RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 16/09/2026 | aceito: 23/09/2026 | publicação: 28/09/2026

Data security in the digital and archival chain of custody in Criminal Procedural Law with a focus on the Anti-Crime Package Act

A segurança de dados na cadeia de custódia digital e arquivística do Direito Processual Penal com enfoque na Lei do Pacote Anticrime

La seguridad de los datos en la cadena de custodia digital y archivística del Derecho Procesal Penal con énfasis en la Ley del Paquete Anticrimen

João Pedro Prucoli Cortes – Faculdade de Direito de Cachoeiro de Itapemirim (FDCI), joao.cortes@aluno.fdci.edu.br – Undergraduate law student.
Ticiano Yazegy Perim – Faculdade de Direito de Cachoeiro de Itapemirim (FDCI), ticianoperim@hotmail.com – Doctoral student in Education at Estácio de Sá University (UNESA); Master in Legal and Social Sciences from Fluminense Federal University (UFF); Specialist in Public Law from Candido Mendes University (UCAM); University professor at FDCI | ORCID: 0000-0003-2761-1824.

Abstract:

The chain of custody of forensic evidence is an institute of criminal procedural law of total relevance to procedural results, and as such, it has adapted to cutting-edge technological advances to act with greater agility, precision, transparency and efficiency in operations involving procedures concerning criminal evidence. Thus, this study aimed to study the relevance and challenges to the data security of the digital and archival custody chain, discussing its peculiarities, legal regulations, forensic procedures, applications and storages, identifying the main challenges to the preservation of their files, the breaking of the chain and the possible loopholes in Law n. 13.964/19 - Anti-crime package. This is a literature review with a qualitative approach and exploratory-narrative character based on a time frame that considered the years 2015 to 2026, based on CAPES, Google Academic, SciELo and legal platforms. The results achieved denote a large volume of regulations and challenges especially directed at breaking the digital custody chain, which makes the issue more interesting and relevant to be deepened. It is concluded that the Anti-Crime Package is integrated into the chain of custody pen, digital and digital archival that needs to follow to the letter the legal norms and specific standards to ensure the security of data from cabal evidence responsible for the judicial results.
Keywords: Custody chain. Criminal Prosecution Law. Law No. 13.964/2019. Data security. Point Technologies.

Resumo:

A cadeia de custódia de provas periciais é um instituto do Direito Processual Penal de total relevância aos resultados processuais, e como tal, se adequou aos avanços tecnológicos de ponta para atuar com maior agilidade, precisão, transparência e eficiência nas operações que envolvem os procedimentos concernentes às provas criminais. Desse modo, esse estudo se objetivou a estudar a relevância e desafios à segurança de dados da cadeia de custódia digital e arquivística discorrendo sobre suas peculiaridades, normativas legais, procedimentos periciais, aplicações e armazenamentos, identificando os principais desafios à preservação dos seus arquivos, à quebra da cadeia e às possíveis brechas na Lei n. 13.964/19 -Pacote Anticrime. Se trata de uma revisão de literatura com abordagem qualitativa e caráter exploratório-narrativo embasada em um recorte temporal que considerou os anos de 2015 a 2026, tendo como base de coleta o CAPES, o Google Acadêmico, a SciELo e plataformas jurídicas. Os resultados

alcançados denotam um grande volume de regulamentações e aos desafios especialmente direcionados à quebra da cadeia de custódia digital, o que torna o tema mais interessante e relevante de ser aprofundado. Conclui-se que o Pacote Anticrime é integrado à cadeia de custódia pena, digital e digital arquivística que precisa seguir à risca as normatizações legais e padrões específicos com vistas a garantir a segurança de dados de provas cabais responsáveis pelos resultados judiciais.
Palavras-chave: Cadeia de Custódia. Direito Processual Penal. Lei n. 13.964/2019. Segurança de Dados. Tecnologias de Ponta.

