ESTADO DE GOIÁS
SECRETARIA DE SEGURANÇA PÚBLICA
UNIVERSIDADE ESTADUAL DE GOIÁS – UEG
COORDENADORIA DE ENSINO
COORDENAÇÃO DE ENSINO PRESENCIAL DE ENSINO PRESENCIAL E DE PÓS-GRADUAÇÃO
ESPECIALIZAÇÃO EM GERENCIAMENTO EM SEGURANÇA PÚBLICA

DIEISON CÂNDIDO RIBEIRO DO CARMO

A INTELIGÊNCIA POLICIAL COMO MECANISMO DE COMBATE AOS CRIMES CIBERNÉTICOS

Goiânia-Go
2024

DIEISON CÂNDIDO RIBEIRO DO CARMO

A INTELIGÊNCIA POLICIAL COMO MECANISMO DE COMBATE AOS CRIMES CIBERNÉTICOS

Artigo Científico apresentado como exigência parcial para aprovação na disciplina de Metodologia do Trabalho Científico do Curso de Pós-Graduação em Gerenciamento em Segurança Pública, sob a orientação do Prof. Ms. Orientador Patrick Barros Barbosa.

Goiânia-Go

2024

A INTELIGÊNCIA POLICIAL COMO MECANISMO DE COMBATE AOS CRIMES CIBERNÉTICOS

Dieison Cândido Ribeiro do Carmo[1]

Patrick Barros Barbosa[2]

RESUMO

As tecnologias continuam avançando, e a internet tem desempenhado um papel revolucionário como a mais vasta biblioteca virtual acessível aos seres humanos. No entanto, essa mesma ferramenta é também explorada para atividades ilícitas por indivíduos criminosos. Crimes como extorsão, estelionato e fraudes bancárias são apenas alguns exemplos do amplo espectro dos crimes cibernéticos. Em resposta a essas ameaças, emerge o serviço de inteligência da Polícia Militar, atuando decisivamente na proteção da sociedade contra esses infratores. Este artigo propõe-se a contribuir para a prevenção e combate desses delitos, baseando-se em uma revisão bibliográfica que inclui livros, artigos científicos e sites especializados, adotando uma metodologia qualitativa. O foco desta pesquisa é explorar como o serviço de inteligência da Polícia Militar do estado de Goiás pode ser eficaz no combate aos crimes cibernéticos. Considerando cenários onde criminosos digitais comprometem a segurança financeira de indivíduos através de roubos de senha, sequestros, e extorsões exigindo transferências via PIX, a Polícia Militar tem se mostrado fundamental na prevenção, detenção e captura desses criminosos, garantindo a integridade das redes sociais e protegendo a sociedade contra tais vulnerabilidades

Palavras-chave: Violência. Roubo. Criminologia. Crime Digital. Letalidade.

ABSTRACT

Technology has reached its apex. The internet is a revolution and no one can doubt it. It is from this formidable resource that human beings have access to the largest

[1] Pós graduando em especialização em Gerenciamento em Segurança Pública pela UEG, 2024.

[2] Professor Ms e Orientador do Curso de Especialização em Gerenciamento em Segurança Pública pela UEG, 2024 Mestrado em Governança, Tecnologia e Inovação pela Universidade Católica de Brasília - UCB; MBA – Master of Business Administration em Gerenciamento de Projeto pela FGV - Fundação Getúlio Vargas; Pós-graduação, nível especialização, Segurança Pública pela Faculdade Projeção (2013); nível especialização, Direito Militar pela UNEB - União Educacional de Brasília (2007); Graduado em Administração de Empresas pela Faculdade Michelangelo (2006). E-mail: patrickraftter@gmail.com.

virtual library on the planet. The information happens in real time. However, people who are not good deviates from the good intentions that social networks can provide, using them to extort, do evil, steal, murder and other evils. It is at this moment that it is necessary to restrain these enemies of good. The Military Police, with its intelligence service, is in a position to curb cybercrimes. This is what this article set out to demonstrate in order to protect society, as it is exposed in this bibliographic research. This study in the form of a scientific article exposed that cybercrime is a reality, where hackers appropriate passwords and cause losses to credit or debit card owners. There are also the kidnappings of people to pass on under torture and threats to transfer money via PIX in a clear demonstration of extortion, which in some situations even result in some homicides. The importance of the Military Police has proven to be fundamental in preventing, curbing and arresting these types of criminals in times of social networks so that they do not continue to be vulnerable.

Palavras-chave: Violence. Theft. Criminology. Digital Crime. Lethality.

1. INTRODUÇÃO

O desenvolvimento tecnológico e da sociedade tornou mais manifesto a função da informação como uma marca da atividade humana. Nesses tempos modernos conhecido como a sociedade da informação, distintos expedientes da tecnologia são utilizados para o armazenamento e veiculação de informações e dados.

No atual panorama de crescente diversidade e complexidade dos delitos, incluindo os crimes cibernéticos, a Polícia Militar encara desafios cada vez mais complexos. A evolução tecnológica, embora tenha trazido benefícios significativos à sociedade em termos de comunicação rápida e acesso à informação, também trouxe consigo uma série de problemas destacado-se a invasão de privacidade em várias plataformas online como contas bancárias e-mails e redes sociais como Facebook e Instagram.

Esses desafios exigem que a instituição policial adote uma abordagem cada vez mais estratégica e baseada em inteligência para conter a criminalidade, especialmente no que se refere aos hackers e outras formas de cibercriminosos.

Esse aspecto, essencial para compreender e abordar a problemática em questão demanda uma análise detalhada das estratégias tecnológicas e práticas que podem ser adotadas pela polícia para enfrentar essa crescente ameaça à segurança digital e à ordem pública.

Portanto, no contexto da escrita científica em formato de artigo, é crucial explorar e discutir as potenciais abordagens da inteligência policial nesse domínio,

considerando tanto aspectos teóricos quanto práticos a fim de fornecer *insigths* e orientações relevantes para políticas públicas e práticas policiais voltadas à mitigação dos crimes cibernéticos.

Para realizar esta pesquisa, na qual foram coletados dados por meio de revisão bibliográfica, questionou-se se a inteligência policial poderia ser eficaz no combate aos crimes cibernéticos.

Do ponto de vista das hipóteses, levando-se em conta a ampla gama de abordagens adotadas pelas instituições policiais, que incluem a prevenção, o combate, a investigação e o confronto, a inteligência policial emerge como um mecanismo crucial no enfrentamento dos crimes cibernéticos. Ao empregar estratégias de inteligência, é viável não apenas evitar a ocorrência do crime, mas também elucidá-lo quando necessário.

Nesse contexto, a Polícia Militar tem buscado acompanhar as atualizações informáticas a fim de coibir os delitos cibernéticos.

