Coordenação
Higor Vinicius Nogueira Jorge

INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA PÚBLICA E JUSTIÇA CRIMINAL

O futuro do direito

Autores
Antonio Carlos Munuera Silveira
Denize dos Santos Ortiz
Ellen Thays Brandão
Higor Vinicius Nogueira Jorge
Ilício Francisco Júnior
Joaquim Leitão Júnior
Kássia Regina Poersch
Marcos Vinícius Alves e Silva Filho
Patrícia Soares Godoy
Pedro Henrique Gomes Alonso
Ricardo Magno Teixeira Fonseca
Sérgio Bautzer
Valéria Cheque Granato
William Lima Rocha

2027

EDITORA JusPODIVM
www.editorajuspodivm.com.br

CAPÍTULO 12

IA APLICADA À INTELIGÊNCIA POLICIAL E À OSINT: ANÁLISE DE REDES, TRIANGULAÇÃO E LIMITES JURÍDICOS

Higor Vinicius Nogueira Jorge

12.1. INTRODUÇÃO

A atividade de inteligência na segurança pública sempre conviveu com uma tensão produtiva: de um lado, a necessidade de produzir conhecimento útil, com rapidez e em escala; de outro, a exigência de operar sob limites jurídicos e controles institucionais que preservem direitos fundamentais e evitem a captura da investigação por atalhos cognitivos. A incorporação de inteligência artificial (IA) e de técnicas de inteligência em fontes abertas – *open source intelligence* (OSINT), ou inteligência de fontes abertas – torna essa tensão ainda mais evidente, porque amplia o alcance da coleta, a capacidade de correlação e a velocidade da disseminação de produtos analíticos. O ponto central deste capítulo é demonstrar que, nesse novo ambiente, a legitimidade do resultado não decorre do "poder" da ferramenta, mas do método que disciplina sua utilização (BRASIL, 2025).

Ao longo das últimas décadas, modelos de policiamento orientado por inteligência (*intelligence-led policing*) consolidaram uma ideia prática: o valor da inteligência está em transformar dados e informações em análise, e análise em decisão orientada por prioridades e por evidências, com mecanismos de validação e de prestação de contas (OSCE, 2017). A IA potencializa exatamente esse movimento. Porém, ao calcular probabilidades e sugerir padrões, ela também cria um risco conhecido: a "ancoragem" do operador no resultado do sistema, com redução da crítica e do contraditório interno, fenômeno descrito como viés de automação (INTERPOL; UNICRI, 2024).

Este capítulo, portanto, propõe uma resposta institucional: empregar IA e OSINT como aceleradores do ciclo de inteligência, mas com documentação reprodutível, prudência inferencial, triangulação de fontes, critérios de minimização e delimitação de escopo, separação rigorosa entre produtos de inteligência e produtos probatórios, e protocolos internos que assegurem legalidade, registro e auditabilidade (BRASIL, 2025).

12.2. IA COMO ACELERADOR DO CICLO DE INTELIGÊNCIA: COLETA, PROCESSAMENTO, ANÁLISE E DISSEMINAÇÃO

O ciclo de inteligência, em termos operacionais, pode ser entendido como um fluxo iterativo de (i) definição de necessidades e prioridades, (ii) coleta, (iii) processamento e organização, (iv) análise, (v) produção e disseminação, e (vi) retroalimentação (OSCE, 2017). A IA se insere sobretudo em três pontos: na coleta e triagem (filtragem e priorização), no processamento (extração de entidades, normalização, deduplicação), e na análise (correlação, detecção de padrões, análise de redes, sumarização).

A vantagem imediata é evidente: ao reduzir o custo marginal de tratar grandes volumes de dados, a IA permite que a inteligência policial opere com bases heterogêneas e, em alguns casos, em tempo quase real. O desafio é menos tecnológico e mais epistêmico: a saída da IA não é "verdade", mas cálculo probabilístico. Por isso, quanto mais automatizada a cadeia de produção de conhecimento, maior deve ser a disciplina de revisão crítica do operador e maior a transparência interna sobre premissas, fontes e limitações (INTERPOL; UNICRI, 2024).