Resumen:

La cadena de custodia de pruebas periciales es un instituto del Derecho penal de total relevancia a los resultados procesales, y como tal, se adecuó a los avances tecnológicos de punta para actuar con mayor agilidad, precisión, transparencia y eficiencia en las operaciones que involucran los procedimientos concernientes a las pruebas criminales. De ese modo, este estudio se objetivó a estudiar la relevancia y desafíos a la seguridad de datos de la cadena de custodia digital y arquivística discrepando sobre sus peculiaridades, normativas legales, procedimientos periciales, aplicaciones y almacenamientos, identificando los principales desafíos a la preservación de sus archivos, a la quiebra de la cadena y a las posibles brechas en la Ley n. 13.964/19 -Pacote Anticrime. Se trata de una revisión de literatura con abordaje cualitativo y carácter exploratorio-narrativo embasada en un recorte temporal que consideró los años de 2015 a 2026, teniendo como base de recolección el CAPES, el Google Académico, la SciELo y plataformas jurídicas. Los resultados alcanzados indican un gran volumen de regulaciones y desafíos especialmente dirigidos a la quiebra de la cadena de custodia digital, lo que hace que el tema sea más interesante y relevante de ser profundizado. Se concluye que el paquete Anticrime es integrado a la cadena de custodia pena, digital y digital archivada que necesita seguir rayando las normas legales y estándares específicos con el fin de garantizar la seguridad de los datos de pruebas leales responsables de los resultados judiciales.
Palabras clave: Cadena de Custódia. Derecho penal. Ley n. 13.964/2019. Seguridad de datos. Tecnologías de Ponta.

1. Introduction

In the context of Criminal Procedural Law (PPD), realistic evidence is indispensable to the conduct of various criminal cases, which means that within the institution of Public Security (SP) there is a proposal to preserve the proven fidelity of the chain of custody of criminal evidence (Stecker; Damian, 2021), henceforth used by the acronym CoC.

In Brazil, over the past 10 years, the CoC has been proving its need, importance and efficiency in the conduct of fairer and more expressive sentences, as well as the application of more elaborate protective measures, promoting greater effectiveness in the arrest and detention of criminal individuals, in addition to providing more concise custody hearings to any type of

criminal offense (National Council of Justice - CNJ, 2025). Its preservation represents a strategic item unique to the operational excellence of criminal cases, considering its objectives in ensuring the integrity and authenticity of criminal evidence, involving in this, processes ranging from collection to presentation in court (Supreme Court of Justice - STJ, 2023).

The CoC involves three types of forensic custody: criminal evidence, digital evidence and archival digital evidence, regulated by the Code of Criminal Procedure (CPP) which establishes the procedures/regulations of the collection, storage, integrity preservation, maintenance of cohesive, clear and accurate records, as well as the presentation corresponding to the traces applicable to the ongoing criminal proceedings. The preservation of integrity prevents contamination and/or tampering with the proof (Motta, 2022; Gava; Flores, 2023). Law No. 13.964/19 who implemented the so-called “Anti-crime package” (Brazil, 2019), blames the integrative CoC to the DPP, the use of diverse and specific technologies that involve all legal processes in procedural and massive use of cybersecurity (Stecker; Damian, 2021).

The effectiveness of the CoC as a whole requires mandatory secrecy of justice and evidence duly documented in specific and standardized forensic records and reports, whether physical or digital, considering for this purpose the preservation of divergent factors and the breach of the CoC, as primordial elements for validating and preserving the traces of the criminal offence previously examined by experts and, presented in court when necessary (Supreme Court of Justice - STJ, 2023).

Consequently, it is stated that the theme is broad, complex and conductive to a range of questions, which led to the choice of the guiding research problem to this study, structured on the following question: To what extent the technologies applied to the chain of custody can ensure the authenticity, integrity and reliability of digital evidence in the criminal process, and what are the legal consequences of failures in its preservation?

