

[Home](#) › [Rankings](#) › [Brazil](#) ›

Medina Osorio Advogados

🌐 medinaosorio.com.br

Brazil

[Rankings](#)[About](#)[Lawyers](#)[Client testimonials](#)[Interview with...](#)[News and developments](#)

NEWS AND DEVELOPMENTS

THE CNMP NATIONAL DATABASE IN THE AGE OF INVESTIGATIVE COMPLEXITY: CONSTITUTIONAL, STATISTICAL AND ALGORITHMIC FOUNDATIONS OF CRIMINAL TRACEABILITY

The CNMP National Data Repository in the Age of Investigative Complexity: Constitutional, Statistical, and Algorithmic Foundations of Penal Traceability

Fábio Medina Osório

Managing partner of Medina Osório Advogados. PhD in Administrative Law from the Complutense University of Madrid (Spain). Master's degree in Public Law from the Faculty of Law of the Federal University of Rio Grande do Sul (UFRGS). Former Prosecutor in Rio Grande do Sul. Former Assistant Secretary of Justice and Public Security of the State of Rio Grande do Sul. Former Chief Minister of the Attorney General's Office. President of the Special Commission on Administrative Sanctioning Law of the Federal Council of the OAB. Advisor to the MDA – Advocacy Defense Movement. President of the International Institute of State Law Studies (IIEDE).

This article expresses the academic opinion of the author and not of any institution of which he is part or has been a member.

This essay examines the institutional need for a National Database under the governance of the National Council of the Public Prosecutor's Office (CNMP), conceived as an infrastructure for traceability, coherence and self-criticism in criminal prosecution. It is argued that the private ownership of public criminal action, the external control of police activity and the investigative power of the Public Prosecutor's Office, when interpreted in the context of the Digital Age, presuppose material conditions of intelligibility that cannot be achieved without structured bases, semantic standardization and systemic auditability. In data-driven investigation, the efficiency and integrity of the criminal justice system depend on uniform methodology for collecting, normalizing, resolving identity, and recording decisional and access trails. The article demonstrates – based on comparative evidence extracted from the national and international specialized literature – that the current Brazilian scenario is marked by severe fragmentation: twenty-seven distinct criminal statistical systems, absence of a national semantic standard, refusal of states to share microdata, and documented episodes of vulnerability of databases to criminal actors. Thus, a model of "informational unit" of the Public Prosecutor's Office is proposed, which does not replace national banks of the Executive (nor does it intend to absorb state banks), but organizes the data core of the Public Prosecutor's Office and establishes governed interoperability with external systems, according to standards of quality, security and algorithmic governance. The proposal is contextualized in the light of the General Data Protection Law (LGPD – Law 13,709/2018), CNMP Resolution 318/2025 (BDP/MP), MJSP Ordinance 1,123/2026 (Sinic) and relevant international regulatory frameworks.

Keywords: National database – CNMP – Public Prosecutor's Office – External control – Statistics – Artificial intelligence – Auditability – Traceability – LGPD – Data protection.

Abstract

This essay discusses the institutional need for a National Data Repository governed by Brazil's National Council of the Public Prosecutor's Office (CNMP), conceived as infrastructure for traceability, coherence, and institutional self-critique in criminal prosecution. It argues that the Prosecutor's exclusive authority to bring public criminal actions, its external oversight of police

structured databases, semantic standardization, and systemic auditability. In data-driven investigations, efficiency and integrity depend on uniform methodologies of collection, normalization, entity resolution, and robust trails for access and decision-making. Drawing on comparative evidence from national and international specialized literature, the paper demonstrates that the current Brazilian landscape is characterized by severe fragmentation – twenty-seven distinct criminal statistics systems, absence of national semantic standards, states refusing to share microdata, and documented episodes of database vulnerability to criminal actors. The paper proposes an informational unity model for the Public Prosecutor's Office, which does not replace Executive-branch national databases nor absorb state police databases, but organizes the Prosecutor's own core data and enables governed interoperability with external systems under quality, security, and AI governance standards. The proposal is contextualized in light of Brazil's General Data Protection Law (LGPD – Law 13,709/2018), CNMP Resolution 318/2025 (BDP/MP), Ministry of Justice Ordinance 1,123/2026 (Sinic), and relevant international normative frameworks.

Keywords: National data repository – CNMP – Public Prosecutor – External oversight – Statistics – Artificial intelligence – Auditability – Traceability – Data protection – LGPD.

