UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 3, e98664, p. 1-26, 2026 • https://dx.doi.org/10.5902/2357797598664
Submissão: 04/09/2026 • Aprovação: 14/09/2026 • Publicação: 02/10/2026

Artigos Dossiê

O contributo das tecnologias emergentes para a prevenção da criminalidade

The contribution of emerging technologies to crime prevention

Ricardo Caiado[I]

[I]Instituto Universitário de Lisboa, Lisboa, Portugal

Resumo

A transformação tecnológica do ambiente de segurança tem deslocado progressivamente a prevenção da criminalidade de uma lógica predominantemente reativa para modelos assentes em dados, antecipação, inteligência e capacidade de resposta em tempo quase real. Este artigo analisa o contributo das tecnologias emergentes para a prevenção da criminalidade, com especial atenção à inteligência artificial, ao big data, à análise preditiva, ao policiamento orientado pelas informações, à inteligência forense e à identificação biométrica. Partindo do enquadramento da mutação do paradigma da segurança, sustenta-se que estas tecnologias podem aumentar a capacidade de deteção de padrões, apoiar a afetação de recursos, melhorar a partilha de informação e reforçar a antecipação de riscos. Contudo, os benefícios não são automáticos: dependem da qualidade dos dados, da competência institucional, da interoperabilidade dos sistemas, da supervisão humana e da existência de salvaguardas jurídicas e éticas. O artigo adota uma metodologia qualitativa, de natureza teórico-analítica, baseada em revisão bibliográfica e análise documental. A discussão é ainda situada no contexto do Sul Global, onde a adoção tecnológica enfrenta limitações de infraestrutura, dados, competências e capacidade regulatória. A conclusão é que a tecnologia deve ser entendida como capacidade institucional e não apenas como aquisição de equipamentos, exigindo modelos de governação inclusivos, cooperação internacional e desenvolvimento de autonomia tecnológica.

Palavras-chave: Tecnologias emergentes; Prevenção da criminalidade; Inteligência artificial; *Big data*; Policiamento preditivo

Artigo publicado por InterAção sob uma licença CC BY-NC-SA 4.0.

Abstract

Technological transformation in the security environment is progressively shifting crime prevention from a predominantly reactive logic towards models based on data, anticipation, intelligence and near-real-time response. This article examines the contribution of emerging technologies to crime prevention, focusing on artificial intelligence, big data, predictive analytics, intelligence-led policing, forensic intelligence and biometric identification. Based on the changing security paradigm, the article argues that these technologies can strengthen pattern detection, resource allocation, information sharing and risk anticipation. However, their benefits are not automatic: they depend on data quality, institutional capacity, system interoperability, professional expertise, human oversight and effective legal and ethical safeguards. The study adopts a qualitative, theoretical-analytical methodology grounded in bibliographic review and documentary analysis. The discussion is also situated in the Global South, where technological adoption faces constraints related to infrastructure, data availability, skills and regulatory capacity. The main conclusion is that technology should be understood as an institutional capability rather than merely as the acquisition of equipment or software. Sustainable crime prevention therefore requires inclusive governance, international cooperation, capacity building and technological autonomy, while ensuring that the pursuit of security remains compatible with privacy, proportionality, equality and fundamental rights.

Keywords: Emerging technologies; Crime prevention; Artificial intelligence; Big data; Predictive policing

1 INTRODUÇÃO

A transformação tecnológica das sociedades alterou profundamente o ambiente em que se desenvolvem as políticas de segurança. A expansão das redes digitais, a generalização de dispositivos conectados, a produção massiva de dados e a evolução da inteligência artificial (IA) modificaram simultaneamente as oportunidades de prevenção da criminalidade e as formas através das quais os fenómenos criminais podem ser praticados. A segurança deixou, assim, de poder ser compreendida exclusivamente a partir de uma dimensão militar ou territorial, passando a integrar ameaças e riscos multidimensionais, transversais e reticulares.

Esta alteração corresponde ao que a literatura sobre o novo paradigma da segurança tem identificado como uma passagem para uma conceção mais ampla, integrada e dinâmica da segurança. GOUVEIA (2018) enquadra esta transformação numa arquitetura que articula defesa nacional, segurança interna, informações, proteção civil e segurança comunitária. LOURENÇO et al. (2015) e LOURENÇO e COSTA

(2018) reforçam, por sua vez, a necessidade de pensar a segurança nacional como um sistema de sistemas, assente na complementaridade e interdependência entre diferentes capacidades estatais e não estatais.

No domínio da prevenção da criminalidade, a transformação tecnológica é particularmente evidente. A ubiquidade dos meios de comunicação digital e a sua utilização por indivíduos e organizações criminosas obrigam as forças de segurança a adaptar métodos, processos e competências. O policiamento apoiado em dados, a análise criminal, o intelligence-led policing, o policiamento preditivo, a inteligência forense e a utilização de sistemas de IA constituem manifestações desta transformação.

Neste contexto, surge a questão central deste artigo: de que modo as tecnologias emergentes podem contribuir para a prevenção da criminalidade e quais são as condições necessárias para que esse contributo seja compatível com o Estado de Direito? A hipótese defendida é que o principal valor das tecnologias emergentes não reside na substituição do decisor humano, mas na capacidade de ampliar a produção, integração e interpretação de informação relevante para a prevenção, desde que exista governação adequada dos dados, controlo humano e respeito pelos direitos fundamentais.

Este tema assume particular pertinência no âmbito do 3.º Dossiê Temático da Revista InterAção, dedicado aos desafios tecnológicos para a construção da defesa e segurança no Sul Global. O debate não pode, por isso, limitar-se à capacidade técnica dos sistemas, porquanto é necessário considerar também as desigualdades de infraestrutura, dependências tecnológicas, disponibilidade de dados, competências profissionais, soberania digital e capacidade regulatória. A questão tecnológica é, simultaneamente, uma questão de capacidade estatal, autonomia estratégica e justiça na distribuição dos benefícios e riscos da inovação.