Hypothetically, the answers to this question come from the following conditions: (i) the complexity of the management and control of the digital CoC through the range of devices, laws and subjective specificities that structure it; (ii) the susceptibility of alteration, reprogramming and attacks by hackers to the processes of surveying and preserving criminal evidence, this reality, critical and challenging to criminal procedural law; (c) possible gaps, especially those associated with the breaking of the chain involving issues of communication, various secrecys, search and seizure, preservation/alteration of the subject and the expert environment, legal rights and duties, structures of flawed processes, among others, essential to the forensic and legal results.

For this purpose, this research aimed to study aspects of data security of the Digital and Digital Archivistic CoC, knowing characteristics, legalizations and the main challenges to the preservation of their files with a focus on chain breaking and possible loopholes in Law n. 13.964/19. Such scope demanded secondarily: (i) to characterize data security under criminal procedural law; (ii) to conceptualize the chain of custody in the spheres of criminal evidence, digital evidence and archival condition; (iii) to know the laws concerning the digital custody chain and the main applicable technologies; (iv) to clarify the anti-crime package established by Law n. 13,964/19; (v) identify the main challenges involved in the digital CdC that affect its data security, according to studies with evidence and case-law of the STJ.

Based on the contextualization of the theme already discussed, it is understood that the expansion of knowledge about the phenomenon of data security of the digital CdC is also very current, expressively important to reflect on the robustness of the subject and to corroborate the minimization of the thematic gap, still rarely addressed by the academy. Therefore, it is justified the choice and relevance of the study, whose results are promoters of excellent academic, legal, public and social gains and, of exponential applicability in the sphere of PPD.

This study was structured in addition to its pretextual data and this introductory chapter, by the chapters associated with the theoretical framework, applied methodology, results/discussions and final considerations, ending with the post-textual element that lists the bibliographic references used. It is noteworthy that the same followed the norms of the FDCI Manual for the related discipline, and also the provisions of the Brazilian Association of Technical Norms (ABNT) for academic-scientific work.

2. Theoretical framework

This chapter was structured to map and sustain the objectives proposed by this research, presenting the bibliographic references corresponding to what was theoretically achieved in recent publications, analyzed and legitimized by scientific academic sources, STF and STJ.

For the theme focused on the characterization of data security, according to Stecker and Damian (2021) it concerns a valuable and essential concept in the scope of the DPP, as it brings together a range of practices, methods, technologies and policies aimed at protecting digital information in the context of unauthorized access, theft, loss and corruption.

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 16/09/2026 | aceito: 23/09/2026 | publicação: 28/09/2026

It focuses on the technical defense required to guarantee the confidentiality, integrity and availability of data, and the legitimacy of users to access, aiming at protecting against external/internal threats arising from human failures, digital viruses and hackers, making use of tools such as encryption, facial and biometric authentication, accuracy in access control and continuous multifactorial monitoring, intuiting to minimize the occurrence of risks in physical, digital and cloud environments (Luke et al., 2023).

It should be noted that in Brazil, the security of personal data, is based previously on the aegis of Law No. 13,709/2018 (General Data Protection Law - LGPD) regulating the processing of digital data in general, but with a more expressive focus on data privacy. With regard to prosecution and prosecution of criminal offences applicable to the DPP, data security follows the provisions of the article. 4, Chapter III, "a" - public safety and "d" - activities of investigation and repression of criminal offences), c/c §1o of LGPD (Brazil, 2018), which determines:

> § 1 The processing of personal data provided for in item III will be governed by specific legislation, which should provide for proportionate and strictly necessary measures to meet the public interest, observing due legal process, the general principles of protection and the rights of the holder provided for in this Law (Brazil, 2018, p.1).