Uma das abordagens eficazes para combater o crime cibernético é a utilização da vigilância e monitoramento proporcionados pela inteligência policial. Além disso, a adoção de técnicas como a inserção de um policial disfarçado, operando com um perfil falso, representa outra ferramenta valiosa neste contexto.

As hipóteses que deram sentido a essa pesquisa de cunho bibliográfico, na hipótese de número 1 considerou que a utilização da inteligência policial (P2) pode aprimorar a identificação e monitoramento de atividades suspeitas online, possibilitando a detecção precoce de potenciais crimes cibernéticos, como invasões a sistemas bancários e roubo de informações pessoais.

Na hipótese de número 2, levou-se em conta que a integração da inteligência policial com tecnologias de análise de dados pode permitir a identificação de padrões de comportamento criminoso e a construção de perfis de criminosos digitais, facilitando a investigação e a captura desses indivíduos.

E em terceiro colocado, a hipótese 3, a qual aponta que a cooperação entre a inteligência policial e órgãos de segurança cibernética pode resultar em uma abordagem mais eficaz na prevenção e combate aos crimes digitais, permitindo uma resposta mais rápida e coordenada diante de ameaças emergentes na esfera virtual.

Quanto às justificativas para ter desenvolvido esse artigo, no atual cenário de aumento dos crimes digitais, a sociedade enfrenta crescente insegurança. Quadrilhas especializadas desenvolvem constantemente novas técnicas de fraude,

incluindo invasões a senhas bancárias, roubo de dados pessoais e corporativos, além de desvio de recursos financeiros.

A rápida disseminação e processamento em tempo real das informações facilitam a ação dos criminosos, que se especializam na invasão de sistemas e na organização de encontros para sequestros em ambientes propícios.

Este quadro é exacerbado pelo acesso não autorizado a informações confidenciais de entidades públicas e privadas, o que exige a implementação de atividades constantes de monitoramento e vigilância como medidas de prevenção ou repressão contra essas práticas ilícitas. É crucial deter esses grupos criminosos.

No que se refere aos objetivos desse estudo de pesquisa bibliográfica, o geral analisou a inteligência policial na prevenção e combate aos crimes cibernéticos.

Especificamente buscou conhecer que o analisar e compreender os diferentes tipos de crime cibernético, levando-se em conta as suas características, modalidades e impactos na sociedade contemporânea, constituem possibilidades para obter o conhecimento sobre essa forma de delinquência digital?

Em seguida buscou investigar os métodos e técnicas utilizados pelos hackers para invadir sistemas de informações, explorando suas motivações, ferramentas e vulnerabilidades exploradas, com o intuito de identificar os pontos críticos e desenvolver medidas preventivas e repressivas mais eficazes.

No item 3, verificou-se a possibilidade de proporcionar uma análise das estratégias específicas utilizadas pela inteligência policial no combate aos hackers e outros agentes de crimes cibernéticos. Esse estudo se destaca quando houve pessoas que solicitou tirar uma foto

Esse trabalho de pesquisa pode ser identificada quanto à sua abordagem como (mista) quantitativa e qualitativa, quanto aos fins como descritivo, quanto aos meios como investigação como bibliográfica Moresi (2003) *apud* Barbosa (2022). Deste modo, a procura de informações em uma revisão literária com o emprego de estratégias de busca, de ordens, tanto primária como secundária (MARCONI & LAKATOS, 2003).

Nas buscas primárias foi feito um levantamento bibliográfico e uma busca ativa nas bases de dados Scielo, Portal Capes utilizando-se dos seguintes descritores: Violência. Roubo. Criminologia. Crime Digital. Letalidade. No que se refere a busca secundária foram utilizadas outras fontes, do tipo, revistas científicas especializadas, periódicos associados à temática (GIL, 2002).

Foram atendidos os critérios de inclusão, artigos publicados nos idiomas português e inglês que estivesse relacionado com o tema de “Crime Cibernético”. Portanto, foi utilizada a bibliográfica onde se buscou dados em periódicos e artigos, busca na internet em diferentes sites.

Ao se considerar o aumento da sofisticação desses delitos e pelas dificuldades no combate, pois a cada dia são criados novos golpes para essa modalidade é que veio justificar a elaboração desse artigo, conferindo maior importância a esse estudo, devido aos benefícios e proteção junto a sociedade como um todo a partir da atuação da Polícia Militar, uma instituição habilitada para enfrentar o crime cibernético, sobretudo nos casos graves como o sequestro em momentos de transferências e pagamentos por ferramentas como o Pix.

2 CRIMES CIBERNÉTICOS E SEGURANÇA PÚBLICA

2.1 Histórico dos crimes cibernéticos

Na década de 1960, a tecnologia da informação, precursora da internet, iniciou seu processo de integração gradual à sociedade. Ao longo do tempo, essa integração se consolidou e se aprimorou, destacando-se especialmente na década de 1980, quando a internet se transformou em um canal de comunicação acessível a todas as pessoas. Esse avanço abriu caminho para uma ampla variedade de atividades, que vão desde comunicações comerciais até interações sociais, entretenimento, educação e acesso a notícias (TEIXEIRA, 2002).

No entanto, juntamente com esses benefícios, surgiram os crimes cibernéticos. O que inicialmente era uma ferramenta para o bem e o progresso social acabou sendo explorado por indivíduos mal-intencionados. A rapidez do desenvolvimento tecnológico e a disseminação da internet levaram à proliferação de crimes que podiam ser cometidos anonimamente por trás de uma tela de computador.

Gustavo Testa Corrêa (2002) define os crimes de informática como aqueles com o uso indevido de utilização fraudulenta de informações armazenadas ou trânsito por meio de computadores. Sendo necessários dois elementos essenciais para a caracterização do crime: que atentem contra os dados armazenados e que seja executado por computadores, envolvendo tanto software quanto hardware.

Já o Tarcísio Teixeira (2014) destaca duas modalidades de crime de informática, a primeira se referindo a atos diretos contra o sistema de informática, desde os danos físicos ou componentes do computador, até alterações não autorizadas em dados ou programas. Já a segunda modalidade, chamada de crimes de informática impróprios, engloba delitos que se valem da informática como meio para sua execução. Aqui está incluídos uma variedade de crimes, como estelionato, calúnia, violação de privacidade e direitos autorais, entre outros, em que a tecnologia é utilizada como ferramenta para cometer o delito (TEIXEIRA, 2014, p. 368).

Percebemos uma rápida e significativa evolução nos crimes envolvendo tecnologia, uma inteligência em constante mutação, atualização e expansão. Essa dinâmica nos confronta com desafios desconhecidos, exigindo que aprendamos rapidamente sobre informações que indivíduos mal-intencionados utilizam para cometer crimes.

