EM PARCERIAS COM A FACULDADE IGUAÇU.

TRANSFORMAÇÃO DIGITAL NA SEGURANÇA PÚBLICA E PRIVADA: O PAPEL DA INTELIGÊNCIA ARTIFICIAL, DA INTELIGÊNCIA CIBERNÉTICA E DA ANÁLISE DE DADOS

RAFAEL FEITOSA MARTINS

Segurança Pública e Privada

RESUMO

A transformação digital tem provocado mudanças significativas na segurança pública e privada, especialmente pela utilização da inteligência artificial, da inteligência cibernética e da análise de dados. Essas tecnologias permitem o processamento rápido de grandes volumes de informações, auxiliando na identificação de padrões, no reconhecimento de situações suspeitas e na prevenção de riscos. Na segurança pública, podem contribuir para o planejamento das ações policiais, o mapeamento de áreas com maior incidência criminal, a investigação de delitos e a distribuição mais eficiente dos recursos disponíveis. Na segurança privada, favorecem o aperfeiçoamento do controle de acesso, do monitoramento eletrônico, da proteção patrimonial e da detecção de possíveis ameaças. A inteligência cibernética também desempenha papel fundamental na identificação e no enfrentamento de ataques virtuais, fraudes eletrônicas, vazamentos de informações e outras práticas criminosas realizadas no ambiente digital. Por sua vez, a análise de dados transforma informações dispersas em conhecimento útil para a tomada de decisões estratégicas. Entretanto, o emprego dessas ferramentas deve respeitar a legislação, a proteção dos dados pessoais, a privacidade e os direitos fundamentais. Dessa forma, a transformação digital representa uma oportunidade para tornar as atividades de segurança mais preventivas, integradas e eficientes, desde que acompanhada de investimentos em tecnologia, qualificação profissional, transparência e mecanismos de controle.

Palavras-chave: Transformação digital. Segurança pública. Segurança privada. Inteligência artificial. Inteligência cibernética. Análise de dados.

1. INTRODUÇÃO

A transformação digital tem modificado profundamente a forma como as instituições planejam, executam e avaliam suas atividades. Na área da segurança, esse processo tornou-se especialmente relevante diante do crescimento das ameaças virtuais, da complexidade das práticas criminosas e da necessidade de respostas mais rápidas e eficientes. Tanto os órgãos públicos quanto as empresas privadas passaram a utilizar ferramentas tecnológicas capazes de ampliar a prevenção, o monitoramento e a investigação de ocorrências.

Nesse contexto, a inteligência artificial ocupa uma posição de destaque por possibilitar o processamento de grandes quantidades de informações em um período reduzido. Sistemas inteligentes podem identificar comportamentos fora do padrão, reconhecer imagens, analisar registros e auxiliar na localização de situações que representem riscos. Essas ferramentas não substituem a atuação dos profissionais de segurança, mas oferecem informações que podem contribuir para decisões mais fundamentadas.

Na segurança pública, a tecnologia pode ser empregada no planejamento operacional, no mapeamento de áreas com maior incidência de crimes, na análise de imagens, no cruzamento de informações e no apoio às investigações. A análise de dados permite compreender melhor a dinâmica criminal e direcionar os recursos humanos e materiais de acordo com as necessidades de cada localidade. Assim, as ações deixam de depender apenas de respostas posteriores aos acontecimentos e passam a incorporar uma atuação mais preventiva.

Na segurança privada, a transformação digital também está presente nos sistemas de videomonitoramento, no controle de acesso, na identificação biométrica, na proteção de instalações e no acompanhamento de movimentações suspeitas. A integração dessas tecnologias contribui para a proteção de pessoas, empresas, documentos e patrimônios. Além disso, permite que possíveis ameaças sejam identificadas com maior rapidez, reduzindo o tempo de resposta das equipes responsáveis.

Outro aspecto importante é o papel da inteligência cibernética na proteção das informações e dos sistemas digitais. O avanço da tecnologia trouxe benefícios para a sociedade, mas também favoreceu o surgimento de crimes cibernéticos, fraudes eletrônicas, invasões de sistemas, vazamentos de dados e ataques contra instituições públicas e privadas. Diante dessa realidade, tornou-se necessário desenvolver mecanismos capazes de identificar vulnerabilidades, acompanhar ameaças e prevenir ações que possam comprometer informações estratégicas.

