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 I

CRIMES CIBERNÉTICOS

CARACTERÍSTICAS, PECULIARIDADES DA INVESTIGAÇÃO E AS AMEAÇAS NA ‘’ REDE MUNDIAL DE COMPUTADORES’’

ORIENTANDO - GUSTAVO AMERICANO ROCHA
ORIENTADORA - PROF° DRA. EDWIGES CONCEIÇÃO CARVALHO CORRÊA

GOIÂNIA-GO
2023

GUSTAVO AMERICANO ROCHA

CRIMES CIBERNÉTICOS

CARACTERÍSTICAS, PECULIARIDADES DA INVESTIGAÇÃO E AS AMEAÇAS NA ‘’ REDE MUNDIAL DE COMPUTADORES’’

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito , Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).
Prof. Orientadora – Dra. Edwiges Conceição Carvalho Corrêa.

GOIÂNIA-GO

2023

GUSTAVO AMERICANO ROCHA

CRIMES CIBERNÉTICOS

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientadora: Prof. Doutora Edwiges Conceição Carvalho Corrêa Nota

_____

Examinadora Convidada: Prof. Doutora Eufrosina Saraiva Silva Nota

RESUMO

GUSTAVO AMERICANO ROCHA

Neste estudo, serão exploradas as diversas formas de delitos digitais, juntamente com conceitos da criminalidade virtual e uma análise das leis em vigor no Brasil que tratam desse assunto. Contudo, o foco desta pesquisa reside na investigação das consequências provocadas pelos ataques à reputação e à imagem de um indivíduo por meio desta rede global de comunicação, além dos obstáculos enfrentados para punir os responsáveis por tais crimes cibernéticos. A 1° seção do trabalho foca em um breve conceito da cibercriminalidade, apresentando os crimes cibernéticos próprios e impróprios. Na 2° seção, será abordado os crimes cibernéticos impróprios, sendo demonstrado alguns crimes presentes na rede mundial de computadores. Já a 3°seção focará nas investigações realizadas para chegar até esses cibercriminosos. As seções deste estudo procuram examinar trabalhos relacionados ao tema por parte de renomados autores no meio acadêmico. Por fim, serão propostas potenciais soluções para o questionamento central deste trabalho, que diz respeito aos métodos viáveis para prevenir os ataques perpetrados por criminosos digitais. A metodologia adotada para este artigo abarca aspectos teóricos, recorrendo a livros, artigos e trabalhos acadêmicos, assim como a casos práticos pertinentes ao assunto em pauta.

Palavras-chave: Crimes cibernéticos. Internet. Legislação. Investigação. Cibercrimes.

SUMÁRIO

INTRODUÇÃO ……..…6
1 CONCEITOS BÁSICOS DE DELITOS CIBERNÉTICOS……....8
1.1 CRIMES CIBERNÉTICOS PRÓPRIOS E IMPRÓPRIOS……....9
2. CRIMES CIBERNÉTICOSIMPRÓPRIOS.....……...11
2.1 ATOS DE INVASÃO DA PRIVACIDADE …… ..11
2.2 DELITOS CONTRA A HONRA……..13
2.3 CYBERBULLYING……...15
2.4 ESTELIONATO E FURTO MEDIANTE FRAUDE…….18
3 A COMPLEXIDADE POR TRÁS DAS INVESTIGAÇÕES……..20
3.1 CYBERGAECO…….23
4. ESTRATÉGIAS DE PROTEÇÃO CONTRA DELITOS NA ESFERA DIGITAL 25
CONSIDERAÇÕES FINAIS.....……..27
ABSTRACT.....…….....28
REFERÊNCIAS.....……...29

INTRODUÇÃO

Nos últimos anos, o avanço da tecnologia e a crescente interconectividade proporcionaram inúmeros benefícios à sociedade. No entanto, juntamente com essas vantagens, surgiu um lado sombrio e preocupante: os crimes cibernéticos. Esses delitos envolvem o uso ilícito da tecnologia da informação e das redes digitais para perpetrar atividades criminosas.

Os crimes cibernéticos abrangem uma ampla gama de atividades ilícitas, como invasões de sistemas, fraudes eletrônicas, roubo de dados pessoais, phishing, espionagem cibernética, disseminação de malware, entre outros. Essas ações são realizadas por indivíduos ou grupos que exploram as vulnerabilidades do mundo digital para obter benefícios financeiros, prejudicar outras pessoas, empresas e até mesmo governos.

Uma das características mais preocupantes dos crimes cibernéticos é a sua natureza transnacional. Os criminosos podem operar a partir de qualquer lugar do mundo, visando vítimas em qualquer parte do globo. Essa falta de fronteiras físicas dificulta a aplicação da lei e a cooperação internacional para combater essas ameaças.

Os crimes cibernéticos têm um impacto significativo na sociedade, na economia e na segurança global. Empresas sofrem prejuízos financeiros, perda de dados sensíveis e danos à reputação. Indivíduos têm suas identidades roubadas, sofrem extorsões e são vítimas de fraudes. Governos enfrentam a ameaça à segurança nacional e à infraestrutura crítica.

Para combater essa crescente onda desses crimes, é necessário um esforço conjunto de governos, empresas e indivíduos. Investimentos em segurança cibernética, educação e conscientização são essenciais para proteger-se contra essas ameaças. Além disso, a cooperação internacional e a atualização constante das leis e regulamentações são fundamentais para enfrentar os desafios do mundo digital.

