FORENSIC ODONTOLOGY: DIGITAL SYSTEMS AND A PROPOSAL FOR A BRAZILIAN INTEROPERABLE NATIONAL REGISTRY

ODONTOLOGIA LEGAL: SISTEMAS DIGITAIS E PROPOSTA DE UM REGISTRO NACIONAL INTEROPERÁVEL BRASILEIRO

ODONTOLOGÍA FORENSE: SISTEMAS DIGITALES Y PROPUESTA PARA UN REGISTRO NACIONAL BRASILEÑO INTEROPERABLE

doi https://doi.org/10.56238/sevened2025.014-008

Walter Rosas Dias[1]

ABSTRACT

Brazilian forensic odontology faces significant challenges in the digitalization of its procedures, particularly regarding standardization, traceability, and legal admissibility of dental evidence. This article provides an overview of the systems currently in use, identifies regulatory gaps, and proposes the creation of a national forensic dental record system (sinarof), based on dicom standards, sha 256 hashing, icp-brasil digital signatures, and encrypted audit logs. Although the proposal is grounded in the brazilian context, it offers valuable insights for other federative countries facing similar challenges in the digital integration of dental identification systems.

Keywords: Forensic Odontology. Digital Chain of Custody. Forensic Systems. Human Identification. Interoperability. Cryptographic Hash. Digital Signature.

RESUMO

A odontologia legal brasileira enfrenta desafios significativos na digitalização de seus procedimentos, especialmente no que se refere à padronização, rastreabilidade e validade jurídica dos vestígios dentários. Este artigo apresenta um panorama dos sistemas utilizados, analisa lacunas regulatórias e propõe a criação do sistema nacional de registro odontológico forense (sinarof), com base em padrões como dicom, hash sha 256, assinatura digital icp brasil e logs criptografados. Embora a proposta seja ancorada na realidade brasileira, ela oferece contribuições relevantes para outras nações federativas que enfrentam desafios semelhantes na integração digital da identificação odontológica forense.

Palavras-chave: Odontologia Legal. Cadeia de Custódia Digital. Sistemas Forenses. Identificação Humana. Interoperabilidade. Hash Criptográfico. Assinatura Digital.

RESUMEN

La odontología forense brasileña enfrenta importantes desafíos en la digitalización de sus procedimientos, especialmente en lo que se refiere a la estandarización, trazabilidad y validez legal de los restos dentales. Este artículo presenta una visión general de los sistemas utilizados, analiza las lagunas regulatorias y propone la creación del Sistema Nacional de Registro Odontológico Forense (SINAROF), basado en estándares como DICOM, hash SHA

[1] Master's Degree in Administration with an emphasis on Information Technology. Federal University of Paraíba (UFPB).
E-mail: wdiasit@gmail.com

256, firma digital ICP Brasil y registros encriptados. Aunque la propuesta está anclada en la realidad brasileña, ofrece contribuciones relevantes para otras naciones federativas que enfrentan desafíos similares en la integración digital de la identificación odontológica forense.

Palabras clave: Odontología Forense. Cadena de Custodia Digital. Sistemas Forenses. Identificación Humana. Interoperabilidad. Hash Criptográfico. Firma Digital.

1 THE IMPORTANCE OF A NATIONAL DIGITAL FORENSIC ODONTOLOGY SYSTEM

The creation and consolidation of a national digital forensic odontology system represent a crucial step in strengthening forensic institutions and modernizing the Brazilian justice system. Forensic odontology is a well-established scientific field, recognized for its technical precision, but it still lacks a standardized and integrated digital infrastructure in Brazil. The absence of a national repository with cryptographic security and interoperability among states limits the full potential of forensic dentistry as a tool for human identification, postmortem recognition, and the production of legally robust evidence.

One of the main applications of forensic odontology lies in the identification of bodies in advanced stages of decomposition, skeletonization, or carbonization, in which traditional methods such as fingerprint analysis or visual recognition become unfeasible. Dental arches are highly resistant to high temperatures and environmental degradation, preserving structures and treatments that are unique and allow comparison with antemortem dental records. In mass disaster scenarios, dental identification is often the only viable method for ensuring the accurate identification of victims and the proper issuance of death certificates.

Beyond disaster contexts, forensic odontology plays a central role in policies for locating missing persons. Automated comparison between postmortem dental records and antemortem databases is an effective strategy for locating missing individuals, even in long-standing cases. An integrated digital system would enable rapid cross-checking of unidentified cadavers with the dental records of people reported missing, significantly increasing case resolution rates and contributing to the effective implementation of Law No. 13.812/2019, which established the National Policy for the Search of Missing Persons.

The existence of a standardized national system also directly impacts legal certainty and the prevention of errors. In a context where digital evidence must meet increasingly rigorous standards of chain of custody and reliability, the lack of access controls, cryptographic hashes, digital certification, and audit logs can compromise the procedural validity of odontological reports. Non-auditable forensic systems or those that can be altered without traceability place the admissibility of evidence at risk and open the door to nullities, omissions, or technical challenges in court.

