doi.org/10.51891/rease.v11i11.21936

# A IMPORTÂNCIA DA COOPERAÇÃO DA INTELIGÊNCIA DA POLÍCIA MILITAR DO PARANÁ COM O DEPEN

## THE IMPORTANCE OF COOPERATION BETWEEN THE PARANÁ MILITARY POLICE INTELLIGENCE AND DEPEN

**Marcel Felipe Alves Miléo Gomes**[1]

RESUMO: O artigo discute a importância da cooperação entre a Inteligência da Polícia Militar do Paraná (PMPR) e o Departamento Penitenciário (DEPEN/PR), sustentando que a integração de ciclos, métodos e sistemas de informação potencializa a prevenção e a resposta a crimes e eventos críticos intra e extramuros. Parte-se da doutrina de inteligência de segurança pública e de inteligência penitenciária, destacando-se funções, etapas do ciclo e requisitos de governança (sigilo, necessidade de compartilhar, proteção de dados). Argumenta-se que a interoperabilidade técnica, semântica, organizacional e jurídica, aliada a protocolos formais, comitês e métricas compartilhadas, torna mais oportuna a difusão de alertas e a produção de conhecimentos aplicáveis a problemas complexos como facções, mercados ilícitos e violência territorializada. Conclui-se que três alavancas, profissionalização, padronização técnico-metodológica e infraestrutura tecnológica segura, são determinantes para consolidar a cooperação PMPR–DEPEN/PR e elevar a efetividade de políticas e operações orientadas por inteligência.



**Palavras-chave:** Inteligência de Segurança Pública. Inteligência Penitenciária. Cooperação Interagências. Interoperabilidade. Governança em Rede.

ABSTRACT: This article discusses the importance of cooperation between the Paraná Military Police (PMPR) Intelligence Unit and the Penitentiary Department (DEPEN/PR), arguing that the integration of information cycles, methods, and systems enhances the prevention and response to crimes and critical events within and outside the prison walls. It draws on the doctrine of public security intelligence and penitentiary intelligence, highlighting functions, cycle stages, and governance requirements (confidentiality, need to share, data protection). It argues that technical, semantic, organizational, and legal interoperability, combined with formal protocols, committees, and shared metrics, makes the dissemination of alerts and the production of knowledge applicable to complex problems such as factions, illicit markets, and territorialized violence more timely. It concludes that three levers: professionalization, technical and methodological standardization, and secure technological infrastructure are crucial for consolidating PMPR-DEPEN/PR cooperation and increasing the effectiveness of intelligence-driven policies and operations.

**Keywords:** Public Security Intelligence. Penitentiary Intelligence. Interagency Cooperation. Interoperability. Networked Governance.

[1]Agente de Inteligência. Bope/PMPR.

# 1 INTRODUÇÃO

A atividade de inteligência de segurança pública compreende ações de busca, processamento, análise e difusão de conhecimentos para apoiar decisões estratégicas, operacionais e táticas, observando legalidade, precisão e pertinência. O ciclo de inteligência, direção, obtenção, processamento, análise, difusão e retroalimentação, oferece arcabouço metodológico para transformar dados em estimativas e cenários úteis ao decisor.

No contexto estadual, a inteligência conecta-se a arquiteturas de integração de dados e arranjos interorganizacionais, o que impõe desafios adicionais de padronização, qualidade de dados e sincronização de agendas. A coordenação por objetivos estratégicos e o uso de indicadores favorecem o foco em problemas complexos, como organizações criminosas e mercados ilícitos, reforçando a inteligência como insumo de políticas baseadas em evidências.

A inteligência penitenciária, por sua vez, especializa-se na ambiência prisional, com foco em lideranças, dinâmicas faccionais, fluxos ilícitos e riscos de eventos críticos. Seu fluxo informacional demandam bases dedicadas, padronização, rastreabilidade e interoperabilidade com sistemas correlatos, possibilitando antecipar articulações intra e extramuros e apoiar decisões de classificação, movimentação e mitigação de riscos.



Dado que redes criminosas operam simultaneamente dentro e fora do cárcere, a cooperação entre a inteligência da PMPR e a do DEPEN/PR torna-se condição para prevenir e responder a rebeliões, resgates e atentados, desarticular organizações e estabilizar territórios, cuja cooperação exige regras claras de sigilo, interoperabilidade de sistemas, protocolos de difusão e métricas compartilhadas de desempenho.