2.2 O que é crime cibernético

Crime cibernético, também conhecido como cibercrime, é toda atividade criminosa que envolve a utilização de computadores, redes de computadores ou dispositivos eletrônicos conectados à internet. Esses delitos abrangem uma variedade de práticas, como *hacking*, fraudes online, *phishing*, roubo de identidade, ataques de *malware*, pornografia infantil, assédio online, entre outros (TEIXEIRA, 2014).

Os objetivos dos criminosos cibernéticos podem ser diversos, desde o roubo de informações pessoais e financeiras até a interrupção de serviços essenciais ou a propagação de desinformação. A investigação e prevenção do cibercrime são desafiadoras devido à sua natureza altamente técnica e transnacional TEIXEIRA, 2014).

2.3 A investigação no ciberespaço

Os crimes informáticos se destacam dos demais devido a uma característica peculiar: são cometidos por meio do uso de tecnologia moderna. O ciberespaço representa o ambiente virtual onde se desenrolam as comunicações e a troca de

informações. É a representação e a interação entre a sociedade e as tecnologias da comunicação, informação e cultura. Nesse desse contexto, estão incluídos espaços onde a tecnologia é amplamente concentrada, tais como a internet, e-mails, redes sociais, blogs, entre outras plataformas digitais.

Nossa legislação foi elaborada antes da transformação da internet, sem considerar a extensão que a rede mundial de computadores alcançaria e as consequências que traria para o mundo moderno, dificultando a investigação no ciberespaço.

A abordagem para investigar essa forma de crime está em constante evolução, adaptando-se continuamente às mudanças. Inicialmente centrada em disquetes, evoluiu para incluir a análise de dados em uma variedade de plataformas, como sistemas de computação em nuvem, redes sociais, smartphones, pen drives, arquivos de áudio, e outros. Atualmente, a tecnologia permite formas altamente intrusivas de invasão da privacidade das pessoas sujeitas a investigações policiais, através de programas espiões, conhecidos como trojans, que monitoram tanto o fluxo quanto o conteúdo das comunicações em sistemas informáticos e telemáticos.

Principal preocupação social relacionada ao mundo cibernético reside na vigilância indiscriminada e sem critérios definidos - uma situação em que não há identificação do vigia nem explicação clara para a vigilância. Isso pode ser utilizado por entidades com o propósito, por exemplo, de categorizar as pessoas de maneira injusta.

A vigilância, antes considerada excepcional, tornou-se parte do cotidiano, abrangendo não apenas grupos específicos, mas toda a população em geral. Ela deixou de ser limitada ao âmbito nacional para abranger o mundo global e dinâmico. Os indivíduos já não desfrutam do anonimato; estão constantemente expostos. A digitalização de imagens e o uso de técnicas de reconhecimento facial permitem identificar e rastrear indivíduos em meio à multidão. Por meio do data mining, uma busca incessante por informações sobre o comportamento de indivíduos, são gerados perfis individuais, familiares, territoriais e grupais de forma contínua. A vigilância transcende fronteiras (PINHEIRO, 2016).

Conforme mencionado por Alexandre Jean Daoun (1999), os avanços da modernidade e a rapidez proporcionados pela internet global também resultam na ocorrência de crimes que não só confundem as vítimas, mas também desafiam as autoridades responsáveis pela aplicação da lei.

As investigações no ciberespaço frequentemente enfrentam desafios devido à ampla gama de opções disponíveis e à falta de controle que as vítimas muitas vezes têm sobre seus dados. A fragilidade da segurança cibernética permite que os criminosos tenham fácil acesso a informações que deveriam ser confidenciais, como dados pessoais, bancários, fotos privadas, documentos de trabalho, entre outros.

As alterações acontecem invariavelmente, modificando intensamente a vida da coletividade (ASSMANN, 2000), forçando a transformações na conduta do recebimento de notícias que, conforme Carandina (2021), com os recursos tecnológicos sendo incorporados às técnicas sociais. Registra-se um local de intercâmbio sobre a infraestrutura técnica da rede mundial da informação (internet), que possibilita que diversas pessoas, utilizando de distintos recursos, a saber, computadores, *Smartphones*, *Smart Tvs*, e outros dispositivos, possam se comunicar em um ambiente virtual. Nestes recintos acontecem interações pessoais negócios, fruto das relações que os indivíduos travam nas redes sociais, disponíveis 24 horas.

Estas informações estão em fluxo ou registradas em aparelhos, constituem um recurso precioso e essa situação leva ao surgimento de ações que fere a moral ou se enquadram no quadro de situações criminosas nestes espaços, por exemplo, os ataques de hackers, que de modo atrevido invadem sistemas e chegam a informações de órgãos públicos e particulares (CANONGIA; MANDARINO JÚNIOR, 2010).

É importante apontar que a demarcação entre a monitoração e a investigação pode ser imperceptível. Deste modo, ações de monitoração e vigilância, tomadas como formato de cautela ou luta contra crimes nestes recintos, podem ser encaradas como passaporte para atividades ilícitas ou antiéticas.

Atualmente, a criminalidade vem aumentando e gerando sensação de insegurança por parte da população. Nesse viés, se faz necessário o estudo da criminologia e políticas criminais, de forma avançada, pelo profissional responsável pela segurança pública, objetivando a redução nos índices criminais, seja examinando padrões comportamentais ou criando estratégias para coibir atividades criminosas e, consequentemente, tornando o policial mais capacitado (MARTINS, 2014).

Para Choo (2003), a notícia é um componente fundamental para as ações do ser humano, sejam elas do domínio pessoal, sejam parte de procedimentos

organizacionais. O exercer atividades corresponde, na maioria das vezes, a necessidade de informações que norteiem estas mesmas ações. A notícia é, deste modo, um incentivo admirável para as pessoas.

Santos *et al.* (2021) e Silva e Razzolini Filho (2020) destacam que a função que a informação apresenta nos processos decisórios de organizações, em seus variados panoramas.

A necessidade do estudo da criminologia e políticas criminais na atuação policial se torna necessário em função da alta taxa de crimes que tem ocorrido no Brasil. A criminologia tem o objetivo de analisar e entender o crime, intervir na pessoa do criminoso e da vítima, e estudar os aspectos que envolvem a criminalidade, com exclusividade, o crime cibernético (CARANDINA, 2021).

Prontamente o Policial Militar poderá compreender melhor a importância ou não de determinadas medidas preventivas, por exemplo, o aumento do policiamento ostensivo visando a redução nos índices de criminalidade.

2.4 A infiltração policial na investigação de cibercrime

A internet que já foi um ambiente inexplorado, hoje abriga uma vasta parcela da população global. Isso nos leva a questionar: deveriam as normas processuais ser aplicadas ao ambiente virtual, onde frequentemente o adversário é invisível? A necessidade de ação policial técnica no ciberespaço se torna essencial devido ao aumento de atividades criminosas online.