From a humanitarian perspective, the accurate and timely identification of victims fulfills the principle of restorative justice. Families have the right to know the fate and whereabouts of their loved ones and to carry out funerary rituals in accordance with their beliefs and cultures. The State’s failure to provide adequate technical means for identification violates the principle of human dignity and prolongs the suffering of families, especially in cases of enforced disappearances, urban violence, or mass tragedies. A structured digital system reinforces the right to truth and memory.

In a country as large and federated as Brazil, national interoperability is both a technical and political necessity. The lack of interconnection among state databases hinders the efficient flow of information across jurisdictions, delaying interstate investigations and coordinated responses to emergencies. Furthermore, an interoperable system aligned with international standards (such as those recommended by Interpol and DVI protocols) facilitates transnational cooperation, bilateral agreements, and technical-scientific exchange with other nations.

Finally, structuring a digital forensic odontology system enables the systematization of statistical data and the scientific advancement of the field. The ability to collect, standardize, and analyze large volumes of data supports epidemiological studies, the development of artificial intelligence algorithms for automatic identification, and the formulation of public policies based on evidence. Once digitized and integrated, forensic odontology contributes not only to case resolution but also to the advancement of scientific knowledge and technological innovation in human identification.

2 DIGITALIZATION OF FORENSIC ODONTOLOGY: GLOBAL AND BRAZILIAN OVERVIEW

Digitalization in forensic odontology has evolved in parallel with the broader digitization of forensic sciences, a process that began in the 1980s with the development of computer systems for human identification. In the dental field, this shift was largely driven by the need to accelerate and standardize the comparison between antemortem and postmortem records, especially in the context of mass Disaster Victim Identification

(DVI). Early initiatives included the digitization of dental charts, the introduction of structured odontological databases, and the use of digitized radiographic imaging. However, these efforts were initially limited in scope and characterized by low interoperability between institutions and jurisdictions (Senn; Weems, 2013). Over time, as forensic demands increased and computational resources became more accessible, forensic odontology gradually embraced more robust data management technologies, laying the foundation for current efforts toward integration and automation.

In the United States, the development of WinID in the 1990s marked a significant milestone in the digitalization of forensic odontology. Originally designed to meet the operational needs of the Armed Forces and the FBI, the software enabled the codified recording of dental characteristics and facilitated automated searches using compatibility algorithms. By integrating radiographic images, graphic odontograms, and partial match filters, WinID became the standard tool for victim identification in large-scale disasters. Its effectiveness was notably demonstrated in high-profile events such as the Oklahoma City bombing in 1995 and the September 11 attacks in 2001 (Senn; Weems, 2013; Gomes; Almeida, 2020). The system's adaptability and precision in cross-referencing dental data contributed to its widespread adoption among forensic teams in both military and civilian contexts.

In parallel, Interpol began developing and standardizing the Disaster Victim Identification (DVI) protocol, structured around codified forms and digital systems for data storage and cross-referencing. The Dental Identification Software (DIS) and the PlassData DVI System were implemented as support platforms for international missions involving the identification of victims in natural disasters and terrorist attacks. These tools significantly enhanced the responsiveness of forensic teams by enabling interoperability across countries, standardization of data fields, and traceability of dental information collected in the field (Interpol, 2017; Mendonça; Santos, 2022). Through these platforms, forensic odontologists gained access to secure, centralized systems capable of handling multilingual records, improving efficiency and consistency in multinational forensic operations.

In Europe, Australia, and Canada, national forensic identification systems began to incorporate digital dental modules compatible with existing civil and criminal databases.

Initiatives such as DAVID (Disaster and Victim Identification Database) in Australia, as well as the use of blockchain-integrated systems in the United Kingdom and Estonia, reinforced the growing trend of integrating forensic odontology into national biometric identification networks. These developments reflect a broader shift toward technologically unified forensic infrastructures, in which dental data is treated with the same precision and interoperability standards as fingerprints or DNA. However, such progress has required substantial investments in digital infrastructure, the establishment of technical regulatory frameworks, and the training of forensic experts in emerging technologies (Cavalcanti; Leite, 2021).

In Brazil, the digitalization of forensic odontology occurred later and progressed unevenly across regions. Until the early 2000s, most Institutes of Legal Medicine still relied on handwritten dental records, manually drawn odontograms, and radiographs stored in physical envelopes. This analog system severely limited communication between forensic units from different states and hindered the integration of clinical dental records into criminal investigations, especially in cases involving missing persons or charred remains (Ferraz et al., 2020; Santos et al., 2021). The absence of standardized digital protocols not only delayed identification processes but also contributed to the fragmentation of forensic workflows, exposing the need for national strategies aimed at modernization and data interoperability.