# 2 REFERENCIAL TEÓRICO

## 2.1 INTELIGÊNCIA DE SEGURANÇA PÚBLICA: CONCEITOS, FUNÇÕES E CICLO DE INTELIGÊNCIA

A atividade de inteligência de segurança pública pode ser compreendida como o conjunto de ações especializadas de busca, processamento e difusão de conhecimentos que subsidiam decisões estratégicas, operacionais e táticas no enfrentamento ao crime e na preservação da ordem, observando princípios de legalidade, oportunidade, precisão e pertinência. No Brasil, a doutrina atualizada da atividade de inteligência enfatiza a produção de conhecimento para a tomada de decisão em contextos complexos e incertos, articulando-se com a democracia e com

a proteção de direitos fundamentais, sem perder de vista a finalidade de antecipação de ameaças e mitigação de riscos em segurança pública (ABIN, 2023; BRASIL, 1999; LOWENTHAL, 2017).

As funções clássicas da inteligência, coleta, análise, proteção do conhecimento (contrainteligência) e difusão, ganham especificidade quando transpostas ao domínio policial, dada a necessidade de integração com operações ostensivas e investigativas, gestão de crises e policiamento orientado por dados. Nessa perspectiva, a função "coleta" demandam fontes humanas, técnicas e abertas, com critérios de validação e rastreabilidade; a "análise" agrega métodos estruturados e colaborativos para transformar dados em estimativas e cenários; a "proteção" envolve segurança da informação, de pessoal e de instalações; e a "difusão" condiciona-se ao princípio do "*need to know*" e à governança do sigilo (ABIN, 2023; BRASIL, 1999; LOWENTHAL, 2017).

O ciclo de inteligência, conforme a doutrina contemporânea, estrutura-se em etapas iterativas: direção (definição de necessidades e prioridades), obtenção (coleta planejada), processamento (depuração, classificação e armazenamento), análise (interpretação, avaliação e inferência), difusão (entrega ao decisor no formato e tempo adequados) e retroalimentação (*feedback* do usuário para ajuste de requisitos). A efetividade do ciclo depende da clareza dos requisitos, da disciplina metodológica na análise e da interoperabilidade dos sistemas de informação que suportam a difusão segura e tempestiva do conhecimento (ABIN, 2023; BRASIL, 1999; LOWENTHAL, 2017).



No contexto da segurança pública estadual, o ciclo de inteligência se conecta a arquiteturas sistêmicas de integração de dados e a arranjos interorganizacionais (como redes e centros integrados), o que impõe desafios adicionais de padronização terminológica, qualidade de dados e sincronização de agendas políticas e operacionais. A coordenação por objetivos estratégicos e o uso de indicadores de desempenho favorecem a priorização da produção de conhecimentos aplicáveis a problemas complexos, como organizações criminosas, mercados ilícitos e violência territorializada, reforçando a inteligência como insumo para políticas baseadas em evidências (ABIN, 2023; BRASIL, 1999; LOWENTHAL, 2017).

A relação entre inteligência e operações é dialética e, desta forma, a ação policial bem-informada retroalimenta o ciclo com dados de campo de alta relevância; ao mesmo tempo, estimativas estratégicas orientam o emprego seletivo e proporcional da força, a gestão do portfólio de investigações e a prevenção situacional. Em instituições militares estaduais, isso se materializa em células de análise vinculadas a comandos operacionais e em protocolos de

difusão que alinham confidencialidade, urgência e utilidade (ABIN, 2023; BRASIL, 1999; LOWENTHAL, 2017).

## 2.2 INTELIGÊNCIA PENITENCIÁRIA: ESPECIFICIDADES, FLUXO INFORMACIONAL E VALOR ESTRATÉGICO

A inteligência penitenciária constitui um campo especializado da atividade de inteligência voltado à ambiência prisional, com foco na identificação de lideranças, dinâmicas de facções, fluxos ilícitos, corrupção, vulnerabilidades de segurança e riscos de eventos críticos. Sua especificidade decorre do ambiente de privação de liberdade, da presença de estruturas hierárquicas criminosas e da necessidade de equilíbrio entre segurança, disciplina e direitos das pessoas privadas de liberdade, o que exige doutrina própria e competências técnicas ajustadas (BRASIL, 2013; DIPEN, 2022; BRASIL, 2012).

O fluxo informacional na inteligência penitenciária demanda mecanismos estáveis de coleta e registro em bases dedicadas, com ênfase em padronização, acurácia e rastreabilidade. A doutrina nacional estabelece princípios como oportunidade, permanência, precisão e simplicidade para orientar a produção do conhecimento, reforçando a necessidade de rotinas de validação, classificação por sensibilidade e interoperabilidade com sistemas correlatos, além de repositórios colaborativos para a rede de inteligência penitenciária (BRASIL, 2013; DIPEN, 2022; BRASIL, 2012).