Entretanto, a utilização da inteligência artificial e da análise de dados na segurança exige responsabilidade. O tratamento de informações pessoais deve respeitar a privacidade, a proteção de dados e os direitos fundamentais. Também é necessário evitar decisões automatizadas baseadas em informações incompletas, preconceitos ou padrões que possam produzir abordagens injustas. Por essa razão, a atuação humana, a transparência e o controle institucional continuam sendo indispensáveis.

Diante do exposto, este trabalho tem como objetivo analisar o papel da inteligência artificial, da inteligência cibernética e da análise de dados no processo de transformação digital da segurança pública e privada. Busca-se compreender as principais contribuições dessas tecnologias para a prevenção de riscos, o enfrentamento da criminalidade e a tomada de decisões, considerando também os desafios éticos, jurídicos e profissionais relacionados à sua utilização.

1.1 Metodologia

O presente trabalho foi desenvolvido por meio de uma revisão bibliográfica, com abordagem qualitativa e caráter descritivo. A pesquisa baseou-se na consulta a livros, artigos científicos, trabalhos acadêmicos, legislações e publicações especializadas relacionadas à transformação digital, à segurança pública e privada, à inteligência artificial, à inteligência cibernética e à análise de dados.

A revisão bibliográfica permitiu reunir diferentes conhecimentos sobre a utilização das tecnologias digitais nas atividades de segurança, bem como identificar suas contribuições, limitações e principais desafios. Os materiais foram selecionados conforme sua relação com o tema e analisados de maneira interpretativa, buscando estabelecer uma ligação entre os avanços tecnológicos e as necessidades atuais das instituições públicas e privadas.

Após a seleção das fontes, as informações foram organizadas por assuntos, considerando a aplicação da inteligência artificial, o uso estratégico dos dados, a prevenção de ameaças cibernéticas e os cuidados relacionados à privacidade e aos direitos fundamentais. Dessa forma, a metodologia adotada possibilitou construir uma discussão fundamentada sobre os efeitos da transformação digital na modernização e no aperfeiçoamento das atividades de segurança.

2 DESENVOLVIMENTO

A transformação digital aplicada à segurança corresponde à incorporação de tecnologias capazes de melhorar a prevenção, o monitoramento, a investigação e a resposta diante de situações de risco. Esse processo envolve não apenas a aquisição de equipamentos modernos, mas também a integração de sistemas, o compartilhamento

seguro de informações e a qualificação dos profissionais responsáveis pela utilização dessas ferramentas.

Na segurança pública e privada, a tecnologia passou a ocupar uma função estratégica. Recursos como inteligência artificial, análise de dados, videomonitoramento inteligente, reconhecimento biométrico e sistemas de proteção cibernética ampliam a capacidade de identificar ameaças e de tomar decisões. Entretanto, sua utilização deve ocorrer de maneira responsável, respeitando os limites legais, éticos e institucionais.

2.1 Transformação digital na segurança pública

Na segurança pública, a transformação digital contribui para a modernização das atividades realizadas pelas instituições policiais e pelos demais órgãos integrantes do sistema de proteção social. A digitalização de registros, a integração de bancos de dados e o uso de plataformas de comunicação facilitam o acesso às informações e reduzem o tempo necessário para o atendimento das ocorrências.

O emprego dessas tecnologias também pode auxiliar no planejamento das ações de policiamento. A partir da análise de registros anteriores, torna-se possível identificar áreas, horários e circunstâncias em que determinados crimes acontecem com maior frequência. Essas informações permitem direcionar viaturas, equipes e equipamentos para os locais que apresentam maior necessidade de atuação preventiva.

A transformação digital também favorece a comunicação entre diferentes instituições. Quando os sistemas são integrados, informações relevantes podem ser consultadas com maior rapidez durante fiscalizações, investigações e operações. Contudo, a integração deve contar com mecanismos de segurança que impeçam acessos indevidos, alterações ou vazamentos de dados.