The first digitalization efforts in Brazil emerged through the adaptation of clinical software originally developed for private dental practices, such as Digora®, Sidexis®, Carestream®, and Dolphin Imaging®. These platforms enabled the acquisition of radiographic images in DICOM format and allowed their export to digital media, thus facilitating the preliminary organization of forensic dental archives. However, they lacked key forensic features such as access control, audit logs, and cryptographic hash functions to ensure data integrity—essential components for compliance with the chain of custody requirements in forensic evidence handling (Soares; Barbosa, 2022; Lopes; Gonçalves, 2019). As a result, while these tools represented a technical improvement over analog methods, they remained insufficient for legally robust forensic documentation.

The mining disasters of Mariana (2015) and Brumadinho (2019)[2] revealed profound limitations in Brazil's forensic odontology system, particularly the absence of a unified infrastructure for managing dental records. The urgent need to identify nearly 300 victims—many of whom were severely disfigured, decomposed, or fragmented—exposed critical deficiencies in institutional coordination and highlighted the lack of a centralized national dental chart database. In response, certain Brazilian states initiated pilot programs utilizing platforms such as WinID and began experimenting with digital identification protocols. However, these initiatives remained isolated and lacked support from a cohesive federal regulatory framework (Santos; Macedo, 2023; Gomes; Almeida, 2020). These environmental catastrophes underscored the pressing need to modernize Brazil's forensic infrastructure and to establish nationwide coordination mechanisms for digital dental identification systems.

Throughout the 2010s, proposals emerged to establish regional dental data repositories, linked either to Scientific Police departments or to Regional Dental Councils. However, the lack of technical regulations, federal funding, and specialized training rendered the standardization of these initiatives unfeasible. As a result, each Brazilian state continued to adopt distinct software systems, with varying levels of digital implementation, thereby perpetuating fragmentation and undermining interoperability among forensic units across the country (Abreu; Campos, 2021).

In the contemporary context, Brazil faces the challenge of aligning its digital forensic odontology practices with international standards. This involves not only the adoption of systems compatible with DICOM formats and cryptographic hash functions, but also the development of national protocols for digital chain of custody, integration with the General Data Protection Law (LGPD), and certification of systems by specialized regulatory bodies. The technical training of forensic experts, along with coordinated action among the Ministry of Justice, the Federal Council of Dentistry (CFO), and State Public

[2] The Mariana (2015) and Brumadinho (2019) disasters were two of the most devastating mining tragedies in Brazilian history. In Mariana, the collapse of the Fundão tailings dam—operated by Samarco (a joint venture between Vale and BHP Billiton)—released over 40 million cubic meters of mining waste, contaminating the Doce River and affecting communities across two states. In Brumadinho, the failure of a tailings dam at the Córrego do Feijão mine—owned by Vale S.A.—resulted in a massive mudflow that killed 270 people and caused severe environmental and social damage. Both events raised global concerns about the safety and regulation of tailings dams in the mining industry.

Security Departments, constitutes a crucial foundation for this transition (Brasil, 2018; Brasil, 2022).

Thus, the history of forensic odontology digitalization in Brazil reveals a trajectory marked by fragmented and inconsistent progress, primarily driven by isolated local efforts rather than a unified national strategy. These efforts, while valuable, have failed to establish a cohesive and standardized infrastructure capable of supporting the increasing demands of digital forensic investigations. Unlike countries with longstanding forensic traditions—such as the United States, the United Kingdom, and some European nations—that have successfully implemented interoperable, secure, and auditable platforms for dental data management, Brazil remains significantly behind in terms of policy coordination, system certification, and institutional integration.

The lack of a centralized regulatory framework results in operational disparities across states, undermining the legal robustness and scientific credibility of dental evidence in judicial proceedings. To address these structural deficiencies, it is imperative to engage in comprehensive institutional planning, allocate targeted technological investments, and update existing regulatory norms in alignment with the digital realities and international standards of contemporary forensic practice. Only through such a coordinated approach will it be possible to ensure the reliability, traceability, and admissibility of digital dental evidence within the Brazilian legal system and beyond.

In this context, the present study advances the proposal for the creation of a National Forensic Dental Record System (SINAROF), specifically designed to address the unique structural, legal, and technological characteristics of the Brazilian forensic infrastructure. The proposed system envisions the development of a centralized yet federatively distributed digital platform for the registration, storage, and management of dental evidence, incorporating essential features such as interoperability, end-to-end encryption, cryptographic hash verification, digital signatures compliant with national standards (ICP-Brasil), and immutable audit logs. By establishing standardized protocols and integrating state-level units into a cohesive network, SINAROF aims to overcome the current fragmentation of procedures, ensuring that dental records are admissible, secure, and traceable across all phases of forensic processing.

Although this proposal is rooted in the Brazilian context, its conceptual framework and operational logic may hold broader applicability to other federative nations that experience similar institutional and technical fragmentation in their forensic practices. Countries with decentralized criminal justice systems often face challenges related to system incompatibility, lack of uniform data governance, and procedural inconsistencies between jurisdictions—barriers that SINAROF is explicitly designed to mitigate. As such, the proposal not only addresses a pressing national need but also contributes to the global discourse on best practices for the digital transformation of forensic odontology, offering a potentially replicable model for international implementation and cooperation.