Como ativo estratégico, a inteligência penitenciária permite antecipar articulações criminosas intra e extramuros, apoiar decisões de classificação e movimentação de presos, orientar varreduras e inspeções, identificar fluxos financeiros ilícitos e detectar padrões de comunicação clandestina. Integrada a órgãos policiais e de justiça, agrega valor ao desmonte de organizações criminosas, ao enfraquecimento de mercados ilícitos e à redução de letalidade associada a conflitos faccionais (BRASIL, 2013; DIPEN, 2022; BRASIL, 2012).

A governança desse fluxo exige um órgão central com capacidade de direção, coordenação e normatização, bem como redes estaduais integradas (RENIPEN), eventos técnicos e visitas de orientação, além de plataformas tecnológicas que facilitem o compartilhamento seguro. A atuação da Diretoria de Inteligência Penitenciária (DIPEN) no âmbito federal exemplifica a importância de rotinas de capacitação, relatórios periódicos e protocolos de articulação com agências coirmãs (DIPEN, 2022; BRASIL, 2013; BRASIL, 2012).

Ferramentas como o SISDEPEN e seus módulos de informação sobre estabelecimentos e indivíduos são vetores estruturantes do fluxo informacional, ao possibilitar leituras

estratégicas sobre a população carcerária, sobre perfis de risco e sobre a geografia do crime organizado. Integradas por APIs com órgãos de justiça e segurança, essas ferramentas ampliam a capacidade de análise e o tempo de resposta, mantendo trilhas de auditoria e controles de acesso (BRASIL, 2012; BRASIL, 2024; DIPEN, 2022).

## 2.3 COOPERAÇÃO INTERAGÊNCIAS: MODELOS, GOVERNANÇA E INTEROPERABILIDADE

A cooperação interagências em segurança pública e administração penal pode ser analisada à luz da literatura de governança em redes, que identifica arranjos variando de estruturas autogovernadas a modelos com organização líder ou entidades administrativas separadas. A escolha do modelo depende do nível de confiança, do número de participantes, da clareza de metas e da necessidade de legitimidade externa, com impactos na tomada de decisão, no desempenho e na responsabilidade (PROVAN; KENIS, 2008; AGRANOFF; MCGUIRE, 2003; BRASIL, 2018).

No plano brasileiro, o Sistema Único de Segurança Pública (SUSP) instituiu princípios e diretrizes para integração federativa, promovendo compartilhamento de dados, operações integradas e arranjos colaborativos entre polícias, órgãos penitenciários e justiça criminal. Essa arquitetura impõe a construção de governanças que conciliem autonomia organizacional e coordenação estratégica, com protocolos para a gestão de conhecimento e de incidentes (BRASIL, 2018; AGRANOFF; MCGUIRE, 2003; PROVAN; KENIS, 2008).



A interoperabilidade, técnica, semântica, organizacional e jurídica, é o cerne da cooperação efetiva e, desta forma, sistemas como o SINESP, marcos de classificação da informação e acordos de nível de serviço para difusão de inteligência sustentam a capacidade de produzir "quadro comum de situação" e de sincronizar respostas entre polícia ostensiva, polícia judiciária e gestão penal (BRASIL, 2012; PROVAN; KENIS, 2008; AGRANOFF; MCGUIRE, 2003).

A governança da cooperação demanda instâncias deliberativas e consultivas com representação das agências, análise de risco compartilhada, priorização de problemas e portfólios conjuntos de operações. O equilíbrio entre centralização e autonomia operacional é dinâmico, sendo certo que em contextos de alta incerteza e múltiplos atores, arranjos com organização líder costumam ganhar tração, desde que disponham de legitimidade, recursos e transparência (PROVAN; KENIS, 2008; BRASIL, 2018; AGRANOFF; MCGUIRE, 2003).

Quando aplicada à relação entre a Inteligência da Polícia Militar do Paraná e o DEPEN/SENAPPEN, a cooperação interagências potencializa a prevenção e a resposta a eventos críticos (rebeliões, resgates, atentados), a neutralização de lideranças e a estabilização territorial. A governança por metas compartilhadas, regras claras de sigilo e interoperabilidade de sistemas torna a difusão de alertas e relatórios mais oportuna, com ganhos mensuráveis em dissuasão e redução de danos (BRASIL, 2018; BRASIL, 2012; PROVAN; KENIS, 2008).