Historicamente, a infiltração como método de obtenção de provas foi primeiramente regulamentada pela Lei 9.034/95, destinada à prevenção e repressão de atos de organizações criminosas. Esta lei, contudo, era genérica e não detalhava procedimentos específicos de aplicação, sendo frequentemente mencionada junto à legislação sobre drogas e ao Estatuto da Criança e do Adolescente.

Em 2013, a introdução da Lei 12.850/13 marcou uma evolução significativa ao preencher lacunas legislativas e revogar a legislação anterior. O artigo 10, parágrafo 2º da nova lei estipula que a infiltração só será permitida se houver indícios de infrações penais severas e quando não for possível produzir prova através de outros meios.

Essa medida é considerada excepcional, restrita a crimes cometidos por organizações criminosas e aplicável somente quando outras formas de obtenção de

prova falham. O artigo 10 também determina que qualquer infiltração de agentes policiais em investigações deve ser autorizada judicialmente de forma detalhada, motivada e confidencial, estabelecendo limites claros para a operação.

A legislação requer que tanto o delegado quanto o juiz envolvidos representem a operação, com consultas obrigatórias ao Ministério Público. O prazo para a infiltração é de seis meses, renovável. Após esse período, um relatório detalhado deve ser apresentado. Notavelmente, a lei admite agentes infiltrados virtuais, especificando detalhes como datas, horários, duração e endereços de IP utilizados.

O parágrafo único reforça o sigilo das operações, limitando o acesso aos autos a figuras chave como o juiz, o Ministério Público e o delegado responsável, até a conclusão da operação. Essa abordagem é vital para proteger a integridade da investigações e a segurança dos agentes envolvidos, especialmente em um ambiente tão fluído e expansivo quanto a internet.

2.5 Segurança pública

A questão da segurança pública no Brasil é preocupante em função do aumento da criminalidade, enfim, da violência, o que exige mais ainda dos trabalhadores responsáveis pela segurança pública. Nesse estudo, as policias tem contato cada vez mais com as ciências para a efetivação de seu trabalho, trazendo maiores benefícios no serviço prestado à população (MARTINS, 2014).

E ao mencionar segurança pública, importante se faz também indicar os tipos de situações que promovem grande preocupação na sociedade, ou seja, aquelas infrações penais com maior incidência como, por exemplo, o roubo, o furto, o homicídio, as agressões físicas, os conflitos entre as pessoas, o stress no trânsito e outras situações que requerem grande dedicação dos policiais responsáveis pela ordem pública, tão comum hoje em dia na sociedade brasileira marcada pela violência.

Percebe-se que o aumento da violência no Brasil é preocupante, pois além dos crimes já existentes, tem-se verificado novos tipos de golpes como os crimes cibernéticos

2.6 A criminalidade

O crime, dentro da Ciência Jurídica, é visto por diversos aspectos, dentre os principais, sob o aspecto formal, material e analítico, desse último, deriva-se a teoria mais aceita atualmente acerca do crime, que o define no conceito tripartido como fato típico, antijurídico e culpável, os dois primeiros componentes são explicados a seguir pelo autor abaixo:

> Fato típico é o comportamento humano (positivo ou negativo) que provoca, em regra, um resultado, e é previsto como infração penal. Assim, se *A* mata *B* em comportamento voluntário, pratica o fato típico descrito no art. 121 do CP (matar alguém) e, em princípio, um crime de homicídio. Fato antijurídico é aquele que contraria o ordenamento jurídico. No Direito Penal, a antijuridicidade é a relação de contrariedade entre o fato típico praticado e o ordenamento jurídico. Se em princípio for injurídico o fato típico, não será contrário ao direito quando estiver protegido pela própria lei penal. Exemplificando: matar alguém é fato típico se o agente o fez dolosa ou culposamente, mas não será antijurídico se o agente praticar a conduta em estado de necessidade, em legítima defesa etc. Não há, nessas hipóteses, crime. A *culpabilidade,* tida como componente do crime pelos doutrinadores causalistas, é conceituada pela teoria finalista da ação como a reprovação da ordem jurídica em face de estar ligado o homem a um fato típico e antijurídico (MIRABETTE, 2008, p. 84-85).

O último, a culpabilidade relaciona o agente ao fato, analisando sua subjetividade. Simplificando, se a prática do fato foi reprovável perante a sociedade. São elementos da culpabilidade: a possibilidade de conhecimento do ilícito, a exigibilidade de conduta diversa e a imputabilidade.

Os dois primeiros se referem, respectivamente, ao poder de compreensão do fato como crime e; à possibilidade do agente ter agido de forma diferente.

2.7 Conceito de violência

Para Machado; Gonçalves (2012), a palavra violência é oriunda do termo latim “violentia” e que significa força e vigor e, em sentido geral significa todo e qualquer comportamento, sendo também identificado como a utilização em excesso do emprego da força.

A violência se apresenta de diferentes maneiras ou formas, como os psicopatas e que também representam grande perigo para a sociedade e maior

esforço e dedicação dos policiais, como se pode verificar no item seguinte (CARANDINA, 2021).

Além de inúmeros crimes que o policial militar enfrenta para solucionar, há ainda os crimes bárbaros praticados por psicopatas. É recomendado expor sobre esse tipo de criminoso, pois é um sujeito que causa muito trabalho ao policial militar e traz grande risco à sociedade (MACHADO; GONÇALVES, 2012).

De acordo com essa contextualização, se pode notar que a prática de trabalho do policial militar é repleta de surpresas que implica em riscos à sua vida como é o caso de ter que enfrentar indivíduos que surtam os quais poderão a qualquer momento partir para a agressão.

2.8 O que é criminologia?

A criminologia determina a prática de trabalho do policial, uma vez que esse profissional depara com diferentes tipos de crimes, tendo que enfrentar o criminoso ou aquele que comete pequenos delitos, bem como o marginal contumaz. A atuação é proporcional ao tipo de criminoso que enfrenta, ou seja, aquele bandido perigoso exige maior cautela em sua abordagem e preparo, por vezes necessitando de apoio operacional e especializado, pois o que está em jogo é a segurança pública e a própria vida do policial militar (MACHADO, 2012).

Por outro lado, a polícia militar tem o compromisso de zelar pelo controle da violência e crimes na sociedade, portanto, realiza o seu trabalho com empenho, ética e proteção à sociedade (SILVA, 2009).

Verifica-se que é de grande importância estudar as ciências criminais, uma vez que tendo conhecimento de causa, concorre para promover a redução dos índices de criminalidade e prevenção de crimes. Ademais, esta pesquisa se busca conhecer que o estudo da criminologia e políticas criminais é essencial para a atuação policial com a proposta de reduzir a alta taxa de crimes que tem ocorrido no Brasil principalmente os crimes cibernéticos que tem aumentado muito nos últimos anos (MARTINS, 2014).