In this scenario, Constitutional Amendment EC No 115/2022 added section LXXIX to article 5 of the FC of 88 with regard to general data protection, including digital data, as a fundamental right, duly guaranteed in the form of the law. Its legal basis involves the axes below:

(i) Informational Self-determination - a fundamental right that guarantees the citizen control over his personal data, limiting the State's action and preventing abuse or selectivity in criminal prosecution; (ii) Crime of Invasion of Computer Device – art. 154-A of the CP (according to Law No. 14.155/2021), typifies the crime of trespassing on computer devices of other people's use to obtain, adulterate or destroy data or information without authorization, or to install vulnerabilities aimed at illicit advantage, and; (iii) Requirement of Specific Law: the processing of personal data given by public authorities, observes the principles of legality, proportionality, need and existing legal process, aiming at the adoption of measures necessary for the public interest, even when there is no direct application of the LGPD (Souza, 2022). The concept of the term “Cyde of custody (CdC)” used in the legal and DPP domain and, in the words of the Exmos. Prosecutors Levy E. Magno and Mylene Comploier (2021, p. 196) the CoC consists of “[...] a systematization of procedures that aim to preserve the evidentiary value of the expert test, more precisely, of its authenticity”.

This means that from the inclusion of art. 158-A and art. 158-B to CPP by Law n. 13,964/19, this is the collection of all procedures that maintain and document the chronological history of a crude vestige, visible or not, perceived, found and/or collected in places or, in victims of crimes, required to trace factors such as possession and handling, involving in this, the stages that range from their recognition to their disposals (Brazil, 2019).

In line with the above context, the CoC is at least based on four fundamental principles governed by Art. 158-A CPP. The first is consistent with the "authenticity" referring to the originality of the object in expert analysis, originating from truthful sources and announced in the collection stage, without any type of tampering during a process, thus ensuring the identification and security at the origin of the information, which requires the guardianship of the expert agent. The second, in turn, corresponds to the "integrity" that validates the criminal evidence from its recognition to its transit on trial, thus guaranteeing its merit as procedural proof maintained under the same conditions in which it was identified (Ramalho et al., 2023). In addition, there is the principle of "trust or reliability" as a criterion for valuing the criminal evidence in terms of its suitability, which is relevant to the basis of the judicial argument and enables the verification of third parties despite the appropriateness of the procedures adopted. Furthermore, there is the principle of "sameness" associated with the formation of the judge's conviction on the criminal evidence that must be identical to the trace identified and collected at the crime scene, thus becoming the basis that guarantees the principles of identity and traceability of evidence (Fischer, 2025).

In addition to what has already been described, the CoC involves three groupings: (i) the Custody Chain of the Criminal Proof (CdCPP); (ii) the Custody Chain of the Digital Proof (CdCPD) and (iii) the Digital Archivistic Custody Chain (CCDA), each with its specificities and legal purposes as presented in Table 1.

Table 1 - Chain of custody groupings in legal order

Group	Legal characteristics
Custody Chain of Criminal Evidence (CdCPP)	Follow the dispositions of the Arts. 158-A to 158-F of the CPP dealing with the legal requirement of admissibility in criminal proceedings, aiming at ensuring the suitability, traceability and authenticity of any and all traces, at all procedural stages, regardless of their physical or digital structure. It covers the chronological documentation, detailed and complete of the historicity of the vestige intuiting questions about possible adulterations and/or contaminations, taking into account the break in the chain and its consequences that tend to conduct the inadmissibility or nullity of the proof, in view of the principles of integrity and guarantee of the legal process in order.
Digital Proof Custody Chain (CDCPD)	Associated with the specific application of the principles of the chain presented above, the electronic possibilities,

	intuiting the recognition of the volatile and changeable nature of the digital proof, and thereby ensuring that the copy attached to the records of a process is identical to the original trace seized, preserving the integrity of the content and metadata.
Digital Archivistic Custody Chain (CCDA)	It refers to the archival concept based on the management of the digital document's life cycle, as well as its long-term preservation, ensuring its legal principles of authenticity and reliability and also, the not breaking of its archival custody. It focuses on the technical and legal integrity of documents whose purposes are memory, transparency and future proof.

Source: Adapted by the author of Matida (2020); Motta (2022); Gava and Flores (2023); Fischer (2025).