2.2 Transformação digital na segurança privada

A segurança privada também passou por importantes mudanças com a introdução das tecnologias digitais. Empresas, estabelecimentos comerciais, condomínios e instituições utilizam sistemas eletrônicos para proteger pessoas, instalações, equipamentos e informações. Câmeras inteligentes, alarmes integrados, sensores e controles de acesso tornaram o monitoramento mais preciso e contínuo.

Os sistemas de controle de acesso podem utilizar cartões, senhas, reconhecimento facial ou identificação biométrica para autorizar a entrada de pessoas em ambientes restritos. Quando integrados a bancos de dados, esses mecanismos permitem registrar horários, movimentações e tentativas de acesso não autorizadas. Dessa maneira, a tecnologia amplia a capacidade de prevenção e facilita a apuração de incidentes.

Apesar desses benefícios, a presença da tecnologia não elimina a importância do

profissional de segurança. A interpretação das informações, a avaliação das circunstâncias e a adoção das medidas adequadas continuam dependendo da atuação humana. Portanto, a eficiência da segurança privada resulta da combinação entre recursos tecnológicos, treinamento e procedimentos bem definidos.

2.3 Inteligência artificial aplicada à segurança

A inteligência artificial permite que sistemas computacionais realizem análises complexas, reconheçam padrões e apresentem respostas com base nas informações processadas. Na área da segurança, essa tecnologia pode ser aplicada à análise de imagens, à identificação de objetos, ao reconhecimento de comportamentos incomuns e à organização de grandes volumes de registros.

No videomonitoramento, por exemplo, sistemas inteligentes conseguem localizar movimentações suspeitas, identificar a permanência de pessoas em áreas restritas e emitir alertas para as equipes responsáveis. Na investigação, a inteligência artificial pode auxiliar no cruzamento de informações provenientes de diferentes fontes, reduzindo o tempo necessário para localizar relações entre pessoas, locais e acontecimentos.

Entretanto, os resultados produzidos pelos sistemas dependem da qualidade dos dados utilizados. Informações incorretas, incompletas ou discriminatórias podem gerar análises equivocadas e prejudicar pessoas. Por isso, as decisões não devem ser tomadas exclusivamente por máquinas. É necessário manter a supervisão humana, revisar os resultados e assegurar que a tecnologia seja empregada de forma ética e responsável.

2.4 Inteligência cibernética e proteção das informações

A inteligência cibernética reúne procedimentos destinados à identificação, análise e prevenção de ameaças presentes no ambiente digital. Sua importância aumentou devido à expansão do uso da internet, dos sistemas informatizados e do armazenamento de dados em plataformas digitais. Quanto maior a dependência tecnológica de uma instituição, maiores são os cuidados necessários para proteger suas informações.

Entre as principais ameaças estão as invasões de sistemas, os programas maliciosos, as fraudes eletrônicas, o roubo de dados e os ataques que impedem o funcionamento de serviços. Na segurança pública, uma falha pode comprometer investigações, informações pessoais e operações. Na segurança privada, pode causar prejuízos financeiros, interrupção das atividades e exposição de dados de clientes e funcionários.

A prevenção dessas ocorrências exige atualização dos sistemas, controle de acesso, cópias de segurança, monitoramento das redes e capacitação dos usuários. A inteligência cibernética também permite acompanhar indícios de ataques e identificar

possíveis vulnerabilidades antes que sejam exploradas. Dessa forma, sua atuação deve ser permanente e integrada ao planejamento das instituições.

2.5 Análise de dados e tomada de decisões

A análise de dados consiste na organização e interpretação de informações para produzir conhecimentos úteis. Na segurança, os dados podem ser obtidos por meio de registros de ocorrências, sistemas de videomonitoramento, relatórios operacionais, sensores, controles de acesso e outras fontes autorizadas. Quando analisadas em conjunto, essas informações ajudam a compreender a realidade e a estabelecer prioridades.

Na segurança pública, a análise de dados pode indicar alterações na incidência de determinados crimes, permitindo que os gestores planejem ações preventivas e avaliem os resultados das medidas adotadas. Na segurança privada, pode revelar falhas no controle de acesso, horários de maior risco e locais que necessitam de reforço no monitoramento.