A criminologia deverá intervir na pessoa do criminoso e da vítima, e estudar os aspectos que envolvem a criminalidade para que o criminoso seja enquadrado no tipo de crime cometido para em seguida ser submetido ao cumprimento da pena (MIRABETE, 2008).

Se pode apontar que os crimes são inúmeros de diferente natureza. No caso em estudo, o foco é o crime digital ou cibernético, uma prática criminosa que tem aumentado de forma desproporcional, existindo hackers que se especializa em invadir senhas ou contas realizando roubos significativos, inclusive a extorsão de moedas digitais, criptomoedas.

2.9 O que é crime cibernético?

O avanço científico se ampliou de modo muito rápido, principalmente com o advento da internet, com a comunicação ocorrendo em tempo real. Na sociedade da informação, inúmeros recursos tecnológicos são aplicados tanto para armazenar como para a transmissão de dados. Tais mudanças acontecem através dos recursos tecnológicos e também pelos recursos incorporados às práticas sociais (CARANDINA, 2021).

Assim, configura-se um espaço de interação através da infraestrutura técnica da internet, que permite que diversas pessoas, utilizando uma variedade de recursos ou dispositivos, como os vários dispositivos disponibilizados no mercado possam manter interações sociais em um ambiente virtual. Dentro desse ambiente, é possível realizar atividades como negociações comerciais, troca de informações, lazer, jogos, entre outros, com os usuários operando seus dispositivos por meio de senhas (CANONGIA, MANARINO JÚNIOR, 2010)..

No entanto, a crescente necessidade de segurança das senhas é destacada devido aos ataques realizados por hackers, que visam acessar informações tanto de órgãos públicos quanto de empresas privada.

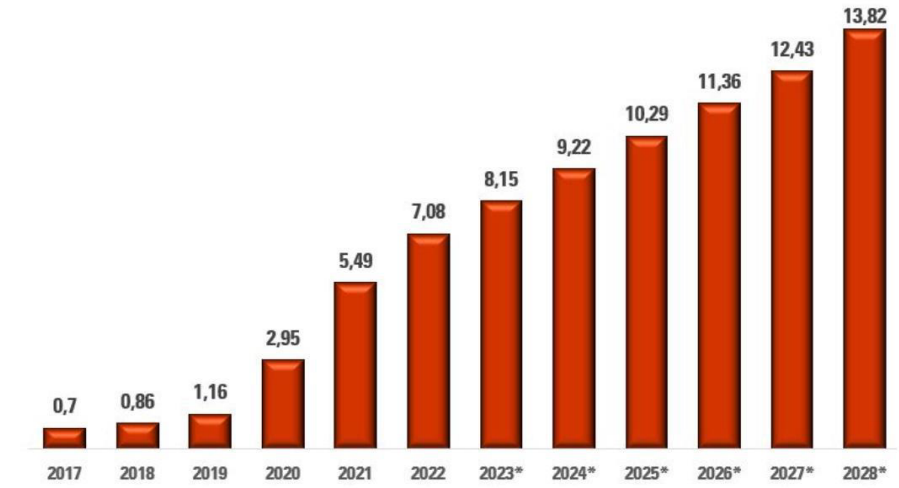
Cada vez mais se faz necessário que as autoridades de segurança da polícia apliquem meios de proteger e identificar os invasores de contas, monitorando e espionando possíveis criminosos do sistema virtual (VAN DIJCK, 2017).

Desse modo, as atividades de monitoração e vigilância exigem meios de prevenção ou combate como estratégia de combate os crimes cibernéticos nestes ambientes.

Custo estimado dos crimes cibernéticos no mundo de de 2017 com estimativa de 2028 e seus gastos.

Gráfico 1 – Crimes Cibernéticos

Custo Estimado dos Crimes Cibernéticos no Mundo 2017-2028
Trilhões US Dólares



Fonte: Statista e Banco Mundial.

A tabela abaixo revela que algumas economias com avançado desenvolvimento tecnológico e importância geopolítica estão aquém do esperado em segurança cibernética. Entre 176 países avaliados, o Brasil ocupa a 71ª posição. Isso se deve à supervisão ineficaz dos provedores de serviços digitais, à falta de um plano de gestão para incidentes cibernéticos de grande escala e à baixa participação em acordos de segurança cibernética internacionais.

Tabela 1 – Índice Nacional de Segurança Cibernética

POSIÇÃO	PAÍS	ÍNDICE NACIONAL DE SEGURANÇA CIBERNÉTICA
1º	Bélgica	94.81
5º	Alemanha	90.91
9º	Reino Unido	89,61
15º	França	84,42
30º	Rússia	71,43
45º	Estados unidos	64,94
54º	Índia	59,74
56º	Uruguay	59,74
71º	Brasil	51,95
72º	China	51,95
95º	África do Sul	36,36

Fonte: NCSI - National Cyber Security Index

3 Investigação e/ou monitoramento da informação do ambiente virtual

O monitoramento informativo é uma prática necessária por permitir às organizações a atingirem seus objetivos. Desse modo, a informação demanda uma vigilância em distintos modos, seja ele político; econômico; tecnológico; ambiental; legal e; f) informacional. Investigar os diferentes ambientes em que a informação percorre impede ameaças desnecessárias, nas decisões uma pessoa, como também nas decisões do ambiente organizacional que se apresentam com maior complexidade (RAZZOLINI FILHO, 2020).

Dando continuidade ao processo de monitoramento de dados, Razzolini Filho (2020) afirma que com o avanço dos recursos tecnológicos e os distintos modos de interação possibilitada por esses mecanismos, se tem verificado um excesso de informação orbitando em diversos recintos. Diante das novidades tecnológicas e alterações no comportamento das pessoas no que se refere ao uso de tais mecanismos é verificado um aumento contínuo do número de indivíduos e a propagação de dados em grupos virtuais, e as atitudes neste espaço, mesmo contra as leis, podem prejudicar as empresas.

Desse modo, é inteligível que existam processos de monitoração para agenciar ou resguardar os negócios de organizações, sendo fundamental para as empresas policiar o curso de dados provocado no ambiente virtual, na busca de novas estratégias de competitividade (HOFFMANN, 2011).

Avaliando a questão na iniciativa pública, de acordo com Damião (2018), ocorre a questão dos crimes que podem acontecer nesse ambiente virtual em função das vulnerabilidades em existentes nos equipamentos e redes ou às práticas ilícitas nestes locais, os quais têm causado polêmicas, principalmente quando estão relacionados com o racismo, o ódio, a pedofilia, desvios de dados e ainda, a formação de quadrilhas ou organizações criminosas para o cometimento de crimes dessa natureza.

Estas inquietações também induziram à prática em vigiar os dados que orbitam nesse ambiente, condição em que um usuário pode vir a se tornar vítima ou protagonista de um delito (LIMA, 2020). A monitoração é sempre exigida e encontra barreiras nessa modalidade de crimes cibernéticos.