Summary

1 Introduction – 2 External control, criminal prosecution and investigative power: the constitutional tripod of traceability – 3 Investigation as an informational phenomenon: when efficiency depends on language and method – 4 National database of the CNMP and national banks of the Executive: necessary distinctions – 5 Metric transparency in criminal prosecution: statistics as institutional listening – 6 Algorithmic standardization and auditability: from search to graph – 7 Public data infrastructure, Interinstitutional Agreements and Informational Sovereignty – 8 Protection of Personal Data and Safeguards in Criminal Prosecution – 9 Conclusion: A New Architecture of External Control – 10 Bibliographic References – 11 Legislative References

The 1988 Constitution enshrined a set of classic guarantees – publicity, transparency, reasoning, due process, adversarial proceedings, ample defense – which, historically, were read as requirements oriented to the final decision-making act: the sentence, the judgment, the sanctioning administrative act. The Digital Age has shifted the center of gravity of this debate. Today, the concrete restriction of rights, in the criminal sphere, often materializes before the trial: in the investigative choices, in the criteria for prioritizing targets, in the construction of evidentiary narratives, in intelligence records, in the selection of what is sought and what is ignored. In other words: the decision, in the contemporary world, is composed of a chain of micro-decisions, often invisible, whose legitimacy depends on traceability.

This scenario requires recognizing a methodological premise: one does not understand what cannot be reconstructed. Formal publicity of acts and classic transparency are no longer enough when criminal prosecution becomes dependent on massive databases, structured searches, and algorithmic correlations. If information is fragmented, if records are semantically incompatible between states, if there are no audit trails, the very rationality of the system loses density: the investigation may produce results, but it does not produce intelligibility; it can generate criminal action, but weakens the capacity for critical review; it can condemn, but it dissolves the legitimacy of the course.^[1]

The empirical diagnosis confirms this premise with force. A comprehensive survey on the situation of public security technologies in the Brazilian Federation Units revealed that twelve states do not even use disruptive technologies and another nine did not respond to requests for information during the survey.^[2] The 2023-2024 Public Security Statistical Yearbook, prepared jointly by Ipea and the National Public Security Secretariat (Senasp/MJSP), is even more accurate: Brazil has twenty-seven different criminal statistics systems among civil police forces alone, and the country "still does not have a structured public security information system, with reliable data."^[3] The regulatory vacuum is also documented: the General Data Protection Law (LGPD – Law No. 13,709/2018) provides, in its article 4, an exception for public security and criminal prosecution activities, but this

treated by state agencies.^[4]

In this context, it is important to observe the role of the National Council of the Public Prosecutor's Office (CNMP) which, according to its own official definition, carries out the administrative, financial and disciplinary oversight of the Public Prosecutor's Office in Brazil and its members, respecting the autonomy of the institution. The body, created on December 30, 2004 by Constitutional Amendment No. 45, had its installation completed on June 21, 2005, with headquarters in Brasília-DF. Formed by 14 members representing different sectors of society, the CNMP aims to imprint a national vision to the MP, which is a result of the constitutional principle of institutional unity.

The Council is responsible for guiding and supervising all branches of the Brazilian Public Prosecutor's Office: the Federal Public Prosecutor's Office (MPU), composed of the Federal Public Prosecutor's Office (MPF), the Military Public Prosecutor's Office (MPM), the Labor Public Prosecutor's Office (MPT) and the Federal District and Territories (MPDFT); and the Public Prosecutor's Office of the States (MPE).

Chaired by the Attorney General of the Republic, the Council is composed of four members of the MPU, three members of the MPE, two judges appointed one by the Federal Supreme Court and the other by the Superior Court of Justice, two lawyers appointed by the Federal Council of the Brazilian Bar Association, and two citizens of notable legal knowledge and unblemished reputation, one appointed by the Chamber of Deputies and the other by the Federal Senate.

Before taking office at the CNMP, the names presented are considered by the Commission on Constitution and Justice and Citizenship (CCJ) of the Federal Senate, then go to the Senate Plenary and go to the sanction of the President of the Republic.

Guided by the control and administrative transparency of the Public Prosecutor's Office and its members, the CNMP is an entity open to social control and to Brazilian entities, which can forward complaints against

Such principles must be interpreted in harmony with the principles of efficiency, impersonality, legality, due process, economy, administrative morality, prohibition of arbitrariness by public authorities and the right to understand the content of decisions taken by public authorities.[5]

The implementation of the institutional unity of the Public Prosecutor's Office, in the criminal sphere and in the fight against violent and organized crime, involves national control of the exercise of the institution's investigative power and external control of the police in an integrated and harmonious manner, through strategic and nationally articulated planning.

It is at this point that the constitutional architecture of the Public Prosecutor's Office gains centrality. The CNMP must ensure institutional unity in the management of intelligence of the Brazilian Public Prosecutor's Office and, above all, this management should have a first major impact on public security and criminal investigations throughout the national territory. The Public Prosecutor's Office is not only the private holder of public criminal action (article 129, I, of the Federal Constitution), but also exercises external control of police activity (article 129, VII), in addition to holding requisition powers and, in the jurisprudential horizon consolidated by the Federal Supreme Court (RE 593.727, Topic 184), investigative powers compatible with the Constitution, as long as it is under guarantees. The tripod accusation-control-investigation puts the Public Prosecutor's Office in an inevitable position: it is the recipient and inspector of the investigative product. However, recipient and controller can only operate in a data environment if they have adequate infrastructure. The absence of this infrastructure produces an essential contradiction: the Public Prosecutor's Office carries increasing constitutional responsibilities, but inherits a dispersed, heterogeneous and often opaque informational universe.