Em suma, os crimes cibernéticos representam uma ameaça séria e em constante evolução. À medida que a tecnologia avança, novas formas de delitos surgem, exigindo uma resposta robusta e colaborativa. Somente através de uma abordagem integrada e proativa podemos mitigar os riscos e proteger a sociedade digital.

O presente trabalho tem o objetivo de apresentar algumas espécies de crimes cibernéticos, bem como uma explanação das atuais leis brasileiras que tratam do tema. Não obstante, o enfoque da presente pesquisa é um estudo sobre as repercussões dos ataques à honra e à imagem de um indivíduo através desse meio de comunicação global e os desafios para punir os cibercriminosos.

Como o objeto do trabalho foca nos crimes cibernéticos, estes que se veem cada vez mais presentes nos dias atuais, os problemas acerca da pesquisa será apresentar as ameaças presentes na internet; Quais as sanções cabíveis; E quais os procedimentos especializados para a investigação?

A 1° seção do trabalho foca em um breve conceito da cibercriminalidade, apresentando os crimes cibernéticos próprios e impróprios. Na 2° seção, aprofundaremos o estudo nos crimes cibernéticos imprópios, sendo demonstrado alguns crimes presentes na rede mundial de computadores. Já na 3°seção focará investigações realizadas, para chegar até esses cibercriminosos.

A metodologia escolhida para o presente artigo são assuntos teóricos, utilizando livros, artigos e trabalhos acadêmicos, bem como fatos envolvendo o tema abordad

1 CONCEITOS BÁSICOS DE DELITOS CIBERNÉTICOS

A rede mundial de computadores, também conhecida como internet, apresenta uma série de ameaças que podem comprometer a segurança e a privacidade dos usuários. Essas ameaças podem ter diferentes origens e objetivos, mas todas representam riscos significativos. As ameaças na internet estão em constante evolução, e os invasores frequentemente desenvolvem novas técnicas e abordagens. O criminoso sempre utiliza de destreza para que o usuário execute uma ação ou preste informações, nesta seção, apresentaremos as espécies de crimes cibernéticos.

Com a expansão generalizada da internet e sua crescente integração em uma variedade de atividades, surge uma crescente inquietação em relação à proteção das informações compartilhadas no ambiente online.

À medida que a tecnologia avança, torna-se cada vez mais desafiador enfrentar os delitos cibernéticos. Com a ampla adoção da internet, certos indivíduos com habilidades técnicas avançadas passaram a se apropriar de informações criptografadas, seja por ganhos financeiros ou simples entretenimento (JESUS; MILAGRES, 2016).

Indivíduos conhecidos como "hackers", um termo moderno de origem inglesa, são aqueles que possuem um profundo conhecimento em informática e cujas habilidades estão voltadas para a invasão de sistemas, com o propósito de roubar, adulterar ou, em alguns casos, apenas acessar dados e informações de terceiros, motivados por diversas razões.

Essa mudança de paradigma transformou a quebra de códigos e a invasão de sistemas de uma ferramenta de guerra em uma oportunidade de lucro ou simples passatempo. Por exemplo, estelionatários encontraram na internet uma plataforma para aplicar golpes.

A internet oferece um terreno vasto para uma ampla gama de atividades criminosas, incluindo pedofilia, prostituição, tráfico, pirataria e até mesmo atos de terrorismo. Embora a digitalização dos processos de trabalho economize bilhões de dólares para as empresas anualmente, também gera uma série de desafios e problemas para pessoas em todo o mundo. Somente este ano, inúmeros casos de sequestros de dados e vazamento de informações confidenciais foram registrados em todo o mundo.

Além de causarem transtornos, alguns crimes geram enorme prejuízo ao país, a pirataria tem sido um problema cada vez mais difícil de enfrentar, seja ela nos filmes, livros, musicas, propriedade intelectual e artística, nunca estiveram tão vulnerável.

A internet não apenas simplificou o acesso a informações, mas também deu origem a uma realidade virtual na qual os usuários desenvolveram uma linguagem e um meio de interação próprios. Isso resultou na criação de um submundo sombrio, onde direitos fundamentais assegurados pela Constituição Federal, como dignidade, privacidade e igualdade, foram desrespeitados e violados, uma vez que a aplicação da lei ainda não alcançava esses infratores.

No contexto brasileiro, diversas leis foram promulgadas para lidar com essa nova categoria de crimes, destacando-se a Lei Nº 12.737, conhecida como "Lei Carolina Dieckmann". Essa lei modificou o Código Penal para classificar uma série de comportamentos no ambiente digital como infrações, com ênfase na invasão de sistemas de computadores, e estabeleceu penalidades específicas para tais condutas.

1.1 CRIMES CIBERNÉTICOS PRÓPRIOS E IMPRÓPRIOS

Crimes cibernéticos abertos ou Crimes cibernéticos impróprios: Forma tradicional ou por intermédio/contra computador; Crimes exclusivamente cibernéticos ou Crimes cibernéticos próprios: Somente por intermédio/contra computador.