No contexto brasileiro, a governança dessa aceleração não é facultativa. A Portaria MJSP nº 961/2025 fixa diretrizes de legalidade, adequação, necessidade e proporcionalidade como condições do uso de sistemas de tecnologia da informação em investigação criminal e inteligência quando houver risco à privacidade e a outros direitos fundamentais, além de vedar o uso indiscriminado sem objetivo certo ou declarado (BRASIL, 2025). Ela também impõe dever de registro em logs com identificação de usuário, IP, data/hora e natureza da operação, criando trilha de auditoria indispensável ao controle e à responsabilização (BRASIL, 2025).

A consequência metodológica é direta: em ambientes com IA, o ciclo de inteligência deve ser redesenhado para incluir, como etapa explícita, a validação e a auditoria interna do produto analítico. A eficiência passa a ser avaliada não apenas pelo "tempo de resposta", mas pela robustez do caminho: qualidade da fonte, possibilidade de reprodução do achado e grau de independência entre elementos que sustentam a inferência.

12.3. OSINT COM MÉTODO: DOCUMENTAÇÃO, REPRODUTIBILIDADE E PRUDÊNCIA INFERENCIAL

OSINT não é sinônimo de "tudo o que está na internet", nem de "vale tudo porque é público". Trata-se de um modo de obtenção e análise de informação baseado em fontes abertas, cujo valor depende de método e de documentação. Em investigações e análises criminais, a regra é simples: quanto mais frágil a fonte, mais forte deve ser a validação; quanto mais relevante a conclusão, mais independente deve ser a corroboração.

A primeira exigência é a documentação reprodutível. Isso significa registrar, com precisão, o caminho de coleta: data e hora, fonte, forma de acesso, identificadores do conteúdo (URL, ID da publicação, usuário, hash quando aplicável) e evidências do contexto (capturas integrais, metadados disponíveis e, se necessário, preservação do conteúdo em formato que permita auditoria). **Hashing** (função de resumo criptográfico) é um recurso de integridade: ao gerar uma assinatura do arquivo, permite demonstrar que a evidência não foi alterada após a coleta. **Metadados**, por sua vez, são informações sobre a própria informação (por exemplo, data de criação, localização, dispositivo, autor, histórico), úteis tanto para corroborar quanto para refutar hipóteses.

A segunda exigência é a prudência inferencial: separar observação de interpretação. Conteúdos em redes sociais, por exemplo, são altamente sujeitos a anonimato, ironia, manipulação, contas falsas e postagens fora de contexto. O método responsável é declarar o que se observa (o dado) e explicitar o que se infere (a hipótese), incluindo o grau de confiança e as lacunas.

A terceira exigência é a triangulação. Triangular não é "achar mais do mesmo"; é buscar confirmação em fontes independentes, preferencialmente com natureza distinta (por exemplo, fonte aberta + registro administrativo lícito + diligência de campo). Triangulação também serve para reduzir o risco de narrativas autocontidas: a análise deve resistir a um teste básico de falsificação.

12.4. ANÁLISE DE VÍNCULOS: GRAFOS, ENTIDADES, EVENTOS E CORRELAÇÃO (SEM "NARRATIVA PRONTA")

Uma das aplicações mais valiosas – e mais perigosas – da IA na inteligência policial é a análise de vínculos. Em termos técnicos, costuma-se representar relações por grafos: entidades (pessoas, contas, números, veículos, endereços,

dispositivos) são nós; relações (contato, transação, coocorrência, proximidade temporal ou espacial) são arestas. A IA pode auxiliar na extração de entidades, na resolução de identidades (*entity resolution*) e na detecção de comunidades e padrões.

O perigo está na sedução da "história pronta": quando um grafo parece explicar tudo, a equipe passa a ler o mundo a partir dele. Por isso, três cautelas são indispensáveis.

A primeira é evitar equivalências indevidas. Sem um identificador forte, "conta" não é "pessoa"; "IP" não é "autor"; "aparelho" não é "agente". A análise de redes deve explicitar, para cada vínculo, o tipo de evidência que sustenta a relação e o risco de ambiguidade.

