas como invasão de dispositivos, obtenção, adulteração ou destruição de dados, além da divulgação não autorizada de informações pessoais.

O crime virtual apresenta desafios para a aplicação da lei, uma vez que os criminosos podem operar de forma anônima e global, dificultando a identificação e responsabilização. É importante tomar medidas de precaução, como utilizar senhas fortes, evitar fornecer informações pessoais sensíveis em sites não confiáveis e manter o software de segurança atualizado, para ajudar a proteger-se contra crimes virtuais.

Com a pandemia, o aumento alarmante dos crimes cometidos no ambiente digital é evidente. No Brasil, as denúncias de delitos ocorridos online mais do que duplicaram de 2019 para 2020. A gama de crimes também é surpreendentemente ampla, abrangendo desde ameaças simples até delitos como racismo, pornografia infantil, estelionato, entre outros. É fundamental destacar que os cibercrimes ou crimes virtuais. (g1.globo.com/2020)

Tendo em vista o sólido comprometimento do Brasil com a Convenção de Budapeste(2001), um tratado internacional que aborda questões relacionadas aos cibercrimes, também é notável o empenho do legislador nacional em combater essas infrações penais. Dentre as principais leis que abordam esse tema, podemos mencionar as seguintes:

Lei nº 11.829/2008: Esta lei introduziu alterações no Estatuto da Criança e do Adolescente, visando reprimir a pornografia e a exploração sexual infantojuvenil no ambiente virtual.

Lei nº 9.983/2000: Esta legislação incorporou ao Código Penal brasileiro novos tipos criminais, especificamente nos artigos 313-A e 313-B, que tratam da inserção de dados falsos ou da modificação não autorizada de sistemas informatizados.

Lei nº 12.737/2012: Essa lei é conhecida principalmente por criar as figuras típicas previstas nos artigos 154-A e 154-B do Código Penal, que tratam da invasão de dispositivos eletrônicos e da divulgação de segredos obtidos ilegalmente.

Lei nº 12.735/2012: Ela estabeleceu a criação de delegacias especializadas no combate aos crimes cibernéticos, fortalecendo a capacidade de investigação e resposta a esses delitos.

Lei nº 13.185/2015: Essa lei tem como objetivo combater o bullying praticado pela internet, reconhecendo a importância de abordar o cyberbullying como um problema grave e prejudicial.

Lei nº 13.718/2018: Introduziu no ordenamento jurídico os artigos 218-C, que criminalizam a divulgação de imagens de sexo, nudez ou estupro sem o consentimento da vítima, entre outras disposições.

Lei nº 14.155 de 2021: Além das leis mencionadas anteriormente, é importante destacar a promulgação da Lei nº 14.155/2021, que trouxe alterações significativas no Código Penal brasileiro. Esta lei abordou especificamente a pena para crimes como a violação de dispositivo informático, furto e estelionato cometidos no ambiente digital. Além disso, ela também modificou disposições no Código de Processo Penal brasileiro, esclarecendo a competência em casos de estelionato.

Essas leis representam esforços significativos do Brasil para adaptar sua legislação à era digital e combater os cibercrimes, abordando questões que vão desde a proteção de crianças até a criminalização de práticas prejudiciais na internet.

1.1 CONCEITO E CLASSIFICAÇÃO DE CRIME VIRTUAL

1.1.1 Conceito

O conceito de crime virtual refere-se a atividades criminosas que são cometidas através do uso da tecnologia e da internet. Também é conhecido como cibercrime ou crime digital. O crime virtual abrange uma ampla gama de atividades ilícitas, incluindo roubo de identidade, fraude online, phishing, ataques cibernéticos, distribuição de malware, pornografia infantil, hacking, entre outros.

Os criminosos virtuais geralmente utilizam habilidades técnicas avançadas para explorar vulnerabilidades em sistemas de computador, redes e dispositivos eletrônicos. Eles podem roubar informações pessoais e financeiras, interromper serviços online, danificar sistemas de computador e causar prejuízos significativos a indivíduos, empresas e até mesmo governos.

> O crime virtual apresenta desafios únicos para a aplicação da lei, uma vez que os criminosos podem operar em uma escala global e esconder sua identidade por trás de várias camadas de anonimato. Além disso, as fronteiras nacionais muitas vezes não são barreiras efetivas para os criminosos virtuais, tornando a cooperação internacional fundamental para combater esse tipo de crime. (Pinheiro 2016).