3 SPECIALIZED TECHNOLOGICAL SOLUTIONS IN FORENSIC ODONTOLOGY: CURRENT LANDSCAPE AND COMPARATIVE ANALYSIS OF SYSTEMS

The digitalization of forensic procedures has ushered in a paradigm shift in the field of forensic odontology, fundamentally altering how dental data is generated, managed, and interpreted. The integration of computerized systems into routine forensic practice has become indispensable, particularly in cases involving mass disasters, unidentified remains, or transnational investigations. These systems facilitate the rapid acquisition, organization, and analysis of dental records—encompassing radiographs, intraoral images, and clinical annotations—thereby enhancing both the accuracy and efficiency of identification processes. Moreover, digital tools allow for the storage of large datasets, enable cross-referencing across multiple jurisdictions, and provide platforms for visual comparison and algorithmic matching between antemortem and postmortem records.

In this evolving landscape, a wide array of technological solutions has been developed or adapted for forensic application, each presenting varying degrees of technical sophistication, security compliance, and forensic reliability. Some systems are purpose-built for legal medicine, incorporating cryptographic protections and audit mechanisms, while others are derived from clinical environments and require adaptation to meet evidentiary standards. This section provides a comparative overview of the principal systems currently deployed or undergoing pilot implementation in different national contexts. It highlights not only their technical features—such as support for DICOM imaging, digital signatures, and hash validation—but also their limitations and degrees of compliance with internationally recognized protocols for the forensic chain of custody. Such analysis is crucial for understanding the current state of forensic odontology digitalization and for guiding future policy and technological development.

WinID is a software originally developed in the United States with a primary focus on the comparison of antemortem and postmortem dental records. It operates using encoded dental arch data and allows the attachment of radiographs and intraoral images. Its fuzzy search algorithm enables automated comparisons across multiple records, facilitating rapid identification processes. The latest version, WinID-4Web, introduced significant improvements such as user authentication, log control, and a web-based interface. However, the system still lacks native features such as cryptographic hashing, digital signatures, or data encryption, which limits its robustness in meeting the most recent standards for digital chain of custody compliance (Senn; Weems, 2013).

The Dental Identification Software (DIS) is integrated into Interpol's international Disaster Victim Identification (DVI) protocol. Designed to enable rapid and standardized comparisons across different countries, the system works with digitized AM/PM forms, allows the upload of images in DICOM format, and stores metadata such as anatomical location, dental conditions, and clinical interventions. DIS maintains detailed logs of user activity, offers structured XML export in accordance with DVI standards, and supports integration with digital authentication and certification systems. These features provide greater legal security and traceability for forensic odontological reports (Interpol, 2017).

The PlassData DVI System is a multidisciplinary data management platform used by various forensic units across Europe and in countries affiliated with Interpol. Its distinguishing feature lies in its integration of multiple types of forensic evidence—including dental, genetic, digital, and anthropological—within a single auditable environment. The dental module supports DICOM, JPEG, and PNG file formats, enables precise anatomical annotation, and links files to specific cases with strict version control. Additionally, the system maintains immutable log records, offers automatic cloud-based replication, and adheres to security protocols compliant with ISO/IEC 27001 standards (Cavalcanti; Leite, 2021).

In addition to purpose-built forensic software, several clinical programs have been adapted for forensic use. Among the most commonly employed are Digora®, Sidexis®, Carestream®, and Dolphin Imaging®, which enable the acquisition, visualization, and export of high-definition dental radiographs. These systems operate with DICOM files and, although not originally designed for forensic purposes, offer substantial compatibility with platforms such as WinID and PlassData. However, these programs do not natively include features such as log generation, access control, or integrity verification—requiring their integration with supplementary tools to ensure digital traceability (Soares; Barbosa, 2022).

To address these security gaps, encryption tools such as VeraCrypt, AxCrypt, and 7-Zip are commonly employed to encapsulate digital files within containers protected by algorithms such as AES-256. These solutions ensure confidentiality and prevent unauthorized access to dental data during transmission or storage. Although they do not replace purpose-built forensic systems, these software tools provide a minimum level of protection and can be integrated into forensic workflows in low-infrastructure environments—provided they are properly configured and managed by technically trained personnel (Lopes; Gonçalves, 2019).

Complementing security measures, the application of cryptographic hash functions, such as SHA-256, has become essential for ensuring the integrity of digital forensic dental files. A hash acts as a digital fingerprint of the document, allowing verification of whether the content has been altered since its creation. Systems like PlassData and DIS automatically generate this code at the moment the file is uploaded. In environments that use WinID or clinical software, however, the hash must be generated manually, with the code recorded separately, which increases the likelihood of human error and judicial challenges (International Organization for Standardization, 2012).

In more advanced contexts, the international forensic community has been testing forensic blockchain platforms aimed at ensuring the immutability of chain-of-custody records. Countries such as Canada, Estonia, and the United Kingdom have been conducting pilot projects in which each action performed on a piece of evidence—such as uploading, modification, or access—generates a cryptographically validated block inserted into a distributed ledger. This system prevents retroactive edits, offers auditable transparency, and can be adapted for forensic dental contexts, although it still lacks regulatory frameworks and operational infrastructure in Latin American countries (Mendonça; Santos, 2022).