Hence the hypothesis of this essay: external control, although not hierarchical, has a conformative nature in the digital world. It conforms to the minimum of registerability, auditability and semantic standardization required for police activity to be controllable, comparable and correctable, and for the ownership of the criminal action to be exercised with national coherence. From this perspective, the CNMP's National Database emerges as an infrastructure of

systems.

It is essential, however, to delimit the object to avoid misunderstandings. The National Bank of the CNMP does not intend to replace national banks of the Executive Branch. The Ministry of Justice and Public Security (MJSP) established the National Criminal Information System (Sinic), by Ordinance No. 1,123/2026, as the official basis for consolidating and making criminal information available. The recent legislative environment – based on the SUSP Law (Law No. 13,675/2018) – also designs thematic national databases in the fight against organized crime, with a federative logic of interoperability. The CNMP Bank has its own vocation: to organize the data center of the Public Prosecutor's Office and allow controlled, auditable and finalistic interoperability – without indiscriminate absorption of state police databases.

2. External control, criminal action and investigative power: the constitutional tripod of traceability

External control is not an administrative command. This statement, although correct, is often misused: as if the absence of hierarchy implies the absence of institutional power. In the Digital Age, precisely the opposite occurs. When police activity materializes in systems, records, and information chains, external control needs to focus on what makes the activity verifiable: minimal records, metadata integrity, traceability of changes, preservation of versions, minimum standardization of remittance, and the ability to reconstruct investigative decisions.

The private ownership of the public criminal action imposes on the Public Prosecutor's Office the responsibility for organizing the accusation based on comprehensible and criticizable evidence. This increasingly requires that investigative acts reach the Public Prosecutor's Office accompanied by essential metadata and trails that allow subsequent measurement. Each piece of a police investigation sent to the Public Prosecutor's Office carries, in the digital age, implicit metadata – timestamps, terminal identifiers, access logs, history of changes – which, when preserved, allow the evidential integrity to be assessed, and, when suppressed or corrupted, make control unfeasible.

External control gains density when it becomes a requirement for auditability, and this auditability, in an informational environment, is always a standard phenomenon. Forensic analysis systems that apply large-scale language models (LLMs) to evidence extracted from mobile devices—such as the framework developed by the South Korean National Police Agency—demonstrate that minimal metadata structuring is a condition of epistemic validity: without precise identification of sender, recipient, timestamp, and conversational context, Digital evidence loses the chain of custody that makes it usable in prosecution.[6]

The inter-organizational dimension of this challenge is equally relevant. In Brazil, investigative powers are distributed among the civil police, the federal police, the military police (in some states), and the Public Prosecutor's Office itself – with shared attributions that historically generate distortions in the production and sharing of intelligence.[7] The absence of a structured data-driven intelligence model – such as the Intelligence-Led Policing (ILP) practiced in the United Kingdom (National Intelligence Model) and adopted as a guideline by the Public Security Intelligence Subsystem (SISP) in Brazil – results in intuition-based patrolling, historically low case resolution rates, and inability to detect criminal networks with interstate operations.[8]

3. Investigation as an informational phenomenon: when efficiency depends on language and method

The investigative inefficiency in Brazil is not explained only by the scarcity of human or technological resources. It is explained, in a significant part, by the absence of a common language between databases. Data-driven investigation relies on finding relationships between scattered records—people, addresses, vehicles, weapons, corporate ties, communications, georeferences. When each state registers in its own language, the national system does not see networks – it sees fragments.

This phenomenon produces a paradox: the investigation is digitized, but the analog logic of the record is preserved. The consequences are predictable: the search does not work, the correlation is precarious, homonyms proliferate, duplicity sets in, and statistical analysis loses validity. The quality of the data is

The 2023-2024 Public Security Statistical Yearbook documents this paradox accurately: most states use their own collection systems (such as RAI in Goiás, SROP in Mato Grosso, and Millenium in the Federal District) and then export spreadsheets or employ Business Intelligence tools to pass on statistical data to the federal government via Sinesp VDE. Some states refuse to send microdata alleging barriers linked to the LGPD "inadequately", compromising the statistical validity and, by extension, the rationality of public policies based on this data.

International research on disruptive technologies in public security provides instructive contrast. The SafetySmart platform, operated by SoundThinking, Inc. in the United States, processes more than 1.3 billion structured and unstructured records from multiple jurisdictions through a federated search engine, CrimeTracer, which allows it to "access and cross-reference crucial information from multiple IT agencies across cities, counties, states and across the country." The CaseBuilder module digitally structures all case information in a unified format, eliminating manual processes and siloed systems. The comparison is not a recommendation for the privatization of criminal intelligence – a model that raises serious objections of informational sovereignty and democratic control, as discussed later – but a demonstration that semantic standardization and federated search are technically feasible and operationally transformative.