Para combater o crime virtual, são necessárias medidas de segurança cibernéticas robustas, leis atualizadas e uma maior conscientização por parte dos usuários de tecnologia. As autoridades policiais e as agências de aplicação da lei também devem desenvolver habilidades e recursos especializados para investigar e processar os criminosos virtuais. (TEIXEIRA.2014).

Em resumo, o crime virtual é uma forma de atividade criminosa que ocorre no ambiente digital e se aproveita das vulnerabilidades da tecnologia e da internet. É um desafio em constante evolução que requer esforços contínuos para proteger indivíduos e organizações contra ameaças virtuais.

1.2. CLASSIFICAÇÃO DOS CRIMES VIRTUAIS

A classificação de crimes virtuais, também conhecidos como crimes cibernéticos, pode variar de acordo com o sistema legal de cada país. No entanto, existem algumas categorias comuns que são utilizadas para classificar esses tipos de crimes. (TEIXEIRA, 2014).

> Assim explica: “o primeiro são aqueles em que o sujeito visa especialmente o sistema de informática; as ações materializam, por exemplo, por atos de vandalismo contra a integridade do sistema ou pelo acesso desautorizado ao computador. Crime de informática misto se consubstancia nas ações em que o agente visa o bem juridicamente protegido diverso da informática, porém o sistema de informática é ferramenta imprescindível. E os crimes de informática comum são condutas em que a gente utiliza o sistema de informática como mera ferramenta, não essencial à consumação do delito”. (TEIXEIRA,2014).

Assim sendo, inclui nos crimes em que uma pessoa obtém acesso não autorizado a sistemas de computador, redes ou contas pessoais, como invasão de sistemas, hacking ou roubo de senhas.

Fraude virtual envolvem a utilização de informações falsas ou enganosas para obter benefícios financeiros ilegais. Isso pode incluir fraudes bancárias, esquemas de phishing, golpes online ou fraude de cartão de crédito. (PASCHOAL, 2020).

Phishing é uma técnica em que os criminosos enviam e-mails falsos ou criam sites falsos que se parecem com instituições legítimas, como bancos ou empresas conhecidas, para enganar as pessoas e obter suas informações pessoais. Isso pode levar ao roubo de identidade ou ao acesso não autorizado a contas pessoais. (AO KASPERSKY, Lab.2023)

Violação de direitos autorais isso envolve a cópia, distribuição ou uso não autorizado de obras protegidas por direitos autorais, como filmes, músicas, software e livros eletrônicos. (PASCHOAL, 2020).

Extorsão virtual ocorre quando alguém ameaça divulgar informações pessoais, comprometedoras ou privadas, a menos que a vítima pague um resgate ou cumpra suas exigências. (PASCHOAL, 2020).

Dessa forma, crimes cometidos em meio digital poderão incluir: difamação, calúnia, ameaça, roubo, falsificação de documentos, fraude, espionagem industrial, violação de segredos, promoção de atividades criminosas, racismo, atentado contra serviços públicos essenciais e invasão de dispositivos informáticos. (PASCHOAL, 2020).

Venda de drogas ilegais e armas internet também pode ser usada como um mercado para a venda de drogas ilícitas e armas, o que constitui um crime virtual significativo etc. (PASCHOAL, 2020).

> Para Higor Vinícius Nogueira Jorge (2012) e Emerson Wendt (2012), existem as ações prejudiciais atípicas e os crimes cibernéticos. As ações prejudiciais atípicas, são aquelas condutas que causam prejuízo ou transtorno para vítima através da rede mundial de computadores, mas não são tipificados em lei. Por sua vez os crimes cibernéticos se dividem em "crimes cibernéticos abertos" e "crimes exclusivamente cibernéticos". Os "crimes exclusivamente cibernéticos" são aqueles que necessariamente precisam do meio da informática para cometer tal crime (como é o caso do crime de invasão de dispositivo informático, artigos 154-A e154-B do código penal, introduzido pela Lei 12.735/2012, conhecido como Lei Carolina Dieckmann). Portanto os crimes cibernéticos abertos são aqueles que podem ou não ser praticados pelo meio informático, como é o caso de estudo os crimes de violação de direito do autor, pode ser praticado tanto no ambiente virtual como no analógico.