Assim, o artigo tem como objetivo geral analisar o contributo das tecnologias emergentes para a prevenção da criminalidade, identificando as suas principais potencialidades, limitações e condições de utilização responsável. Especificamente, procura-se: (i) enquadrar a relação entre a transformação tecnológica e o novo

paradigma da segurança; (ii) analisar o contributo do big data, da análise preditiva e da IA para a prevenção criminal; (iii) discutir o papel do intelligence-led policing e da inteligência forense; (iv) apreciar as oportunidades e riscos associados à identificação biométrica; e (v) refletir sobre os desafios particulares de adoção tecnológica no Sul Global.

2 ENQUADRAMENTO TEÓRICO: DA SEGURANÇA REATIVA À SEGURANÇA ANTECIPATÓRIA

A ideia de segurança encontra-se atualmente associada a um ambiente de risco complexo, marcado por ameaças que ultrapassam fronteiras institucionais, territoriais e disciplinares. BECK (1992) descreve a sociedade contemporânea como uma sociedade de risco, na qual a produção de riqueza e inovação coexiste com riscos produzidos pelo próprio desenvolvimento social, industrial e tecnológico. No campo da segurança, esta condição traduz-se na necessidade de identificar vulnerabilidades, compreender dinâmicas criminais e construir respostas antes que os danos se materializem.

LOURENÇO et al. (2015) defendem uma abordagem integrada da segurança, na qual a distinção rígida entre segurança interna e segurança externa perde progressivamente utilidade perante ameaças transnacionais e fenómenos híbridos. O ciberespaço, as redes criminosas transnacionais e o terrorismo constituem exemplos de fenómenos que exigem articulação entre diferentes produtores de segurança, bem como entre autoridades públicas e entidades privadas.

A prevenção da criminalidade insere-se, neste contexto, numa lógica de antecipação. Não se trata de presumir que todos os comportamentos futuros podem ser previstos, mas de aumentar a capacidade institucional de reconhecer sinais, padrões e relações relevantes. CLEMENTE (2013) associa a transformação dos modelos policiais à crescente importância da informação, enquanto ELIAS (2009) relaciona o policiamento orientado pelas informações com a utilização do produto informacional para dirigir o esforço policial.

O intelligence-led policing representa, assim, uma alteração relevante do ciclo de decisão policial. A informação deixa de ser mero produto auxiliar da ação e passa a constituir elemento estruturante da definição de prioridades, da alocação de recursos e da orientação das operações. RATCLIFFE (2003) conceptualiza este modelo como um processo em que a interpretação do ambiente criminal, a decisão e a intervenção se encontram continuamente articuladas.

Esta lógica é reforçada pela digitalização. A existência de grandes volumes de dados permite identificar relações que seriam difíceis de detetar através de processos exclusivamente manuais. Porém, a quantidade não equivale automaticamente a conhecimento. A informação só produz valor preventivo quando é pertinente, contextualizada, validada e interpretada por profissionais capazes de compreender as limitações dos métodos analíticos.

Daqui resulta uma premissa essencial para a análise das tecnologias emergentes: o avanço tecnológico não elimina a necessidade de instituições fortes; pelo contrário, aumenta a exigência de competências, supervisão, interoperabilidade, governança e responsabilidade. A tecnologia pode acelerar uma decisão correta, mas também pode acelerar uma decisão errada se os dados forem deficientes, enviesados ou utilizados fora do contexto.

3 METODOLOGIA

O estudo adota uma metodologia qualitativa, de natureza teórico-analítica, baseada em revisão bibliográfica e análise documental. O ponto de partida foi um draft sobre a mutação do paradigma da segurança, cuja abordagem articula a segurança nacional, segurança interna, policiamento orientado pelas informações, policiamento preditivo, big data, inteligência forense, inteligência artificial e identificação biométrica. A análise e desenvolvimento deste draft permitiu identificar conceitos, argumentos e relações relevantes para a construção do objeto do artigo.

Complementarmente, procedeu-se à consulta de literatura científica e documentos institucionais relativos à governação da IA, direitos fundamentais, segurança digital e desenvolvimento de capacidades tecnológicas, com particular atenção aos desafios dos países em desenvolvimento. Aqui, foram privilegiadas fontes institucionais e académicas com relevância para a segurança, tecnologia e governação.

Não se pretende realizar uma avaliação quantitativa da eficácia de uma tecnologia policial específica, nem apresentar resultados experimentais. Os resultados assumem, por isso, natureza analítica: correspondem à sistematização das principais formas pelas quais as tecnologias emergentes podem reforçar a prevenção criminal e à identificação das condições institucionais, jurídicas e éticas que condicionam esse contributo.

4 TECNOLOGIAS EMERGENTES E PREVENÇÃO DA CRIMINALIDADE

4.1 Big data e mineração de dados

O *big data* constitui uma das infraestruturas fundamentais da transformação contemporânea da segurança. A multiplicação de dispositivos digitais, câmaras, sensores, plataformas, bases de dados e sistemas de comunicação produz volumes de informação que excedem a capacidade de tratamento através de métodos tradicionais. No domínio policial, a questão central passa por transformar esses dados em conhecimento operacionalmente útil.

NEIVA (2019) evidencia que o big data pode permitir a recolha e conversão de grandes quantidades de informação em classificações, categorias e indicadores destinados à prevenção e repressão criminal. A mineração de dados acrescenta uma dimensão analítica a este processo, permitindo explorar grandes bases estruturadas ou não estruturadas com o objetivo de identificar padrões relevantes.

A prevenção criminal beneficia desta capacidade sobretudo em três dimensões. Em primeiro lugar, na identificação de padrões espaciais e temporais de ocorrência

criminal. Em segundo lugar, no cruzamento de informação proveniente de diferentes fontes, permitindo reconhecer relações entre ocorrências, pessoas, locais e objetos. Em terceiro lugar, no apoio à gestão de recursos, possibilitando que as forças de segurança priorizem áreas, fenómenos ou situações de maior risco.

Contudo, a utilização de big data apresenta uma ambivalência estrutural. Quanto maior for a capacidade de recolha e correlação de dados, maior é também o potencial de vigilância. LYON (2014) chama a atenção para o impacto da expansão de conjuntos de dados interligados e das ferramentas de análise preditiva sobre a privacidade. O desafio consiste, portanto, em impedir que a prevenção criminal seja convertida numa lógica de vigilância indiscriminada.