Entretanto, o tratamento desses dados deve observar a finalidade da coleta, a necessidade das informações e a proteção da privacidade. O acesso deve ser limitado aos profissionais autorizados, e os dados não podem ser utilizados para objetivos diferentes daqueles que justificaram sua obtenção. Assim, a análise de dados deve contribuir para a eficiência da segurança sem desrespeitar os direitos individuais.

2.6 Ferramentas tecnológicas aplicadas à análise, à proteção da informação e à tomada de decisão

A transformação digital disponibilizou diferentes ferramentas capazes de aperfeiçoar as atividades de segurança pública e privada. Entre elas, destacam-se os sistemas de videomonitoramento inteligente, softwares de análise de dados, plataformas de integração de informações, controles biométricos, sensores, drones, sistemas de reconhecimento de placas veiculares e ferramentas de proteção cibernética. Esses recursos permitem coletar, organizar e analisar informações que auxiliam na prevenção de riscos e na tomada de decisões.

Na segurança pública, a análise de dados pode ser utilizada para identificar locais, horários e circunstâncias em que determinadas ocorrências se repetem. Como exemplo, os registros de roubos e furtos podem ser organizados em mapas digitais, facilitando a visualização das áreas com maior concentração criminal. A partir dessas informações, os gestores podem definir os locais que necessitam de reforço no policiamento, reorganizar as equipes e distribuir viaturas de forma mais adequada.

Outra ferramenta utilizada é o sistema de reconhecimento automático de placas

veiculares. Câmeras instaladas em pontos estratégicos podem registrar as placas dos veículos e comparar os dados com informações de veículos roubados, furtados ou envolvidos em práticas criminosas. Quando uma situação suspeita é identificada, o sistema emite um alerta para que os agentes realizem a verificação. Os drones também podem auxiliar no acompanhamento de grandes eventos, na localização de pessoas desaparecidas e no monitoramento de áreas de difícil acesso.

Na segurança privada, a inteligência artificial pode ser aplicada em câmeras capazes de identificar movimentações incomuns, invasões de áreas restritas, abandono de objetos e circulação de pessoas fora dos horários autorizados. Em condomínios, empresas e estabelecimentos comerciais, sistemas de reconhecimento facial e biometria podem controlar a entrada e a saída de pessoas. Sensores inteligentes também podem detectar abertura indevida de portas, presença em ambientes restritos, fumaça ou alterações que indiquem riscos ao patrimônio e às pessoas.

A inteligência cibernética, por sua vez, é essencial para a proteção das informações utilizadas pelas instituições. Ferramentas como antivírus, sistemas de detecção de invasões, autenticação em dois fatores, criptografia, controle de acesso e cópias de segurança reduzem os riscos de ataques e vazamentos de dados. Por exemplo, uma tentativa de acesso incomum ao banco de dados de uma instituição pode ser identificada pelo sistema, que bloqueia a atividade e alerta a equipe responsável.

A análise das informações coletadas também contribui para decisões mais rápidas e fundamentadas. Um gestor da segurança pública pode utilizar relatórios digitais para decidir onde concentrar uma operação policial. Na segurança privada, o responsável pode analisar registros de alarmes e tentativas de acesso para reforçar a vigilância em determinado local ou horário. Dessa forma, a decisão passa a ser baseada em informações organizadas, e não apenas em percepções individuais.

Entretanto, essas ferramentas devem ser utilizadas com supervisão humana e respeito à legislação. O reconhecimento facial, o tratamento de dados pessoais e o monitoramento de ambientes precisam observar a privacidade, a finalidade da coleta e a proteção das informações. Além disso, os resultados gerados pelos sistemas devem ser conferidos por profissionais capacitados, pois nenhuma tecnologia está completamente livre de falhas.

Portanto, a inteligência artificial, a inteligência cibernética e a análise de dados representam recursos importantes para a segurança pública e privada. Quando utilizadas de maneira integrada e responsável, essas ferramentas fortalecem a prevenção, melhoram a proteção das informações e oferecem suporte para decisões mais eficientes diante das ameaças existentes.