Crimes cibernéticos podem ser estudados, levando-se em consideração o papel desempenhado pelo computador no contexto da prática do ato ilícito. Nesse sentido, conforme esclarece Pinheiro (2013, apud Ferreira, 2001)

1.2.1 Crimes Virtuais Próprios

Crimes virtuais próprios são tipos penais que descreve a ação delituosa que somente acontece pela prática por meio virtual ou informático.

> A elevação pela não autorização tem sido considerado através do acesso externo, obtendo informações devido à vulnerabilidade da rede, não havendo necessidade para funcionar o sistema computacional e segurança do próprio aparelho. Existem duas modalidades: a primeira modalidade fala-se em aos atos dirigidos contra o sistema da informática, essa modalidade para os autores são chamados de "crimes informáticos próprios", praticados por meio da informática, sem a informática o crime não ocorrerá (como é o caso do crime de inserção de dados falsos em sistema de informações, art. 313-A do CP), a segunda modalidade portanto são "crimes informáticos impróprios", podem ser praticados de várias formas, sendo ela por meio da informática ou não, como são os casos os crimes contra a honra e violação direitos do autor, estelionato, pornografia infantil dentre outros. (IVETTE SENISE FERREIRA (2001) E MARCELO XAVIER DE FREITAS CRESPO (2011).

Considerado próprio tem que ser cometido com o uso do computador. O bem jurídico violado são os dados armazenados no computador ou rede. Tem-se como exemplo, a invasão de dados informatizados.

1.2.2. Crimes Virtuais Impróprios

Crimes virtuais impróprios são os praticados pelo método virtual ou eletrônico, delitos previstos, comumente crimes contra honra. Crespo (2011, p.87-93) descreve:

a) Ameaça
b) Participação em suicídio
c) Incitação e apologia ao crime
d) Falsa identidade e falsidade ideológica
e) Violação de direitos autorais (pirataria)
f) Pornografia infantil
g) Crimes contra a honra.

É importante ressaltar que os crimes virtuais impróprios são ilegais e têm consequências legais graves. As autoridades policiais e os órgãos responsáveis pela aplicação da lei estão cada vez mais focados em combater essas atividades criminosas, desenvolvendo mecanismos de investigação e legislação específica para lidar com a criminalidade digital.

> Em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais (JESUS e MILAGRE, 2016, p. 52)

Com relação ao patrimônio, enfrenta-se certa dificuldade em identificar os crimes cibernéticos impróprios, uma vez que não é possível classificar as informações armazenadas como bens materiais, mas sim como bens imateriais, não passíveis de apreensão física. Um exemplo disso são os crimes de transferência de valores em contas bancárias, nos quais os criminosos utilizam os sistemas informáticos meramente como meio de execução, ou seja, eles furtam dinheiro das contas das vítimas por meio de um sistema conectado à internet. (RITADECÁSSIALOPES.2013)

2. DESENVOLVIMENTO DIGITAL

No século XXI uniu pontos positivos e negativos da internet, positivos pela facilidade proporcionada pela rede, por outro lado, a mesma facilidade que se torna vítima. O crime digital (virtual), tem como conduta ilícita manifestada através dos meios eletrônicos, utilizando a rede de internet para a prática errada, envolvendo arquivos ou sistema. No ambiente empresarial, o crime costuma relacionar a roubo de dados para espionagem industrial. (PASCHOAL, 2020).

Quando se fala de crime virtual passa-se a imagem do transgressor com habilidades de grande porte, como um gênio que utiliza para fazer o mal, só que é isso mesmo, perfil com vasto conhecimento informático, matemático e até mesmo psicológico. Podendo ser capaz de iludir qualquer vítima sem mesmo olhar nos olhos. Por isso a dificuldade de se identificar o criminoso não é tão fácil, podendo ser qualquer um, nem sequer dá para vê-los, uma ameaça invisível que destrói a vida de várias pessoas pela rede de internet.

As vítimas podem ser qualquer pessoa, física ou jurídica, podendo sofrer danos materiais ou morais;

> Entende-se por vítima qualquer pessoa natural que tenha sofrido danos físicos, emocionais, em sua própria pessoa ou em seus bens, causados diretamente pela prática de um crime, ato infracional, calamidade pública, desastres naturais ou graves violações de direitos humanos. (art. 3º da Resolução nº 243/2021/CNMP).

