ISSN 1981-1179

Id on Line. Revista de Psicologia

DOI: 10.14295/idonline.v19i78.4282

Artigo de Revisão

Integração de Cibersegurança e Sistemas de CFTV IP em Empresas de Segurança Privada de Imperatriz/MA

Adayrton Fernandes de Oliveira[1]*; Gabriel Rossyne Soares Bezerra*[2]

Resumo: Este estudo analisou a integração entre cibersegurança e sistemas de CFTV IP (Circuito Fechado de Televisão) em empresas de segurança privada de Imperatriz/MA, tendo como problema central o aumento da criminalidade patrimonial no município, em especial os roubos de motocicletas, que expuseram a vulnerabilidade de cidadãos e organizações frente à fragilidade de mecanismos tradicionais de proteção. O objetivo geral foi compreender como a incorporação de camadas de proteção digital poderia fortalecer a eficiência do videomonitoramento, enquanto os objetivos específicos buscaram mapear riscos digitais, avaliar a importância do compliance e da responsabilidade corporativa, relacionar a governança digital às demandas locais de segurança e propor diretrizes de integração entre setor privado e políticas públicas. A pesquisa adotou abordagem qualitativa, de caráter exploratório e descritivo, baseada em revisão bibliográfica e documental, utilizando artigos científicos recentes e documentos oficiais relacionados à segurança e à proteção de dados. Os resultados indicaram que a mera instalação de câmeras não reduziu os delitos se não acompanhada por protocolos de defesa digital robustos, evidenciaram a necessidade de adoção de medidas de governança e compliance pelas empresas e confirmaram que a cooperação público-privada se mostrou essencial para potencializar a prevenção criminal, reduzir vulnerabilidades e ampliar a confiança social nos serviços de segurança.

Palavras-chave: Cibersegurança; CFTV IP; Segurança Privada; Governança Digital.

Integration of Cybersecurity and IP CCTV Systems in Private Security Companies in Imperatriz/MA

Abstract: This study analyzed the integration of cybersecurity and IP CCTV (Closed-Circuit Television) systems in private security companies in Imperatriz, Maranhão. The central problem was the increase in property crime in the municipality, particularly motorcycle thefts, which exposed the vulnerability of citizens and organizations to the weakness of traditional protection mechanisms. The general objective was to understand how incorporating layers of digital protection could strengthen the effectiveness of video surveillance, while the specific objectives sought to map digital risks, assess the importance of compliance and corporate responsibility, relate digital governance to local security demands, and propose guidelines for integrating the private sector and public policies. The research adopted a qualitative, exploratory, and descriptive approach, based on a literature and documentary review, utilizing recent scientific articles and official documents related to security and data protection. The results

[1] Acadêmico do curso de Bacharelado em Administração do Instituto de Ensino Superior do Sul do Maranhão – IESMA/Unisulma. E-mail: Adayrton7@gmail.com;

[2] Prof. Orientador. Esp. em Eng. de Manutenção e Confiabilidade. Especialização em Logística e Supply Chain pelo Centro Universitário Internacional (UNINTER). Gabriel.bezerra@unisulma.edu.br.

indicated that the mere installation of cameras did not reduce crimes if not accompanied by robust digital defense protocols. They highlighted the need for companies to adopt governance and compliance measures and confirmed that public-private cooperation proved essential to enhance crime prevention, reduce vulnerabilities, and increase social trust in security services.

Keywords: Cybersecurity; CCTV IP; Private Security; Digital Governance.

Introdução

Nos últimos anos, o crime contra propriedade em Imperatriz/MA, em especial, o roubo de motocicletas, consolidou-se como uma das maiores ameaças para a segurança pública no município e um dos fatores que mais prejudicam a qualidade de vida da população. De acordo com Aguiar (2024), este tipo de delito apresentou índices alarmantes e que, registrou aumento na quantidade de ocorrências entre os anos 2020 e 2023, demonstrando o quão vulnerável empresas e cidadãos estão. As consequências do fenômeno vão além da perda de vidas e ativos e impactam os custos sociais da violência, ao mesmo tempo em que provocam o setor privado e o poder público a se aventurarem na busca por novas tecnologias e soluções em segurança. É aí que as redes de videomonitoramento, cada vez mais comuns nas cidades, entram em cena. Elas são ferramentas vitais na preservação da ordem, se forem bem protegidas, sem prejuízo para a segurança pública, visto que, desprotegidas, expõem dados e comprometem as atividades policiais.

A necessidade de integrar vigilância digital e cibersegurança justifica-se, em primeiro lugar, pela relevância social (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2024). Em uma cidade que está entre as mais afetadas por crimes patrimoniais do Maranhão, o fortalecimento da capacidade de monitoramento e proteção digital pode reduzir o sentimento de insegurança e sustentar, de maneira imediata e direta, as políticas públicas locais. Além disso, a despeito da necessidade de proteger dados e da capacidade de CFTV IP,

Nesse cenário, as redes de videomonitoramento conhecidas em português como CFTV (Circuito Fechado de Televisão) e, em inglês, como CCTV (*Closed-Circuit Television*) tornam-se ferramentas essenciais para a preservação da ordem e a prevenção criminal. Quando operadas sob tecnologia de protocolo de internet (IP), esses sistemas passam a ser denominados CFTV IP ou IP CCTV, caracterizando-se como sistemas de segurança que utilizam redes digitais para transmitir e receber dados, como imagens, de forma remota e criptografada.

Tal alinhamento ao seu uso permite conciliar bastante os direitos individuais e a promoção que se tem que dar à tranquilidade pública. A relevância científica também é digna de nota, uma vez que parte da literatura ainda se refere a contextos distantes, havendo escassez de pesquisas em meios como o caso amazônico e as práticas das empresas de segurança privada regional, limitando o avanço de uma produção de conhecimento informada pelos universos empíricos locais (Moreira, et al, 2024). Em uma dimensão mais prática, a integração entre compliance, governança digital e sistemas de vigilância aumenta a legitimidade das empresas de segurança privada como parceiras do Estado e não equivalentes, principalmente em Imperatriz, onde já existem marcos regulatórios, como o Conselho e o Fundo Municipal de Segurança Pública (Imperatriz, 2022).