In the context of the complexity of the triple category of the CoC as seen in Chart 1, context, it is important to observe what Santos (2022) points out, by stating that, although the forensic tests started to be inserted into the CoC by the Ordinance SNSP 82/14, its effectiveness in this institute occurred only when the Arts were added. 158-A to 158-F, arranged by Law 13.964/2019.

With reference to the processes adopted by the CoCs whether they are physical, digitized or archival, it is observed in the research conducted by Gava and Flores (2020) and Lima and Romanelli (2023), that these need to be audited by preservation procedures, required to meet their ability to ensure the genuineness and reliability of forensic evidence arising from a digital environment, which by nature are already potentially complex and vulnerable given the fact of their processing between sectors. It is clarified that given the breadth, complexity and detail to the construction of the CoC, each trace within a single criminal scene, demands that the ten stages arranged in the CPP and the Law be met. n. 13,964/19, constituted in Table 2.

Table 2 - Stages involving forensic tests of a CoC

Step	Correspondence	Characteristics
1	Recognition	Identification of trace as potential forensic evidence
2	Isolation	Total conservation of the environment and the forensic trace
3	Fixed	Act to describe in detail the environment and the forensic trace
4	Collection	Trace collection without any change in its originality
5	Packaging	Trace guard in own container, identification label, date and time of collection
6	Transport	Movement of trace to destination site ensuring its integrity
7	Receipt	Documented formalisation of trace transfer
8	Processing	Consistent with the expert examination and the issue of his report
9	Storage	Associated with the conditions of custody of the forensic evidence and its report
10	Discard	It corresponds to the total elimination

		of expert evidence according to laws and related rules

Source: Adapted by the author of Brazil (1941; 2019).

Based on what is presented in Chart 2, and to do justice to the legal purpose, the §1 of art.158-A of the CPP established by Law n. 13,964/19, stating that "the beginning of the custody chain occurs with the preservation of the crime scene or with police or expert procedures in which the existence of trace is detected" (Brazil, 1941, p. 1). This premise recognizes the relevance of the conservation of the crime scene; of its vestige(s); of the adoption of standard security procedures and; of the relevance of the expert (Cavalcanti; Silva, 2026).

This recognition, according to the conception of the Summary No. 361 applied by the Supreme Court (STF, 2026, p.1), states that: "in criminal proceedings, the examination carried out by a single expert is null and void, considering what previously worked in the diligence of apprehension", whose basis is based on the Arts. 151; 159 to 160; 165; 170 to 171; 173; 177; 179, in the sole paragraph of art. 181 e; 279, II, arranged in the CPP. This statement is based on the following three conditions (i) application to Non-Official Experts; (ii) inapplicability to Official Experts (federal and state servants) and; (iii) impediment by Prior Participation. This refers to reflection on the rule of nullity.

By way of knowledge, Motta (2022) and Gava and Flores (2023), point out that the CdC igital/Digital Archivistics integrative to the DPP, use, in particular, divergent Information and Communications Technologies (ICTs) and cybersecurity, which will not be visited in this review, considering that their objective is to seek answers to the risks of data security of criminal evidence held in the CoCs.

However, it is necessary to understand that all technologies applied in the CoCs are governed by divergent guidelines for the legal support of their procedures in general. Within this scenario, the following stand out: Request for Comments RFC n.3227/02 - technical document describing standards, protocols, methods and research conducted digitally, defining the Internet communication base and sharing relevant data from computer engineering (Motta, 2022); Law n. 12.965/14 - Considered as Civil Marco da Internet since it has on the principles of privacy, data protection and record keeping (Brazil, 2014); Resolution CONARQ n. 51/23 Version 2 - It has on the "Directs for the Implementation of Confidential Digital Archivistic Repositories" (National Council of Archives – CONARQ, 2023).