Conforme exposto acima, os crimes cibernéticos são divididos em “Crimes cibernéticos Impróprios” e “Crimes Cibernéticos Próprios”. Os crimes cibernéticos “impróprios” são aqueles que podem ser praticados da forma tradicional ou por intermédio de computadores, o computador é apenas um meio para a prática do delito, que também poderia ser cometido sem o uso dele. Já os Crimes Cibernéticos “ Próprios” são diferentes, pois eles somente podem ser praticados com o uso de um computador ou outro recurso que tenha aceso a internet.

Seguem alguns exemplos de crimes cibernéticos:

CRIMES CIBERNÉTICOS ABERTOS/IMPRÓPRIOS	CRIMES EXCLUSIVAMENTE CIBERNÉTICOS/PRÓPRIOS
✓ Crimes contra a honra ✓ Ameaça ✓ 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 o fim de obter, adulterar ou excluir dados e informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. ✓ Interceptação telemática ilegal ✓ Pornografia infantil por meio de sistema de informática ✓ Corrupção de menores em sala de bate papo ✓ Crimes contra a urna eletrônica

(WENDT; JORGE, 2013, pg. 20).

Os crimes mais comuns são os cometidos contra o sistema financeiro, os crimes de phishing, que são furtos mediante fraude. Uma pessoa recebe uma mensagem falsa, via internet, ela clica no arquivo malicioso e importa um vírus para dentro da máquina. Os criminosos descobriram que é muito melhor atacar o correntista, que é o polo mais fraco, do que atacar o polo mais forte, que é o banco.

2 CRIMES CIBERNÉTICOS IMPRÓPRIOS

Nesta seção, iremos concentrar nossa atenção nos crimes virtuais abertos/impróprios, devido à sua frequência cada vez maior. Isso ocorre porque a internet tem se transformado em uma ferramenta que possibilita o anonimato, o que, teoricamente, incentiva a violação das leis.

Entre esses delitos, merecem destaque os crimes de ódio, os delitos que envolvem invasão de privacidade e intimidade, atos de estelionato, casos de pedofilia, entre outros.

A internet proporciona a criação de uma realidade na qual as distâncias físicas são encurtadas, conectando as pessoas como se estivessem próximas umas das outras. Para que as pessoas possam participar efetivamente do "ciberespaço", é imperativo que o Estado assegure a proteção de seus direitos e garantias fundamentais, impedindo que as novas tecnologias violem esses direitos (PANNAIN, PEZZELLA, 2015).

2.1 ATOS DE INVASÃO DA PRIVACIDADE

A privacidade e intimidade é um direito constitucional previsto no artigo 5º, inciso X, da Constituição Federal: "*X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"* (BRASIL, 2023).

Crimes cibernéticos contra a invasão da privacidade são uma preocupação crescente na era digital. Com o avanço da tecnologia e a crescente dependência da internet, as oportunidades para invadir a privacidade das pessoas também aumentaram. Esses crimes envolvem ações ilegais que visam acessar, coletar, usar ou divulgar informações pessoais de indivíduos sem o seu consentimento, muitas vezes com o objetivo de obter ganhos financeiros, prejudicar a reputação das vítimas ou simplesmente satisfazer a curiosidade.

Um exemplo notório desse tipo de crime ocorreu em 2011, quando a atriz Carolina Dieckmann foi vítima de um ataque cibernético no qual seu computador foi invadido e suas fotos íntimas foram roubadas e divulgadas na internet. O bem jurídico protegido pelo artigo 154-A do Código Penal é a privacidade individual armazenada em dispositivos de computador.

A Lei nº 12.737 de 2012, conhecida popularmente como Lei Carolina Dickmann, foi inserida no código penal brasileiro em seu artigo 154-A, e discorre a respeito da invasão de dispositivos informáticos:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa
> (BRASIL, 2023).

Os bens jurídicos protegidos abrangem a intimidade, a vida privada e o direito ao sigilo de dados. "*A intimidade e a vida privada demandam inviolabilidade de domicílio, de correspondência e de comunicações em geral, chamando-se o Direito Penal para punir as lesões aos referidos bens jurídicos tutelados.*" (NUCCI, 2017, p.26).

Para configurar a primeira parte do crime, é essencial o ato de "invadir", ou seja, violar virtualmente um dispositivo sem a autorização expressa ou implícita do seu proprietário, sem a necessidade de adulterar, destruir ou obter dados.

Para tornar a punição mais efetiva, o legislador incluiu no §3º do artigo 154-A uma qualificadora relevante, diretamente relacionada à privacidade da vítima. Nesse contexto, a invasão resulta na obtenção de informações sigilosas da vítima, como seus segredos, o que leva ao aumento da pena para seis meses a dois anos de reclusão, além de multa (CAPEZ, 2016).

Da mesma forma, o §4º do mesmo artigo estabelece uma majorante do crime, que implica um aumento na pena "de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas" (BRASIL, 2023).

2.2 DELITOS CONTRA HONRA

Na doutrina brasileira, a honra é dividida em duas categorias: objetiva e subjetiva. A honra objetiva está relacionada à reputação e à fama que um indivíduo desfruta na sociedade em que vive, enquanto a honra subjetiva diz respeito à sua dignidade e ao seu senso de decoro pessoal, ou seja, a opinião que cada pessoa tem de si mesma (ASSUNÇÃO, 2018).