## 2.4 MARCO NORMATIVO: CONSTITUIÇÃO, LEP, SISBIN, LGPD E NORMAS ESTADUAIS PERTINENTES

A Constituição da República atribui à segurança pública o *status* de dever do Estado e responsabilidade de todos, definindo a arquitetura de órgãos e competências e orientando a observância de direitos fundamentais na atuação estatal. Essa moldura constitucional abastece a atividade de inteligência com limites e finalidades, reforçando a necessidade de legalidade estrita, controle e proporcionalidade na produção e difusão de conhecimentos (BRASIL, 1988; BRASIL, 2018; BRASIL, 1999).

A Lei de Execução Penal disciplina a administração carcerária e a execução das penas, estabelecendo princípios e mecanismos que impactam diretamente a inteligência penitenciária, como classificação, movimentação, disciplina e segurança dos estabelecimentos. Ao fornecer os contornos legais para o gerenciamento de riscos no ambiente prisional, a LEP serve de parâmetro para a coleta e o uso de informações que subsidiem decisões administrativas e judiciais (BRASIL, 1984; BRASIL, 2012; BRASIL, 2013).



No âmbito da inteligência de Estado, a Lei nº 9.883/1999 institui o SISBIN e cria a ABIN, definindo objetivos, competências e mecanismos de integração e, embora a inteligência de segurança pública tenha doutrina e governança próprias, a coerência com o SISBIN amplia a capacidade de coordenação estratégica e o fluxo de conhecimentos de interesse nacional, especialmente em temas que extrapolam fronteiras estaduais e demandam visão sistêmica (BRASIL, 1999; ABIN, 2023; BRASIL, 2018).

O tratamento de dados pessoais, inclusive sensíveis, na atividade de inteligência, deve observar os princípios e bases legais da LGPD, com atenção a finalidades legítimas, necessidade, segurança e responsabilização. A conformidade exige políticas de governança e de segurança da informação, classificação de dados, controles de acesso, registros de operações e avaliação de impacto, conciliando o interesse público na segurança com a proteção de direitos individuais (BRASIL, 2018; ABIN, 2023; BRASIL, 2018).

Em nível estadual, o Paraná estruturou seu Sistema Estadual de Inteligência de Segurança Pública, com órgão central e subsistemas (incluindo o Centro de Inteligência da Polícia Militar do Paraná), disciplinando canais técnicos de comunicação, instâncias colegiadas e competências para coordenação e integração. A atualização normativa recente reforça o papel do DIEP como órgão central e consolida a interoperabilidade entre Polícia Militar, Polícia Civil e gestão penal, com reflexos diretos na cooperação com o DEPEN estadual (PARANÁ, 2018; PARANÁ, 2025; BRASIL, 2018).

## 3 CONTEXTO INSTITUCIONAL E OPERACIONAL

### 3.1 ATRIBUIÇÕES E CAPACIDADES DA PMPR NO CAMPO DE INTELIGÊNCIA

No desenho constitucional da segurança pública, às polícias militares cabe a polícia ostensiva e a preservação da ordem pública, missão que exige um componente orgânico de inteligência capaz de antecipar ameaças, apoiar o planejamento operacional e subsidiar decisões táticas e estratégicas (BRASIL, 1988; BRASIL, 2018; LOWENTHAL, 2017). Em consonância com o SUSP, a inteligência da Polícia Militar do Paraná (PMPR) estrutura-se como função permanente de Estado, voltada à produção de conhecimentos oportunos e úteis ao comando, respeitando legalidade, finalidade e proporcionalidade (BRASIL, 2018; ABIN, 2023; BRASIL, 2018).



As atribuições nucleares compreendem direção (gestão de requisitos e prioridades), obtenção (coleta em fontes humanas, técnicas e abertas), processamento (depuração, classificação e armazenamento), análise (métodos estruturados e colaborativos) e difusão (entrega conforme o "*need to know*"), além da contrainteligência — proteção de pessoal, instalações, processos e conhecimentos sensíveis (ABIN, 2023; BRASIL, 1999; LOWENTHAL, 2017). Essas funções são moduladas para o ambiente policial-militar, articulando-se com operações de patrulhamento, policiamento orientado por dados, gestão de crises e apoio a ações interagências (ABIN, 2023; BRASIL, 2018; LOWENTHAL, 2017).