Percebe-se que, as vítimas, trata-se de pessoas com comportamentos depressivos, que é seduzida e atraída ou por propaganda enganosa, prêmio prometido ou vantagem de fácil dinheiro, o que traz a entregar dados pessoais, bancários, de cartões de crédito, senhas etc. (HIRIGOYEN, 2002).

2.1 Principais crimes

Os principais crimes cibernéticos ocorrem de dois fatores que é a falta de conhecimento da segurança da informação e a falta de recursos humanos e tecnológicos da segurança pública e jurídica, necessita de vasto treinamento,

prevenção e conduzir a investigação para punir os criminosos virtuais (PINHEIRO,2016)

> Entendem-se por “vítimas” as pessoas que, individual ou coletivamente, tenham sofrido um prejuízo, nomeadamente um atentado à sua integridade física ou mental, um sofrimento de ordem moral, uma perda material, ou um grave atentado aos seus direitos fundamentais, como consequência de atos ou de omissões violadores das leis penais em vigor num Estado-membro, incluindo as que proíbem o abuso de poder (RESOLUÇÃO 40/34, ONU, 1985).

A prevenção é o melhor caminho para conscientizar a sociedade e para isso é ter um antivírus atualizado e registrado, não clicar em links de empresas ou instituição, evitar fazer download de aplicativos gratuitos, não abrir arquivos, anexos, programas executáveis, não emprestar senha de E-mail, internet, cartão, contas, duvidar de perfil de pessoas, registrar ocorrência na delegacia ou na especializada em crimes virtuais. (GARTNER.2011)

> Devido aos avanços tecnológicos, o ambiente virtual expandiu no Brasil, atingiu 49% de crescimento, alcançando o 4º lugar com maior número de conexões simultânea no mundo. A partir daí teve uma noção que algo poderia afetar a vida da sociedade no que tange os Direitos, para proteger os bens que não eram protegidos (AVELAR E DUARTE.2021).

Além de todo esse aumento digital que alterou todo o estilo de vida teve mais uma alteração, com o surgimento da pandemia, o novo coronavírus. Esse isolamento social resultou ainda mais o aumento de uso dos canais digitais, pessoas trabalhando de suas casas, reunião se tornou virtuais (videoconferência), faculdades e escolas suspensas, videoconferência e excessivo aumento de compras virtuais.

Diante do desenvolvimento da internet, redes sociais e aplicativos, os criminosos buscam avanços também nessas mudanças digitais, para aplicar os golpes nas redes. Daí a importância da conscientização da sociedade para dificultar e prevenir a ação dos criminosos.

A prestação de serviço pela internet mais utilizada é world wide web (www); chat; e-mail; compartilhamento de arquivos (redes P2P) mensagem instantânea (ex: WhatsApp, msn…); VoIP; redes sociais e e-commerce. Fora os aplicativos financeiros.

Cada dia mais os usuários de internet estão mais expostos aos crimes, é necessário conhecimento de como agem os criminosos, para que possa defender. De acordo com Gartner;

> Essa onda de crimes praticadas no Brasil cresceu 197% no ano de 2015, principalmente pelo aumento de usuários de aplicações na rede. O acesso cada vez mais facilitado aos serviços da Internet com o uso de computadores e dispositivos móveis expõem, numa escala jamais vista, os dados pessoais dos indivíduos e das organizações (GARTNER,2014).

Um criminoso que utiliza o trojan, por exemplo, conhecido como cavalo de Troia, software que se passa por um programa legítimo, simulando alguma função útil. Esta ameaça abre uma porta para que o criminoso tenha total acesso ao computador, para roubar senhas ou qualquer outro dado sigiloso (HOSTINGER, 2023).

> Os vírus utilizados para roubar os dados, como senhas, agências, contas e qualquer ato sigiloso é os malwares. (MERCÊS,2014). A classificação dos crimes virtuais, tende a capacidade de buscar e atender as necessidades da sua vítima. (CRESPO,2011).