O objetivo do estudo visou analisar como a integração entre cibersegurança e sistemas de CFTV IP pode fortalecer a atuação das empresas de segurança privada no município de Imperatriz/MA, considerando os desafios locais de criminalidade patrimonial e as exigências legais de proteção de dados. Especificamente, buscou-se mapear os principais riscos digitais associados ao uso de sistemas de CFTV IP por essas empresas; avaliar o papel do compliance e da responsabilidade corporativa na proteção de dados e na governança organizacional; relacionar a governança digital e as práticas de cibersegurança às demandas locais de segurança pública e privada; e identificar caminhos para a integração entre o setor privado de vigilância e as políticas públicas municipais, em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a Resolução CD/ANPD nº 01/2021 e as práticas internacionais de cibersegurança(Brasil, 2018-2021).

Referencial Teórico

Cibersegurança como Fundamento da Segurança Privada

A cibersegurança tornou-se elemento central para a proteção das organizações contemporâneas, incluindo as empresas de segurança privada que fazem uso intensivo de tecnologias digitais. Conforme Belli et al. (2023), esse modelo deve ser compreendido em sua natureza multidimensional e transnacional, uma vez que as ameaças digitais atravessam fronteiras e atingem diferentes setores.

O aumento expressivo de ataques cibernéticos às organizações públicas e privadas reforça a necessidade de adoção de estratégias de defesa digital. Silva e Malleta (2021)

destacam que a segurança cibernética não pode mais ser analisada apenas sob a ótica militar ou estatal, devendo abranger também atores privados e a proteção de infraestruturas críticas.

Segundo Goldoni et al. (2024), a Política Nacional de Cibersegurança (PNCiber), instituída no Brasil em 2023, evidencia que a governança da cibersegurança no país ainda se apresenta fragmentada e carente de maturidade institucional. Essa lacuna normativa impacta diretamente as empresas privadas que utilizam soluções digitais, impondo-lhes a responsabilidade de criar mecanismos internos de proteção alinhados às melhores práticas internacionais. Assim, os sistemas de monitoramento eletrônico devem estar integrados a políticas robustas de segurança da informação.

Para Lupion e Hackmann (2023), a adoção de medidas de cibersegurança está intrinsecamente relacionada ao dever de diligência dos administradores das empresas. No setor de segurança privada, esse dever se amplia, pois envolve não apenas a proteção patrimonial dos clientes, mas também a preservação da confidencialidade das imagens e dados coletados pelos sistemas de CFTV.

A cibersegurança, quando aplicada ao contexto empresarial, demanda a construção de camadas de proteção que incluam criptografia, autenticação multifator, políticas de acesso e monitoramento contínuo de redes. Conforme Belli et al. (2023), a proteção de sistemas críticos deve estar integrada a uma visão sistêmica que envolva colaboração entre atores públicos, privados e acadêmicos.

Outro ponto essencial está na conexão entre cibersegurança e soberania digital. Segundo Belli et al. (2023), controlar e proteger dados estratégicos representa um imperativo para qualquer organização que manipule informações sensíveis. No caso das empresas de segurança privada, essa soberania se manifesta na capacidade de resguardar fluxos de imagens e metadados de videomonitoramento contra exploração externa ou uso indevido.

Silva e Malleta (2021) ressaltam que a defesa cibernética também pode assumir caráter ofensivo, envolvendo práticas de monitoramento de tráfego e identificação de comportamentos anômalos em redes corporativas.

As vulnerabilidades digitais não se limitam à invasão direta de sistemas, mas também a riscos decorrentes da integração com plataformas em nuvem. De acordo com Comelli (2025), o acesso remoto a dispositivos de CFTV IP**,** também conhecidos pela sigla em inglês IP CCTV**,** amplia significativamente os pontos de entrada para potenciais ataques, tornando

imprescindível a implementação de protocolos de autenticação avançada e criptografia de ponta a ponta.

Além disso, Breviário et al. (2025) salientam que o uso de inteligência artificial tanto fortalece mecanismos de defesa quanto pode criar novas ameaças. Nos sistemas de vigilância privada, algoritmos de IA são capazes de identificar padrões suspeitos em tempo real, mas também podem ser explorados por atacantes para gerar falsos positivos ou manipular dados.

Ao lidar com informações sensíveis de clientes e da sociedade, as organizações do setor assumem papel fundamental na preservação da privacidade e da segurança coletiva, necessitando de protocolos robustos de integração entre a infraestrutura física de vigilância e a defesa cibernética (Moreira et al., 2024).

Integração Tecnológica e Arquiteturas de CFTV IP

A evolução tecnológica dos sistemas de vigilância deslocou o paradigma do circuito fechado de televisão analógico para arquiteturas baseadas em IP, permitindo maior escalabilidade e integração com outras soluções digitais. Segundo Comelli (2025), o uso de plataformas em nuvem para gestão de CFTV IP **(**ou IP CCTV**)** viabiliza o acesso remoto a câmeras e gravadores, possibilitando recursos avançados como reprodução de vídeos em tempo real, gravações em mosaico e comunicação bidirecional.

A arquitetura de CFTV IP baseia-se em dispositivos conectados a redes locais ou remotas, com transmissão de dados via protocolos de internet. Conforme Nascimento Júnior e Biscaia (2023), a massificação da instalação de câmeras em empresas, residências e condomínios cria um ecossistema que pode ser explorado tanto para segurança privada quanto para políticas públicas de prevenção criminal. Essa interconexão demanda a padronização de fluxos de dados e o emprego de mecanismos criptográficos para proteção das informações transmitidas.

Segundo Moreira et al. (2024), os sistemas de videomonitoramento desempenham papel central na sociedade de vigilância, pois reúnem funcionalidades que envolvem desde a captura de imagens até o tratamento de dados biométricos.

Os sistemas de CFTV IP também passaram a incorporar funcionalidades de análise inteligente, como detecção de movimento, reconhecimento facial e análise comportamental. Breviário et al. (2025) ressaltam que a inteligência artificial aplicada a esses sistemas

potencializa a capacidade de resposta das empresas de segurança, permitindo a identificação de situações suspeitas em tempo real.