A segunda é controlar a propagação de erro. Sistemas que resolvem identidades por similaridade podem errar e, ao errar, espalham o erro por toda a rede. A boa prática é marcar vínculos por níveis de confiança e exigir validação humana reforçada quando o produto analítico for usado para orientar diligências sensíveis.

A terceira é exigir correlação contextual. A mesma ligação (por exemplo, múltiplos contatos) pode significar cooperação criminosa ou mero convívio social. O grafo aponta conexões; o sentido jurídico depende de contexto e de prova.

12.5. LIMITES ENTRE FONTE ABERTA E INTRUSÃO: ONDE A TÉCNICA NÃO AUTORIZA O ABUSO

A fronteira entre OSINT e intrusão é, muitas vezes, uma fronteira de método e de legalidade. A informação pode estar "na internet" e ainda assim exigir proteção jurídica, seja por expectativa legítima de privacidade, seja por barreiras técnicas, seja por sigilo legal.

No plano penal, o ordenamento tipifica condutas intrusivas: a invasão de dispositivo informático alheio, por exemplo, configura crime quando há violação de mecanismo de segurança para obter, adulterar ou destruir dados, ou instalar vulnerabilidades (BRASIL, 1940). No plano das comunicações, a interceptação de comunicações telefônicas, de informática ou telemática sem autorização judicial constitui crime, e o uso de mecanismos de captação deve observar estritamente reserva jurisdicional e limites legais (BRASIL, 1996).

No plano constitucional, a proteção do sigilo de dados e das comunicações integra o núcleo do art. 5º da Constituição, impondo justificativa, necessidade e proporcionalidade para medidas restritivas (BRASIL, 1988). O Marco Civil da Internet reforça a proteção de dados pessoais e do conteúdo de comunicações, condicionando o acesso a determinados dados a hipóteses e formas legais específicas (BRASIL, 2014).

No plano infralegal, a Portaria MJSP nº 961/2025 estabelece que a obtenção de dados sigilosos por soluções de tecnologia da informação somente ocorrerá com decisão judicial específica que autorize a medida, para fins de investigação

criminal e instrução processual penal, reforçando a centralidade do controle jurisdicional (BRASIL, 2025).

Em síntese: o fato de uma técnica existir não significa que seu uso seja legítimo. O método institucional correto é classificar, previamente, o tipo de dado buscado (público, público em sentido estrito, semipúblico, sigiloso), a forma de acesso (sem violação de barreira ou com superação de barreira) e o regime jurídico aplicável. A OSINT responsável é a que resiste a esse filtro sem precisar de "atalhos".

12.6. MINIMIZAÇÃO E FINALIDADE NO TRATAMENTO DE DADOS: REDUZIR DANO COLATERAL

A OSINT, especialmente quando combinada com IA, tende a expandir escopo. O custo de coletar e armazenar é baixo, e a tentação é acumular para "usar depois". Esse movimento é incompatível com um Estado de Direito, porque transforma investigação e inteligência em arquivamento de vidas.

A Lei Geral de Proteção de Dados (LGPD) não se aplica, como regra, ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; contudo, o próprio texto legal condiciona esse tratamento a legislação específica, com medidas proporcionais e estritamente necessárias ao interesse público, observando devido processo e princípios gerais de proteção (BRASIL, 2018b). A Lei nº 15.352/2026 alterou dispositivos da LGPD ligados ao desenho institucional da autoridade nacional e reforça a necessidade de leitura atualizada do regime de proteção de dados no país (BRASIL, 2026).

Além disso, mesmo em ambiente de exceção de aplicabilidade, o dever de minimização é reforçado por normas específicas do setor: a Portaria MJSP nº 961/2025 consagra finalidade, necessidade e proporcionalidade, e exige padrões de segurança e de prevenção a vazamentos, além de impor registro e responsabilização (BRASIL, 2025). A Lei de Acesso à Informação, por sua vez, determina que o tratamento de informações pessoais deve respeitar intimidade, vida privada, honra e imagem (BRASIL, 2011).