O cibercrime tem evoluído ao longo do tempo, adaptando-se às mudanças na tecnologia e nas práticas de segurança. Inicialmente, as atividades cibercriminosas eram mais simples, como vírus e Worms que se espalhavam através de anexos de e-mail. No entanto, com o aumento da conectividade e do uso de dispositivos móveis, as táticas de cibercrime se tornaram mais sofisticadas e diversificadas.

CONCLUSÃO

Apesar de haver várias outras medidas para investigar os crimes cometidos no ciberespaço, o atual serviço objetivou trazer informações básicas acerca dos procedimentos investigativos adotados pelos agentes encarregados da perseguição penal em que ocasião os crimes sanado praticados pelo médio potencial, sendo elas medidas necessárias a todo e qualquer marcha investigativo quão envolvam crimes dessa natureza.

Foram trazidas a essas decomposições algumas noções acerca de quão foi empregada e quão funciona a internet, com saúde quão informações acerca da ideia e conceituação dos crimes cibernéticos, fora de outros tipos de ameaças, com o motivo de destinar ao ledor rudimentos necessários para uma melhor entendimento sobre as investigações policiais sobre as quais o atual artículo trata.

A internet é em verdade uma das grandes obras modernas criadas pelo homem, simbolizando a alcance de produção do existir humano, sendo espacioso de reduzir o tempo e distância entre as pessoas em uma altura em quão a sociedade exige quão vida se movimente cada hora mais breve e em maior quantidade, transformando-se em uma arma do dia da comunhão global, quão cada hora mais necessita da ressaca e atividade quão a internet oferece, sendo, hoje, impensável um universo na qual a mesma não exista, ou seja, necessária.

Contudo, tal âmbito em quão pese seja magnífico e estonteante, ainda é bloqueado de ameaças e de usuários mal-intencionados quão utilizam-se dela para a estudo de suas condutas criminosas. Assim, comissão se faz quão sejam tomadas medidas quão garantam quão a internet seja constituída em um âmbito robusto e desobstruído de ameaças aos seus usuários. A legislação pátrio demonstrou alguns avanços nos últimos anos no quão concerne à concepção de leis quão regulem o âmbito potencial, tal quão o Marco Civil da Internet.

Todavia, até agora é uma legislação tímida, necessitado de uma melhor regulamentação e maior clareza técnica, a intuito de construir tipos penais específicos aos crimes virtuais para premunir quão haja a impenitência dos agentes quão se utilizam da internet para a estudo de condutas ilícitas, com saúde quão traga uma maior regulamentação acerca da andar dos logs. Isso é porque o Marco Civil da Internet não exige quão a andar seja realizada por todos os provedores de acesso, podendo inviabilizar quão o esquadrinhador obtenha as informações necessárias para um seguro apuro dos crimes cibernéticos, por não contar registrados de dados armazenados pelas provedoras não obrigados por lei.

Ainda, é indispensável quão a regulamentação do âmbito potencial ainda abranja os locais com redes Wi-Fi abertas e sem controle, com saúde quão a prática do ofício de internet nas denominadas lan houses e cyber cafés, exigindo-se quão se tenha uma gravura dos usuários quão se utilizam de tais serviços, possibilitando desse modo quão haja a reconhecimento da composição do criminal cometido com a prática da internet, com procedência em tais locais.

Do próprio modo, fica declarado a necessidade de que o Brasil seja signatário de tratados e convenções internacionais que versem sobre crimes de informática, quão por lição a Convenção de Budapeste, uma vez que a própria internet tem por quilate intrínseca a constituição transnacional, dependendo, muitas vezes, para que haja a efetiva cota estatal à ação dos crimes cibernéticos, da coadjuvação dos órgãos causador pela perseguição criminal de outros países para prestarem as informações necessárias para que o Estado exerça o seu jus puniendi, turno que a atmosfera potencial é atemporal e não se limita perante as extremas políticas criadas pelos homens.

Urge a necessidade de que os órgãos responsáveis pela perseguição criminal, quão as Polícias Civil e Federal, com saúde quão o Poder Judiciário e o Ministério Público, instruam seus agentes acerca das infinitas possibilitadas trazidas pela prática da internet e, consequentemente, das ameaças que nela estão presentes.

É necessário que haja uma habilitação técnica específica, para que estejam preparados para tratar com as inúmeras adversidades e situações envolvendo os crimes virtuais, a intuito de que possam, de forma eficaz, disputar os criminosos virtuais, que com certeza alguma estão incessantemente atualizados acerca dos mecanismos disponíveis na rede para a abordagem de seus crimes.