2.7 Discussões e resultados

A partir da revisão bibliográfica realizada, observou-se que a transformação digital produz avanços importantes na segurança pública e privada. A inteligência artificial, a inteligência cibernética e a análise de dados ampliam a capacidade de prevenção, tornam o monitoramento mais eficiente e oferecem informações relevantes para o planejamento e a tomada de decisões.

Os resultados indicam que a inteligência artificial contribui para o reconhecimento de padrões, a análise de imagens e o cruzamento de informações. A análise de dados, por sua vez, permite identificar áreas, horários e situações de maior risco. Já a inteligência cibernética atua na proteção dos sistemas, das redes e das informações utilizadas pelas instituições. Embora possuam funções específicas, essas três áreas apresentam melhores resultados quando utilizadas de forma integrada.

Na segurança pública, essas ferramentas podem contribuir para uma distribuição mais adequada de equipes, viaturas e recursos, além de oferecer apoio às investigações e às ações preventivas. Na segurança privada, podem aperfeiçoar o controle de acesso, o videomonitoramento, a proteção patrimonial e a detecção antecipada de ameaças. Em ambos os setores, a tecnologia pode reduzir o tempo de resposta e melhorar a qualidade das informações disponíveis.

Também foram identificados desafios relacionados ao custo de implantação, à falta de integração entre sistemas, à necessidade de capacitação profissional e ao risco de vazamentos ou acessos indevidos. Além disso, sistemas automatizados podem apresentar erros ou reproduzir desigualdades existentes nos dados utilizados. Por essa razão, seus resultados precisam ser avaliados por profissionais capacitados.

Dessa forma, verificou-se que a transformação digital não deve ser entendida apenas como a substituição de procedimentos tradicionais por equipamentos modernos. Trata-se de uma mudança que envolve planejamento, pessoas, dados e responsabilidade institucional. Os resultados positivos dependem da qualidade das informações, da segurança dos sistemas, da preparação dos profissionais e da existência de normas claras para o uso das tecnologias.

Conclui-se, portanto, que a utilização responsável dessas ferramentas pode fortalecer tanto a segurança pública quanto a privada. Entretanto, a inovação tecnológica deve permanecer submetida à supervisão humana, à legislação e à proteção dos direitos fundamentais, garantindo que o aumento da eficiência não ocorra em prejuízo da privacidade, da igualdade e da dignidade das pessoas.

3 CONSIDERAÇÕES FINAIS

O desenvolvimento deste trabalho permitiu compreender que a transformação

digital representa uma mudança significativa na forma como as atividades de segurança pública e privada são planejadas, executadas e avaliadas. A incorporação da inteligência artificial, da inteligência cibernética e da análise de dados amplia a capacidade das instituições de identificar riscos, proteger informações, prevenir ocorrências e tomar decisões fundamentadas. Entretanto, seus resultados dependem da maneira como essas ferramentas são implementadas e utilizadas pelos profissionais responsáveis.

Na segurança pública, a transformação digital pode contribuir para a modernização do policiamento, das investigações e da gestão das informações. A integração dos registros de ocorrências, o mapeamento das áreas com maior incidência criminal e o cruzamento de dados permitem compreender com mais clareza a distribuição dos delitos. Conforme Beato (2012), a análise da criminalidade deve considerar sua relação com os espaços urbanos e com as características de cada localidade. Dessa maneira, as informações podem auxiliar na distribuição de viaturas, equipes e equipamentos, favorecendo uma atuação preventiva e planejada.

Também foi possível observar que o emprego da tecnologia pode reduzir o tempo necessário para localizar informações relevantes durante investigações e operações. Sistemas de reconhecimento de placas veiculares, câmeras inteligentes, drones, bancos de dados integrados e mapas digitais de ocorrências são exemplos de ferramentas que podem apoiar as instituições públicas. Contudo, os resultados produzidos por esses sistemas precisam ser avaliados por profissionais capacitados, considerando que os dados não conseguem representar, isoladamente, toda a complexidade da realidade social.