Para o efeito, a prevenção baseada em dados deve respeitar princípios de necessidade, finalidade, proporcionalidade, segurança da informação, minimização de dados e responsabilização. O dado não deve ser recolhido porque é tecnicamente possível recolhê-lo; deve existir uma finalidade legítima, uma base jurídica adequada e mecanismos de controlo.

4.2 Análise preditiva e policiamento preditivo

O policiamento preditivo constitui uma das aplicações mais discutidas das tecnologias emergentes na prevenção criminal. Segundo BRAYNE, ROSENBLAT e BOYD (2015), a análise preditiva pode ser utilizada para antecipar eventos, locais ou pessoas associadas a probabilidades de ocorrência criminal. Neste modelo, o processo envolve a ingestão de dados, a aplicação de métodos algorítmicos e a utilização das previsões para orientar decisões policiais.

O contributo potencial é claro: reduzir a incerteza na afetação de recursos e aumentar a capacidade de intervenção preventiva. Se determinados padrões espaciais e temporais forem identificados de forma robusta, os recursos policiais podem ser orientados para contextos onde exista maior probabilidade de ocorrência de determinados ilícitos. A prevenção pode, assim, deslocar-se de uma resposta posterior ao crime para uma intervenção anterior ou imediatamente preventiva.

Porém, a previsão algorítmica não equivale à previsão determinística. Um modelo estatístico identifica probabilidades a partir de dados históricos; não determina que um crime irá ocorrer. Esta distinção é fundamental, porque os dados históricos podem refletir desigualdades, práticas de policiamento anteriores e subnotificação criminal. Um algoritmo treinado sobre dados enviesados pode reproduzir ou ampliar esses enviesamentos.

BRANTINGHAM (2018) e BARRETT (2017) chamam a atenção para este problema: os algoritmos podem melhorar eficiência e precisão, mas também podem diluir critérios de suspeita e produzir efeitos discriminatórios. A utilização responsável exige, portanto, auditoria dos dados, validação dos modelos, avaliação de desempenho, explicabilidade adequada ao contexto e supervisão humana.

Neste sentido, o policiamento preditivo deve ser concebido como instrumento de apoio à decisão e não como mecanismo autónomo de determinação da culpabilidade ou da intervenção coerciva. A tecnologia pode indicar uma área de risco; não deve, por si só, transformar uma pessoa num suspeito.

4.3. Intelligence-led policing e inteligência artificial

O intelligence-led policing constitui talvez a principal ponte entre tecnologia, informação e decisão policial. O seu pressuposto é que a atividade policial deve ser orientada por uma interpretação estruturada do ambiente criminal, onde são identificados três elementos críticos: interpretação do ambiente criminal, processo de decisão e impacto sobre esse ambiente. A tecnologia atua sobretudo no primeiro e no segundo, mas o objetivo último continua a ser produzir efeitos preventivos no terceiro.

A IA amplia as possibilidades deste modelo porque permite processar grandes volumes de informação, reconhecer padrões, classificar conteúdos, apoiar análise de redes, processar linguagem natural e identificar relações entre diferentes conjuntos de dados. BARRENECHE e RAMOS-MARTÍN (2020) mostram como técnicas de machine

learning e mineração de dados permitem identificar padrões implícitos em dados anteriores e produzir previsões algorítmicas.

No âmbito policial, estas capacidades podem ser aplicadas a fontes heterogéneas: registos de ocorrências, comunicações autorizadas, dados geográficos, informação financeira quando legalmente acessível, dados forenses, informação de fontes abertas e registos operacionais. A integração dessas fontes pode produzir produtos de intelligence mais rápidos e completos.

Todavia, importa distinguir capacidade analítica de autoridade decisória. O facto de um sistema conseguir produzir uma correlação não significa que essa correlação seja juridicamente suficiente para justificar uma medida restritiva de direitos. A IA deve apoiar o raciocínio profissional, não substituir os requisitos legais de fundamentação.

A utilização da IA no intelligence-led policing deve, por isso, ser acompanhada de competências especializadas. Não basta adquirir software: são necessários analistas, cientistas de dados, especialistas jurídicos, profissionais de cibersegurança e decisores capazes de interpretar os resultados. A transformação tecnológica é, simultaneamente, uma transformação organizacional.

4.4 Inteligência forense e integração de dados

A inteligência forense constitui outra dimensão relevante da prevenção criminal. LEGRAND e VOGEL (2012) apresentam-na como a utilização de diferentes dados forenses para cruzar referências e relacionar cenas de crime, materiais e suspeitos. Ao contrário da utilização isolada da prova forense num processo concreto, a inteligência forense procura identificar padrões e ligações entre múltiplas ocorrências.

O potencial preventivo decorre precisamente da capacidade de transformar vestígios dispersos em conhecimento sobre fenómenos criminais. Dados relativos a ADN, impressões digitais, balística, vestígios e outros elementos podem, quando legalmente integrados e devidamente tratados, contribuir para identificar séries criminais, conexões entre ocorrências e modus operandi recorrentes.

Esta abordagem exige interoperabilidade e partilha controlada de informação. O valor de um sistema de inteligência forense cresce quando os dados relevantes podem ser comparados entre unidades, regiões e, quando legalmente admissível, jurisdições. A cooperação é particularmente importante perante criminalidade organizada, terrorismo e cibercriminalidade transnacional.

Os benefícios, porém, dependem da qualidade dos dados e da capacidade de interpretar corretamente as relações identificadas. Um falso positivo pode direcionar uma investigação para um caminho incorreto; um falso negativo pode impedir a identificação de uma ligação relevante. A inteligência forense deve, por isso, permanecer integrada num processo profissional de validação.

4.5. Identificação biométrica e reconhecimento facial

Os sistemas de identificação biométrica representam uma das aplicações mais sensíveis das tecnologias emergentes. O reconhecimento facial pode apoiar processos de verificação e identificação e, em determinadas circunstâncias, contribuir para localizar pessoas procuradas, identificar vítimas ou apoiar investigações. A sua capacidade de operar em grandes conjuntos de imagens torna-o potencialmente relevante para a prevenção e investigação criminal.

PEREIRA (2022) salienta, contudo, que estes sistemas apresentam riscos relacionados com intrusão, erros, discriminação, proteção de dados e privacidade. A discussão jurídica não pode, portanto, ser separada da avaliação tecnológica. A taxa de erro, a qualidade das imagens, a composição das bases de referência e o contexto de utilização podem influenciar substancialmente os resultados.