The effective application of digital technologies in forensic odontology requires a systemic and coordinated approach within forensic institutions. Rather than relying on isolated solutions, it is crucial to establish integrated workflows that combine tools for data acquisition, processing, and long-term preservation with robust digital security mechanisms. These tools must support the implementation of core forensic principles, including authenticity, integrity, and traceability of digital evidence. Importantly, no single software platform is capable of addressing all operational demands—ranging from image capture and metadata preservation to secure archival and courtroom presentation. As such, a modular and interoperable framework is needed to ensure that each component, whether clinical or forensic in origin, contributes to the overall reliability of the evidence.

To this end, establishing standardized protocols is vital. These should include detailed procedures for exporting dental images and radiographs in compatible formats (such as DICOM), generating cryptographic hash values (e.g., SHA-256) at the moment of file creation, and securely encapsulating the data using encryption tools. Furthermore, log auditing must be enabled and enforced, with immutable records of all user interactions and file modifications. These workflows must be supported by continuous professional development programs that train forensic experts in cybersecurity, digital chain of custody, and legal requirements for data handling. At the institutional level, only certified software platforms—evaluated under recognized standards such as ISO/IEC 27001 and local data protection laws—should be authorized for forensic use. This dual emphasis on technical standardization and professional training is essential for ensuring the legal admissibility and scientific credibility of digital dental evidence.

Brazil still lacks a national policy for the standardization of digital forensic odontology systems. Each state adopts different tools, often incompatible with one another. The absence of interoperability hinders the exchange of information in interstate or cross-border cases, complicates evidence tracking, and weakens the legal defense of the chain of custody in court. The legal recognition of digital odontological reports depends on clearly defined technical standards, and the use of technologies such as digital signatures, hash functions, and log records must be regulated through national resolutions (Ferraz et al., 2020).

Beyond technical aspects, these systems must comply with the requirements of the General Data Protection Law (LGPD), as dental evidence—particularly when linked to patient records—constitutes sensitive data of a biometric nature. Systems such as PlassData and DIS already incorporate anonymization protocols and end-to-end encryption. In Brazil, such compliance must be ensured prior to the establishment of any national forensic dental database, as is already the case with DNA databases (Brasil, 2018; Brasil, 2022).

Finally, the selection and adoption of systems should be guided by criteria of forensic functionality, technical feasibility, and legal security. Systems such as WinID are more accessible and suitable for local-level application, while PlassData and DIS require more robust infrastructure but offer greater traceability and international integration. Although limited in forensic capabilities, clinical software remains useful for capturing dental images and examinations, provided it is incorporated into a forensic digital ecosystem that upholds chain-of-custody protocols, data integrity, and the protection of sensitive information.

Table 1

Comparative Table of Systems and Tools

System/Tool	Type	Hash	Logs/Audit	Digital Signature	Interoperability	Forensic Applicability
WinID/WinID-4Web	Forensic odontology	Manual (limited)	Partial (4Web)	Not native	Moderate	High
Dental Identification Software (DIS)	International / DVI	Automatic	Yes	Yes (via integration)	High (Interpol)	Very high
PlassData DVI System	Multievidence platform	Automatic	Yes	Yes	Very high	Very high
Digora®, Sidexis®, Carestream®, Dolphin	Clinical radiology	Not native	No	No	Moderate	Moderate
Veracrypt / AxCrypt / 7-Zip	Local encryption	Yes (AES)	No	No	Low	Supplementary
SHA-256 Hash (external)	Integrity validation	Yes	No	No	High	Essential
Forensic Blockchain (pilot)	Immutable ledger	Integrated	Yes (immutable)	Yes (cryptographic)	Emerging	High (experimental)

Source: The author (2025).

4 SYSTEMIC FRAGMENTATION IN BRAZILIAN FORENSIC ODONTOLOGY: STATE-LEVEL DIVERSITY, INTEGRATION CHALLENGES, AND THE CHAIN OF CUSTODY FOR DENTAL EVIDENCE

The practice of forensic odontology in Brazil is federally regulated but primarily implemented in a decentralized manner by state-level forensic institutes. This federative structure results in a wide diversity of practices, protocols, and systems employed in the collection, analysis, documentation, and storage of dental evidence. Such technological and institutional heterogeneity poses a significant challenge to the establishment of a standardized and reliable digital forensic odontology framework—particularly regarding the preservation of the chain of custody for odontological digital data (Ferraz et al., 2020; Cavalcanti; Leite, 2021).

Currently, Brazil lacks a unified national system for managing forensic dental data. States such as São Paulo, Minas Gerais, and Paraná demonstrate more advanced technological infrastructure and specialized human resources, with some forensic units conducting localized trials of software like WinID (Santos et al., 2021). In contrast, in many states across the North and parts of the Northeast regions, forensic odontological procedures are still predominantly manual, with reports drafted as free-text documents and radiographs stored on physical media or digitized without standardized technical metadata.