In addition, they stand out: the judgments of the STJ and STF - nullify evidence collected without due judicial authorization, or even, through improper handling prior to official expertise (Motta, 2022; Fischer, 2025; Pereira, Torres, 2025); the Normative Instruction IN DG/PF n. 299/25 - lays down and details technical guidelines aimed at the preservation, analysis

and use of digital elements raised in the investigative processes of PF (Souza, 2026) and; International Regulatory Standards (NRs) and Brazilian Regulatory Standards (NBRs) - guidelines of recommendation, regulation and standardization of processes, good practices to the Information Security Management System (SGSI) (Brazil, 2026).

In this legal context, the Anticrime Package (AP) established by Law n. 13.964/2019 which aimed to improve criminal and procedural legislation, whose idealization took place in the search to reduce gaps in public security, since it has 70 specific measures aimed at strengthening the penal system, thus conferring the imputation of more rigid and less bureaucratic actions aimed at mitigating violent occurrences, impunity and recurrences in this scenario. The prospects for its implementation involve the mobilization of societies; the transparency of actions; the integration of private and public sectors; elections; and, of course, criminal persecution (Brazil, 2019).

According to Santos (2022), the building of BP was based on the high rate of active, passive, necessary and predictive corruption. That is why the problems of over-invoicing, competition, digital fraud and false fiscal notes have been adhered to. All, experienced in the country in its divergent sectors of socio-economics, but with emphasis on Public Administration. The researcher points out that with BP, the forensic tests started to be inserted into the CoC, effectively. The problem of corruption is one of the main fears of the Brazilian population, and raises the reflection about the execution of the prison in a restraining seat or sentence on trial. In this scenario, Law n. 13.964/2019 included the so-called “Guarantee Judge” as responsible for the stages of criminal investigation differentiating him from the judge who acts in the instruction and trial of criminal proceedings, intuiting the guarantee of impartiality of this magistrate and his non-contact with any criminal evidence to infer a prejudgment (Brazil, 2019). That is, “[...] the performance of the guarantee judge would ensure, in the sequence, another impartial judge, who had no prior contact with the investigation, this would give parity of arms between the prosecution and the defense” (Santos, 2022, p. 112).

Assuming that the Theory of the Criminal Process inserts the full proof within the AP, in the explanation of Abreu; Cardoso and Passos (2022), this condition gives it the status of reconstructive mechanism of events investigated in a certain judicial process. In the field of licit/ilicit evidence, the authors argue that the PA is based on the assumptions of the DPP concerning three theories, summarized as follows: (i) Fruit Theory of the Poisoned Tree – based on the contamination and inadmissibility of evidence derived from illicit sources; (ii) Theory of Independent Source – allows evidence of a lawful nature and no causal relationship with the

original illicit proof; and (iii) Theory of Inevitable Discovery – considers the derivation of the proof if discovered by lawful means.

Regarding the identification of the main challenges experienced by the DCCD and CCDA and the possible gaps in Law n. 13.964/19 that affect the data security of the DPP institute, the literature of Motta (2022), Santos (2022), Gava and Flores (2025), and Pereira and Torres (2025) emphasize that cybersecurity is indispensable to procedural results, once they offer greater security and legal and criminal transparency. However, on the other hand, they show a range of legal and infrastructural problems. This is justified by Lucas et al. (2023), when punctuating the exponential growth of the scientific community interest in the application of cybersecurity techniques to mitigate attacks on computer networks, configuring the potential relevance of such methods. In view of this, it is highlighted as the main challenging element, the "break in the chain of custody", represented by the "[...] failure or interruption of the trajectory of the tests, such as in the identification, handling and disposal of the information used in the investigation, which impairs reliability and contradictory because it does not allow the guarantee of the integrality of the test" (Marques; Barbosa, 2025, p.?).