O Regulamento (UE) 2024/1689, conhecido como AI Act, estabelece uma abordagem baseada no risco e impõe salvaguardas específicas para determinados usos de sistemas biométricos e de IA no contexto da aplicação da lei. O regime europeu demonstra que a utilidade operacional não é suficiente para legitimar qualquer utilização tecnológica: necessidade, proporcionalidade, autorização, documentação,

supervisão e proteção de direitos fundamentais devem integrar o desenho da utilização. (UNIÃO EUROPEIA, 2024).

Para a prevenção criminal, a principal lição é que a identificação biométrica deve ser orientada para finalidades concretas e legalmente delimitadas. Sistemas de vigilância massiva e indiscriminada podem produzir um efeito securitário incompatível com uma sociedade democrática. A prevenção deve ser construída como uma capacidade dirigida e controlada, e não como uma autorização geral para monitorizar a população.

4.6 Cibersegurança e IA aplicada à deteção de ameaças

A prevenção criminal contemporânea não pode ignorar a dimensão cibernética. O ciberespaço constitui simultaneamente infraestrutura essencial, espaço de atividade económica e ambiente de atuação de atores criminosos. A IA pode ser utilizada para deteção de anomalias, classificação de eventos, identificação de comportamentos suspeitos, priorização de alertas e apoio à resposta a incidentes.

BONFANTI (2022) evidencia a natureza de duplo uso da IA: as mesmas capacidades que podem reforçar a defesa cibernética podem também ser utilizadas para fins ofensivos. Esta caraterística é particularmente relevante para a prevenção da criminalidade, porque as organizações criminosas também podem explorar automação, análise de dados, engenharia social e ferramentas inteligentes.

Daqui resulta que a prevenção deve ser concebida em termos de resiliência. Não basta detetar ataques; é necessário proteger infraestruturas, reduzir vulnerabilidades, partilhar indicadores de ameaça e recuperar rapidamente de incidentes. A cooperação entre Estado e setor privado assume importância particular, uma vez que uma parte significativa das infraestruturas digitais críticas é operada ou suportada por entidades privadas.

A tecnologia emergente, portanto, amplia simultaneamente a superfície de ataque e a capacidade defensiva. A política pública deve procurar manter uma vantagem institucional de conhecimento, competências e coordenação sobre os atores criminosos.

5 RESULTADOS E DISCUSSÃO: O VALOR PREVENTIVO DAS TECNOLOGIAS EMERGENTES

A análise desenvolvida permite identificar cinco contributos principais das tecnologias emergentes para a prevenção da criminalidade: antecipação, integração, focalização, velocidade e aprendizagem institucional.

O primeiro é a antecipação. Big data, análise preditiva e IA permitem identificar padrões e sinais que podem apoiar a intervenção antes da ocorrência de determinados eventos. Esta capacidade não deve ser confundida com previsão absoluta, mas constitui uma melhoria da capacidade de avaliação de risco.

O segundo é a integração. A criminalidade contemporânea é frequentemente organizada em redes que atravessam territórios e setores. Sistemas interoperáveis permitem cruzar informação de diferentes fontes e produzir uma visão mais completa do fenómeno criminal. A partilha deve, contudo, respeitar os princípios de necessidade, competência, finalidade e proteção da informação.

O terceiro é a focalização. A utilização de informação permite direcionar recursos para fenómenos, locais e situações prioritárias. Em ambientes de recursos limitados, esta capacidade pode ter particular relevância. A eficiência, porém, não deve ser avaliada apenas pelo número de ocorrências ou detenções, mas também pela redução de danos, pela prevenção efetiva e pela qualidade das decisões.

O quarto é a velocidade. Sistemas automatizados podem processar informação em períodos muito inferiores aos processos exclusivamente manuais. Em situações de ameaça cibernética, terrorismo ou criminalidade em rede, a rapidez pode ser decisiva. A velocidade deve, contudo, ser equilibrada com mecanismos de validação quando estejam em causa direitos fundamentais.

O quinto é a aprendizagem institucional. A digitalização permite registar decisões, resultados, padrões e indicadores, criando condições para avaliar políticas e melhorar modelos de prevenção. A instituição de segurança pode, assim, passar de uma lógica de reação casuística para uma lógica de aprendizagem contínua.

Estes resultados sustentam a hipótese de que a tecnologia tem maior valor quando integrada num ciclo institucional de prevenção: recolha legítima de dados, tratamento e validação, análise, produção de intelligence, decisão humana, intervenção, avaliação e retroalimentação. A tecnologia não é o ciclo; é uma capacidade transversal que o pode tornar mais rápido e informado.

Em consequência, o principal indicador de maturidade tecnológica de uma organização de segurança não deve ser a quantidade de equipamentos adquiridos, mas a sua capacidade de transformar dados em decisões legítimas, úteis e avaliáveis.

6 DESAFIOS PARA O SUL GLOBAL: TECNOLOGIA, CAPACIDADE E AUTONOMIA

A análise do contributo das tecnologias emergentes assume uma dimensão particular quando transportada para o Sul Global. A adoção de sistemas avançados não ocorre num vazio institucional, uma vez que existem diferenças significativas no acesso a infraestrutura digital, capacidade computacional, disponibilidade e qualidade dos dados, formação de recursos humanos, financiamento e capacidade regulatória.

O Global Digital Compact reconhece que os países em desenvolvimento enfrentam desafios específicos relacionados com recursos limitados e desigualdades digitais, defendendo cooperação internacional, capacitação, transferência de tecnologia e desenvolvimento de soluções inclusivas. Em 2026, a própria discussão internacional sobre a "intelligence divide" evidencia que a desigualdade deixou de ser apenas uma questão de acesso à Internet e passou a envolver a capacidade de compreender, desenvolver, aplicar e governar IA. (UNITED NATIONS, 2024a).

Para a prevenção da criminalidade, esta desigualdade pode produzir dois efeitos. O primeiro é a dependência tecnológica: sistemas críticos podem ser adquiridos a fornecedores externos, com limitações de interoperabilidade, transparência, manutenção e soberania sobre os dados. O segundo é a assimetria de conhecimento: organizações criminosas podem utilizar tecnologias acessíveis globalmente, enquanto instituições públicas enfrentam restrições de infraestrutura e competências.