Como prática institucional, minimização envolve: (i) delimitar palavras-chave, recortes temporais e geográficos; (ii) filtrar e descartar dados de terceiros sem pertinência; (iii) definir prazos de retenção; (iv) restringir acesso por perfil e necessidade; (v) manter logs e auditoria; (vi) descrever, no produto final, o que foi coletado, o que foi descartado e por quê.

12.7. CONTROLE DE VIÉS INVESTIGATIVO (CVI): HIPÓTESE PRINCIPAL, HIPÓTESE ALTERNATIVA E TESTE

A combinação de OSINT e IA amplifica vieses clássicos. O primeiro é o viés de confirmação: a equipe tende a procurar elementos que confirmem a hipótese

inicial. O segundo é o viés de automação: tende-se a confiar no sistema por sua aparência de objetividade e por sua capacidade de produzir respostas rápidas (INTERPOL; UNICRI, 2024). O terceiro é o viés narrativo: com muitos dados, constrói-se uma história coerente, mas não necessariamente verdadeira.

O Controle de Viés Investigativo (CVI) pode ser operacionalizado por uma regra de ouro: toda hipótese principal deve ser acompanhada de (a) uma hipótese alternativa plausível; (b) o indício que poderia sustentá-la; e (c) a diligência ou o teste que a confirmaria ou afastaria.

Exemplo: uma análise de rede sugere que duas contas pertencem ao mesmo indivíduo por similaridade de escrita e padrão de horários. Hipótese principal: identidade comum. Hipótese alternativa: coordenação de grupo, conta compartilhada ou automação. Testes: busca de identificadores independentes (vínculos técnicos lícitos, eventos presenciais, registros oficiais), comparação com amostras controladas e validação por fontes autônomas. Esse roteiro evita que o grafo seja tratado como prova e preserva o princípio da investigação orientada por evidências.

12.8. PRODUTOS DE INTELIGÊNCIA X PRODUTOS PROBATÓRIOS: O QUE ENTRA (E COMO ENTRA) NO PROCESSO

A inteligência policial produz conhecimento para orientar decisão e priorização. O produto probatório, por sua vez, serve à instrução, sob contraditório. Misturar esses planos gera dois resultados ruins: ou a inteligência perde flexibilidade (porque tenta antecipar o processo), ou o processo perde qualidade (porque recebe inferências como se fossem provas).

A regra correta é separar: produtos de inteligência podem fundamentar planejamento, orientar alvos e justificar pedidos judiciais; porém, quando se pretende inserir um conteúdo de fonte aberta como elemento probatório, é preciso submetê-lo ao percurso de validação e de preservação de integridade. Isso envolve coleta íntegra, registro de contexto, preservação de metadados quando existentes, documentação do caminho e, se necessário, mecanismos de preservação e de obtenção de dados junto a provedores e plataformas, dentro do regime jurídico aplicável (BRASIL, 2014; BRASIL, 2025).

No plano institucional, essa separação também funciona como proteção: ela reduz o risco de nulidades e evita que o processo seja contaminado por inferências não testadas. Em linguagem simples: inteligência aponta onde olhar; prova sustenta o que se afirma.

12.9. MONITORAMENTO DE RISCO CONCRETO VS. CATALOGAÇÃO DE OPINIÕES: RECORTES LEGÍTIMOS

A tecnologia torna possível monitorar discursos, tendências e redes em larga escala. O fato de ser possível, entretanto, não significa que seja legítimo. Em regimes democráticos, o poder estatal de observar precisa ser delimitado por

finalidade, necessidade e controle. A Constituição assegura liberdades de expressão e comunicação e protege a intimidade e a vida privada, de modo que recortes generalizados e permanentes, sem objeto certo, tendem a produzir um efeito de vigilância incompatível com direitos fundamentais (BRASIL, 1988).