At the level of evidentiary microanalysis, recent research demonstrates that structuring the metadata of messages extracted from smartphones—with standardized fields of sender, recipient, timestamp, chat room identifier, and message type—allows language models (such as GPT, in its more advanced versions, and Claude, in its more advanced versions) to automate reading, understanding context and extracting hidden criminal evidence, dramatically reducing the time required to analyze massive volumes of data in strict procedural timelines. The Italian study on Knowledge Graphs and NLP applied to the analysis of messages from real fraud and corruption investigations points in the same direction: the structuring of metadata (list of participants, times, senders, attachments, entities identified by NER – Recognition of Named

"Contestable AI" – a concept proposed by German researchers at the Federal University of the Bundeswehr in Munich – goes further: it proposes that criminal intelligence analysis systems are not only explainable, but contestable, allowing the human investigator to question, correct, and refine algorithmic outputs through semantic modeling and structured human supervision.^[9] These developments converge on the same conclusion: the quality of the input data—its completeness, semantic standardization, traceability, and completeness—determines the quality ceiling of the output analysis, whether done by humans or algorithms.

4. National bank of the CNMP and national banks of the Executive: necessary distinctions

CNMP Resolution No. 318/2025 establishes the Procedural Database of the Public Prosecutor's Office (BDP/MP) and establishes rules for treatment, governance, and use. It is the institutional core of the CNMP's National Bank: procedural and extrajudicial data of the MP, organized under national standards and its own governance. The basis is justified by the constitutional nature of the Public Prosecutor's Office as the holder of criminal and fiscal action in the legal system: without a structured institutional memory, the exercise of these functions is systematically dependent on information produced by third parties – which compromises both functional independence and the quality of prosecution.

Sinic, in turn, was established by the MJSP, by Ordinance No. 1,123/2026, as the official basis for consolidating and making available criminal information – indictments, complaints, and convictions – with the vocation of becoming the "single source" for issuing the National Criminal Certificate and the Criminal Records Sheet, progressively replacing the fragmented systems of courts, civil police, and identification institutes of the Federation Units.^[10] The SUSP ecosystem (Law No. 13,675/2018) provides the legal framework for national integration of public security data, with Sinesp as the reference system for police statistics.^[11]

produced by the Public Prosecutor's Office in all spheres; (ii) governed interoperability with federal and state bases (bridge), through technical protocols, sharing agreements and audit trails; and (iii) analytical and statistical layer (institutional intelligence), which allows the CNMP to exercise its function of planning, evaluating, and controlling criminal prosecution. The legitimacy of the project depends precisely on this distinction: not to duplicate, not to absorb indiscriminately, but to integrate with governance.

The distinction between controller and operator, under the terms of the LGPD (Law No. 13,709/2018), is essential here. The CNMP, as the public controller of BDP/MP's data, defines the purposes and means of processing; the police and other agencies that feed the system operate as sources; and any technology companies hired to develop state connectors and normalize data act as technical operators, subject to the controller's instructions and subject to periodic audits. This responsibility architecture is a condition of compliance with article 23 of the LGPD, which imposes on the Government the duty to publish its processing rules and to appoint the Data Protection Officer (DPO).

Sinic incorporates, as an express normative guideline, records of people convicted of being part of criminal organizations or factions – which densifies criminal intelligence against organized crime at the national level. The experience of the Integrated Network of Genetic Profile Banks (RIBPG), which already accumulates more than 254 thousand genetic profiles in federated architecture (23 state banks connected to the National Bank of Genetic Profiles – BNPG), demonstrates that this interoperability is technically feasible and institutionally sustainable.^[12] The RIBPG model – with a technical standard defined in the Manual of Operational Procedures, standardized software (CODIS) and connectivity to the INTERPOL base – offers a template for the CNMP Bank: federated architecture, centralized technical standard, public governance and external auditability.

5. Metric transparency in criminal prosecution: statistics as institutional listening

In criminal prosecution, statistics should not be reduced to annual reports or occurrence counts. In the Age of Complexity, statistics is the scientific form of

comparable data and with measurable quality.

The 2023-2024 Statistical Yearbook of Public Security documents that organized crime (such as PCC and CV) operates strongly in border regions (North and Midwest), using transnational routes for the flow of drugs and weapons, but "there is currently no federal initiative or single and consolidated database that integrates the various institutions (Senappen, CNJ, Federal Police, Coaf, Abin) for a comprehensive diagnosis of organized crime". The absence of an integrated database forces researchers to construct proxies – indirect markers – using existing databases (Sinesp), such as the ratio between completed and attempted homicides, seizures of large-caliber weapons, and rates of intentional deaths within the prison system.