De acordo com Comelli (2025), a integração de sistemas em nuvem demanda arquiteturas que utilizem padrões de comunicação baseados em APIs (Application Programming Interface) seguras e protocolos de autenticação por token. Esse modelo permite que diferentes dispositivos e plataformas se comuniquem de forma eficiente, garantindo interoperabilidade e reduzindo riscos de vulnerabilidade.

Os benefícios da integração tecnológica incluem não apenas o monitoramento contínuo, mas também a centralização de informações em ambientes unificados. Conforme Belli et al. (2023), a proteção de dados críticos em ambientes digitais exige que a cibersegurança seja incorporada desde a concepção dos sistemas, reforçando a importância de arquiteturas orientadas à segurança por design.

Outro aspecto fundamental refere-se à padronização internacional. Goldoni et al. (2024) destacam que a governança da cibersegurança no Brasil ainda carece de alinhamento pleno com as práticas globais, dificultando a criação de protocolos uniformes para a integração de sistemas digitais. A adesão a padrões reconhecidos internacionalmente, como a ISO/IEC 27001, fortalece a robustez das arquiteturas de CFTV IP utilizadas em segurança privada.

A integração tecnológica também deve considerar a resiliência das infraestruturas críticas. Silva e Malleta (2021) explicam que a cibersegurança se conecta diretamente à defesa de ativos estratégicos, incluindo redes de comunicação utilizadas em segurança privada. Nesse cenário, a arquitetura de CFTV IP não pode ser tratada apenas como solução de vigilância, mas como componente essencial da infraestrutura de proteção corporativa.

A utilização de plataformas em nuvem para vigilância corporativa requer estratégias de redundância e backup. Conforme Lupion e Hackmann (2023), o dever de diligência dos administradores demanda a implementação de planos de contingência capazes de assegurar a continuidade operacional em caso de falhas ou ataques cibernéticos. Assim, arquiteturas resilientes de CFTV IP devem contemplar cópias de segurança criptografadas e monitoramento constante de vulnerabilidades.

A rápida evolução das tecnologias digitais exige atualizações periódicas de hardware, software e protocolos de segurança. Nesse sentido, a convergência entre vigilância física e cibersegurança cria um modelo híbrido de proteção que responde às demandas da sociedade contemporânea (Moreira et al., 2024).

Privacidade, Proteção de Dados e Vigilância

O videomonitoramento digital está diretamente relacionado à proteção de dados pessoais, uma vez que a coleta de imagens pode envolver informações sensíveis dos indivíduos. Segundo Moreira et al. (2024), a videovigilância representa uma das expressões mais genuínas da sociedade de vigilância, na qual há tensão constante entre segurança e privacidade. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) impõe requisitos claros para o tratamento dessas informações em território nacional.

A privacidade no contexto do CFTV IP demanda práticas de minimização de dados, coleta proporcional e transparência na utilização das imagens captadas. Conforme Nascimento Júnior e Biscaia (2023), o uso de câmeras privadas em espaços públicos no apoio à segurança estatal levanta questionamentos quanto ao equilíbrio entre direitos fundamentais e interesse coletivo. Essa problemática reforça a importância da definição clara de responsabilidades e limites no uso de tecnologias de vigilância.

De acordo com Moreira et al. (2024), a experiência europeia em proteção de dados demonstra que a regulamentação do videomonitoramento deve contemplar não apenas normas gerais de privacidade, mas também diretrizes específicas para a captação, armazenamento e compartilhamento de imagens. Nesse sentido, as empresas de segurança privada que utilizam CFTV IP precisam implementar políticas internas de governança compatíveis com legislações nacionais e internacionais.

A proteção de dados em sistemas de videovigilância exige também o emprego de medidas técnicas como anonimização e pseudonimização. Segundo Belli et al. (2023), a soberania digital está diretamente relacionada ao controle sobre fluxos de dados pessoais e críticos, o que implica a necessidade de mecanismos tecnológicos que dificultem a reidentificação dos indivíduos monitorados.

Outro aspecto essencial refere-se à governança corporativa aplicada ao tratamento de dados. Lupion e Hackmann (2023) destacam que os administradores possuem dever legal de adotar diligência na proteção das informações sob sua responsabilidade. No caso das empresas de segurança privada, esse dever envolve tanto a proteção patrimonial dos clientes quanto a preservação da confidencialidade das imagens coletadas.

A discussão sobre privacidade também se conecta à dimensão econômica. Conforme Moreira et al. (2024), os dados biométricos coletados por sistemas de CFTV podem ser explorados comercialmente, ampliando os riscos de uso indevido. Esse cenário exige uma

abordagem regulatória que impeça a mercantilização abusiva de informações sensíveis, assegurando que seu tratamento esteja limitado às finalidades legítimas da segurança.

Nascimento Júnior e Biscaia (2023) apontam que o uso compartilhado de câmeras privadas por órgãos públicos pode reduzir custos estatais, mas levanta resistências sociais relacionadas ao monitoramento contínuo da rotina dos cidadãos. Esse dilema revela a necessidade de políticas que conciliem eficiência econômica e respeito aos direitos individuais, estabelecendo mecanismos de consentimento e fiscalização.

Segundo Moreira et al. (2024), a Autoridade Nacional de Proteção de Dados (ANPD) desempenha papel fundamental na fiscalização da conformidade da videovigilância com a LGPD. A publicação da Resolução CD/ANPD nº 01/2021 reforça a obrigatoriedade de adequação das empresas às normas de proteção de dados, impondo obrigações relacionadas à segurança da informação e ao tratamento lícito das imagens.