Modelos internacionais de policiamento orientado por inteligência enfatizam que a inteligência serve à priorização e à alocação de recursos contra ameaças concretas, não à construção de acervos de "perfilamento" social sem pertinência (OSCE, 2017). No mesmo sentido, a Portaria MJSP nº 961/2025 veda o uso indiscriminado de soluções tecnológicas sem objetivo certo ou declarado, e exige que o uso seja limitado ao estritamente necessário (BRASIL, 2025).

Como critério prático, propõe-se: (i) definir claramente a ameaça ou o risco investigativo; (ii) vincular a coleta a indícios e a recortes objetivos; (iii) submeter operações de maior risco a autorização e controle superiores; (iv) documentar bases e resultados; (v) prever rotas de descarte e revisão. Isso preserva a legitimidade do trabalho e evita que a inteligência se converta em catalogação de opiniões.

12.10. INTEGRAÇÃO FEDERATIVA E INTEROPERABILIDADE: PADRÃO, QUALIDADE E CONTROLE

A inteligência moderna depende de integração: crimes são transnacionais, plataformas são globais, e cadeias financeiras e logísticas atravessam jurisdições. No Brasil, a Lei nº 13.675/2018, ao instituir o Sistema Único de Segurança Pública (SUSP), orienta a atuação conjunta e integrada e prevê compartilhamento de informações, preferencialmente por meio eletrônico e com acesso recíproco a bancos de dados, sob regras e padrões (BRASIL, 2018a). Interoperabilidade, contudo, não pode significar "acesso indiscriminado". Significa padrões comuns com governança, perfis de acesso e trilha de auditoria.

A Portaria MJSP nº 961/2025 reconhece expressamente plataformas de interoperabilidade e soluções de tratamento de dados e impõe registros em logs e mecanismos de segurança para impedir acessos não autorizados e vazamentos (BRASIL, 2025). O desafio institucional é evitar que a integração multiplique o erro e o abuso: dados ruins geram inferências ruins; acessos sem controle geram responsabilização e dano institucional.

A boa interoperabilidade é, portanto, aquela que combina três camadas: qualidade (dados completos e atualizados), governança (regras claras de acesso e finalidade) e controle (logs, auditoria e responsabilização).

12.11. PROTOCOLOS INTERNOS: CHECKLISTS CURTOS DE LEGALIDADE, REGISTRO E AUDITORIA

Para evitar que OSINT e IA virem improviso tecnológico, recomenda-se a adoção de protocolos internos simples, de baixa fricção, mas alto impacto. Um "protocolo mínimo" pode conter, ao menos, os seguintes passos:

a) Definição do objetivo: qual pergunta se pretende responder e por que ela é pertinente ao caso ou à ameaça.

b) Delimitação do escopo: recorte temporal, geográfico e temático; exclusões explícitas para reduzir dano colateral.

c) Classificação do dado: público, semipúblico, sigiloso; identificação do regime jurídico aplicável e necessidade de autorização.

d) Registro da coleta: data/hora, fonte, caminho, identificadores do conteúdo e condições de acesso.

e) Preservação de integridade: armazenamento controlado e, quando aplicável, hash e preservação de metadados.

f) Triangulação: confirmação por fontes independentes e de natureza diversa.

g) CVI: hipótese principal, hipótese alternativa e teste de falsificação.

h) Revisão humana: checagem de erros, vieses e ambiguidade antes da disseminação do produto.

i) Disseminação proporcional: "quem precisa saber" e "para qual finalidade", com registro.

j) Auditoria e descarte: logs, revisões periódicas, prazos de retenção e descarte do irrelevante.

A Portaria MJSP nº 961/2025 fornece, no plano normativo, a base para essa cultura de registro e responsabilização, especialmente ao impor logs e ao vedar uso indiscriminado (BRASIL, 2025). O ganho é duplo: melhora-se a qualidade analítica e protege-se a legitimidade institucional.

CONSIDERAÇÕES FINAIS

A IA aplicada à inteligência policial e à OSINT pode ampliar capacidades de forma decisiva: reduzir tempo de resposta, aumentar a detecção de padrões e tornar mais eficaz a alocação de recursos. O mesmo potencial, contudo, pode degradar garantias se for operado como atalho probatório, como vigilância de largo espectro ou como automação sem revisão crítica.