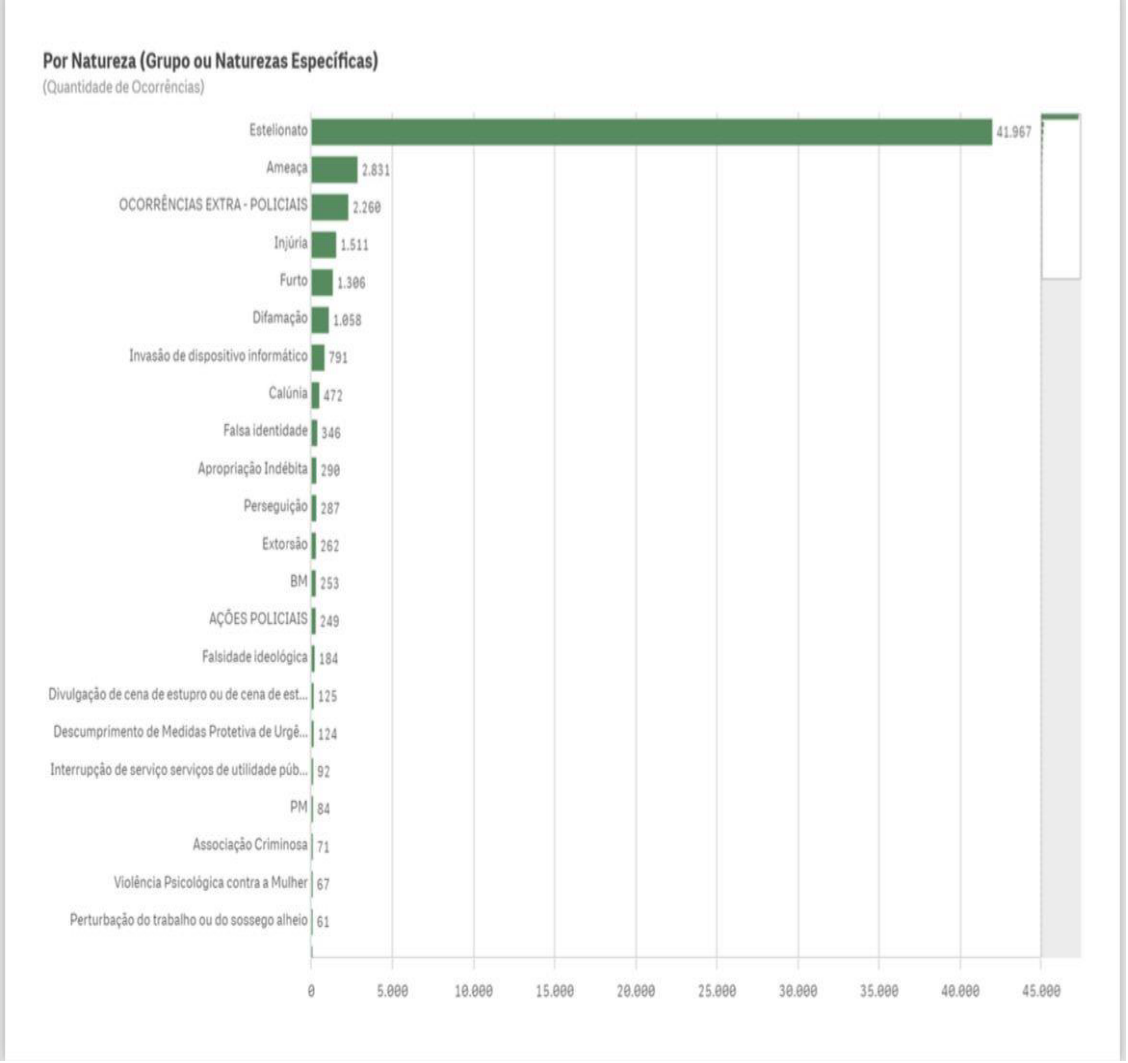
Tais impedimentos esbarram na esfera jurídica por estas não estarem ainda atualizadas em termos de leis para coibirem e punirem os autores que fraudam o espaço cibernético, tornando sem efeito a investigação (GOULART, 2021).

Diferentes técnicas têm sido utilizadas nos processos investigativos alcançando bons resultados nessa modalidade de crimes. Uma dessas técnicas é o policial que fica disfarçado, utilizando um perfil falso (GOULART, 2021). Interessante é o fato de ao adotar essa postura se poderá adotar um posicionamento de usuário que poderá assumir diferentes identidades em busca de resultados positivos.

Nessa perspectiva, existem processos de monitoração fidedignos trazidos por empresas com a intenção de proteger seus interesses no ciberespaço, monitorando as plataformas visando prevenir como incriminar os fraudadores.

Abaixo o quantitativo de crimes em AMBIENTE VIRTUAL INTERNET e LOCAL ESPECÍFICO = AMBIENTE VIRTUAL INTERNET, do Estado de Goiás registrado pela Policia Militar no sistema de segurança pública – painel estratégico Q-link sense, com crimes em geral e os registrados em invasão de dispositivos informativos nos anos de 2022 2023 e até Abril de 2024, mostrando que existe uma crescente em tais naturezas criminais.