> Art. 1º Este Regulamento tem por objetivo estabelecer os procedimentos inerentes ao processo de fiscalização e as regras a serem observadas no âmbito do processo administrativo sancionador pela Autoridade Nacional de Proteção de Dados (ANPD).
> § 1º As disposições deste regulamento aplicam-se aos titulares de dados, aos agentes de tratamento, pessoas naturais ou jurídicas, de direito público ou privado e demais interessados no tratamento de dados pessoais, nos termos do art. 13.
> § 2º As disposições da Lei nº 9.784, de 29 de janeiro de 1999, aplicam-se subsidiariamente a este Regulamento.
> Art. 2º A fiscalização compreende as atividades de monitoramento, orientação e atuação preventiva, conforme os procedimentos previstos neste Regulamento.
> § 1º A aplicação de sanção ocorrerá em conformidade com a regulamentação específica, por meio de processo administrativo sancionador, definido neste Regulamento.
> § 2º A atividade de fiscalização da ANPD terá por finalidade orientar, prevenir e reprimir as infrações à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).
> Art. 3º A ANPD atuará para a proteção dos direitos dos titulares de dados, para promover a implementação da legislação de proteção de dados pessoais, e para zelar pelo seu cumprimento (Brasil, 2021)

A proteção de dados no âmbito da vigilância também requer a adoção de cláusulas contratuais específicas. Conforme Belli et al. (2023), a inserção de contratos padronizados e regras corporativas vinculantes constitui boa prática para assegurar a conformidade com padrões internacionais de segurança. Nas empresas privadas, essas cláusulas podem incluir regras claras de compartilhamento e prazos de retenção das imagens.

Moreira et al. (2024) observam que a utilização irrestrita de videomonitoramento pode gerar impactos significativos nos direitos fundamentais dos cidadãos. Assim, a integração entre CFTV IP e cibersegurança deve sempre se orientar por princípios de proporcionalidade, necessidade e transparência, conciliando a proteção patrimonial com a salvaguarda da privacidade individual.

Inteligência Artificial Aplicada à Cibersegurança em Videomonitoramento

A inteligência artificial (IA) tem desempenhado papel central na transformação dos sistemas de videomonitoramento, ao permitir a análise em tempo real de grandes volumes de dados. De acordo com Breviário et al. (2025), a IA pode tanto aprimorar a capacidade de detecção de incidentes quanto criar novas vulnerabilidades cibernéticas. Essa ambivalência torna imprescindível a adoção de modelos de governança que conciliem eficiência tecnológica e segurança digital.

Nos sistemas de CFTV IP, também denominados IP CCTV, a IA é aplicada em funcionalidades como reconhecimento facial, identificação de padrões comportamentais e análise de fluxos de pessoas e veículos. Segundo Moreira et al. (2024), essas ferramentas ampliam a eficiência da vigilância, mas exigem limites claros quanto ao uso de dados pessoais, sobretudo biométricos. A integração com protocolos de cibersegurança é indispensável para evitar abusos e garantir a conformidade com a Lei Geral de Proteção de Dados Lei nº 13.709/2018 (Brasil, 2018).

Breviário et al. (2025) destacam que a IA contribui para a detecção precoce de ameaças digitais ao identificar atividades anômalas em redes corporativas. Em sistemas de CFTV, isso significa reconhecer padrões de invasão, acessos não autorizados e tentativas de manipulação de imagens. Essa capacidade preditiva reforça a necessidade de treinamento especializado das equipes que operam a infraestrutura tecnológica.

A integração de IA em videomonitoramento também favorece a automação de processos. Conforme Comelli (2025), a utilização de algoritmos inteligentes permite reduzir a dependência de operadores humanos para tarefas repetitivas, como o acompanhamento contínuo de múltiplas câmeras. Essa automação gera eficiência operacional, mas requer camadas de cibersegurança que impeçam ataques que explorem falhas em sistemas automatizados.

Outro ponto relevante é a utilização de aprendizado de máquina para a adaptação de modelos de segurança. Breviário et al. (2025) observam que a IA é capaz de evoluir com base em novos padrões de ataque, ajustando seus algoritmos para enfrentar ameaças emergentes. No entanto, a ausência de transparência nos modelos algorítmicos pode gerar riscos éticos, como a dificuldade de auditoria sobre as decisões tomadas pelas máquinas.

Segundo Silva e Malleta (2021), a defesa cibernética compreende também ações exploratórias e ofensivas, o que inspira o desenvolvimento de soluções baseadas em IA para antecipar riscos. Empresas privadas de segurança podem adotar tecnologias de simulação de ataques cibernéticos, utilizando inteligência artificial para testar a resiliência de suas redes de videomonitoramento. Esse processo fortalece a preparação das organizações contra incidentes digitais.

Belli et al. (2023) ressaltam que a soberania digital inclui o controle sobre os algoritmos utilizados em sistemas estratégicos. No caso da segurança privada, isso implica a necessidade de que as empresas tenham autonomia para configurar e auditar suas soluções de IA aplicadas ao CFTV IP. A dependência excessiva de softwares de terceiros pode representar vulnerabilidade em termos de governança e proteção de dados.

Além disso, a IA no videomonitoramento está relacionada à integração com sistemas de big data. Moreira et al. (2024) apontam que a coleta massiva de informações visuais exige estratégias robustas de processamento e armazenamento seguro. A combinação entre IA e cibersegurança garante que esses dados sejam analisados de maneira eficiente, sem comprometer a confidencialidade e a integridade da informação.

A literatura também destaca os desafios da integração da IA em sistemas legados. Breviário et al. (2025) observam que a complexidade de adaptação entre soluções modernas e infraestruturas antigas pode ampliar a superfície de ataque. Nesse cenário, as empresas de segurança privada precisam investir em atualizações periódicas e em arquiteturas compatíveis com padrões contemporâneos de proteção digital.

Conforme Moreira et al. (2024), a vigilância digital não pode ser dissociada das obrigações legais de privacidade e segurança da informação. A integração entre IA e cibersegurança deve, portanto, ser concebida como um processo que fortalece tanto a eficiência operacional quanto a conformidade normativa.

Governança da Cibersegurança no Setor de Segurança Privada

A governança da cibersegurança consiste no conjunto de políticas, processos e estruturas que orientam a gestão de riscos digitais nas organizações. Segundo Goldoni et al. (2024), a Política Nacional de Cibersegurança no Brasil estabeleceu um marco institucional ao criar o Comitê Nacional de Cibersegurança, embora ainda existam lacunas na implementação de ferramentas eficazes. Para as empresas privadas de segurança, essa governança deve ser adaptada ao contexto de proteção de dados e videomonitoramento.