International frameworks of statistical quality gain relevance here. The IMF's Data Quality Assessment Framework (DQAF) and the United Nations Fundamental Principles of Official Statistics (UN Resolution 68/261) enshrine integrity, reliability, confidentiality, and responsible use as conditions of public trust.^[13] These principles have direct implications for the CNMP Bank: (i) UN Principle 6 determines that individual data collected by statistical agencies must be "strictly confidential and used exclusively for statistical purposes", which imposes a structural separation between the aggregated analytical layer of the database and the individual procedural data, with differentiated access controls; (ii) Principle 8 prescribes that "coordination between statistical agencies within countries is essential to achieve consistency and efficiency in the statistical system", justifying the role of the CNMP as national coordinator of statistics of the Public Prosecutor's Office; and (iii) Principle 9 defends the international standardization of concepts and classifications, guiding the choices of schema and legal ontology for the system.

Research on predictive policing in Brazil reveals that states and municipalities have adopted "self-regulation" in the application of algorithms, "subjecting public security to methodological flaws, government discretion, data leakage, and discriminatory bias."^[14] This fragmentary self-regulation compromises not only investigative efficiency, but the legitimacy of the statistics produced: when a state's algorithm is fed with data that "portrays the selectivity of the

auditing the Detecta system, found "conflicts between operational systems, lack of infrastructure and training", which illustrates that the absence of structured governance affects both the operational validity and the statistical reliability of the data.

A documented episode dramatically illustrates the risk of the absence of governance: in 2023, an investigation by the Federal Police revealed that the PCC (First Command of the Capital) was able to access the Detecta camera system, using the state database to monitor an unmarked Civil Police vehicle in the midst of an assassination plot.^[15] The episode demonstrates that public security databases without adequate access controls, authentication, anomaly monitoring, and vulnerability management can be instrumentalized by organized crime itself – converting it from a protection tool into a threat vector.

6. Algorithmic standardization and auditability: from search to graph

Algorithmic standardization does not mean imposing a single software on states. It means enforcing minimal properties: (i) versioned canonical schema – data structure with defined fields and types, version-controlled to ensure backward compatibility; (ii) semantic dictionary – controlled vocabulary of legal and criminological terms that ensures that the same phenomenon is described in the same way in all systems; (iii) identity resolution rules – algorithms that identify whether two records refer to the same individual, entity, or event, eliminating duplicates and homonyms; (iv) immutable logs – access and operation records that cannot be changed retroactively, essential to the digital chain of custody; (v) transformation trails (data lineage) – tracking of all transformations undergone by the data from collection to analytical use; and (vi) quality metrics by source and by state – measurable indicators of completeness, consistency, accuracy, and timeliness.

AI risk governance, as emphasized by the NIST AI RMF 1.0 (Artificial Intelligence Risk Management Framework), is based on the premise that risks emerge from the interaction between technical components and social and institutional factors, requiring documentation, control, and continuous management.^[16] The framework organizes the governance of AI systems into four functions – Govern, Map, Measure, and Manage – directly applicable to

The European AI Act (Regulation (EU) 2024/1689) enshrines risk management, transparency and governance obligations that are especially relevant when systems impact fundamental rights and enforcement activities.^[17] The regulation classifies AI systems aimed at law enforcement as high-risk, requiring impact assessment on fundamental rights before deployment, structured human oversight, accuracy testing, and assessment of demographic disparities. Although it is a rule of European law, the AI Act works as a reference parameter for the governance of similar systems in Brazil, especially in the absence of specific legislation for AI applied to public security.

The U.S. Department of Justice's Final Report on AI and Criminal Justice (2024) – prepared in compliance with Section 7.1(b) of Executive Order 14.110 (repealed on January 20, 2025 by President Trump, without prejudice to the documents produced during its validity) – points out that AI tools used to "identify criminal suspects, predict crimes, apply digital forensics techniques, monitor social networks, or track the physical location of individuals" must be subject to AI Impact Assessments and structured risk management practices, with procedures to audit input data and avoid discriminatory feedback loops.^[18] White House Memorandum M-25-21 (OMB, 2025) reinforces this guidance, mandating that Chief AI Officers and Chief Data Officers coordinate cross-agency interoperability criteria and invest in "quality data assets, technology infrastructure, and governance in the collection, curation, and preparation of information."^[19]

These milestones help give contemporary density to the central argument: databases and algorithms are not just tools; they are infrastructures of power that require auditability. UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021) is explicit in prohibiting the use of AI for "social scoring or mass surveillance" and in requiring systems deployed by States for law enforcement to submit to independent oversight mechanisms, ensuring that training data "does not reinforce bias, inequalities or discrimination".^[20]