A resposta não passa necessariamente pela procura de autossuficiência tecnológica absoluta. Mais realista é construir autonomia estratégica suficiente para compreender tecnologias, avaliar fornecedores, definir requisitos, auditar sistemas, proteger dados e adaptar soluções às realidades locais. A autonomia tecnológica, neste sentido, é antes de mais autonomia de decisão.

O Sul Global apresenta ainda um desafio epistemológico. Modelos algorítmicos desenvolvidos a partir de dados de outras sociedades podem não representar adequadamente contextos locais. Um sistema de previsão criminal treinado com padrões urbanos de um país pode produzir resultados inadequados noutro país, onde estruturas sociais, mobilidade, formas de denúncia e padrões criminais sejam diferentes. A localização dos dados e a produção de conhecimento local são, portanto, componentes da segurança tecnológica.

Daqui decorre a importância da cooperação Sul-Sul e triangular, da formação de profissionais, do desenvolvimento de dados representativos e da criação de infraestruturas digitais públicas seguras. O objetivo deve ser construir capacidades locais para utilizar tecnologia de forma crítica, e não simplesmente importar modelos tecnológicos.

7 GOVERNANÇA, DIREITOS FUNDAMENTAIS E RESPONSABILIDADE

A prevenção tecnológica só é sustentável quando acompanhada de legitimidade. A expansão de sistemas de vigilância, IA e biometria cria uma tensão permanente entre segurança e liberdade. O próprio material de base alerta para o risco de um trade-off entre segurança e liberdade que transforme a perceção de insegurança em fundamento para a restrição excessiva de direitos.

O princípio orientador deve ser o de que a eficácia não constitui, por si só, legitimidade. Um sistema pode ser tecnicamente eficiente e juridicamente inadmissível. A governança deve, portanto, começar antes da aquisição ou implementação, incluindo avaliação de impacto, definição de finalidades, análise de riscos, requisitos de segurança, controlo de acesso, auditoria e mecanismos de responsabilização.

O AI Act europeu constitui um exemplo de regulação baseada no risco. No domínio da aplicação da lei, determinadas utilizações biométricas estão sujeitas a requisitos e limitações específicos. O regulamento exige, em situações previstas, autorização, avaliação de impacto sobre direitos fundamentais, documentação e limites de utilização. O princípio subjacente é particularmente relevante para a prevenção criminal: quanto maior o impacto potencial sobre direitos, maior deve ser o nível de controlo.

A supervisão humana é igualmente essencial. Sistemas de IA podem apoiar decisões, mas não devem ser transformados em autoridades autónomas quando estão em causa consequências jurídicas relevantes para pessoas. A decisão deve permanecer atribuível a agentes humanos e instituições juridicamente responsáveis.

A responsabilidade deve ainda abranger todo o ciclo de vida tecnológico. Não basta responsabilizar o utilizador final por uma decisão problemática; é necessário considerar qualidade dos dados, desenho do algoritmo, validação, aquisição, configuração, utilização e monitorização. A cadeia de responsabilidade deve acompanhar a cadeia tecnológica.

Finalmente, a confiança pública deve ser tratada como um recurso de segurança. Uma política de prevenção tecnologicamente avançada, mas opaca pode gerar resistência social, reduzir cooperação e aumentar a perceção de vigilância. A transparência adequada, a prestação de contas e a possibilidade de controlo jurisdicional contribuem para transformar a tecnologia num instrumento de segurança democrática. Nesta perspetiva, atente-se no Quadro 1.

Quadro 1 – Tecnologias emergentes na prevenção da criminalidade: contributos, riscos e salvaguardas

Tecnologia	Contributo preventivo	Risco principal	Salvaguarda prioritária
Big data e mineração de dados	Integração de grandes volumes de informação e deteção de padrões.	Correlação espúria, dados incompletos e sobrecarga analítica.	Governança de dados, qualidade e validação contextual.
Policiamento preditivo	Identificação de padrões espaciais e temporais e apoio à alocação de recursos.	Reprodução de vieses históricos e ciclos de retroalimentação.	Auditoria, avaliação de impacto e supervisão humana.
Inteligência artificial	Classificação, análise automatizada e apoio à produção de inteligência.	Opacidade, erros e dependência de modelos ou fornecedores.	Explicabilidade, testes independentes e responsabilização.
Inteligência forense	Ligação de vestígios, ocorrências e casos para produzir conhecimento preventivo.	Falsos vínculos e interpretação excessiva de correlações.	Cadeia de custódia, validação pericial e controlo de acesso.
Biometria e reconhecimento facial	Identificação ou verificação de pessoas em contextos delimitados.	Intrusão, falsos positivos, discriminação e vigilância massiva.	Base legal, necessidade, proporcionalidade e supervisão.
IA na cibersegurança	Deteção de anomalias, ameaças e padrões de ataque.	Falsos positivos, adversarial attacks e automatização excessiva.	Red teaming, supervisão humana e planos de resposta.

Fonte: Autor (2026)

8 PROPOSTA DE UM MODELO INTEGRADO DE PREVENÇÃO TECNOLÓGICA

Com base na análise realizada, propõe-se um modelo integrado de prevenção tecnológica assente em seis dimensões: dados, inteligência, decisão, intervenção, avaliação e governança.

A primeira dimensão é a governação dos dados, onde devem ser definidos quais os dados necessários, com que finalidade podem ser recolhidos, quem pode aceder-lhes, durante quanto tempo e com que mecanismos de segurança. A qualidade deve ser tratada como requisito operacional e jurídico.

A segunda dimensão é a inteligência. Os dados devem ser transformados em produtos analíticos através de técnicas de mineração, estatística, IA e análise criminal. A participação de analistas humanos é indispensável para contextualizar resultados e identificar limitações.

A terceira dimensão é a decisão. Os produtos de intelligence devem apoiar decisores policiais e autoridades competentes, sem substituir a sua responsabilidade. A decisão deve considerar informação tecnológica, conhecimento profissional, contexto territorial e requisitos jurídicos.

A quarta dimensão é a intervenção. A prevenção pode assumir diferentes formas: presença policial orientada por informação, proteção de infraestruturas, intervenção comunitária, investigação, ciberdefesa, proteção de vítimas ou encaminhamento para outras políticas públicas. A tecnologia deve apoiar a escolha da resposta mais adequada, não impor automaticamente uma única resposta.