A honra é constitucionalmente protegida, sendo um direito fundamental (art. 5º, x, da Constituição Federal). Os crimes contra a honra são bem conhecidos no meio jurídico, além de ser considerado um direito da personalidade, tendo a proteção da dignidade pessoal do individuo e sua reputação.

"*A honra demanda a proteção do ordenamento jurídico, por mecanismo civis e penais, sancionando-se a calúnia, a difamação e a injúria*" (NUCCI, 2017, p.26). A honra objetiva pode ser considerada o "objeto jurídico", representando a reputação ou a imagem que um indivíduo possui perante a sociedade, enquanto a honra subjetiva é referida como o "objeto material".

No contexto dos crimes contra a honra, a legislação penal brasileira prevê três tipos de delitos: calúnia, difamação e injúria.

O professor Rogério Sanches (2014) esclarece que nos casos de calúnia e difamação, é essencial a presença de uma conduta específica, ou seja, a imputação de um fato concreto e ofensivo, que deve ser necessariamente falso no caso da calúnia, configurando-o como um crime. Já na injúria, trata-se de uma imputação genérica, envolvendo um defeito ou

menosprezo à vítima. Nos dois primeiros casos, é necessário que a frase desonrosa chegue ao conhecimento de terceiros, o que não é necessário para o crime de injúria. No caso da injúria, ao contrário dos delitos anteriores, o bem protegido é a honra subjetiva da vítima. Este crime é caracterizado por ofender uma pessoa por ação ou omissão, prejudicando sua dignidade. Aqui, não há a necessidade de imputação de fatos específicos, mas sim uma avaliação negativa da vítima (ASSUNÇÃO, 2018).

O artigo 141 do Código Penal estabelece um aumento de pena em seu segundo parágrafo, aplicável aos crimes contra a honra, ou seja, calúnia, difamação e injúria. Esse aumento de pena ocorre quando o crime é cometido ou divulgado em qualquer modalidade das redes sociais da internet, triplicando a pena.

É importante lembrar a importância da liberdade de expressão. A base da liberdade de expressão está ligada diretamente à autonomia e dignidade humanas, sendo crucial o respeito pelos direitos fundamentais das pessoas. As tecnologias da informação proporcionam um novo olhar sobre a liberdade de expressão, com um aumento positivo na participação social e interação cultural, promovendo o acesso a uma verdadeira democracia (PANNAIN; PEZZELLA, 2015).

O conflito entre a liberdade de expressão individual e as ações que prejudicam a honra (objetiva ou subjetiva) das vítimas é evidente. A liberdade de expressão não pode ser exercida de forma completamente irrestrita e é necessário estabelecer limites, equilibrando o direito de expressar-se com o direito dos outros. No entanto, nem sempre as condutas criminosas realizadas na internet são punidas penalmente, seja devido à dificuldade de identificar o verdadeiro infrator ou à falta de preparo do Estado para lidar com essas situações.

Essas condutas muitas vezes são motivadas pelo ódio puro e simples, sem nenhum filtro social.

2.3 CYBERBULLYING

Muitas pessoas concebem a violência apenas como agressão física direta contra outras indivíduos, ou seja, o ato de infligir dor física à vítima por meio de tapas, socos ou empurrões. O que as pessoas geralmente não consideram é que existem formas diversas de violência. Um exemplo disso é a agressão moral e, mais recentemente, a mesma forma de ofensa, porém praticada por meio de dispositivos eletrônicos.

As ofensas perpetradas por meios eletrônicos se assemelham a outras formas de violência, mas seus impactos podem ser mais graves e, por vezes, durar a vida inteira da vítima. Nesse contexto, temos o bullying, e mais recentemente, o cyberbullying.

Independentemente do tipo de agressão, quando ocorre de maneira repetida, pode ser denominado bullying. Essa palavra tem origem no inglês e significa valentão. Já o termo cyberbullying refere-se à mesma forma de agressão, mas praticada por meio de computadores ou outros dispositivos tecnológicos. Esse tipo de ofensa pode ser perpetrado de várias maneiras e se caracteriza pela rápida disseminação pela rede, ou seja, em pouco tempo, a ofensa se propaga por uma infinidade de sites e blogs. É difícil para a vítima remover todas as informações dos locais em que foram compartilhadas.

Entre as modalidades de cyberbullying, destacam-se o envio de e-mails ofensivos para a vítima ou pessoas conhecidas, o envio de mensagens SMS por meio de celulares, a postagem de vídeos, a publicação de ofensas em sites, blogs, redes sociais, fóruns de discussão, hotéis virtuais, mensageiros instantâneos, entre outros.

O cyberbullying é muito comum no ambiente escolar, entre jovens, mas também pode ocorrer no ambiente de trabalho, na família, entre vizinhos, amigos ou em outros contextos.

No nosso cotidiano, temos testemunhado o cyberbullying sendo praticado por diversos motivos, desde diferenças nas características físicas das pessoas, como no caso de indivíduos obesos ou com deformidades físicas, até outras características, como o destaque intelectual de um jovem ou sua religião, etnia ou orientação sexual diferente da maioria.

É importante ressaltar que alguns casos de cyberbullying ultrapassam os limites da legalidade e se enquadram em crimes previstos pela lei. Nessas circunstâncias, também entram em ação as autoridades responsáveis pela persecução penal, como a Polícia Civil ou a Polícia Federal, que têm a função de investigar infrações penais, conforme estabelecido no artigo 144 da Constituição Federal.