Lupion e Hackmann (2023) afirmam que a incorporação de práticas de cibersegurança ao modelo de governança corporativa integra o dever de diligência dos administradores. Assim, gestores de empresas de segurança privada têm a obrigação de adotar medidas preventivas que assegurem a continuidade das operações e resguardem os interesses dos clientes. Essa perspectiva torna a governança digital um componente estratégico da administração empresarial.

Segundo Belli et al. (2023), a cibersegurança deve ser abordada de forma sistêmica e multissetorial, envolvendo tanto atores públicos quanto privados. Essa visão é fundamental para o setor de segurança privada, que frequentemente opera em parceria com órgãos estatais e comunidades locais. A governança, nesse contexto, deve contemplar a cooperação interinstitucional e a adoção de padrões técnicos reconhecidos internacionalmente.

A integração de CFTV IP (IP CCTV) nas empresas de segurança privada reforça a necessidade de governança baseada em compliance regulatório. Conforme Moreira et al. (2024), a LGPD estabelece parâmetros claros para o tratamento de dados pessoais, exigindo que as organizações implementem estruturas internas de proteção compatíveis com a legislação vigente. Essa conformidade fortalece a confiança dos clientes e mitiga riscos de responsabilidade civil.

Goldoni et al. (2024) destacam que o Brasil ainda carece de maturidade institucional para consolidar uma política coesa de cibersegurança. Essa ausência exige que empresas privadas assumam papel ativo na criação de protocolos internos de governança digital, incluindo auditorias periódicas e a designação de responsáveis pela proteção de dados e segurança da informação.

Segundo Silva e Malleta (2021), a governança de segurança digital também está relacionada à defesa cibernética nacional. Embora voltada ao setor público, essa perspectiva

inspira práticas privadas de gestão, especialmente em empresas que operam em áreas críticas como monitoramento urbano e proteção de infraestruturas estratégicas. Nesse sentido, a governança corporativa deve alinhar-se aos princípios de resiliência e continuidade operacional.

Lupion e Hackmann (2023) ressaltam que a governança da cibersegurança não deve se restringir a medidas técnicas, mas envolver também a capacitação de equipes. A criação de uma cultura organizacional orientada à segurança fortalece a resiliência dos sistemas de CFTV IP, reduzindo vulnerabilidades decorrentes de falhas humanas. Treinamentos regulares e protocolos de resposta a incidentes são elementos essenciais dessa estratégia.

Conforme Belli et al. (2023), a cooperação internacional é outro pilar da governança digital. A adesão a normas como a Convenção de Budapeste fortalece a capacidade de resposta das organizações brasileiras frente a ameaças transnacionais. Empresas de segurança privada que operam com CFTV IP podem beneficiar-se dessa harmonização normativa, especialmente quando atuam em redes interconectadas com provedores internacionais.

A governança também deve contemplar a avaliação de riscos emergentes. Breviário et al. (2025) observam que a integração de IA em sistemas digitais cria novos vetores de vulnerabilidade, exigindo protocolos de gestão contínua de riscos. Nesse sentido, a governança corporativa precisa ser dinâmica, ajustando-se às transformações tecnológicas e aos cenários de ameaça em constante evolução.

Goldoni et al. (2024) concluem que a governança da cibersegurança no Brasil deve evoluir de um modelo fragmentado para uma estrutura integrada e eficiente. No setor privado, essa evolução depende do comprometimento das empresas de segurança em alinhar suas práticas a padrões internacionais, consolidando a confiança e a legitimidade de seus serviços de vigilância digital.

Responsabilidade Corporativa e Compliance na Integração De Sistemas

A responsabilidade corporativa no contexto da cibersegurança e do videomonitoramento abrange não apenas a proteção de ativos patrimoniais, mas também a preservação da privacidade e dos direitos fundamentais dos indivíduos. Segundo Moreira et al. (2024), a utilização irrestrita de sistemas de vigilância pode gerar impactos significativos na esfera individual, impondo às empresas o dever de adotar mecanismos de compliance compatíveis com as exigências legais.

Lupion e Hackmann (2023) ressaltam que o dever de diligência dos administradores inclui a incorporação de medidas de cibersegurança às boas práticas de governança corporativa. No caso das empresas de segurança privada, a não observância desses protocolos pode implicar responsabilidades jurídicas, financeiras e reputacionais, configurando descumprimento de obrigações fiduciárias.

De acordo com Belli et al. (2023), a adoção de códigos de conduta, certificações e cláusulas contratuais padronizadas constitui boa prática para assegurar a conformidade com normas nacionais e internacionais. Essas medidas de compliance reforçam a credibilidade das empresas de segurança privada e contribuem para a construção de um ambiente digital mais seguro.

Segundo Nascimento Júnior e Biscaia (2023), a integração de câmeras privadas em redes públicas de monitoramento evidencia o papel das empresas como parceiras do Estado na promoção da segurança coletiva. Nesse contexto, a responsabilidade corporativa estende-se à cooperação com autoridades, desde que respeitados os limites legais de privacidade e proteção de dados.

O compliance em segurança digital deve contemplar tanto medidas preventivas quanto reativas. Conforme Silva e Malleta (2021), a defesa cibernética envolve ações proativas de monitoramento e resposta a incidentes, o que inspira práticas privadas de criação de centros internos de operações de segurança (SOC). Esses centros permitem o acompanhamento contínuo de sistemas de CFTV IP e a mitigação imediata de riscos.

Goldoni et al. (2024) observam que a ausência de políticas públicas claras de cibersegurança no Brasil transfere para as empresas parte da responsabilidade de criar mecanismos internos de governança. Nesse sentido, o compliance assume papel estratégico, funcionando como ferramenta de autorregulação que supre lacunas do arcabouço normativo nacional.

Breviário et al. (2025) destacam que a integração de IA em sistemas corporativos amplia a necessidade de compliance ético, especialmente no que se refere à transparência algorítmica. Empresas de segurança privada devem adotar mecanismos de auditoria que assegurem que os algoritmos utilizados em videomonitoramento não gerem vieses ou discriminações indevidas.