A quinta dimensão é a avaliação. Cada tecnologia deve ser sujeita a indicadores de eficácia, precisão, custos, erros, impactos sobre direitos e efeitos distributivos. Sistemas que não produzam benefícios proporcionais aos seus riscos devem ser reformulados ou descontinuados.

A sexta dimensão é a governança, a qual inclui regras jurídicas, auditoria, supervisão independente, transparência, participação de especialistas e sociedade civil, segurança cibernética e mecanismos de responsabilização. No Sul Global, deve acrescentar-se uma dimensão explícita de capacitação e autonomia tecnológica.

Este modelo permite superar duas visões extremas: a visão tecnocêntrica, segundo a qual a tecnologia resolveria por si mesma os problemas de segurança, e a visão tecnofóbica, que ignora os benefícios concretos da inovação. A posição defendida é institucional: tecnologias emergentes são instrumentos poderosos cujo valor depende da qualidade das instituições que as concebem, utilizam e controlam.

8.1. Critérios para avaliar o valor preventivo dos sistemas algorítmicos

A literatura recente recomenda que a avaliação de tecnologias algorítmicas na segurança não seja reduzida à precisão estatística. Um sistema pode apresentar elevada capacidade de classificação e, simultaneamente, produzir efeitos socialmente indesejáveis quando é alimentado por dados incompletos, enviesados ou produzidos por práticas policiais anteriores. A questão decisiva passa, portanto, de "o algoritmo funciona?" para "para que finalidade funciona, com que dados, para quem, em que contexto e sob que mecanismos de controlo?". Esta mudança é particularmente importante no domínio da prevenção criminal, porque o objeto da decisão é frequentemente um risco futuro e não um facto já comprovado. (VAN BRAKEL, 2025).

No policiamento preditivo, a literatura evidencia que os dados policiais não constituem um espelho neutro da criminalidade. Registos de ocorrências, detenções, patrulhamento, denúncias e fiscalizações refletem também prioridades institucionais, desigualdades territoriais, capacidade de presença policial e padrões históricos de intervenção. Consequentemente, um sistema que aprenda exclusivamente a partir desses dados pode reproduzir e reforçar os padrões que deveria apenas descrever. BRANTINGHAM (2018) chama atenção para a relação entre viés dos dados e policiamento preditivo baseado em lugares, enquanto trabalhos mais recentes sobre justiça algorítmica identificam riscos associados a diferentes atributos sociodemográficos e recomendam validação humana e diversificação geográfica dos conjuntos de dados (ALMASOUD; IDOWU, 2025).

Esta questão é especialmente relevante para o Sul Global. Parte significativa da investigação empírica sobre policiamento algorítmico continua concentrada em contextos norte-americanos e europeus. O estudo etnográfico de NARAYAN (2023), centrado na polícia de Delhi, é importante precisamente por mostrar que a adoção de ferramentas de mapeamento e análise de hotspots depende de práticas organizacionais, culturas institucionais e interpretações locais. A tecnologia não é

simplesmente transferida de um laboratório para uma força policial; ela é reinterpretada por organizações concretas. Daí resulta que a importação de sistemas treinados com dados de outros países pode produzir resultados pouco adequados ao contexto local, mesmo quando o desempenho técnico apresentado pelo fornecedor parece elevado.

Assim, propõe-se que qualquer tecnologia empregue na prevenção criminal seja submetida a uma avaliação multidimensional composta por, pelo menos, seis critérios: eficácia preventiva; qualidade e representatividade dos dados; proporcionalidade da intervenção; explicabilidade e auditabilidade; impacto sobre direitos fundamentais; e sustentabilidade institucional. A eficácia deve ser medida não apenas pelo número de alertas ou previsões corretas, mas também pela capacidade de reduzir danos e orientar recursos para problemas reais. A qualidade dos dados exige documentação da origem, cobertura, atualidade e limitações. A proporcionalidade requer que a intensidade da intervenção seja compatível com a gravidade e probabilidade do risco. A auditabilidade exige rastreabilidade das decisões e possibilidade de revisão. Finalmente, a sustentabilidade institucional implica capacidade interna para operar, avaliar, atualizar e, quando necessário, abandonar o sistema.

Esta abordagem evita uma consequência frequente da inovação tecnológica: a transformação de uma ferramenta auxiliar em autoridade decisória. Em matéria de segurança pública, os sistemas algorítmicos devem produzir informação para apoiar decisões legitimadas por normas, procedimentos e agentes responsáveis. O resultado algorítmico pode ser relevante para orientar uma investigação, distribuir patrulhas ou priorizar análise, mas não deve ser tratado como prova automática da perigosidade de uma pessoa. A distinção entre indicador de risco, suspeita, prova e decisão jurídica é essencial para preservar o Estado de Direito.

8.2. Capacitação, interoperabilidade e soberania tecnológica

No Sul Global, a discussão sobre tecnologias emergentes para a prevenção da criminalidade não pode ser separada das condições materiais de produção e utilização

da tecnologia. Infraestruturas de conectividade, capacidade computacional, qualidade dos sistemas de informação, disponibilidade de dados, formação especializada, financiamento público e capacidade regulatória condicionam o valor real de qualquer solução algorítmica. A existência de uma aplicação tecnicamente avançada não significa, por si só, existência de capacidade institucional para a utilizar de forma segura e sustentável.

A discussão internacional sobre governança da inteligência artificial reconhece crescentemente esta assimetria. O Global Dialogue on AI Governance das Nações Unidas, realizado em julho de 2026, colocou entre os seus eixos a redução das divisões de capacidade, o desenvolvimento de competências e a necessidade de transparência, responsabilização e supervisão humana. O relatório preliminar do Independent International Scientific Panel on AI igualmente identifica desigualdades de capacidade e lacunas de governança como fatores centrais para a distribuição dos benefícios e riscos da IA (UNITED NATIONS, 2026a; 2026b).