Deve-se proporcionar instrumentos de tarefas compatíveis com a novidade realidade criminosa, turno que é público que, em diversas repartições públicas os equipamentos não possuem o mínimo de condições para seguir a evolução tecnológica.

Por intuito, e não menos importante, é necessário que o Governo adote políticas públicas no desconsolado de conscientizar a comunidade em geral acerca do acertado prática dos serviços disponíveis na internet, com saúde quão acerca das ameaças que nela espreitam e as formas de combatê-las.

acerca dos riscos apresentados pela prática inconsequente da rede, com saúde quão do comportamento pelas quais os criminosos se utilizam para delinquir, os usuários estão mais capazes de se propugnar de ataques virtuais, diminuindo deste modo a verossimilhança de parto das investidas dos criminosos na atmosfera potencial, pois a precaução é, sem dúvidas, uma das medidas mais eficientes à ação dos crimes cibernéticos

REFERÊNCIAS

ARAÚJO, Fábio Lucena de. Aspectos jurídicos no combate e prevenção ao ransomware. Crimes cibernéticos / 2ª Câmara de Coordenação e Revisão, Criminal, MPF, Coletânea de artigos, v. 3, 2018.

CRESPO, Marcelo. Crimes Digitais. Canal Ciências Criminais, 2016.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2011. Acesso em: 09/06/2023.

CASTRO, C. R. A. Crimes de Informática e seus Aspectos Processuais. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

CAVALCANTE, W. F. Crimes cibernéticos: noções básicas de investigação e ameaças na internet. Disponível em: <https://jus.com.br/artigos/25743/crimes-ciberneticos. Acesso em: 09/08/23.

COSTA, M. A. R. Crimes de informática. Disponível em: <https://jus.com.br/artigos/1826/crimes-de-informatica >. Acesso em: 20/08/23.

Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf

ONU, Organização das Nações Unidas. Resolução 40/34, de 29 de novembro de 1985. Declaração dos Princípios Básicos de Justiça Relativos às Vítimas da Criminalidade e de Abuso de Poder. In: Biblioteca Virtual de Direitos Humanos. Universidade de São Paulo.

NOVELINO, Marcelo. Curso de Direito Constitucional. 11ª. ed. Rev. Ampl. E atual. - Salvador: Ed. JusPodivm, 2016.

Disponível em: BRASIL. Lei nº 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: 05/05/2023

Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando/.

GARTNER. Gartner Says More than 75 Percent of Mobile Applications will Fail Basic Security Tests Through 2014.

Livro crimes cibernéticos: Ameaças e procedimentos de investigação (vol.01) Edição padrão, 11 outubro 2021 Edição Português por Emerson Wendt (Autor), Higor Jorge

Livro INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS (2022). Higor Vinicius Nogueira Jorge, Gaetano Vergine. Ed.01.

Livro Crimes cibernéticos: Ameaças e procedimentos de investigação - 2ª Edição ebook Kindle por Emerson Wendt (Autor), Higor Vinicius Nogueira Jorge (Autor) Formato: ebook Kindle.

Livro Crimes Virtuais, Vítimas Reais De Moisés de Oliveira Cassanti.

Disponível em file:///C:/Users/Usuario/Downloads/2013-Texto%20do%20artigo-6696-1-10-20150326.pdf. Acesso em: 09/06/2023.

Disponível em: https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes. Acesso em: 09/06/2023.

Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 09/06/2023.

Disponível em: http: //www.gartner.com/newsroom/id/2846017>. Acesso em: 09/06/2023.

Disponível em: https://www.avellareduarte.com.br/internet-no-brasil-2021-estatisticas. Acesso em: 09/06/2023.

Disponível em: https://www.jusbrasil.com.br/artigos/classificacao-dos-crimes-digitais/307254758. Acesso em: 09/06/2023.

Disponível em: https://immes.edu.br/wp-content/uploads/2020/10/2017-Crimes-Cibern%C3%A9ticos.pdf. Acesso em: 09/06/2023.

Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 09/06/2023.

Disponível em: https://www.hostinger.com.br/tutoriais/cavalo-de-troia-virus. Acesso em: 09/06/2023.