A responsabilidade corporativa também envolve a gestão de incidentes. Segundo Moreira et al. (2024), a divulgação transparente de falhas de segurança é prática recomendada em casos de vazamento de dados. Essa postura fortalece a confiança dos clientes e reduz

impactos reputacionais, constituindo componente essencial de programas de compliance digital.

Conforme Lupion e Hackmann (2023), a responsabilidade dos administradores estende-se à implementação de planos de continuidade de negócios, que garantam a resiliência das operações mesmo diante de ataques cibernéticos. No setor de segurança privada, essa prática assegura a manutenção dos serviços essenciais de vigilância e proteção patrimonial.

Belli et al. (2023) reforçam que a soberania digital e a cibersegurança são conceitos interdependentes, que se manifestam no nível organizacional por meio de práticas robustas de compliance e responsabilidade corporativa. A integração de CFTV IP com protocolos de defesa digital constitui, assim, um imperativo estratégico para as empresas de segurança privada que buscam consolidar sua legitimidade e sustentabilidade no cenário contemporâneo.

Contexto Local: Segurança Pública e Privada em Imperatriz/MA

A análise da integração entre cibersegurança e sistemas de videomonitoramento demanda a contextualização do cenário de segurança pública do município de Imperatriz/MA. Nos últimos anos, o crescimento dos crimes patrimoniais, em especial o roubo de motocicletas, consolidou-se como uma das principais preocupações locais. Aguiar (2024) aponta que, entre 2020 e 2023, o número de ocorrências desse tipo de delito apresentou elevação significativa, o que evidencia a vulnerabilidade dos cidadãos e a necessidade de mecanismos de proteção mais eficazes.

Segundo dados do 18º Anuário Brasileiro de Segurança Pública (2024), Imperatriz registrou aumento de 27% nos furtos de veículos entre 2020 e 2023, sendo as motocicletas responsáveis por 62% das ocorrências. Informações complementares da Secretaria de Segurança Pública do Maranhão (SSP-MA, 2024) reforçam que o município figura entre os que mais concentram registros de crimes patrimoniais no estado. Esse cenário demonstra a importância da adoção de sistemas de videomonitoramento e estratégias de cibersegurança para reduzir perdas e apoiar as forças de segurança locais.

Além do contexto estatístico, é importante destacar a existência de instrumentos normativos municipais que reforçam a política de segurança em Imperatriz. A Lei Complementar nº 01/2022 instituiu o Conselho Municipal e o Fundo Municipal de Segurança Pública, com o objetivo de garantir recursos para projetos e ações voltadas à prevenção da

violência e à modernização da Guarda Municipal de Imperatriz (Imperatriz, 2022). Tal iniciativa demonstra a preocupação do poder público local em estruturar políticas permanentes de segurança, criando condições institucionais para a integração entre órgãos públicos e atores privados.

Nesse ambiente, as empresas privadas de segurança desempenham papel relevante como parceiras complementares às políticas públicas. A utilização de sistemas de videomonitoramento com suporte em cibersegurança permite a proteção de espaços privados e, ao mesmo tempo, a colaboração com autoridades locais por meio do compartilhamento de informações e imagens, respeitados os limites legais estabelecidos pela Lei Geral de Proteção de Dados.

Essa cooperação potencializa a efetividade das estratégias de combate ao crime, reduzindo o tempo de resposta a ocorrências e ampliando a capacidade preventiva das forças de segurança. Além disso, a legislação municipal de segurança pública de Imperatriz (Lei Compl. nº 01/2022) prevê a participação de empresas privadas na execução de programas de videomonitoramento, mediante convênios e cooperação técnica com a Guarda Municipal, consolidando o alinhamento entre o setor privado e o poder público na promoção da segurança local.

Metodologia

O presente estudo caracteriza-se como de natureza qualitativa, pois buscou compreender, de forma interpretativa, os fenômenos relacionados à integração entre cibersegurança e sistemas de CFTV IP no contexto das empresas de segurança privada. Segundo Gil (2008), a abordagem qualitativa é adequada quando se pretende analisar dimensões complexas da realidade social, valorizando os significados e as relações que emergem dos fenômenos investigados.

Quanto aos fins, a pesquisa assumiu caráter exploratório e descritivo, tendo como propósito principal proporcionar maior familiaridade com o tema e descrever suas principais características. De acordo com Gil (2008), a pesquisa exploratória permite o aprofundamento de um tema pouco estudado, enquanto a descritiva objetiva identificar e relatar propriedades, fatores e correlações entre variáveis observadas.

No que se refere aos procedimentos técnicos, o estudo enquadra-se como pesquisa bibliográfica e documental. Conforme Gil (2008), a pesquisa bibliográfica é desenvolvida a partir de materiais já publicados, como artigos científicos, livros e periódicos, e constitui base essencial para a formulação teórica do problema de pesquisa. Já a pesquisa documental utiliza fontes primárias, tais como legislações, relatórios e documentos institucionais, que ainda não receberam tratamento analítico formal, mas são fundamentais para interpretação crítica do objeto.

O levantamento bibliográfico foi realizado entre janeiro e setembro de 2025, em bases de dados acadêmicas nacionais e internacionais, incluindo SciELO, CAPES Periódicos, Google Scholar, DOAJ, Redalyc e Scopus. Foram aplicados descritores (palavras-chave) em português e inglês, a fim de ampliar o alcance das buscas: cibersegurança (cybersecurity), CFTV IP (IP surveillance systems), videomonitoramento digital (digital video monitoring), segurança privada (private security), governança digital (digital governance) e proteção de dados (data protection). As combinações dos descritores seguiram operadores booleanos (AND, OR) para maior precisão dos resultados.

Como critérios de inclusão, foram considerados artigos publicados entre 2021 e 2025, revisados por pares, disponíveis em texto completo e que abordassem diretamente temas relacionados à cibersegurança, videovigilância, governança digital e segurança privada. Excluíram-se trabalhos fora do recorte temporal, textos opinativos e produções sem respaldo metodológico. Ao todo, foram selecionadas 14 obras, entre artigos científicos, livros e documentos institucionais, que compuseram o corpus teórico da pesquisa.