Para a segurança pública, isto significa que a autonomia tecnológica não deve ser entendida como autossuficiência absoluta, mas como capacidade de compreender, selecionar, contratar, auditar, adaptar e, quando necessário, substituir tecnologias críticas. Uma instituição que depende integralmente de fornecedores externos para interpretar o funcionamento de um sistema, atualizar modelos, conservar dados ou investigar falhas encontra-se numa posição de vulnerabilidade. A soberania tecnológica aplicada à segurança exige, portanto, competências internas, padrões de interoperabilidade, documentação técnica, capacidade de auditoria e cláusulas contratuais que preservem a responsabilidade pública.

A cooperação internacional pode contribuir para superar estas limitações, mas deve ser estruturada de modo a evitar uma simples transferência assimétrica de soluções. Programas de formação, laboratórios conjuntos, investigação aplicada, desenvolvimento de conjuntos de dados representativos, software aberto quando adequado, padrões interoperáveis e cooperação Sul-Sul podem fortalecer capacidades

locais. O objetivo deve ser transformar a aquisição de tecnologia em aquisição de capacidade. Esta distinção é decisiva para que a inovação tecnológica contribua para a segurança de longo prazo e não produza novas dependências estratégicas.

8.3. Governança algorítmica e legitimidade da prevenção

A experiência regulatória europeia oferece um exemplo particularmente relevante para a discussão sobre prevenção criminal. O Regulamento (UE) 2024/1689, conhecido como AI Act, classifica determinados sistemas utilizados pelas autoridades de aplicação da lei como de alto risco e estabelece requisitos relacionados com gestão de riscos, qualidade dos dados, documentação, transparência, supervisão humana, robustez, exatidão e cibersegurança. No domínio biométrico, o regime estabelece limites particularmente exigentes para a identificação biométrica remota em espaços públicos e restringe a utilização em tempo real a situações estritamente delimitadas, sujeitas a salvaguardas e, em determinados casos, autorização específica (UNIÃO EUROPEIA, 2024).

O interesse deste enquadramento para o Sul Global não reside em pressupor que a legislação europeia deva ser simplesmente reproduzida. O seu valor está em demonstrar que a adoção de tecnologia de segurança exige uma arquitetura normativa que acompanhe o ciclo completo do sistema: aquisição, desenvolvimento, teste, implementação, utilização, monitorização, auditoria e retirada. Países com outros sistemas jurídicos podem construir mecanismos equivalentes, adequados às suas constituições, leis de proteção de dados e modelos institucionais.

A legitimidade da prevenção tecnológica depende, por isso, de uma relação equilibrada entre eficácia e direitos. Quanto maior a capacidade de um sistema para recolher, cruzar e inferir informação sobre indivíduos, maior deve ser a exigência de justificação, necessidade, proporcionalidade, segurança e controlo. A prevenção não pode converter-se numa autorização genérica para monitorizar populações. A finalidade preventiva deve permanecer vinculada a objetivos legítimos, critérios verificáveis e mecanismos de responsabilização.

Em última instância, a governança deve produzir confiança. Sistemas de segurança que não conseguem explicar como utilizam dados, quem pode aceder aos resultados, como corrigem erros ou quem responde pelos danos tendem a enfraquecer a legitimidade institucional. A transparência não significa revelar informação operacional sensível, mas permitir que os cidadãos, os tribunais, os órgãos de fiscalização e os responsáveis políticos compreendam suficientemente as regras e os limites que orientam o uso da tecnologia.

8.4. Contributos e limitações do estudo

O principal contributo deste estudo é propor uma leitura integrada das tecnologias emergentes como instrumentos de prevenção, articulando capacidade analítica, inteligência, intervenção, avaliação e governança. Em vez de tratar cada tecnologia como solução autónoma, o artigo sustenta que o valor preventivo resulta da combinação entre dados confiáveis, competências profissionais, processos decisórios e mecanismos de controlo. A análise também procura deslocar o debate para o Sul Global, onde a questão não é apenas adotar inovação, mas construir capacidade para a governar.

O estudo apresenta, contudo, limitações. Trata-se de uma investigação teórico-analítica e documental, não de uma avaliação empírica de um sistema policial específico. As conclusões sobre eficácia preventiva devem, portanto, ser entendidas como proposições analíticas a testar em estudos de caso, avaliações comparativas e investigações quantitativas. Em futuras investigações, deverão ser examinados resultados concretos de sistemas de análise criminal, biometria, inteligência forense e cibersegurança em diferentes países do Sul Global, incluindo indicadores de eficácia, custos, erros, impactos sobre direitos e sustentabilidade institucional.

9 CONCLUSÃO

A prevenção da criminalidade encontra-se perante uma transformação estrutural. A digitalização, o big data, a análise preditiva, a inteligência artificial, a inteligência forense e a biometria ampliaram a capacidade de recolher, integrar e interpretar informação. Esta transformação contribui para deslocar a atividade de segurança de uma lógica predominantemente reativa para uma lógica mais antecipatória e orientada por intelligence.

O contributo das tecnologias emergentes é particularmente relevante em cinco planos: identificação de padrões, antecipação de riscos, focalização de recursos, aceleração da análise e aprendizagem institucional. A tecnologia pode, deste modo, reforçar a capacidade preventiva das forças de segurança e melhorar a compreensão de fenómenos criminais complexos.

Contudo, a análise demonstra igualmente que não existe uma relação automática entre inovação tecnológica e segurança. Dados de má qualidade, modelos enviesados, ausência de interoperabilidade, dependência tecnológica, falta de competências e insuficiência regulatória, podem reduzir ou inverter os benefícios esperados. O risco é especialmente relevante quando tecnologias de vigilância e decisão algorítmica produzem efeitos sobre direitos fundamentais.

No contexto do Sul Global, a questão tecnológica deve ser entendida como questão de capacidade e autonomia. A superação da divisão digital e da crescente "intelligence divide" exige investimento em infraestrutura, competências, dados representativos, investigação, cooperação e capacidade regulatória. A cooperação internacional deve evitar relações puramente assimétricas de aquisição e privilegiar transferência de conhecimento, desenvolvimento de capacidades e soluções adaptadas aos contextos locais.

A prevenção criminal tecnologicamente avançada deve, por isso, assentar num princípio simples: a tecnologia deve ampliar a capacidade humana e institucional

de prevenir o crime, não substituir a responsabilidade humana nem enfraquecer o Estado de Direito. O futuro da segurança não dependerá apenas de algoritmos mais sofisticados, mas da capacidade de construir instituições suficientemente competentes para os compreender, suficientemente responsáveis para os controlar e suficientemente legítimas para merecer a confiança das populações.