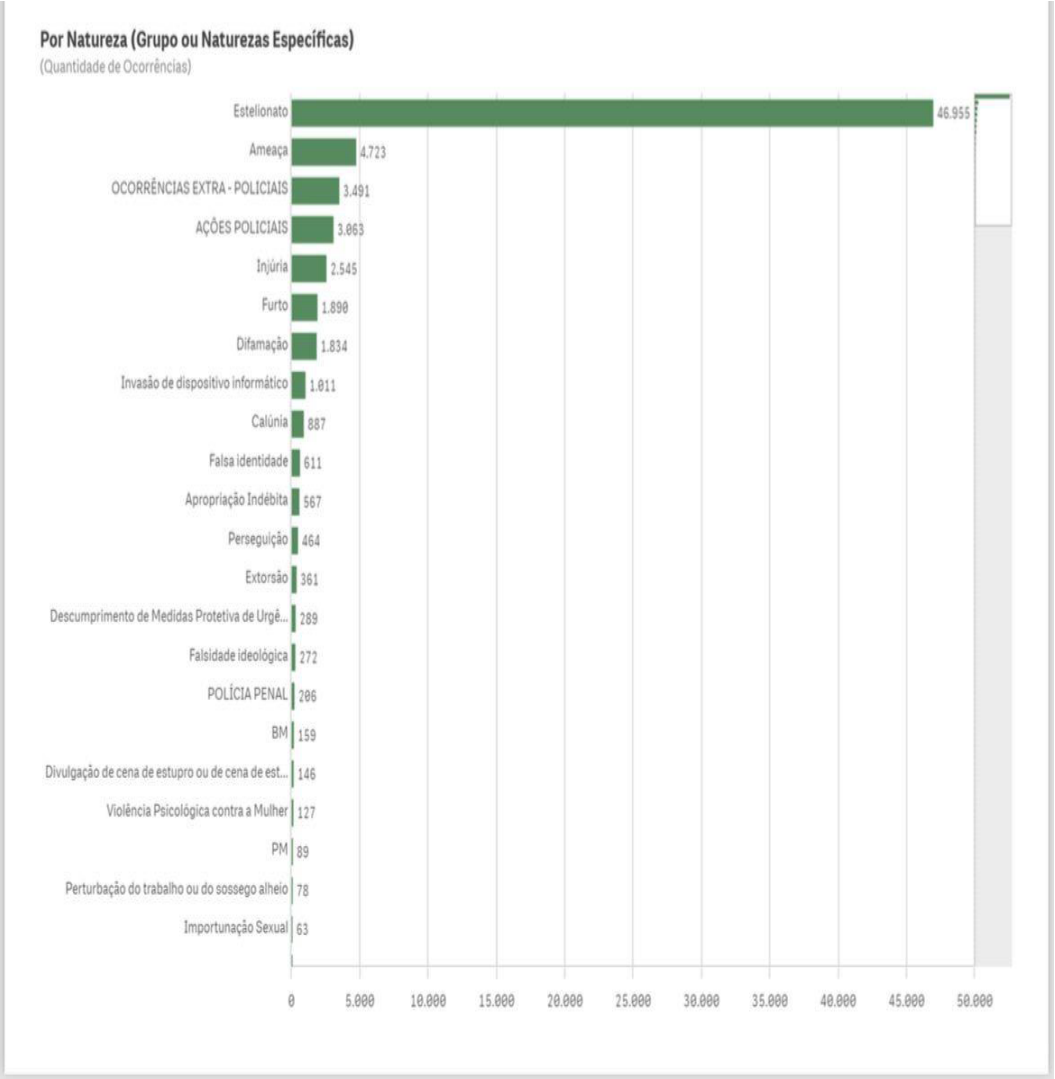
Figura 1 – Quantidade de crimes por natureza



Fonte: Site Q-Link sense – Secretária de Segurança Pública ano de 2022

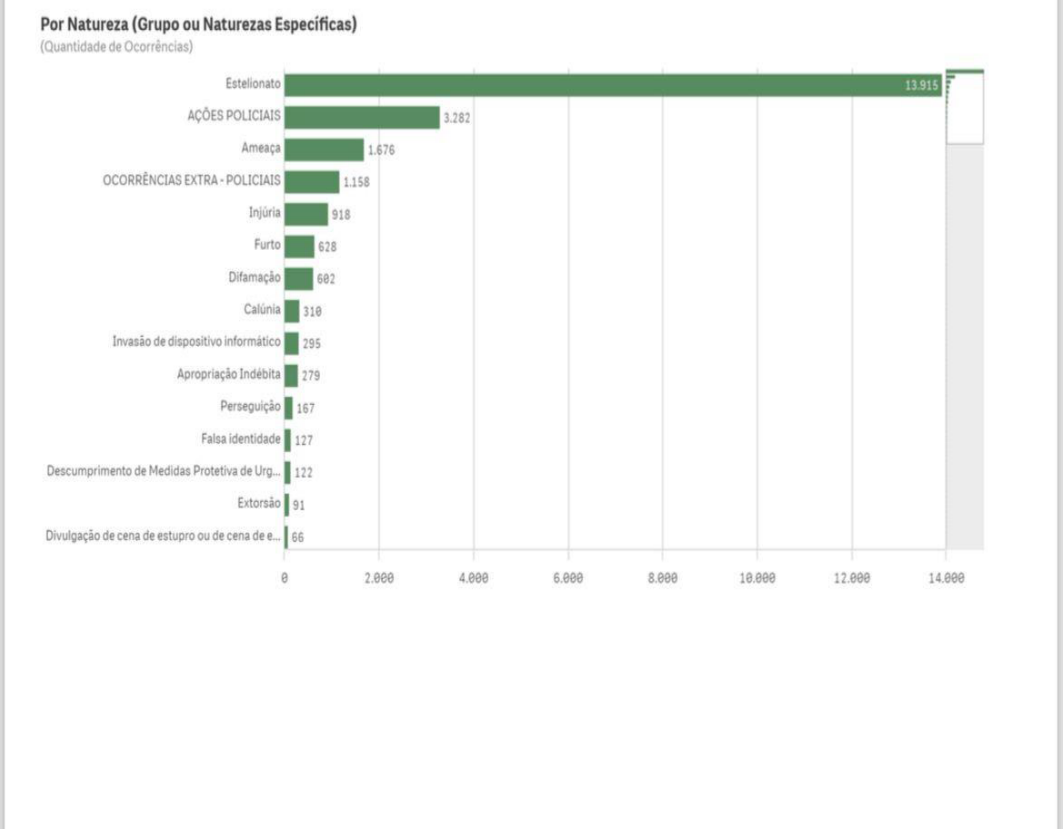
.

Figura 2 – Quantidade de crimes por natureza



Fonte: Site Q-Link sense – Secretária de Segurança Pública ano de 2023

Figura 3 – Quantidade de crimes por natureza



Fonte: Site Q-Link sense – Secretária de Segurança Pública ano de 2024 até Abril.

4 CONCLUSÃO

Respondendo às hipóteses de número 1, verificou-se que A partir da utilização da inteligência policial (P2) é possível aprimorar a identificação e monitoramento de atividades suspeitas online, o que permitirá a detecção bem antes do tempo cronometrado de potenciais crimes cibernéticos, tais como, invasões a

sistemas bancários e roubo de informações pessoais. Essa resposta responde a hipótese 1 com a conclusão que se mostrou verdadeira.

Quanto à hipótese 2, mencionou que a integração da inteligência policial com tecnologias de análise de dados leva à identificação de padrões de comportamento criminoso e a edificação de perfis de criminosos digitais, contribuindo para a investigação e a prisão desses meliantes. Sendo assim, se pode apontar que tal hipótese de número 2 é verdadeira.

Com relação à hipótese de número 3 que dispôs que a cooperação entre a inteligência policial e órgãos de segurança cibernética pode resultar em uma abordagem mais eficaz na prevenção e combate aos crimes digitais, permitindo uma resposta mais rápida e coordenada diante de ameaças emergentes na esfera virtual, colocação essa que procede, uma vez que a vinculação entre as policias e o serviço de inteligência, já conhecido e aprovado pela sociedade, faz com que provoque nas pessoas certa segurança. Portanto se pode apontar que essa hipótese também é verdadeira.

Em resposta ao 2.4 a pergunta de que deveriam as normas processuais ser aplicada ao ambiente virtual, a resposta é sim! Devemos adaptar as mudanças e as novas formas de ataques e mudanças na internet, qualificando profissionais de inteligências para atuações virtuais.