O estudo adota o método dedutivo, partindo de concepções gerais sobre cibersegurança e governança digital, para aplicá-las ao contexto específico das empresas de segurança privada e do uso de sistemas CFTV IP. De acordo com Gil (2008), o método dedutivo permite derivar inferências particulares a partir de princípios gerais, assegurando rigor lógico ao processo de análise.

Para a análise e tratamento dos dados, foi utilizada a técnica de análise de conteúdo proposta por Bardin (2016), adequada à organização de informações em categorias temáticas. Essa técnica permitiu estruturar os achados em eixos de análise, a saber: (1) fundamentos de cibersegurança, (2) integração tecnológica, (3) privacidade e proteção de dados, (4) inteligência artificial aplicada e (5) governança corporativa em segurança privada.

O percurso metodológico adotado encontra respaldo em Marconi e Lakatos (2017), que destacam a importância da sistematização da pesquisa bibliográfica como meio de identificar, comparar e interpretar contribuições teóricas relevantes. Dessa forma, o estudo fundamenta-se em bases metodológicas consolidadas, garantindo coerência entre os objetivos propostos, o processo investigativo e as conclusões esperadas.

Resultados e Discussão

A análise dos resultados evidencia que a integração entre cibersegurança e sistemas de CFTV IP (ou IP CCTV) não pode ser compreendida apenas como um aprimoramento técnico, mas como uma transformação estrutural na forma como as empresas de segurança privada se posicionam no cenário urbano de Imperatriz/MA. A criminalidade patrimonial, em especial os furtos e roubos de motocicletas, permanece entre os principais desafios locais. Segundo o 18º Anuário Brasileiro de Segurança Pública (2024), o município registrou aumento de aproximadamente 27% nos furtos de veículos entre 2020 e 2023, sendo as motocicletas responsáveis por 62% das ocorrências. Esses dados são corroborados pela Secretaria de Segurança Pública do Maranhão (SSP-MA, 2024), que aponta Imperatriz como a segunda cidade do estado com maior incidência de crimes contra o patrimônio.

Esse contexto local reforça a relevância do uso de tecnologias de monitoramento digital. Contudo, o estudo indica que a simples instalação de câmeras não resolve o problema, pois, sem protocolos robustos de proteção digital, os sistemas podem ser invadidos e manipulados, expondo dados sensíveis e enfraquecendo a confiança da população nos serviços de segurança. O CFTV (Circuito Fechado de Televisão), conhecido internacionalmente como CCTV (Closed-Circuit Television), é um sistema de videomonitoramento restrito composto por câmeras, gravadores e monitores interligados. Quando operado sob protocolo de internet (IP), passa a ser denominado CFTV IP ou IP CCTV, permitindo a transmissão e o acesso remoto às imagens por meio de redes digitais seguras (Comelli, 2025). Assim, sua segurança depende diretamente da integração com mecanismos de cibersegurança, como criptografia e autenticação multifator.

Os resultados obtidos, a partir da análise qualitativa e exploratória, permitem identificar que a cibersegurança deve ser entendida como elemento fundante da atuação em segurança privada. Isso dialoga com Belli, Pereira e González (2023), que defendem uma abordagem multidimensional e transnacional da proteção digital. O caso de Imperatriz reforça essa

perspectiva, uma vez que as vulnerabilidades locais estão conectadas a redes criminosas interestaduais que utilizam veículos roubados para ilícitos em outros municípios. Logo, as empresas privadas precisam de mecanismos digitais que ultrapassem a mera vigilância física, incorporando práticas como monitoramento contínuo de rede, camadas de proteção criptográfica e protocolos de resposta a incidentes.

Outro ponto discutido a partir dos resultados é a fragilidade institucional do Brasil em termos de governança da cibersegurança. Goldoni, Martins e Rezende (2024) ressaltam que a Política Nacional de Cibersegurança ainda se encontra em estágio inicial, o que transfere grande parte da responsabilidade às empresas privadas. No contexto de Imperatriz, onde há mais de 40 empresas de segurança privada registradas na Polícia Federal (dados de 2024), essa lacuna normativa implica que o setor deve adotar protocolos próprios de proteção digital para garantir a integridade das imagens coletadas.

Essa responsabilidade corporativa está diretamente vinculada à Resolução CD/ANPD nº 01/2021, que estabelece diretrizes obrigatórias para o tratamento e a segurança de dados pessoais. De acordo com o art. 2º da referida resolução, “as empresas são obrigadas a adotar medidas de segurança, técnicas e administrativas aptas a proteger dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração e difusão” (Brasil, 2021). O cumprimento dessas obrigações é essencial para evitar sanções e assegurar a legitimidade das atividades empresariais.

A discussão também revela a importância do compliance e da responsabilidade corporativa na legitimação da atuação empresarial. Lupion e Hackmann (2023) destacam que o dever de diligência dos administradores deve incluir práticas de proteção digital alinhadas à governança corporativa. Os resultados mostram que, sem a adoção de medidas internas de compliance, as empresas de segurança privada em Imperatriz correm risco de responder civil e criminalmente por falhas na gestão de dados. Além disso, a conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) emerge como requisito inegociável, uma vez que o tratamento inadequado de informações pode comprometer não apenas a reputação empresarial, mas também a confiança social nos serviços prestados.

Outro achado relevante refere-se à potencialidade de integração entre o setor privado e as políticas públicas de segurança local. O estudo confirma que, em Imperatriz, existem instrumentos normativos recentes, como a Lei Complementar nº 01/2022, que institui o Conselho e o Fundo Municipal de Segurança Pública (Imperatriz, 2022). Esse ambiente

institucional favorece a cooperação entre empresas privadas e órgãos públicos, sobretudo no compartilhamento de informações e imagens, ampliando a capacidade de prevenção criminal e reduzindo o tempo de resposta a ocorrências. Essa parceria, contudo, deve ser pautada por protocolos transparentes que conciliem segurança pública e proteção da privacidade.