In the design of the legal order in a procedural document, it was found additionally that:

> [...] the institute of breaking the chain of custody concerns the suitability of the path that must be followed by the proof until its analysis by the magistrate, being certain that any interference during the procedural procedure may result in its impracticality. It aims to ensure to all accused due legal process and the resources inherent to it, such as broad defense, contradictory and mainly the right to legal proof (STJ. Special Appeal Abuse No. 1,847,296-PR (2021/0049381-6).

In addition, Exmo. Prosecutor Douglas Fischer (2025) reports that in the field of nullities/invalencies promoted by the breach of the CoC, the case law of the STJ in various Resources and Procedural issues, understands that in order to configure this breach, the aspects should be thoroughly analyzed: effectiveness of the proof (possible tampering); demonstration of effective damage to the process; guarantee of the suitability and reliability of the proof, explaining that: If a proof is unlawful (invalid), it would not even be up to the judge to analyze its reliability. One excludes the other. Illicit evidence cannot be used in the process. The legal evidence, even with the breach of the chain of custody, has to be analyzed to see if it confers credibility for the trial. That is, it has to be evaluated by the judge and not eventually excluded (Fischer, 2025, p. 1).

Also, Alves and Bezerra (2023, p.1) observe that the PA represents an innovation to the Brazilian legal system, once "the regulation of the custody chain is elevated to the level of the

RCMOS – Revista Científica Multidisciplinar O
Saber. ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 16/09/2026 | aceito: 23/09/2026 | publicação: 28/09/2026

law". However, it weighs necessary adjustments in what is associated with non-compliance with regulatory requirements to the CoC, whose results impute to the case law, the responsibility on its analyses in terms of absolute or relative nullity. The nullity according to the CPP from your article. 563 onward, rules that when absolute is associated with non-admission of convalidation, assuming a nature that should never exist. When relative, in turn, she admits the convalidation without any prejudice to the public interest, prosecution or defence. Regarding the above, the case law in the 720 of the STJ (6th Class), there is the understanding that "the irregularities contained in the chain of custody should be weighed by the magistrate with all the elements produced in the instruction, in order to assess whether the proof is reliable" (Alves; Bezerra, 2023, p.8). However, Cavalcanti e Silva (2026) mention the legislative omission in the face of the breach of the CoC, which fosters debates about the admissibility or not of the proof. This connects directly with: (i) the value of it; (ii) the act corresponding to such break, and (iii) the legal guidelines in the context.

As extra factors to those already visited that involve the challenges to data security in the CoC, Chart 4 summarized the findings of the other literatures studied.

Chart 4 - Challenges found in the literature on nullity, breach of custody chain and BP gaps

Challenges	Author/year
Illegality of screen prints (WhatsApp / social media) and data extraction from mobile phones - holders of controversial proof status, facing the legal understanding regarding the sending and deletion of messages freely, by those who send and/or receive, without any trace or storage of them.	Motta (2022)
Lack of documentary record of all stages of the full test; loss or inaccessibility to the media experienced in its originality, preventing the authentication or construction of technical counter-provement; difficulties imposed by the police/experts in the accessibility to the image or physical consistency of the proof required by the defense; non-registration of access and non-authorization of third parties prior to expert actions; problems in the preservation of encryption and/or digital signature.	Marques and Barbosa (2025)
Lack of specific regulation and standardization in the treatment of the evidence; historical subjectivity and characterization of each test; tampering of the evidence; problems of access and transit of the data; definition of the proof as documentary record of legal expertise; immateriality, independence and reliability of the digital trace; CoC documentation in ensuring the authenticity of the test; ethics and governance; technical training; use of technology in an irresponsible way.	Gava and Flores (2023), Lima and Romanelli (2023), Pereira and Torres (2025) and Silva and Lopes (2025)
Breaches of Law No. 13,964/19 demand immediate improvement measures to standardize procedures, implement screening technologies and enhance interinstitutional integration, facing personal conditions, insufficient materials and economic divergences between states and municipalities that affect official criminal expertise agencies.	Pereira and Torres (2025), Cavalcanti e Silva (2026)

Source: Adapted by the author (2026).