This disparity generates significant challenges for the interoperability of dental data, especially in scenarios involving multiple jurisdictions, such as mass disasters, interstate investigations, and missing persons cases. In the absence of a common protocol for file formats, dental coding standards, and metadata recording, the exchange of information between federative units becomes slow, error-prone, and often technically unfeasible (Abreu; Campos, 2021).

With regard to the chain of custody, systemic fragmentation undermines the integrity and legal validity of dental evidence. The absence of cryptographic hashing, audit logs, version control, and digital signatures in many local systems prevents digital files from being deemed forensically valid, particularly in criminal proceedings that require proof of authenticity and data integrity (International Organization for Standardization, 2012; Brasil, 2019).

Studies indicate that most state forensic institutes in Brazil operate autonomously, adopting distinct tools for image acquisition (e.g., Sidexis, Carestream, Digora®), data storage (external hard drives, local servers, or private cloud solutions), and report generation (simple text editors or PDF format), without platform integration or national standardization (Ferraz et al., 2020). These conditions render unfeasible any attempt to establish a national forensic dental database comparable to those already in place for DNA or fingerprint records (AFIS[3]).

In high-profile cases such as the aforementioned disasters in Mariana and Brumadinho, or in aviation accidents involving victims from multiple states, the absence of a centralized repository of dental records severely hindered the work of forensic experts. In these instances, it became necessary to individually contact regional dental councils and

[3] AFIS (Automated Fingerprint Identification System) is a computerized system that enables the registration, comparison, and automated identification of fingerprints with a high degree of accuracy. It is widely employed by civil identification agencies and criminal forensic units.

private clinics to obtain the victims' clinical charts. A similar situation arises in the search for missing persons, where the comparison of dental records across state boundaries is unfeasible due to technical and governance barriers (Santos; Macedo, 2023).

Beyond technological issues, there is also a lack of specific regulations requiring state forensic agencies to adopt certified and interoperable tools. Unlike the Integrated Network of Genetic Profile Databases (RIBPG), coordinated by SENASP, there is no legal mandate or technical guideline establishing minimum criteria for the digitization of dental evidence, nor clear protocols for the preservation and traceability of such data (Brasil, 2022; Cavalcanti; Leite, 2021).

This regulatory gap creates a permissive environment in which individual states may adopt non-certified software solutions for forensic dental procedures, often without proper security configurations, access restrictions, or data backup protocols. In many cases, these systems were originally designed for clinical rather than forensic use, and thus lack essential features such as log auditing, cryptographic hash functions, and user authentication. The absence of these safeguards compromises the traceability and integrity of digital records, leaving them vulnerable to tampering, unauthorized access, or accidental data loss. This situation becomes even more critical when the forensic evidence in question serves as the basis for legal decisions, such as the identification of victims or the confirmation of suspects' identities.

Brazilian courts have become increasingly attentive to the reliability of digital evidence, particularly in light of the principles established by Law No. 13.964/2019—commonly referred to as the "Anti-Crime Package." This law incorporates the doctrine of exclusion of tainted evidence, which mandates that any proof obtained without proper legal procedures, including violations of the chain of custody, must be declared inadmissible. As a result, pericial reports based on data extracted from unregulated or non-certified systems may be rejected in judicial proceedings. This underscores the urgent need for regulatory harmonization, with national standards that mandate the use of certified software platforms capable of ensuring the authenticity, integrity, and legal admissibility of forensic dental records.

The practical outcome is that, although forensic odontology is scientifically established as an effective method of identification, its legal credibility may be undermined by documentary inconsistencies and the lack of digital standardization. Without tools that ensure the immutability, authenticity, and integrity of digital files, it is impossible to guarantee that the evidence analyzed is exactly the same as that presented in court—thus creating opportunities for legal challenges (Gomes; Almeida, 2020).

5 PROPOSED IMPROVEMENTS IN FORENSIC ODONTOLOGY: DIGITAL PROTOCOLS, HASH FUNCTIONS, AND SYSTEM CERTIFICATION

International forensic literature has already emphasized the need to adopt interoperable and auditable systems for the storage of dental data. Tools such as WinID, PlassData DVI, and DAVID are recommended by international bodies, including Interpol, particularly in contexts involving mass disasters and cross-border cooperation. These systems include standardized protocols for logging, native hash generation, version control, and export in structured formats (Senn; Weems, 2013).

In Brazil, however, the adoption of such systems remains limited, sporadic, and largely dependent on the individual initiative of forensic experts or partnerships with universities. There is no national program to fund or promote the digital standardization of forensic odontology, which perpetuates a landscape of technological isolation among states. As a result, cases requiring national cooperation rely on informal mechanisms, increasing both response time and the likelihood of error (Abreu; Campos, 2021; Santos et al., 2021).