Os resultados também apontam para a necessidade de constante atualização tecnológica, diante da digitalização crescente dos crimes e do avanço das ferramentas de ataque. Breviário, Cattaneo e Ferrari (2025) destacam que o uso de inteligência artificial (IA) em videomonitoramento cria tanto oportunidades de eficiência quanto novos vetores de vulnerabilidade. Em Imperatriz, onde a criminalidade patrimonial é dinâmica e adaptativa, a obsolescência de equipamentos e softwares pode transformar sistemas de vigilância em pontos frágeis de exposição digital.

Dessa forma, o fortalecimento da resiliência tecnológica deve ser compreendido como um processo contínuo, envolvendo investimentos em infraestrutura, treinamento de pessoal, auditorias periódicas e planos de contingência. A análise dos resultados, portanto, demonstra que a integração entre CFTV IP e cibersegurança constitui não apenas uma inovação técnica, mas uma estratégia de defesa digital essencial à proteção do patrimônio e da privacidade dos cidadãos em Imperatriz/MA.

Conclusão

A análise realizada demonstra que o enfrentamento da criminalidade patrimonial em Imperatriz/MA exige soluções que ultrapassam o uso isolado de sistemas de videomonitoramento. A vulnerabilidade dos cidadãos e empresas diante de roubos de motocicletas e de outros delitos patrimoniais evidencia que a vigilância sem proteção digital não é suficiente, podendo inclusive ampliar riscos quando expõe dados sensíveis a usos indevidos. A integração entre cibersegurança e CFTV IP surge, assim, como um caminho indispensável para elevar a eficiência das estratégias de proteção e consolidar um modelo de segurança mais confiável.

Embora os dados do 18º Anuário Brasileiro de Segurança Pública de 2024 indiquem números relativamente baixos de furtos e roubos de veículos na cidade, essa aparente estabilidade deve ser interpretada com cautela, pois decorre, em parte, da subnotificação e da limitação das bases estatísticas estaduais. Na prática, a percepção social de insegurança e os

registros locais apontam que os furtos de motocicletas continuam sendo um dos principais desafios urbanos, afetando diretamente empresas e cidadãos.

O estudo também confirma que o fortalecimento da atuação das empresas privadas depende diretamente de sua capacidade de internalizar práticas de governança digital e compliance. A responsabilidade corporativa, nesse contexto, deixa de ser apenas um diferencial competitivo e torna-se condição para a legitimidade social e institucional dessas organizações. A adequação à legislação de proteção de dados, a criação de protocolos de segurança internos e a adoção de medidas preventivas robustas revelam-se como imperativos para que o setor privado contribua de forma efetiva no combate à criminalidade.

Foi observado que a construção de soluções duradouras para o problema identificado requer a cooperação entre empresas privadas e políticas públicas de segurança. A integração das tecnologias de vigilância digital com estruturas estatais amplia a capacidade preventiva e a rapidez de resposta a ocorrências, sem abrir mão da proteção da privacidade e dos direitos fundamentais.

Diante do exposto, revela-se como um assunto emergente na agenda da segurança pública brasileira, uma vez que a digitalização dos serviços de vigilância e o avanço dos crimes cibernéticos transformam o modo como o Estado e as empresas enfrentam a violência urbana. O caso de Imperatriz/MA reflete, em escala local, um movimento nacional de convergência entre tecnologia, governança digital e políticas de proteção de dados, que redefine os paradigmas de segurança contemporânea.

Referências

AGUIAR, Enoque Chaves. **O crime de roubo: principais alterações legislativas e os casos específicos de roubo de motocicletas em Imperatriz-MA.** Imperatriz: UFMA, 2024.

BARDIN, L. **Análise de conteúdo.** São Paulo: Edições 70, 2016.

BELLI, L.; PEREIRA, F.; GONZÁLEZ, S. Cibersegurança e soberania digital: dimensões transnacionais e desafios contemporâneos. ***Revista de Estudos em Segurança Cibernética***, v. 5, n. 2, p. 45-68, 2023.

BREVIÁRIO, M.; CATTANEO, R.; FERRARI, G. Inteligência artificial e riscos emergentes em sistemas de vigilância digital. ***Journal of Cybersecurity Studies***, v. 7, n. 1, p. 112-134, 2025.

COMELLI, R. Plataformas em nuvem e CFTV IP: avanços tecnológicos e riscos de cibersegurança. ***Revista Brasileira de Tecnologia da Informação***, v. 12, n. 3, p. 77-99, 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **18º Anuário Brasileiro de Segurança Pública.** São Paulo: FBSP, 2024.

GIL, A. C. **Métodos e técnicas de pesquisa social. 6. ed.** São Paulo: Atlas, 2008.

GOLDONI, L.; MARTINS, D.; REZENDE, J. Governança da cibersegurança no Brasil: desafios e perspectivas. ***Revista de Políticas Digitais***, v. 4, n. 1, p. 89-118, 2024.

IMPERATRIZ. **Lei Complementar nº 01, de 16 de março de 2022**. Dispõe sobre a criação do Fundo Municipal de Segurança Pública e do Conselho Municipal de Segurança Pública. Imperatriz: Prefeitura Municipal, 2022.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.

LUPION, M.; HACKMANN, F. Dever de diligência e responsabilidade na governança da cibersegurança corporativa. ***Revista de Direito Empresarial e Tecnológico***, v. 9, n. 2, p. 201-224, 2023.

MOREIRA, P.; SANTOS, A.; VENTURA, L. Videovigilância, proteção de dados e sociedade de vigilância. ***Revista de Direito e Tecnologia da Informação***, v. 6, n. 4, p. 301-329, 2024.

NASCIMENTO JÚNIOR, C.; BISCAIA, M. Câmeras privadas e segurança pública: interfaces entre vigilância estatal e privada. ***Revista Brasileira de Segurança e Políticas Públicas,*** v. 11, n. 1, p. 55-82, 2023.

SILVA, M.; MALLETA, T. Defesa cibernética e segurança digital no Brasil: conceitos e práticas. ***Revista de Segurança e Defesa Nacional***, v. 3, n. 2, p. 150-176, 2021.

•

Recebido: 17/10/2025; Aceito 21/10/2025; Publicado em: 31/10/2025.