Apesar da falsa sensação de segurança que o agressor possa ter, é importante ressaltar que ele está cometendo um crime e pode ser punido. O cyberbullying pode ser passível de punição de acordo com o Código Penal, quando configura crimes contra a honra (calúnia, difamação e injúria - Artigo 138,139 e 140 do Código Penal Brasileiro) e exposição de imagens de teor íntimo, erótico ou sexual (Artigo 218-C do Código Penal Brasileiro, incluído pela Lei 13.718, de 2018).

Em todos esses casos, as penalidades previstas no Código Penal Brasileiro podem resultar em até quatro anos de prisão. Além disso, na esfera civil, os agressores podem ser condenados a pagar indenizações por danos morais. Quando o agressor é menor de idade, seus responsáveis legais também podem ser responsabilizados perante o tribunal e serem condenados a pagar indenizações à vítima e sua família.

Entre os principais casos de cyberbullying que são considerados criminosos, há alguns que se destacam:

Calúnia (Artigo 138 do CP): quando alguém afirma que a vítima cometeu um crime, como espalhar mensagens acusatórias em redes sociais, sugerindo que ela praticou um delito. Isso pode resultar em detenção de seis meses a dois anos, além de multa.

Difamação (Artigo 139 do CP): consiste em divulgar informações prejudiciais à reputação da vítima, mesmo que sejam verdadeiras. Por exemplo, expor publicamente que uma pessoa foi vista em um local comprometedor, resultando em detenção de três meses a um ano, mais multa.

Injúria (Artigo 140 do CP): quando alguém ofende a dignidade ou o decoro de outra pessoa, como xingamentos em redes sociais ou divulgação de informações falsas que denigrem a imagem da vítima. A pena varia de um a seis meses de detenção, ou multa, podendo chegar a um ano se houver violência.

Ameaça (Artigo 147 do CP): envolve ameaçar a vítima com um mal sério e injusto, como enviar mensagens, e-mails ou fazer ligações ameaçadoras. Isso pode resultar em detenção de um a seis meses, ou multa.

Constrangimento ilegal (Artigo 146 do CP): ocorre quando se força a vítima a fazer algo que não deseja, como ameaçar um familiar para que ela ligue a câmera do computador. Também se configura quando se impede a vítima de fazer algo permitido por lei. A pena é de detenção, de três meses a um ano, ou multa.

Falsa identidade (Artigo 307 do CP): é quando alguém usa ou atribui a outra pessoa uma identidade falsa para obter vantagens ou causar danos. A pena é de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

Molestar ou perturbar a tranquilidade: isso não é considerado um crime, mas uma contravenção penal. Envolve perturbar alguém de forma reprovável, como enviar mensagens perturbadoras e desagradáveis para incomodar a vítima.

Os perfis falsos e os e-mails utilizados por muitos agressores nas redes sociais, com o objetivo de ocultar sua verdadeira identidade, podem ser rastreados e descobertos por meio da análise do endereço de IP (um tipo de identificação que registra e identifica qualquer ponto de acesso à internet). O endereço de IP pode ser revelado por meio de uma investigação policial autorizada pelo poder judiciário.

2.4 ESTELIONATO E FURTO MEDIANTE FRAUDE

O estelionato e o furto são dois tipos de crimes que envolvem enganos e a obtenção indevida de bens ou valores por meio de estratégias fraudulentas, mas eles têm características distintas e são tratados de forma diferente na maioria dos sistemas legais.

Nosso Código Penal, trata da cibercriminalidade desses delitos citados como qualificadoras:

> **Furto qualificado**
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> **Estelionato**
> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> § 2º - Nas mesmas penas incorre quem:
> Fraude eletrônica
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo
> (BRASIL, 2023).

O estelionato sob fraude eletrônica é uma variação do estelionato tradicional, mas envolve o uso de meios eletrônicos, como a internet, email, mensagens de texto e outros dispositivos eletrônicos para cometer a fraude. Este crime geralmente se manifesta em golpes online, em que os criminosos criam falsos websites, emails, ou aplicativos para enganar as vítimas e obter informações pessoais sensíveis, como senhas, números de cartão de crédito, ou outros dados financeiros.

Exemplos incluem phishing, onde os fraudadores enviam emails que se parecem com comunicações legítimas de bancos ou empresas, a fim de induzir as vítimas a fornecer informações confidenciais. Além disso, golpes de compras online fraudulentas, leilões falsos, ou ofertas de emprego enganosas também são formas comuns de estelionato eletrônico.

O furto mediante fraude por meio de dispositivo eletrônico ou informático é uma forma de furto em que os criminosos usam tecnologia para enganar as vítimas e obter bens ou valores. Isso frequentemente envolve o uso de programas maliciosos, como malware, vírus, ou cavalos de Troia, para ganhar acesso não autorizado a sistemas, contas bancárias ou informações pessoais das vítimas. Eles podem se apropriar de informações financeiras ou bens online, geralmente sem o conhecimento ou consentimento da vítima.