Brazilian forensic odontology currently faces significant challenges regarding the security, integrity, and standardization of digital data produced in the forensic context. The absence of a unified national protocol, the use of heterogeneous software solutions, and the fragility of digital chain of custody mechanisms undermine both the legal and scientific validity of odontological reports. In order for forensic odontology to be consolidated as a robust technical form of evidence, structural improvements must be implemented, grounded in principles of information security, traceability, and digital compliance—practices already adopted in other branches of forensic science such as genetics and fingerprint analysis (Castro; Teixeira; Silva, 2020).

The standardization of the digital format of forensic evidence is the first step toward ensuring evidentiary integrity. The adoption of the DICOM standard (Digital Imaging and Communications in Medicine), already widely used in medical radiology, would enable not only the preservation of high-resolution dental images but also the encapsulation of essential metadata, such as date, time, equipment, and responsible operator. These data are fundamental for traceability and validation of file origin and are also compatible with forensic platforms such as WinID, PlassData, and systems based on the DVI protocol (Senn; Weems, 2013; Senn et al., 2020).

In light of this context, we propose the establishment of a *National Forensic Dental Record System* (SINAROF), coordinated by the Brazilian Ministry of Justice and Public Security (MJSP), consisting of a centralized database connected to state-level forensic units. The system should implement the DICOM standard for medical imaging, cryptographic hash functions such as SHA-256, encrypted audit logs, and digital signatures in compliance with the ICP-Brasil certification authority. While preserving the administrative autonomy of each state, the platform would ensure data replication and national interoperability, following the successful model of the Brazilian Integrated Network of Genetic Profile Databases (RIBPG). Governance could be shared among forensic odontologists, digital forensic specialists, and the Federal Council of Dentistry, fostering a collaborative and technically robust environment.

Such a structure would enhance the legal reliability of forensic evidence, improve identification response times, increase institutional trust, and foster greater collaboration among federal and state agencies. Regional diversity would not be suppressed, but rather structured through a set of common minimum protocols. In this way, it would be possible to preserve the operational autonomy of individual states while ensuring the national reliability and admissibility of forensic dental data (Brasil, 2022).

In addition to adopting appropriate digital formats, the use of cryptographic hash functions is essential to ensure the integrity of forensic files. A hash functions as a unique digital fingerprint, enabling verification that a file has not been altered since its creation. Brazilian jurisprudence has already recognized the legal value of files accompanied by linked hash codes, particularly in the context of digital evidence (Brasil, 2019). In forensic odontology, this would mean ensuring that a radiograph, intraoral photograph, or expert report remains unchanged from the moment of its issuance to its presentation in court.

Digital certification, through Brazil's Public Key Infrastructure (ICP-Brasil), should be implemented as a mechanism to ensure authenticity and non-repudiation. Forensic experts must issue dental reports and related documents using certified digital signatures, linking the content to their individual taxpayer identification (CPF) and technical credentials. The absence of such a mechanism may lead to challenges regarding the authorship, integrity, and temporality of the evidence, thereby violating chain of custody principles as established by Law No. 13.964/2019 (Brasil, 2019; Cavalcanti; Leite, 2021).

The systems used for the generation, storage, and transmission of forensic dental data must include detailed audit logs. This entails maintaining an immutable record of every access, modification, or export of forensic files. Such logs must be protected against overwriting and replicated on secondary servers for security and backup purposes. The ISO/IEC 27037:2012 standard establishes these requirements as fundamental for the preservation of digital evidence (International Organization for Standardization, 2012).

In order for these measures to be institutionalized, the systems employed by Scientific Police units must undergo formal certification processes. It is recommended that the National Institute of Information Technology (ITI), the Federal Data Processing Service (Serpro), and

State Information Technology Centers serve as certifying authorities, evaluating software in accordance with standards such as ISO 27001 and the Brazilian General Data Protection Law (LGPD) (BRASIL, 2018). Non-certified systems should not be authorized for forensic use, in order to prevent critical evidence from being compromised due to technical failures or lack of traceability.

From an operational standpoint, it is recommended to establish a clear separation between the production environment and the forensic archiving environment. The production environment should allow for editing and technical processing, while the archiving environment, accessible only to authorized profiles, must store the signed files with hash values and protected audit logs. This separation reduces the risk of tampering and upholds the chain of custody as required by the Brazilian Code of Criminal Procedure (Cavalcanti; Leite, 2021).

Another key proposal is interoperability with DNA systems (RIBPG) and civil and criminal identification platforms. The SINAROF database would operate in a cloud-based environment, with state-level replication, mandatory digital signatures, and controlled access. Its architecture could rely on technologies such as RESTful APIs, distributed repositories, and the use of blockchain for auditing sensitive records (Mendonça; Santos, 2022).

The implementation of these measures requires the development of Standard Operating Procedures (SOPs), to be defined by working groups composed of forensic experts, digital forensic IT specialists, representatives from the Federal Council of Dentistry (CFO), the National Secretariat of Public Security (SENASP), and public universities. These SOPs should regulate all steps from image acquisition to judicial submission, ensuring that every phase is properly documented, protected, and traceable. This would promote uniformity and legal reliability in forensic dental reports (Abreu; Campos, 2021).