Em síntese, o verdadeiro contributo das tecnologias emergentes para a prevenção da criminalidade reside na sua integração num sistema de segurança orientado por informação, antecipação, cooperação e avaliação, no qual a inovação tecnológica seja acompanhada por direitos, responsabilidade e autonomia estratégica.

REFERÊNCIAS

ALMASOUD, Ahmed S.; IDOWU, Jamiu Adekunle. Algorithmic fairness in predictive policing. **AI and Ethics**, v. 5, p. 2323-2337, 2025. DOI: 10.1007/s43681-024-00541-3.

BARRENECHE, Carlos; RAMOS-MARTÍN, Juan. **Artificial intelligence**. *In*: SAGE International Encyclopedia of Mass Media and Society. Thousand Oaks: SAGE, 2020.

BARRETT, Lindsey. Reasonably suspicious algorithms: predictive policing at the United States border. **New York University Review of Law & Social Change**, New York, v. 41, n. 3, p. 327-392, 2017.

BECK, Ulrich. **Risk society**: towards a new modernity. London: Sage, 1992.

BONFANTI, Matteo. **Artificial intelligence and the offense-defense balance in cyber security**. *In*: CAVELTY, Myriam; WENGER, Andreas (ed.). Cyber security politics: socio-technological transformations and political fragmentation. London: Routledge, 2022. p. 64-78.

BRANTINGHAM, Jeffrey. The logic of data bias and its impact on place-based predictive policing. **Ohio State Journal of Criminal Law**, Columbus, v. 15, n. 2, p. 473-496, 2018.

BRAYNE, Sarah; ROSENBLAT, Alex; BOYD, Danah. **Predictive policing**. Data & Civil Rights: A New Era of Policing and Justice, 2015.

CLEMENTE, Pedro. **Prevenção e segurança**: política e estratégia. *In*: ALMEIDA, Paulo Pereira de (coord.). Como tornar Portugal um país seguro? Segurança nacional e prevenção da criminalidade. Lisboa: Bnomics, 2013. p. 35-57.

ELIAS, Luís. **A (nova) governança da segurança numa contemporaneidade complexa**. *In*: Estudos comemorativos dos 25 anos do ISCPSI em homenagem ao Superintendente-Chefe Afonso de Almeida. Coimbra: Almedina, 2009.

GOUVEIA, Jorge Bacelar. **Direito da segurança**: cidadania, soberania e cosmopolitismo. Coimbra: Almedina, 2018.

LEGRAND, Tim; VOGEL, Lauren. **Forensic intelligence**. Brisbane: ARC Centre of Excellence in Policing and Security, 2012.

LEGRAND, Tim; VOGEL, Lauren. The landscape of forensic intelligence research. **Australian Journal of Forensic Sciences**, v. 47, n. 1, p. 16-26, 2015. DOI: 10.1080/00450618.2014.928830.

LOURENÇO, Nelson; COSTA, Agostinho. **Estratégia de segurança nacional**: Portugal Horizonte 2030. Coimbra: Almedina, 2018.

LOURENÇO, Nelson et al. **Segurança interna**: desafios e perspetivas. Lisboa: Instituto de Defesa Nacional, 2015.

LYON, David. **Surveillance, Snowden, and big data**: capacities, consequences, critique. Big Data & Society, London, 2014.

NARAYAN, Shivangi. **Predictive policing and the construction of the 'criminal'**: an ethnographic study of Delhi Police. Cham: Palgrave Macmillan, 2023. DOI: 10.1007/978-3-031-40102-2.

NEIVA, Laura. **Big data na investigação criminal**: previsão do risco, vigilância e expectativas sociais na União Europeia. 2019. Dissertação (Mestrado) – Universidade do Minho, Braga, 2019.

PEREIRA, Rui. Sobre o uso de sistemas de identificação biométrica (e de tecnologias de reconhecimento facial) para fins de segurança pública: reflexões a propósito da proposta de Regulamento Europeu sobre a Inteligência Artificial. **Revista da Faculdade de Direito da Universidade de Lisboa**, Lisboa, v. 63, n. 1-2, p. 851-878, 2022.

RATCLIFFE, Jerry H. **Intelligence-led policing**. Cullompton: Willan Publishing, 2003.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento da Inteligência Artificial)**. Jornal Oficial da União Europeia, 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj. Acesso em: 2 set. 2026.

UNITED NATIONS. **Global Dialogue on AI Governance**: themes and structure. New York: United Nations, 2026a. Disponível em: https://www.un.org/global-dialogue-ai-governance/en. Acesso em: 2 set. 2026.

UNITED NATIONS. **Global Digital Compact**. New York: United Nations, 2024a. Disponível em: https://www.un.org/pact-for-the-future/en/annex-i-global-digital-compact. Acesso em: 2 set. 2026.

UNITED NATIONS. **Independent International Scientific Panel on AI**: preliminary report. New York: United Nations, 2026b. Disponível em: https://www.un.org/independent-international-scientific-panel-ai/en/preliminary-report. Acesso em: 2 set. 2026.

VAN BRAKEL, Rosamunde Elise. **Legal, ethical and social issues of AI and law enforcement in Europe: the case of predictive policing**. *In*: SMUHA, Nathalie A. (ed.). The Cambridge handbook of the law, ethics and policy of artificial intelligence. Cambridge: Cambridge University Press, 2025. p. 367-382. DOI: 10.1017/9781009367783.022.

Autoria

1 Ricardo Caiado

Oficial da GNR; PhD in Law & Security; Jurista; Auditor de Segurança Interna; Doutor em Direito e Segurança pela Faculdade de Direito da Universidade NOVA de Lisboa; Professor

https://orcid.org/0000-0003-3655-1026 • rarcaiado@gmail.com

Como citar este artigo

CAIADO, R. O contributo das tecnologias emergentes para a prevenção da criminalidade. **InterAção**, Santa Maria, v. 17, n. 3, e98664, p. 1-26, 2026. DOI 10.5902/2357797598664. Disponível em: https://dx.doi.org/10.5902/2357797598664. Acesso em: dia mês abreviado. ano.