Os objetivos foram atendidos uma vez que a inteligência policial se mostrou eficaz à prevenção e combate aos crimes cibernéticos.

Especificamente, analisou e buscou compreender os diferentes tipos de crime cibernético em suas modalidades e impactos com a proposta de aprofundar o conhecimento sobre os crimes digitais.

Foi possível também investigar os métodos e técnicas utilizados pelos hackers para invadir sistemas de informações tendo sido identificado os pontos críticos para em seguida desenvolver medidas preventivas e repressivas mais contundentes.

Verificou-se também que foi possível proporcionar uma análise das estratégias específicas aplicadas pela inteligência policial no combate aos hackers e outros agentes de crimes cibernéticos. Tal eficácia se deveu à utilização de tecnologias de monitoramento, análise de dados e cooperação internacional, com vistas a fortalecer as capacidades de resposta e prevenção desses.

Em conclusão, é preciso concordar com a importância da Polícia Militar que tem se mostrado fundamental para prevenir, frear e prender criminosos numa clara demonstração de proteção à sociedade.

A inteligência policial têm se aprimorado na prevenção e combate a esses crimes. É essencial aumentar os investimentos para alcançar respostas mais ágeis e melhorar a qualificação dos profissionais, dada a natureza mutável desses delitos e o limitado conhecimento da sociedade sobre o assunto. Embora haja uma expectativa de resultados, muitas vezes falta compreensão sobre como esses crimes ocorrem e como podem ser evitados.

Portanto, é crucial encontrar maneiras de conscientizar as pessoas sobre a importância de protegerem seus dados. O que causa preocupação é o fato de a maioria das pessoas adotam comportamentos que facilitam a ação dos criminosos. Esses estão sempre atentos para cometerem crimes, bastando que as pessoas fiquem vulneráveis, cliquem em sites armados pelos hackers, os quais se apropriam das informações e se apropriam de dados e vantagens financeiras de maneira ilícita, complicando a vida das pessoas.

É nesse quadro de assalto às informações das pessoas que ganha importância a prática de trabalho de inteligência da polícia militar que ao utilizar das estratégias já descritas nessa pesquisa, vem prevenindo, combatendo e punindo os malfeitores virtuais.

4 REFERÊNCIAS

ASSMANN, H. **A metamorfose do aprender na sociedade da informação**. Ciência da informação, Brasília, v. 29, p. 07-15, 2000. Disponível em: https://www.scielo.br/j/ci/a/ShzKdLbqJDPfssvSw9xWPrw Acesso em: 14 dez. 2021.

CANONGIA, C; MANDARINO JUNIOR, R. **Segurança cibernética**: o desafio da nova Sociedade da Informação. Parcerias Estratégicas, Brasília, v. 14, n. 29, p. 21-46, 2010. Disponível em: http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342 Acesso em: 15 fev. 2024.

CARANDINA, T. Da gestão da informação ao comportamento informacional. **Revista Científica Multidisciplinar**, São Paulo, v. 2, n. 3, p. 20-35, 2021. Disponível em: https://recima21.com.br/index.php/recima21/article/view/133 Acesso em: 08 fev. 2024.

CHOO, C. W. **A Organização do Conhecimento**. São Paulo: Editora Senac São Paulo, 2003.

DELGADO, Paulo. O espírito da lei n. 10. 216/01. **Revista Jurídica Consulex**, Brasília, Consulex, p. 24-25, 15 maio 2010.
GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4. ed. São Paulo, Atlas, 2002.

GOULART, L. A criação de perfis falsos por agentes policiais para investigação do crime de tráfico de drogas no ambiente virtual com base na Lei nº 13.964/2019. 2021. Trabalho de Conclusão de Curso (Bacharel em Direito). Universidade do Sul de Santa Catarina, Tubarão, 2021. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/19961/1/tcc%20let%c3%adcia.pdf Acesso em: 16 ab. 2024.

HOFFMANN, W. A. M. Monitoramento da informação e inteligência competitiva: realidade organizacional. InCID: Revista de Ciência da Informação e Documentação, São Paulo, v. 2, n. 2, p. 125-144, 2011. Disponível em: https://www.revistas.usp.br/incid/article/view/42356. Acesso em: 16 de ab. 2024. » https://www.revistas.usp.br/incid/article/view/42356.

LIMA, J. D. **Discurso de ódio em ambiente virtual**: contribuições da gestão da informação para aumento da eficiência na investigação policial. 2020. Dissertação (Programa de Mestrado em Ciência da Informação). Universidade Federal de Santa Catarina, Santa Catarina, 2020. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/216647/PCIN0231-D.pdf Acesso em: 16 ab. 2024. » https://repositorio.ufsc.br/bitstream/handle/123456789/216647/PCIN0231-D.pdf

MACHADO, Carla e GONÇALVES, Rui Abrunhosa. **Violência e vítimas de crimes**. 3. ed. Coimbra: Quarteto, 2012.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 5° edição, Editora Atlas. São Paulo, 2003.

MARTINS, Flademir Jerônimo Belinati. **Dignidade da pessoa humana - princípio constitucional fundamental. 4. ed.** Curitiba: Juruá, 2014.

MIRABETE, Julio Fabbrini. FABBRINI, Renato N. **Manual de Direito Penal**. 24 ed. rev. e atual. São Paulo: Atlas, 2008.

PINHEIRO, Patricia Peck. Cyber Rights: Direitos fundamentais dos cidadãos digitais e a existência de uma Ordem Pública global através da internet. **Revista dos Tribunais**. vol. 971, 2016. Disponível em: https://www.jusbrasil.com.br/artigos/metodos-de-investigacoes-no-ambito-cibernetico/1291111434 - Acesso em: 15 ab. 2024.

TEIXEIRA, Tarcísio. **Modalidade de crimes cibernéticos.** Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-a-evolucao-da-tecnologia-da-informacao/1166686576. Acesso em: 15 ab. 2024.

RAZZOLINI FILHO, E. **Introdução à gestão da informação:** a informação para organizações no século XXI. Curitiba: Juruá, 2020.

SILVA, José Afonso da. **Comentário contextual à constituição.** 6. ed. São Paulo: Malheiros, 2009.

VAN DIJCK, J. **Confiamos nos dados? As implicações da datificação para o monitoramento social**. Matrizes, São Paulo, v. 11, n. 1, p. 39-59, 2017. Disponível em: https://www.redalyc.org/pdf/1430/143050607004.pdf Acesso em: 08 mar. 2024.

REVISTA INVEST NEWS (CLAUDIA KODJA)
https://investnews.com.br/colunistas/claudia-kodja/crimes-ciberneticos-e-as-principais-ameacas-impostas-pelas-milicias-digitais/