Como bem assevera Guilherme de Souza Nucci, a fraude *"é uma manobra enganosa destinada a iludir alguém, configurando, também, uma forma de ludibriar a confiança que se estabelece naturalmente nas relações humanas."* (2014, p.748). Então, é um crime que utiliza a boa fé, a distração do cliente, não é como o estelionato, em que você entrega espontaneamente as coisas. No furto mediante fraude, a distinção é que a pessoa usa sua distração, você pensa estar clicando em uma mensagem verdadeira, nesse momento é cometida a fraude, logo após, o furto. A fraude, para a categorização do delito de furto, precisa ocorrer prévia ou simultaneamente à remoção do objeto e com o intuito de tornar mais fácil essa remoção.

Se alguém consegue persuadir a vítima, levando-a a cometer um equívoco e entregar de forma voluntária o que é seu, caracteriza-se como estelionato; no entanto, se o autor, devido ao contexto enganoso, ilude a vigilância da vítima, subtraindo-lhe o bem, é um caso de furto mediante fraude (NUCCI, 2014).

Em ambos os casos, esses crimes exploram a crescente dependência da sociedade na tecnologia e a confiança nas comunicações e transações online. Para combater esses tipos de crimes, é essencial que os indivíduos estejam cientes dos riscos cibernéticos, protejam suas informações pessoais, usem software de segurança, como antivírus, e relatem atividades suspeitas às autoridades competentes.

3 A COMPLEXIDADE POR TRÁS DAS INVESTIGAÇÕES

Esta seção discute de forma abrangente a investigação de crimes cibernéticos, abordando várias áreas do Direito e os desafios que esses tipos de crimes apresentam.

Uma análise sobre delitos digitais pode englobar distintos domínios jurídicos. Na esfera penal, a averiguação é conduzida por intermédio de exames forenses, realizados por especialistas criminais das instituições da Polícia Civil ou Federal.

A investigação de crimes está em constante evolução, e é importante compreender as técnicas desenvolvidas pelos órgãos responsáveis para combater a delinquência.

Essa área requer conhecimento técnico especializado, pois os investigadores precisam compreender as nuances da tecnologia, das redes e dos sistemas utilizados para cometer esses crimes. Além disso, a cooperação internacional muitas vezes se torna essencial, já que os criminosos podem operar de qualquer lugar do mundo, ultrapassando fronteiras e jurisdições.

Os métodos de investigação incluem a análise forense digital, que envolve coletar e analisar evidências eletrônicas, como registros de computador, dispositivos de armazenamento e comunicações online.

Os avanços tecnológicos trouxeram benefícios em termos de modernização e velocidade, mas também deram origem a crimes que confundem tanto as vítimas quanto as autoridades encarregadas da persecução penal.

As equipes de investigação de crimes cibernéticos trabalham em estreita colaboração com profissionais de segurança cibernética, peritos forenses digitais e outros especialistas em tecnologia para rastrear atividades maliciosas, identificar os responsáveis e reunir evidências que possam ser usadas em processos legais.

Em casos de ataques informáticos, distribuição de conteúdo ilegal ou uso da internet para fins criminosos, é irrealista confiar apenas em métodos de investigação tradicionais. O uso de novas tecnologias é essencial para coletar evidências, identificar a fonte dos ataques, rastrear comunicações e prevenir crimes graves contra bens jurídicos coletivos.

Quando há ocorrência de um delito cibernético, é imprescindível conduzir uma investigação para reunir evidências visando um futuro processo penal. A equipe investigativa pode aplicar diversas técnicas e recursos. Da mesma forma que as pessoas possuem números de identificação, como o CPF, os dispositivos conectados à internet também possuem endereços IP únicos que simplificam a identificação dos envolvidos em atividades ilícitas. Contudo, a obtenção desses endereços IP pode ser complexa devido a barreiras burocráticas e ao uso de ferramentas que disfarçam ou ocultam esses números.

A quantidade massiva de dados gerados diariamente nos bancos de dados dos provedores de internet pode levar à impunidade devido à falta de provas e à morosidade nas investigações policiais. Isso é agravado quando crimes envolvem pessoas de diferentes países, tornando a identificação mais complexa.

Os proxies são serviços que ocultam o verdadeiro endereço IP, tornando o rastreamento mais difícil. Além disso, os ambientes públicos, como shopping centers, universidades e lan houses, apresentam desafios adicionais na identificação dos criminosos devido à grande quantidade de pessoas que utilizam as redes.

A Convenção de Budapeste representa um acordo internacional dedicado ao enfrentamento dos delitos cibernéticos e à salvaguarda contra práticas ilegais no ambiente digital. Ratificada em 2001 pelo Conselho da Europa, tal convenção estabelece diretrizes direcionadas aos Estados-membros para lidarem com crimes como fraude informática, pornografia infantil, violações de dados e outros comportamentos criminosos online. Este tratado define procedimentos para a obtenção de provas eletrônicas em situações de delitos cibernéticos. Tais procedimentos envolvem preservação de dados, busca e apreensão de sistemas de computadores, interceptação de informações em tempo real, além de outras medidas para coletar evidências. Os países que aderem à Convenção são compelidos a incorporar essas medidas em suas legislações nacionais para investigar e processar crimes cibernéticos.

A possibilidade de aplicação de medidas para obter evidência eletrônica, portanto, dependerá da natureza e da forma dos dados e do procedimento.