On the technical level, the Knowledge Graph architecture – as proposed in the Neo4j-based system for analyzing messages from criminal investigations –

represents entities (people, organizations, places) and their relationships (communicated with, transferred money to, appeared in the same place as) with semantic enrichment by NER (Named Entity Recognition) and automatic transcription of audios. The FEDLEGAL benchmark, discussed in the Computational Law literature, proposes Federated Learning as an alternative architecture to train AI models on sensitive legal data without physically centralizing the data – preserving the privacy of distributed databases and, at the same time, allowing collective learning.^[21]

7. Public data infrastructure, interinstitutional agreements and informational sovereignty

The viability of the CNMP Bank, on a federative scale, presupposes interoperability agreements and protocols with state systems, with the MJSP SINIC, with Sinesp and with thematic bases such as the RIBPG. These instruments must define: (a) the types of data being shared (category, purpose and sensitivity); (b) the legal bases applicable in each case (article 7, III or VI; article 11, II, f; and article 23 of the LGPD, depending on whether or not the data is of a sensitive nature); (c) the technical safeguards required (encryption at rest and in transit, role-based access control, multi-factor authentication, immutable access logs); (d) the responsibilities of each party (controller, co-controller or processor); and (e) the audit and accountability mechanisms.

The company eventually hired by the CNMP must act as a technical operator, implementing state connectors and normalizing data to the national standard, under the governance of the public controller. This relationship must be governed by a data processing agreement (article 39 of the LGPD), with periodic audit clauses, prohibition of the use of data for purposes other than the contract, mandatory notification in the event of a security incident (article 48 of the LGPD) and secure termination of the processing at the end of the contract. The model is not one of privatization of criminal intelligence – which raises serious objections of informational sovereignty and democratic accountability – but of technical outsourcing with public responsibility preserved.

entities from different spheres can be made possible by "gradual access" mechanisms, conditioned to the fulfillment of technical and legal requirements.^[22] The model of American fusion centers – centers where criminal agencies at the local, state, and federal levels integrate and share intelligence – offers a reference for the articulation between the CNMP Bank and the intelligence centers of the state and federal police.

At the global level, INTERPOL's architecture demonstrates that criminal intelligence databases with transnational reach are viable under strict governance: all data shared by member countries "comply with strict international standards, with a legal basis and built-in security features", with structured access through the secure I-24/7 system and the ability to simultaneously consult the national databases and the central database, in real time.^[23] This reinforces that informational sovereignty is not incompatible with interoperability – as long as access is controlled, the purpose is defined, and the data remains under the governance of public authority.

The objective of the CNMP Bank is not to "copy everything", but to create an auditable bridge that allows search and correlation on a national scale, with preservation of functional confidentiality and compliance with the LGPD. Criminal intelligence data, communications protected by professional secrecy, defendants' mental health data, information on victims of sexual crimes, and protected witness data require differentiated treatment, with more restrictive access controls and more narrowly defined purposes.

8. Protection of personal data and safeguards in criminal prosecution

The articulation between public security and personal data protection is one of the most complex knots in the contemporary Brazilian legal system. The LGPD (Law No. 13,709/2018), in its article 4, III, excludes from its scope of application the processing of data for the exclusive purposes of public security, national defense, State security, and activities of investigation and prosecution of criminal offenses – excluding such processing operations from the general incidence of the law and referring them to the specific law to be enacted.

argument: the fundamental rights to privacy (article 5, X), data protection (article 5, LXXIX, with EC No. 115/2022) and due process of law (article 5, LIV) constitute insurmountable limits even for criminal prosecution, regardless of ordinary law. Second, the systemic argument: the absence of a specific law does not create an absolute normative vacuum, since the following affect the matter: (i) the Code of Criminal Procedure (CPP), which regulates the production of evidence and the integrity of chains of custody; (ii) the CNMP resolutions on data handling and functional secrecy; (iii) Convention 108+ of the Council of Europe, to which Brazil is not a party, but which functions as an interpretative parameter for data protection in law enforcement contexts; and (iv) UNESCO's guidelines on ethics in AI, which impose specific safeguards for data relating to offences, criminal prosecutions and convictions.

For the purposes of application to the CNMP Bank, the principles of data protection operate as follows. The principle of purpose determines that each type of data can only be processed for the purpose that justified its collection – data collected for criminal identification purposes cannot be reused for the purposes of behavioral profiling or continuous surveillance. The principle of necessity imposes that the bank collects only the minimum amount of data indispensable for the defined purposes, prohibiting the speculative collection or storage of unnecessary data. The principle of adequacy requires that the means of processing be proportionate to the purpose pursued. The principle of transparency requires the publication of processing rules and the designation of a data officer (DPO). The principle of security requires the adoption of technical and administrative measures to protect data against unauthorized access, destruction, loss and alteration. The principle of accountability imposes on the controller the obligation to demonstrate compliance and to respond for damages caused as a result of the processing.