O método proposto neste capítulo é um compromisso: acelerar o ciclo de inteligência sem perder o controle. Para isso, é indispensável documentação reprodutível, prudência inferencial, triangulação e CVI; separação entre produtos de inteligência e produtos probatórios; minimização e finalidade; e governança com logs e auditabilidade, conforme diretrizes normativas recentes (BRASIL, 2025). Assim, tecnologia deixa de ser promessa e se torna instrumento legítimo, útil e controlável.

REFERÊNCIAS (ABNT – SISTEMA AUTOR-DATA)

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República, 1988. Disponível em: https://normas.leg.br/?urn=urn:lex:br:federal:constituicao:1988-10-05;1988!art5. Acesso em: 28 fev. 2026.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 28 fev. 2026.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Dispõe sobre a interceptação de comunicações telefônicas e dá outras providências. Brasília, DF: Presidência da República, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 28 fev. 2026.

BRASIL. **Lei nº 9.883, de 7 de dezembro de 1999**. Institui o Sistema Brasileiro de Inteligência e cria a Agência Brasileira de Inteligência - ABIN. Brasília, DF: Presidência da República, 1999. Disponível em: https://legis.senado.leg.br/norma/551759. Acesso em: 28 fev. 2026.

BRASIL. **Decreto nº 3.695, de 21 de dezembro de 2000**. Cria o Subsistema de Inteligência de Segurança Pública, no âmbito do Sistema Brasileiro de Inteligência. Brasília, DF: Presidência da República, 2000. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d3695.htm. Acesso em: 28 fev. 2026.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações. Brasília, DF: Presidência da República, 2011. Disponível em: https://legis.senado.leg.br/norma/584383. Acesso em: 28 fev. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014. Disponível em: https://legis.senado.leg.br/norma/584776. Acesso em: 28 fev. 2026.

BRASIL. **Lei nº 13.675, de 11 de junho de 2018**. Institui o Sistema Único de Segurança Pública (SUSP). Brasília, DF: Presidência da República, 2018a. Disponível em: https://legis.senado.leg.br/norma/27394952. Acesso em: 28 fev. 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, 2018b. Disponível em: https://legis.senado.leg.br/norma/27457334. Acesso em: 28 fev. 2026.

BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Portaria MJSP nº 961, de 24 de junho de 2025**. Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. Brasília, DF: MJSP, 2025. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/portaria-do-mjsp-regulamenta-uso-de-tecnologia-em-investigacoes-criminais-e-inteligencia-de-seguranca-publica/portaria-no961-de-24-de-junho-de-2025. Acesso em: 28 fev. 2026.

BRASIL. **Lei nº 15.352, de 25 de fevereiro de 2026**. Transforma cargos no âmbito do Poder Executivo federal; altera a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), e dá outras providências. Brasília, DF: Presidência da República, 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/Lei/L15352.htm. Acesso em: 28 fev. 2026.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução nº 615, de 11 de março de 2025**. Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário. Brasília, DF: CNJ, 2025. Disponível em: https://atos.cnj.jus.br/atos/detalhar/6001. Acesso em: 28 fev. 2026.

INTERPOL; UNICRI. **AI Toolkit: Introduction to Responsible AI Innovation**. Lyon: International Criminal Police Organization; Turin: United Nations Interregional Crime and Justice Research Institute, 2024. Atualização: 2025. Disponível em: https://www.interpol.int/content/download/20931/file/AI_Toolkit_-_Introduction_to_Responsible_AI_Innovation%5B1%5D.pdf. Acesso em: 28 fev. 2026.

OSCE. **OSCE Guidebook on Intelligence-Led Policing**. Vienna: Organization for Security and Co-operation in Europe, 2017. Disponível em: https://www.osce.org/files/f/documents/d/3/327476.pdf. Acesso em: 28 fev. 2026.

EDITORA JusPODIVM
www.editorajuspodivm.com.br

JUS5674