Na segurança privada, a transformação digital favorece a proteção de pessoas, empresas, estabelecimentos e patrimônios. Recursos como câmeras de videomonitoramento, sensores, alarmes integrados, reconhecimento facial e controle biométrico de acesso possibilitam o acompanhamento contínuo dos ambientes protegidos. Essas ferramentas podem identificar movimentações suspeitas, tentativas de entrada não autorizada e outras situações que exijam a intervenção das equipes de segurança.

Apesar dos benefícios apresentados, a tecnologia não elimina a importância da atuação humana. Os sistemas podem emitir alertas e organizar informações, mas a interpretação das circunstâncias e a escolha da medida adequada continuam dependendo dos profissionais. Portanto, o aumento da eficiência na segurança privada exige a combinação entre equipamentos modernos, treinamento, procedimentos internos e supervisão humana.

A inteligência artificial mostrou-se uma das principais ferramentas da transformação digital. Sua capacidade de processar grandes volumes de informações e identificar padrões pode auxiliar na análise de imagens, no cruzamento de registros e na detecção

de comportamentos incomuns. Kaufman (2022) explica que a inteligência artificial produz importantes mudanças nas atividades econômicas e sociais, mas também apresenta limitações e desafios éticos que precisam ser considerados.

Na segurança pública, a inteligência artificial pode ser utilizada para analisar registros de ocorrências, apoiar investigações, reconhecer veículos e identificar situações suspeitas em imagens. Na segurança privada, pode auxiliar no controle de acesso, no videomonitoramento e na emissão automática de alertas. Em ambos os setores, os sistemas devem ser compreendidos como instrumentos de apoio, e não como substitutos da decisão humana.

Os resultados produzidos pela inteligência artificial dependem diretamente da qualidade dos dados utilizados. Informações incorretas, incompletas ou marcadas por desigualdades podem levar a conclusões equivocadas. Por isso, uma indicação produzida por um sistema automatizado não deve ser considerada prova definitiva de uma conduta irregular. É necessário realizar a conferência das informações e analisar o contexto antes da adoção de qualquer medida.

A análise de dados também se revelou fundamental para o planejamento e a tomada de decisão. Quando os registros são organizados e interpretados corretamente, torna-se possível identificar padrões, alterações na incidência criminal e situações de maior risco. Na segurança pública, essas informações podem orientar o policiamento preventivo e a realização de operações. Na segurança privada, podem indicar horários, locais e procedimentos que necessitam de reforço.

Entretanto, decisões fundamentadas em dados não são completamente neutras. A forma como as informações são coletadas, selecionadas e classificadas pode influenciar os resultados. Assim, os gestores devem analisar os relatórios com responsabilidade e considerar outros elementos da realidade. A tomada de decisão precisa reunir conhecimento profissional, informações confiáveis e compreensão das particularidades de cada situação.

A inteligência cibernética ocupa igualmente uma posição essencial nesse processo. O crescimento dos sistemas informatizados aumentou a quantidade de dados armazenados pelas instituições públicas e privadas. Ao mesmo tempo, ampliou os riscos de invasões, fraudes eletrônicas, vazamentos de informações e interrupções de serviços. Segundo Wendt e Jorge (2021), a investigação dos crimes cibernéticos exige conhecimentos específicos e procedimentos adequados para a identificação e a preservação das evidências digitais.

A proteção das informações requer a adoção de medidas como criptografia, autenticação em dois fatores, atualização dos sistemas, controle de acesso, cópias de segurança e monitoramento das redes. Essas ferramentas reduzem as vulnerabilidades e

permitem identificar possíveis tentativas de ataque. Entretanto, sua eficiência depende da atualização contínua e do comportamento responsável dos usuários.

A capacitação dos profissionais constitui uma medida indispensável para a segurança cibernética. Uma instituição pode possuir equipamentos modernos e, ainda assim, permanecer vulnerável em razão do uso de senhas fracas, do compartilhamento indevido de informações ou da abertura de arquivos maliciosos. Portanto, a proteção tecnológica deve ser acompanhada por treinamentos, protocolos internos e uma cultura institucional de segurança da informação.

Outro aspecto identificado foi a necessidade de proteger os dados pessoais. Doneda (2021) demonstra que a ampliação da capacidade de coleta e processamento de informações exige uma proteção jurídica que ultrapasse a compreensão tradicional da privacidade. No mesmo sentido, Mendes (2014) destaca a importância da proteção dos dados diante das novas relações estabelecidas entre tecnologia, instituições e cidadãos.