These principles impose, in practice, a set of operational safeguards for the CNMP Bank: (a) mapping of data categories and sensitivity assessment (data related to infractions, racial origin, health, sexual orientation and private life receive reinforced protection); (b) role-based access control (RBAC), with differentiated profiles for intelligence consultants, prosecutors, system administrators, and auditors; (c) immutable access logs, periodically audited

specific procedural purposes; (e) Data Protection Impact Assessment (DPIA) prior to the deployment of new analytics modules, especially those using AI; and (f) incident response plan, with notification to the CNMP, the National Data Protection Authority (ANPD) and, when applicable, to the subject of the affected data.

One specific risk deserves attention: algorithmic bias. When the data that feeds a criminal AI system were collected in the context of selective policing – with overrepresentation of certain population groups in the records of suspects, infractions, and convictions – the algorithms trained on this basis reproduce and amplify structural discrimination, violating the principles of equality (article 5, I, of the FC) and non-discrimination. Mitigation requires: (i) bias audit on the input data and on the outputs of the system; (ii) demographic disparity tests in analytical results; (iii) documentation of the model's design choices and limitations; and (iv) mandatory human oversight over decisions that impact individual rights.

9. Conclusion: A New External Control Architecture

External control, in the digital world, is not limited to inspections and recommendations. It is realized as a requirement for traceability. Traceability, in turn, depends on common language, collection methodology, data quality, and auditability of accesses and transformations. Without these conditions, external control remains rhetorical – a formal guarantee that does not reach the field where decisions are actually made: in the chain of investigative micro-decisions that precede the accusatory act.

The construction of the CNMP's National Database, based on the BDP/MP and articulated with the national databases of the Executive – especially Sinic – through governed interoperability, represents an institutional architecture capable of increasing investigative efficiency, strengthening fundamental rights, and allowing self-criticism of the criminal justice system. This architecture is necessary, but not sufficient: it needs to be accompanied by a specific law for the processing of data in criminal prosecution (to be approved in the manner required by article 4, paragraph 1, of the LGPD), a National Data Protection Authority (ANPD) strengthened in its capacity to oversee the Public

The international literature converges, with variations of emphasis, around five fundamental lessons for the construction of this type of infrastructure: (i) data fragmentation is the main obstacle to effective criminal intelligence, and semantic standardization is a precondition for integration; (ii) the centralization of data without adequate governance creates risks of abuse, discrimination, and instrumentalization by criminal actors; (iii) human oversight is irreplaceable – algorithms identify patterns, but do not exercise judgment; (iv) external accountability (auditing, parliamentary oversight, judicial control) is a condition for legitimacy; and (v) federated interoperability – an architecture in which data resides in the agencies of origin and is accessed by controlled consultation, as in the RIBPG and INTERPOL model – is more compatible with Brazilian federalism and data protection principles than unrestricted physical centralization.

The Public Prosecutor's Office, as the holder of the criminal action and guardian of the Democratic Rule of Law (article 127, caput, of the Federal Constitution), is responsible for leading this process – not because the National Bank is its exclusive property, but because no other institutional actor has the same constitutional scope as the mandate to accuse, control and investigate. The informational unity of the Public Prosecutor's Office is not centralism; It is the epistemic presupposition of a criminal prosecution that aspires to coherence, equity and the possibility of being corrected.

10. Bibliographic references

AMBROSIO, Gleiner Pedroso Ferreira; BARBOSA, André Luis Jardini. The paradigm of the implementation of artificial intelligence in Brazilian public security: regulation versus efficiency. *Journal of Legal Studies of UNESP*, v. 28, n. 48, 2024.

ARRIETA, Alejandro Barredo et al. Explainable Artificial Intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, v. 58, p. 82-115, 2020.

policymakers. Cambridge, MA: Shorenstein Center/HKS, 2024.

GROSSI, Alexandre Viezzer. The application of Artificial Intelligence in Brazilian public security: the case of São Paulo and the analysis of PL No. 2338/2023. *Journal of Public Policies & Cities*, v. 14, n. 4, 2025. ISSN: 2359-1552. DOI: <https://doi.org/10.23900/2359-1552v14n4-72-2025>.

INTERPOL. Rules on the Processing of Data (RPD). Lyon: INTERPOL, 2019.

INTERNATIONAL MONETARY FUND (IMF). Data Quality Assessment Framework (DQAF). Washington, D.C.: IMF, 2012.

IPEA; SENASP/MJSP. Statistical Yearbook of Public Security 2023-2024. Brasília: Ipea, 2025. DOI: <https://dx.doi.org/10.38116/ri-anuario-estatistico-2023-2024>.

KERDVIBULVECH, Chutisant. Big Data and AI-driven evidence analysis: a global perspective on citation trends, accessibility, and future research in legal applications. *Journal of Big Data*, v. 11, n. 180, 2024.