Capacidades operacionais típicas incluem células de análise estratégica e tática, equipes de obtenção (com protocolos para fontes humanas e meios técnicos), segurança orgânica e coordenação de salvaguardas, bem como plataformas de análise criminal e de inteligência com trilhas de auditoria e controles de acesso. Tais capacidades são reforçadas por rotinas de certificação, gestão de riscos e indicadores de desempenho que conectam a produção de

conhecimento a metas institucionais de dissuasão, prevenção e redução de danos (ABIN, 2023; BRASIL, 2018; LOWENTHAL, 2017).

No plano da governança, destacam-se procedimentos padronizados para classificação de informações, gestão do sigilo e intercâmbio com outras forças e órgãos do sistema de justiça criminal, observando-se a legislação de dados pessoais e as diretrizes de proteção da informação. A conformidade com a LGPD e com a doutrina nacional de inteligência condiciona formatos de produtos, prazos de guarda, critérios de anonimização e mecanismos de responsabilidade (BRASIL, 2018; ABIN, 2023; BRASIL, 2018).

## 3.2 ATRIBUIÇÕES E CAPACIDADES DO DEPEN (FOCO NO PARANÁ)

A inteligência penitenciária, no âmbito do Departamento Penitenciário (DEPEN), com a coordenação nacional atualmente a cargo da Secretaria Nacional de Políticas Penais e suas estruturas estaduais, tem como finalidade apoiar a gestão prisional e a segurança interna e externa dos estabelecimentos, identificando lideranças, dinâmicas faccionais, fluxos ilícitos e riscos de eventos críticos (BRASIL, 2013; BRASIL, 1984; BRASIL, 2018). No Paraná, a atuação penitenciária se alinha a essa doutrina, com unidades responsáveis pelo ciclo de inteligência adaptado ao ambiente prisional e por salvaguardas de segurança orgânica (BRASIL, 2013; BRASIL, 1984; BRASIL, 2018).



O fluxo informacional envolve captação sistemática em rotinas carcerárias (revistas, procedimentos disciplinares, classificação e movimentação de pessoas privadas de liberdade), análise de conteúdos apreendidos, monitoramento de comunicações ilícitas e integração com bases de dados penais e policiais. O uso de sistemas nacionais como o SINESP/SENAPPEN e cadastros penitenciários amplia a capacidade de correlação de dados intra e extramuros, com benefícios para a antecipação de riscos e a prevenção de incidentes (BRASIL, 2012; BRASIL, 2013; BRASIL, 2018).

As capacidades críticas incluem a análise de redes criminosas com foco em governança de facções; apoio a decisões de classificação e transferência; proposição de medidas de mitigação (separação de lideranças, reforço de barreiras físicas e procedimentais); e, emissão de alertas estratégicos para as forças policiais quando houver risco de resgates, represálias ou ataques coordenados. Estas capacidades exigem métodos de análise estruturada, protocolos de difusão e interoperabilidade técnica e semântica com parceiros (BRASIL, 2013; LOWENTHAL, 2017; BRASIL, 2018).

No campo das salvaguardas, a inteligência penitenciária opera sob rigorosos critérios de proteção de dados pessoais e sensíveis, conciliando segurança institucional e direitos fundamentais. A LGPD orienta bases legais, minimização de dados, controles de acesso e avaliações de impacto, especialmente quando da difusão de produtos a entes externos ao sistema prisional (BRASIL, 2018; BRASIL, 2013; ABIN, 2023).

Em termos de governança, destacam-se instâncias colegiadas e canais técnicos para articulação com polícias militares e civis, Ministério Público e Poder Judiciário, além de equipes mistas e pontos focais que asseguram difusão tempestiva e segura de estimativas. Na prática, isso se traduz em protocolos de acionamento e produtos padronizados (boletins, estimativas, alertas) para eventos críticos, operações integradas e monitoramento de ameaças (BRASIL, 2013; BRASIL, 2018; PROVAN; KENIS, 2008).

## 3.3 PONTOS DE CONTATO E SOBREPOSIÇÕES DE MISSÃO

Há sobreposições claras e legítimas entre a inteligência da PMPR e a inteligência penitenciária do DEPEN/PR, especialmente na observação de lideranças e redes criminosas que operam simultaneamente dentro e fora do cárcere. A convergência ocorre em três frentes: antecipação de eventos críticos (rebeliões, resgates, atentados), desarticulação de organizações criminosas (planejamento de operações e neutralização de ativos) e estabilização territorial (redução de letalidade e de mercados ilícitos) (BRASIL, 2018; BRASIL, 2013; LOWENTHAL, 2017).