É fundamental assegurar eficácia na obtenção de provas em crimes cibernéticos ao dispor de uma força policial altamente especializada. Essa equipe, composta por especialistas em informática, deve possuir um conhecimento amplo das últimas tecnologias. Além disso, devem estar equipados com computadores avançados, permitindo a perícia e análise dos dados coletados, dada a especialização exigida nesse tipo de investigação (BOITEUX, 2010).

Uma estratégia chave em investigações é a "varredura sistemática", visando identificar responsáveis por diferentes delitos na internet. Embora a sensação de anonimato online facilite essa abordagem, é crucial estabelecer limites devido ao grande volume de dados gerados.

Investigadores utilizam técnicas como phishing (é uma técnica usada por criminosos para enganar as pessoas e obter informações confidenciais), vishing (é uma forma de phishing que ocorre por telefone), e impersonation (esse termo se refere à prática de se passar por outra pessoa ou entidade, seja online ou offline), para obter dados relevantes, requerendo a criação de contas fictícias para se infiltrar em grupos criminosos ou identificar suspeitos.

Outro método de investigação é o uso de fontes abertas, buscando informações disponíveis gratuitamente na internet. Isso tem se mostrado útil na identificação de membros de organizações criminosas que operam online.

Em resumo, a investigação de crimes cibernéticos requer uma abordagem multifacetada que combina tecnologia avançada, legislação apropriada e equipes de investigação capacitadas para lidar com os desafios únicos desse tipo de delito.

3.1 CYBERGAECO

O Grupo de Atuação Especial de Combate ao Crime Cibernético, conhecido como CYBERGAECO (Gaeco: Grupo de Atuação Especial de Combate ao Crime Organizado), é uma unidade especializada destinada a combater atividades criminosas no ambiente digital. Surgiu da necessidade de lidar com crimes que se desenvolveram com o avanço da tecnologia e da internet, abrangendo uma ampla gama de delitos que vão desde fraudes financeiras até a exploração infantil online.

O CYBERGAECO tem como missão principal investigar, prevenir e combater crimes cibernéticos, utilizando técnicas avançadas de investigação e colaborando com diferentes órgãos de segurança e instituições públicas e privadas. Seus objetivos incluem:

Investigação de Crimes Digitais: Analisar e investigar atividades ilegais que ocorrem na internet, como hacking, phishing, roubo de dados, entre outros.

Educação e Conscientização: Promover a conscientização sobre segurança digital por meio de campanhas educativas para o público em geral e treinamentos especializados para profissionais da área.

Cooperação Internacional: Colaborar com agências de segurança de outros países para enfrentar crimes cibernéticos transnacionais.

O CYBERGAECO geralmente é composto por especialistas em tecnologia da informação, investigadores, peritos forenses digitais, analistas de dados, entre outros profissionais altamente qualificados. A estrutura hierárquica pode variar dependendo da legislação local e do órgão ao qual está vinculado.

Suas atividades envolvem monitoramento de redes, rastreamento de atividades suspeitas, coleta de evidências digitais, análise forense de dispositivos eletrônicos, colaboração com empresas de tecnologia para identificar ameaças, entre outras ações.

O combate ao crime cibernético enfrenta desafios constantes devido à rápida evolução tecnológica e à sofisticação dos criminosos digitais. Além disso, a privacidade, a legislação internacional e a cooperação entre diferentes jurisdições são questões complexas que afetam as operações do CYBERGAECO.

Recentemente, foi instituído em Goiás, pelo ATO PGJ N. 98, DE 5 DE OUTUBRO DE 2023, a atuação especial de combato ao crime cibernético (CYBERGAECO), no âmbito do Ministério Público do Estado de Goiás, e em primeira operação do órgão, no dia 10/10/2023, o MPGO cumpriu mandados contra hacker investigado por suspeita de invasão a sistemas de órgão públicos. Foi executado um decreto de prisão preventiva e um de busca e apreensão no território de São Paulo, contra um especialista em tecnologia associado a um grupo criminoso. Este conjunto de infratores tem expertise em infiltrar-se em plataformas de informação de

entidades públicas em busca de informações privadas para depois vendê-las a organizações especializadas na coleta e comercialização de dados de usuários na web.

Essa iniciativa será aplicada em toda a extensão do Estado, colaborando em conjunto tanto com o Gaeco quanto com a Coordenadoria de Segurança Institucional e Inteligência (CSI).

Todos os promotores de Justiça que fazem parte do Gaeco atualmente farão parte do CyberGaeco, sem precisar de uma nomeação específica. Além disso, outros membros podem ser designados conforme a exigência para fazer parte dessa nova estrutura.

4 ESTRATÉGIAS DE PROTEÇÃO CONTRA DELITOS NA ESFERA DIGITAL

É crucial permanecer vigilante em relação à prevenção de potenciais questões digitais. Exemplos disso incluem manter o sistema operacional e o software atualizados, já que as atualizações costumam conter correções para evitar brechas de segurança. Usar senhas robustas é fundamental, uma vez que senhas óbvias facilitam o acesso não autorizado a informações pessoais em contas ou dispositivos. Estar alerta a emails suspeitos é imprescindível, pois muitas vezes são tentativas de invasão aos sistemas.

É importante desconfiar de mensagens que pareçam suspeitas, proteger-se contra programas maliciosos e evitar baixar arquivos de fontes não confiáveis. Realizar backups de maneira regular e manter cópias é vital para garantir a segurança das informações e conteúdos.