Disponível em: https://www.fag.edu.br/upload/contemporaneidade/anais/594c13e45d209.pdf. Acesso em: 09/06/2023.

Disponível em: https://www.safernet.org.br/site/institucional. Acesso em: 09/06/2023.

Disponível em: https://www.jusbrasil.com.br/artigos/violacao-dos-direitos-fundamentais-em-crimes-ciberneticos-e-a-necessidade-de-inclusao-do-direito-eletronico-como-legislacao-especifica/653015456.Acesso em: 09/06/2023.

Disponível em: https://ueslima.jusbrasil.com.br/artigos/653015456/violacao-dos-direitos-fundamentais-em-crimes-ciberneticos-e-a-necessidade-de-inclusao-do-direito-eletronico-como-legislacao-especifica. Acesso em: 09/06/2023.

Disponível em: http://www.direitoshumanos.usp.br/index.php/Direitos-Humanos-na-Administra%C3%A7%C3%A3o-da-Justi%C3%A7a.-Prote%C3%A7%C3%A3o-dos-Prisioneiros-e-Detidos.-Prote%C3%A7%C3%A3o-contra-a-Tortura-Maus-tratos-e-. Acesso em: 09/06/2023.

Disponível em: http://desaparecimento/declaracao-dos-principios-basicos-de-justica-relativos-as-vitimas-da-criminalidade-e-de-abuso-de-poder.html. Acesso em: 09/06/2023.

Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml. Acesso em: 09/08/2023.

PONTIFICIA UNIVERSIDADE CATÓLICA DE GOIAS
Pró-Reitoria de Graduação
Escola de Direito, Negócios e Comunicação
Curso de Direito
Núcleo de Prática Jurídica
Coordenação Adjunta de Trabalho de Curso

TERMO DE AUTORIZAÇÃO DE PUBLICAÇÃO DE PRODUÇÃO ACADÊMICA

O estudante **BRUNO PEREIRA BARROS** do Curso de **DIREITO**, matrícula **20192000102749**, telefone: **62 999827401**, e-mail brrunno.ti1@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado **CRIMES CIBERNÉTICOS:** DIFICULDADE PARA OBTER INDÍCIOS DE AUTORIA E MATERIALIDADE, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JEPG): Som (WAVE, MPEG, AIFF, SNS); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 23 de agosto de 2023.

Assinatura do(s): autor(es):

gov.br Documento assinado digitalmente
BRUNO PEREIRA BARROS
Data: 23/08/2023 15:16:27-0300
Verifique em https://validar.iti.gov.br

Nome completo do autor: BRUNO PEREIRA BARROS

Assinatura do professor- orientador

gov.br Documento assinado digitalmente
GIL CESAR COSTA DE PAULA
Data: 20/09/2023 19:53:33-0300
Verifique em https://validar.iti.gov.br

Nome completo do professor-orientador: GIL CESAR COSTA DE PAULA

PONTIFICIA UNIVERSIDADE CATÓLICA DE GOIAS
Pró-Reitoria de Graduação
Escola de Direito, Negócios e Comunicação
Curso de Direito
Núcleo de Prática Jurídica
Coordenação Adjunta de Trabalho de Curso

TERMO DE AUTORIZAÇÃO DE PUBLICAÇÃO DE PRODUÇÃO ACADÊMICA

O estudante **BRUNO PEREIRA BARROS** do Curso de **DIREITO**, matrícula **20192000102749**, telefone: **62 999827401**, e-mail brrunno.ti1@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado **CRIMES CIBERNÉTICOS:** DIFICULDADE PARA OBTER INDÍCIOS DE AUTORIA E MATERIALIDADE, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JEPG): Som (WAVE, MPEG, AIFF, SNS); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 23 de agosto de 2023.

Assinatura do(s): autor(es):

gov.br Documento assinado digitalmente
BRUNO PEREIRA BARROS
Data: 23/08/2023 15:16:27-0300
Verifique em https://validar.iti.gov.br

Nome completo do autor: BRUNO PEREIRA BARROS

Assinatura do professor- orientador

gov.br Documento assinado digitalmente
GIL CESAR COSTA DE PAULA
Data: 20/09/2023 19:53:33-0300
Verifique em https://validar.iti.gov.br

Nome completo do professor-orientador: GIL CESAR COSTA DE PAULA