Os principais pontos de contato operacionais incluem o compartilhamento de requisitos e prioridades; interoperabilidade de bases (com critérios de minimização e necessidade); protocolos de difusão de alertas; equipes mistas para análise de redes e planos de operação; e, coordenação de medidas de contrainteligência para proteção de pessoal, instalações e conhecimentos sensíveis (ABIN, 2023; BRASIL, 2018; BRASIL, 2018).

Para mitigar fricções, a governança deve prever regras claras de sigilo e atribuições, instâncias de deliberação para priorização de alvos e mediação de conflitos, bem como métricas compartilhadas de desempenho (tempo de resposta, utilidade percebida, acurácia e impacto). Modelos de governança em rede sugerem que, em contextos de alta interdependência e risco, arranjos com organização líder ou secretariada favorecem coordenação e responsabilidade — desde que sustentados por legitimidade, transparência e recursos (PROVAN; KENIS, 2008; AGRANOFF; MCGUIRE, 2003; BRASIL, 2018).

No plano jurídico e de compliance, a cooperação exige observância simultânea do marco constitucional, da LEP, do SUSP, da LGPD e das normas internas de ambas as instituições em situações de risco relevante. Procedimentos de registro, classificação, auditoria e revisão periódica dos acordos e das trocas de dados compõem a infraestrutura de confiança entre as partes (BRASIL, 1988; BRASIL, 2018; ABIN, 2023).

É importante salientar, ademais, que a maturidade da cooperação PMPR–DEPEN/PR depende de três alavancas: profissionalização contínua (formação e certificação de analistas e gestores), padronização técnico-metodológica (produtos e taxonomias comuns) e infraestrutura tecnológica segura (interoperabilidade, trilhas de auditoria e gestão de identidades) (ABIN, 2023; BRASIL, 2018; LOWENTHAL, 2017).

## 4 MECANISMOS DE COOPERAÇÃO E INTERCÂMBIO DE INFORMAÇÕES

### 4.1 PROTOCOLOS, ACORDOS E COMITÊS DE INTELIGÊNCIA

Importa ser salientado, neste particular, que a cooperação entre a inteligência da Polícia Militar do Paraná e o DEPEN/PR se concretiza por meio de instrumentos formais, acordos de cooperação, protocolos operacionais e termos de confidencialidade, que definem objetivos, escopo, responsabilidades, critérios de acesso e procedimentos de auditoria das trocas informacionais. Esses instrumentos devem se alinhar às diretrizes do SUSP, que estabelece integração, interoperabilidade e governança colaborativa como princípios para o compartilhamento de dados e a atuação integrada em segurança pública (BRASIL, 2018; ABIN, 2023; BRASIL, 2012).



Os comitês de inteligência e câmaras técnicas, com representação das áreas de inteligência, tecnologia da informação, *compliance* e assessoramento jurídico, funcionam como instâncias de direção e coordenação do ciclo de cooperação. Nesses fóruns, são pactuados requisitos de inteligência, agendas de risco, métricas de desempenho e regras de resolução de conflitos, além de serem homologados modelos de produtos e matrizes de classificação que orientarão a difusão interagências (BRASIL, 2018; ABIN, 2023; PROVAN; KENIS, 2008).

O uso de protocolos de incidentes, por exemplo, para rebeliões, resgates e atentados, padroniza acionamentos, prazos de resposta e responsabilidades, reduzindo assimetrias e aumentando a previsibilidade do fluxo informacional. Estes protocolos se vinculam a “gatilhos de difusão” previamente acordados, associando níveis de gravidade à amplitude de compartilhamento e aos formatos de alerta (BRASIL, 2018; ABIN, 2023; BRASIL, 2012).

Ademais, não se deve deixar de mencionar que acordos devem contemplar cláusulas de proteção do conhecimento (contrainteligência), com trilhas de auditoria, controles de identidades, segregação de funções e mecanismos de responsabilização por uso indevido. A robustez desses dispositivos de salvaguarda eleva a confiança mútua e sustenta a continuidade da cooperação, inclusive em contextos de alta pressão operacional (ABIN, 2023; BRASIL, 2018; PROVAN; KENIS, 2008).

## 4.2 SISTEMAS E BASES DE DADOS (EX.: INFOSEG, PLATAFORMAS ESTADUAIS, SIGS)

Nesse particular, oportuno salientar que a interoperabilidade entre sistemas é condição para a cooperação ágil e segura e, desta forma, o SINESP/INFOSEG, previsto em lei, integra dados de segurança pública, prisionais e de justiça, servindo como *backbone* para consultas e correlações que amparam estimativas estratégicas e táticas, cujo uso coordenado exige acordos de perfil de acesso, trilhas de auditoria e conformidade com o ciclo de inteligência (BRASIL, 2012; BRASIL, 2018; ABIN, 2023).