KIM, Kyung-Jong; LEE, Chan-Hwi; BAE, So-Eun; CHOI, Ju-Hyun; KANG, Wook. Digital forensics in law enforcement: A case study of LLM-driven evidence analysis. *Forensic Science International: Digital Investigation*, v. 54, art. 301939, 2025. DOI: <https://doi.org/10.1016/j.fsidi.2025.301939>.

KÜÇÜK, Dilek; CAN, Fazli. Computational law: datasets, benchmarks, and ontologies. *arXiv*, 2025. Preprint 2503.04305v2.

MAORO, Falk; GEIERHOS, Michaela. Contestable AI for criminal intelligence analysis: improving decision-making through semantic modeling and human oversight. *Frontiers in Artificial Intelligence*, v. 8, art. 1602998, 2025. DOI: [10.3389/frai.2025.1602998](https://doi.org/10.3389/frai.2025.1602998).

MJSP/CG-RIBPG. XXII Report of the Integrated Network of Genetic Profile Banks (RIBPG): Statistical data and results – Nov/2024 to May/2025. Brasília: MJSP, May 2025.

2023. (NIST. AI.100-1). DOI: <https://doi.org/10.6028/NIST.AI.100-1>.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). Recommendation of the Council on Artificial Intelligence. Paris: OECD, 2019 (revisada em 2024).

OSÓRIO, Fábio Medina. The right to understanding in the era of technological complexity: constitutional, statistical and algorithmic foundations of decision-making transparency. *Revista dos Tribunais*, v. 1077/2025, jul. 2025. DTR\2025\7689.

PADIU, Bogdan; IACOB, Radu; REBEDEA, Traian; DASCALU, Mihai. To what extent have LLMs reshaped the legal domain so far? A scoping literature review. *Information*, v. 15, n. 11, 2024.

POZZI, Riccardo; BARBERA, Valentina; PRINCIPE, Renzo Alva; GIARDINI, Davide; PALMONARI, Matteo. Combining Knowledge Graphs and NLP to Analyze Instant Messaging Data in Criminal Investigations. In: *Proceedings of WISE 2024*. Springer, 2024. DOI: https://doi.org/10.1007/978-981-96-0567-5_30.

PYTLOWANCIV, Diogo Fernando Sampaio. Intelligence-Led Policing and its Possibility of Implementation in Brazil. *Brazilian Journal of Police Sciences*, v. 15, n. 1, p. 103-123, Jan./Apr. 2024. ISSN: 2318-6917.

RIGANO, Christopher. Using Artificial Intelligence to Address Criminal Justice Needs. *NIJ Journal*, n. 280. Washington, D.C.: National Institute of Justice, jan. 2019. NCJ 252038.

SOUNDTHINKING, INC. Form 10-K: Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 (Fiscal Year Ended December 31, 2024). U.S. Securities and Exchange Commission, 2025. Commission File Number 001-38107; Nasdaq: SSTI.

TSUNODA, Denise Fukumi; CÂNDIDO, Ana Clara; GUIMARÃES, André José Ribeiro. Disruptive technologies in public security: a Brazilian situational

UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021. Código SHS/BIO/REC-AIETHICS/2021.

UNITED NATIONS. Fundamental Principles of Official Statistics. Resolution 68/261. New York: United Nations Statistics Division, 2014. A/RES/68/261.

UNITED STATES DEPARTMENT OF JUSTICE. Artificial Intelligence and Criminal Justice: Final Report. Washington, D.C.: U.S. DOJ, 3 dez. 2024.

VOUGHT, Russell T. M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust. Washington, D.C.: Executive Office of the President, Office of Management and Budget, 3 abr. 2025.

11. Legislative references

BRAZIL. Constitution of the Federative Republic of Brazil of 1988.

BRAZIL. Constitutional Amendment No. 115, of February 10, 2022. It includes the protection of personal data among the fundamental rights and guarantees (art. 5, LXXIX, FC).

BRAZIL. Law No. 13,675, of June 11, 2018. Establishes the Unified Public Security System (SUSP).

BRAZIL. Law No. 13,709, of August 14, 2018. General Law for the P

RANKINGS

Jurisdictions

Submissions

Future Lawyers

FIRMS & LAWYERS

Service Providers

Barristers' Sets

Networks

Interview with...

[GC Powerlist](#)

[Legal Business](#)

[News & Developments](#)

Comparative Guides

Events

Legal 500 TV

ABOUT US

[Legal 500](#)

[FAQs](#)

[Marketing](#)

[Careers](#)

[Contact us](#)

[Deutschland](#) 

[Paris](#) 



© 2026 Legalease Ltd. All rights reserved

Registered company in England & Wales No. 02427356 VAT GB 321 5727 22

Registered address: 188 Fleet Street, London, EC4A 2AG

[Data Protection policies](#) [Cookies Policy](#) [Supplier Code of Conduct](#) [Modern Slavery and Human Trafficking Statement](#)

[Contact Us](#)