Continuous professional development for forensic experts is also essential. Training and refresher courses must include content on cryptographic hashing, encryption, digital chain of custody, and data protection legislation. Forensic odontology must incorporate principles of information security and digital governance, ensuring that its technical staff is equipped to meet the demands of contemporary digital forensic practice (Gomes; Almeida, 2020).

The initial implementation of these solutions could take place through pilot programs in states with more advanced infrastructure, such as São Paulo, Minas Gerais, and Paraná. Once validated, the models could be replicated nationwide with appropriate regional adaptations. This process requires federal funding—through the National Secretariat of

Public Security (SENASP)—as well as partnerships with universities and resources earmarked for public security and technological innovation (Brasil, 2022).

It is also proposed that the custody and life cycle of digital forensic dental records be subject to formal regulation. These data should be treated as critical state assets, and their handling must comply with specific rules regarding access, backup, audit, and disposal, in accordance with the General Data Protection Law (LGPD) and technical standards for digital records management (Brasil, 2018; Archives and Records Association, 2016).

Finally, it is advisable to establish a National Observatory for Digital Forensic Odontology[4], aimed at monitoring the implementation of protocols, evaluating their effectiveness, and proposing continuous improvements. This observatory should be multidisciplinary and regularly publish reports containing statistics, identified shortcomings, and technical recommendations, functioning as a mechanism of both social and technical oversight of the new model (Santos & Macedo, 2023).

With these measures, forensic odontology may achieve the same level of maturity already observed in other areas of criminal forensics. The digital era demands traceability, security, interoperability, and transparency. Without these elements, dental evidence risks becoming vulnerable and subject to challenge, despite being, from a technical standpoint, one of the most reliable methods in human identification processes. It is now incumbent upon the Brazilian State to equip this field with tools compatible with its scientific and judicial significance.

REFERENCES

Abreu, M. R., & Campos, L. S. (2021). Governança de dados na perícia oficial: Proposta de um modelo para integração forense. Revista Brasileira de Ciências Policiais, 12(1), 33–52.

Archives and Records Association. (2016). Digital preservation guidance note. ARA.

Brasil. (2018). Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709, de 14 de agosto de 2018). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Brasil. (2019). Lei nº 13.964, de 24 de dezembro de 2019. Altera o Código de Processo Penal. Diário Oficial da União. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm

[4] There are already observatories linked to specific areas of criminal forensics, such as the RIBPG Observatory, which monitors and disseminates statistical data on the insertion, matching, and impact of genetic profiles in crime resolution. This type of structure operates as a technical-scientific and managerial body, typically composed of forensic experts, laboratory managers, information technology specialists, and representatives of the Ministry of Justice and Public Security. Its functions include the production of periodic reports, normative recommendations, technical audits, and support for the formulation of evidence-based public policies.

Brasil. Ministério da Justiça e Segurança Pública. (2022). Plano Nacional de Perícias Forenses Digitais. SENASP.

Castro, M. L., Teixeira, D. F., & Silva, R. A. (2020). Governança digital e integridade em perícia odontológica: Desafios contemporâneos. Revista Brasileira de Ciências Forenses, 12(2), 45–62.

Cavalcanti, D. C., & Leite, T. G. (2021). A cadeia de custódia da prova digital no processo penal brasileiro. Revista de Estudos Criminais, 19(73), 99–126.

Ferraz, J. D., & outros. (2020). Odontologia legal e perícia digital: Desafios da cadeia de custódia no século XXI. Revista OdontoLegal, 8(2), 57–68.

Gomes, A. P., & Almeida, F. A. (2020). Formação digital para peritos: Proposta de currículo mínimo para perícia em saúde e forense. Revista Interdisciplinar de Segurança Pública, 4(1), 45–63.

International Organization for Standardization. (2012). ISO/IEC 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO.

INTERPOL. (2017). Disaster victim identification guide. INTERPOL.

Lopes, R. M., & Gonçalves, T. C. (2019). Segurança da informação em perícias digitais: Uso de criptografia. Revista de Direito e Tecnologia, 5(2), 82–98.

Mendonça, V. L., & Santos, I. F. (2022). Blockchain aplicado à cadeia de custódia de provas digitais. Revista Brasileira de Direito e Tecnologia, 6(2), 112–130.

Santos, J. E., & Macedo, R. F. (2023). Observatório da perícia criminal: Proposta institucional e metodológica. Revista de Administração Pública e Segurança, 9(1), 70–89.

Santos, R. R., & outros. (2021). Sistemas periciais e padronização na odontologia legal: Estado da arte e perspectivas. Revista Brasileira de Odontologia Legal, 7(3), 102–117.

Senn, D. R., & Weems, R. A. (2013). Manual of forensic odontology (4th ed.). CRC Press.

Soares, L. F., & Barbosa, A. S. (2022). Imagem digital odontológica: Avaliação pericial de softwares clínicos. Revista de Odontologia Digital, 2(1), 15–29.