As plataformas estaduais de análise criminal e penitenciária, inclusive sistemas de gestão prisional (SIGs), estruturam cadastros, eventos e vínculos, permitindo leitura integrada de redes criminosas intra e extramuros. Para sustentar a qualidade analítica, é necessário estabelecer taxonomias comuns, dicionários de dados e rotinas de saneamento, além de mecanismos de versionamento e catalogação dos *datasets* operacionais (BRASIL, 2018; ABIN, 2023; LOWENTHAL, 2017).



A integração técnica deve considerar camadas de interoperabilidade (técnica, semântica, organizacional e jurídica), com APIs, padrões de metadados e serviços de identidade federada que habilitem autorização granular por missão. Essa arquitetura deve ser acompanhada de testes de resiliência cibernética e exercícios de mesa para validar tempos de resposta e continuidade de negócios (BRASIL, 2018; ABIN, 2023; BRASIL, 2012).

Como prática recomendada, as bases que armazenam dados pessoais e sensíveis devem operar sob princípios de minimização, necessidade e proporcionalidade, com anonimização/pseudonimização sempre que possível, refletindo as exigências de governança e segurança previstas no ordenamento (BRASIL, 2018; BRASIL, 2018; ABIN, 2023).

## 4.3 PROCEDIMENTOS DE CLASSIFICAÇÃO, COMPARTILHAMENTO E PROTEÇÃO DE DADOS

É importante salientar, aqui, que a classificação da informação organiza o equilíbrio entre utilidade e sigilo e, sendo assim, a matriz de classificação deve ser adotada de forma uniforme entre PMPR e DEPEN/PR, com critérios de temporalidade, revisão periódica e indicação explícita de destinatários autorizados, conforme a doutrina nacional e boas práticas de inteligência (ABIN, 2023; BRASIL, 2018; LOWENTHAL, 2017).

O compartilhamento deve observar o princípio do "*need to know*" combinado ao "*responsibility to share*" em cenários de ameaça relevante, com registro de justificativas, carimbo de tempo, identificação do emissor e do receptor e metadados sobre fonte e confiabilidade (ABIN, 2023; BRASIL, 2018; BRASIL, 2012).

A proteção de dados pessoais, inclusive sensíveis, requer bases legais apropriadas, avaliação de impacto à proteção de dados em atividades de alto risco, segregação por perfil, *logs* invioláveis, gestão de credenciais e trilhas de auditoria. A conformidade com a LGPD deve ser documentada em políticas internas, cláusulas contratuais e relatórios de conformidade submetidos às instâncias de governança (BRASIL, 2018; ABIN, 2023; BRASIL, 2018).

No plano da segurança orgânica, a contrainteligência estabelece controles de acesso físico e lógico, verificação de antecedentes, capacitação periódica em proteção do conhecimento, gestão de incidentes de segurança e procedimentos de resposta a vazamentos, com plano de comunicação e lições aprendidas que retroalimentem a maturidade institucional (ABIN, 2023; LOWENTHAL, 2017; BRASIL, 2018).



## 4.4 CAPACITAÇÃO CONJUNTA E PADRONIZAÇÃO DE PRODUTOS DE INTELIGÊNCIA

A capacitação conjunta PMPR–DEPEN/PR fortalece a linguagem comum, confiança e interoperabilidade, ao passo que trilhas formativas compartilhadas devem abranger métodos de análise estruturada, técnicas de obtenção compatíveis com o ambiente prisional e com operações ostensivas, proteção de dados, segurança da informação e gestão de riscos, alinhadas à doutrina nacional (ABIN, 2023; BRASIL, 2018; LOWENTHAL, 2017).

Os exercícios de mesa e simulações de incidentes, como rebeliões, resgates e atentados coordenados, devem integrar agendas anuais, com roteiros que testem protocolos de difusão, tempos de resposta, tomada de decisão e coordenação entre centros de comando e controle e diretorias penitenciárias (BRASIL, 2018; ABIN, 2023; PROVAN; KENIS, 2008).

A padronização de produtos, como boletins, estimativas, dossiês de alvo, alertas e relatórios pós-ação eleva a utilidade para o decisor e diminui retrabalho e, em decorrência disso, os modelos devem explicitar taxa de confiabilidade da fonte, grau de certeza analítica, hipóteses alternativas, indicadores de alerta e recomendações com glossários unificados (ABIN, 2023; LOWENTHAL, 2017; BRASIL, 2018).