Ao se educar sobre segurança cibernética, as pessoas estarão mais preparadas para evitar e se defender de possíveis crimes cibernéticos que possam ser cometidos contra elas

CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo examinar os crimes cibernéticos e a complexidade da investigação por trás deles, ilustrando como o Brasil tem enfrentado essa questão ao longo do tempo. É fundamental analisar as naturezas específicas das principais atividades ilegais ocorrendo no ambiente virtual, assim como as principais estratégias empregadas para combater tais crimes.

É evidente que a legislação brasileira está lutando para manter o ritmo das inovações nos delitos praticados online, tornando-se cada vez mais necessário o desenvolvimento de leis específicas e eficazes nesse contexto.

À medida que examinamos os resultados obtidos ao longo deste estudo, fica claro o quão crucial é a investigação da temática dos crimes virtuais. O cibercrime continua a crescer exponencialmente à medida que a tecnologia e a internet se expandem e se tornam parte integrante da vida cotidiana.

Considerando a evolução contínua do mundo virtual, é imperativo que o sistema jurídico brasileiro se mantenha em constante adaptação para abranger todas as atividades criminosas que surgem nesse ambiente em constante transformação.

CYBERCRIME

ABSTRACT

In this study, we will explore the various forms of digital crimes, alongside concepts of virtual criminality and an analysis of the current laws in force in Brazil regarding this matter. However, the focus of this research lies in investigating the consequences caused by attacks on an individual's reputation and image through this global communication network, as well as the obstacles faced in punishing those responsible for such cybercrimes. The first section of the paper focuses on a brief concept of cybercrime, presenting both proper and improper cybercrimes. In the second section, improper cybercrimes will be addressed, demonstrating some crimes present in the worldwide computer network. Moving to the third section, the focus will be on investigations conducted to reach these cybercriminals. The sections of this study seek to examine related works on the subject by renowned authors in the academic field. Finally, potential solutions will be proposed for the central question of this work, concerning viable methods to prevent attacks perpetrated by digital criminals. The methodology adopted for this article encompasses theoretical aspects, drawing from books, articles, and academic papers, as well as pertinent practical cases related to the subject matter at hand.

Keywords: Cybercrimes. Internet. Legislation. Investigation. Cybercrimes.

REFERÊNCIAS

ASSUNÇÃO, Ana Paula Souza. **CRIMES VIRTUAIS**. Disponível em: <http://repositorio.aee.edu.br/bitstream/aee/538/1/Monografia%20-%20Ana%20Paula%20Souza.pdf>

ATO PGJ N. 98, DE 5 DE OUTUBRO DE 2023. Disponível em: <http://www.mpgo.mp.br/portal/atos_normas/1952>

BOITEUX, Luciana. **Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual**. Revista Brasileira de Ciências Criminais, São Paulo, v. 12, n. 47, p. 146-187, mar./abr. 2004.

BRAGA, Diego Campos Salgado. **Métodos de investigações no âmbito cibernético**. Disponível em: <https://jus.com.br/artigos/71463/metodos-de-investigacoes-no-ambito-cibernetico>

CAPEZ, Fernando Prado. **Código Penal Comentado**. São Paulo: Saraiva, 2016.

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>

CYBERBULLYING. Disponível em: <https://brasilescola.uol.com.br/sociologia/cyberbullying.htm>

DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>

EM PRIMEIRA OPERAÇÃO DO CYBERGAECO, MPGO CUMPRE MANDADOS CONTRA HACKER INVESTIGADO POR SUSPEITA DE INVASÃO A SISTEMAS DE ÓRGÃOS PÚBLICOS. Disponível em: <http://www.mpgo.mp.br/portal/noticia/em-primeira-operacao-do-cybergaeco-mpgo-cumpre-mandados-contra-hacker-investigado-por-suspeita-de-invasao-a-sistemas-de-orgaos-publicos>

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

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Código Penal Brasileiro. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 24 nov. 2023.

LEI Nº 13.718, DE 24 DE SETEMBRO DE 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm>. Acesso em 15 de setembro 2023

MILAGRE, José Antonio. Lei Azeredo, **AI-5 digital e a cultura do contra**.: Uma visão pessoal sobre o manifesto contra a Lei de Crimes de Informática. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 14, n. 2216, 26 jul. 2009. Disponível em: https://jus.com.br/artigos/13211. Acesso em: 17 nov. 2023

MP de Goiás institui Cybergaeco para enfrentamento especializado a crimes cibernéticos. Disponível em: <https://www.rotajuridica.com.br/mp-de-goias-institui-cybergaeco-para-enfrentamento-especializado-a-crimes-ciberneticos/>

NUCCI, Guilherme de Souza. **Manual de direito penal, 10° Edição**. Rio de Janeiro: Forense, 2014.

NUCCI, Guilherme de Souza. **Código Penal comentado, 14° Edição**. Rio de Janeiro: Forense, 2014.

NUCCI, Guilherme de Souza. **Código Penal comentado, 17° Edição**. Rio de Janeiro: Forense, 2017.

PANNAIN, Camila Nunes; PEZELLA, Maria Cristina. **Liberdade de expressão e *Hate Speech* na Sociedade da Informação.** Disponível em: <https://periodicos.ufsm.br/REDESG/article/view/19432/pdf>

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação - 2ª Edição.** Rio de Janeiro: Brasport, 2013.