A utilização de reconhecimento facial, biometria e monitoramento eletrônico deve respeitar a finalidade, a necessidade e a segurança do tratamento das informações. A Lei Geral de Proteção de Dados Pessoais estabelece princípios e obrigações aplicáveis às instituições públicas e privadas (BRASIL, 2018). Dessa forma, a busca por maior eficiência na segurança não autoriza a coleta indiscriminada nem o uso inadequado de informações pessoais.

A transformação digital também exige transparência, fiscalização e responsabilidade institucional. Cepik (2003) demonstra a importância do controle sobre as atividades de inteligência em uma sociedade democrática. A produção de conhecimentos estratégicos deve contribuir para a segurança e a tomada de decisão, mas precisa permanecer submetida às normas legais e aos mecanismos de controle.

Além disso, a simples aquisição de equipamentos não garante a modernização das instituições. É necessário integrar sistemas, estabelecer procedimentos, capacitar profissionais e avaliar continuamente os resultados. Lima, Ratton e Azevedo (2014) evidenciam que a segurança pública envolve diferentes instituições, práticas e políticas, não podendo ser reduzida a uma solução exclusivamente tecnológica.

Com base na revisão bibliográfica, verificou-se que as tecnologias apresentam melhores resultados quando utilizadas de maneira integrada. A inteligência artificial auxilia no reconhecimento de padrões; a análise de dados transforma registros em conhecimento; e a inteligência cibernética protege sistemas e informações. A integração dessas áreas permite uma atuação mais rápida, preventiva e organizada.

Também foram identificados desafios relacionados aos custos de implantação, à falta de integração entre bancos de dados, à necessidade de atualização dos equipamentos e à carência de profissionais qualificados. Existem ainda riscos de falhas

nos sistemas, acessos indevidos, vazamentos de informações e decisões automatizadas injustas. Esses problemas demonstram que a transformação digital precisa ser acompanhada por planejamento, investimento e controle permanente.

Conclui-se, portanto, que a inteligência artificial, a inteligência cibernética e a análise de dados podem fortalecer a segurança pública e privada. Essas tecnologias oferecem ferramentas importantes para o monitoramento, a prevenção, a investigação, a proteção das informações e a tomada de decisões. Contudo, devem ser utilizadas de forma responsável, respeitando a legislação, a privacidade, a igualdade e os demais direitos fundamentais.

Por fim, a transformação digital não deve ser compreendida como substituição dos profissionais pelas máquinas. Seu objetivo deve ser oferecer melhores condições para o trabalho humano e ampliar a capacidade das instituições de proteger a sociedade. O verdadeiro avanço ocorre quando inovação tecnológica, qualificação profissional, responsabilidade jurídica e respeito aos cidadãos caminham conjuntamente. Dessa maneira, será possível construir uma segurança mais eficiente, preventiva, integrada e preparada para enfrentar os riscos existentes nos ambientes físicos e digitais.

REFERÊNCIAS

BEATO FILHO, Cláudio Chaves. Crime e cidades. Belo Horizonte: Editora UFMG, 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 4 ago. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 ago. 2026.

CEPIK, Marco Aurélio Chaves. Espionagem e democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro: Editora FGV, 2003.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Revista dos Tribunais, 2021.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública: 2025. São Paulo: Fórum Brasileiro de Segurança Pública, 2025.

KAUFMAN, Dora. Desmistificando a inteligência artificial. 2. ed. rev. e ampl. Belo Horizonte: Autêntica, 2022.

LIMA, Renato Sérgio de; RATTON, José Luiz; AZEVEDO, Rodrigo Ghiringhelli de (org.). Crime, polícia e justiça no Brasil. São Paulo: Contexto, 2014.

MAGRANI, Eduardo. Entre dados e robôs: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

PINHEIRO, Patrícia Peck. Direito digital. 7. ed. São Paulo: Saraiva Jur, 2021.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes cibernéticos: ameaças e procedimentos de investigação. 3. ed. Rio de Janeiro: Brasport, 2021.