Cabe ainda salientar, ademais, que um programa de certificação de analistas e gestores, com critérios de ingresso, avaliação e manutenção de credenciamento, consolida padrões de desempenho e ética profissional, incentivando a circulação de talentos e a aprendizagem organizacional entre as duas instituições (ABIN, 2023; BRASIL, 2018; LOWENTHAL, 2017).

## 5 CONCLUSÃO

Levando-se em consideração o que foi exposto no decorrer deste estudo, evidencia-se que a cooperação PMPR–DEPEN/PR gera ganhos concretos de oportunidade, utilidade e precisão na produção e difusão do conhecimento, encurtando o tempo entre a detecção do risco e a resposta operacional. A relação dialética entre inteligência e operações reforça um ciclo virtuoso em que a ação em campo retroalimenta estimativas e cenários, elevando a eficácia das decisões.



Para sustentar a cooperação, instrumentos formais, acordos, protocolos e comitês, devem explicitar objetivos, escopo, perfis de acesso, auditoria e salvaguardas de contrainteligência, além de gatilhos de difusão e regras de resolução de conflitos, cujos arranjos ancoram-se em princípios do SUSP e na governança em rede, equilibrando coordenação e autonomia operacional.

A interoperabilidade entre plataformas, como, por exemplo, SINESP/INFOSEG e sistemas estaduais, requer padrões técnicos e semânticos, APIs, identidade federada, trilhas de auditoria e testes de resiliência cibernética, além de observância rigorosa à proteção de dados pessoais (LGPD), com registro de justificativas, carimbo temporal e controle de destinatários.

Por fim, cabe salientar que três alavancas se mostram decisivas para a maturidade da cooperação, a saber: (i) profissionalização contínua de analistas e gestores; (ii) padronização técnico-metodológica de produtos e taxonomias; e, (iii) infraestrutura tecnológica segura com governança de identidades e auditoria. Investir nessas frentes consolida confiança interagências e amplia a capacidade de antecipação e mitigação de ameaças no Paraná.

## REFERÊNCIAS

ABIN. Doutrina da Atividade de Inteligência. Brasília: Agência Brasileira de Inteligência, 2023.

AGRANOFF, R.; MCGUIRE, M. Collaborative Public Management: New Strategies for Local Governments. Washington, DC: Georgetown University Press, 2003.

BRASIL. Lei nº 7.210, de 11 de julho de 1984: Lei de Execução Penal. Brasília: Presidência da República, 1984.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília: Presidência da República, 1988.

BRASIL. Lei nº 9.883, de 7 de dezembro de 1999: institui o Sistema Brasileiro de Inteligência e cria a ABIN. Brasília: Presidência da República, 1999.

BRASIL. Lei nº 12.681, de 4 de julho de 2012: institui o Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas – SINESP. Brasília: Presidência da República, 2012.

BRASIL. Ministério da Justiça e Segurança Pública. Doutrina Nacional de Inteligência Penitenciária. Brasília: MJSP/DEPEN, 2013.

BRASIL. Lei nº 13.675, de 11 de junho de 2018: institui o SUSP e cria a PNSPDS. Brasília: Presidência da República, 2018.



BRASIL. Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018.

BRASIL. Ministério da Justiça e Segurança Pública. SISDEPEN: Manuais e Apostilas. Brasília: SENAPPEN, 2024.

DIPEN. A atuação da Diretoria de Inteligência Penitenciária (DIPEN) no âmbito do Departamento Penitenciário Nacional. Revista Brasileira de Execução Penal, Brasília, v. 3, n. 2, 2022.

LOWENTHAL, M. Intelligence: From Secrets to Policy. 7. ed. Washington, DC: CQ Press, 2017.

PARANÁ. Decreto nº 11.615, de 7 de novembro de 2018: cria o Sistema Estadual de Inteligência de Segurança Pública do Estado do Paraná – SEINSP. Curitiba: Governo do Estado do Paraná, 2018.

PARANÁ. Decreto nº 11.242, de 16 de setembro de 2025: institui o Sistema Estadual de Inteligência de Segurança Pública do Paraná – SEINSP. Curitiba: Governo do Estado do Paraná, 2025.

PROVAN, K. G.; KENIS, P. Modes of network governance: structure, management, and effectiveness. Journal of Public Administration Research and Theory, v. 18, n. 2, p. 229–252, 2008.