Digital evidence, especially collections on mobile devices, drones, social media and applications in general, STJ ministers (2023a) attest that no type of digital evidence is admissible without the proper record regarding the procedures adopted by the police, in order to preserve the integrity, authenticity and reliability of the components in these conditions, this condition, current until now.

An example of this was given in the decision of the STJ relevant to drug trafficking and the seizure of cell phone seizure, data extraction and screen capture, based on the possible breach of the CoC given by volatility, auditability, repeatability, reproducibility, and the justification of susceptibility to the alteration of digital evidence, following the principle of sameness. Unanimously, it provided for the regimental problem, in view of the failure of the CoC to adopt procedures to ensure the suitability of digital evidence, on the following allegation:

> [...] it is not possible to infer the suitability of the evidence extracted by direct access to the seized cell phone, without the use of forensic tool to guarantee the accuracy of the evidence, there are no records that the elements initially collected are identical to what corroborated the conviction (STJ, AgRg in HC No 828054 - RN (2023/0189615-0), 2024).

Furthermore, in Agravo Regimental on the process concerning the murder and criminal association, involving pre-trial arrest, digital proof, CoC, demand for complementary technical expertise and proof of the reliability of digital evidence, aiming to know and discuss the breach of the CdC of digital evidence and illegal embarrassment through preventive arrest, analyzing the peculiarities related to the volatility and modifiability of the evidence to prove its integrity and reliability, aspects such generators of doubts that cannot be unfavorable to the defendant, it was unanimously decided to provide it (STJ, AgRg no HC 1014212 / ES – Agravo Regimental no HC 2025/0231341-3, 2026).

Finally, Matida (2020) and Ramalho et al. (2023), emphasize that although there are still challenges presented in this study, the guarantee of authenticity, integrity, reliability and sameness of evidence integrated into the physical, digital or digital archival CdCs, have a decisive character in the conduct of procedural results of legal order, minimizing the risks of condemning innocent subjects and misleading criminal individuals, but also inducing financial losses to public coffers, unfair compensations and, waste of time, which results in the construction of population mistrust to the judicial system.

3. Methodology

This study adopted according to Henrique and Medeiros (2017), a basic research considering its purpose in expanding scientific knowledge without a practical application regarding the phenomenon of data security in the Digital and Digital Archivistic CoC that composes the DPP, its challenges and possible breaches of Law n. 13,964/19, based on academic-scientific bibliographies. To this end, it adopted a qualitative approach, as it sought to analyze the subjective context of this phenomenon, that is, its cultural, historical, humanistic aspects, values and perceptions, which are not measurable. As for the classification of their objectives, these were exploratory, exploring this thematic context, reporting and discussing the literary findings.

For the data collection procedure, the literature review technique was used, given by the determination of the keywords: Custody Chain, Criminal Procedural Law, Law n. 13.964/2019, Data Security and Ponta Technologies, crossed by the term “and” that integrates the Boolean method of collection aiming the refinement of materials. The inclusion criteria that were considered were: academic, scientific and technical physical and digital articles with a time frame from 2015 to 2026, except for legislation and legal regulations published in the Portuguese language. For exclusion: studies with access only to the abstract or without availability of the full text; studies in languages other than the specific ones; studies that escape the central theme proposed, and; duplicity of the work in the sources of collection analyzed.

The database of CAPES and Google Academic and SciELO platforms and diverse legal entities were used as data sources. The analytical procedure of the project followed the steps: 1) reading basic data such as title, abstract and summary; 2) discarding based on the exclusion criteria; 3) compilation of the materials effectively chosen in Excel spreadsheet from the variants: author/year and title; type of article and place of publication; objectives; results and conclusions, to facilitate their access and identify the citations applied; 4) integralized reading of the remaining articles; 5) analysis of results and comparative discussions between the various authors.

4. Results and discussion

The literature studied, in general, identifies that the promulgation of the Carta Magna of 88 (Brazil, 1988) focused on the democratic political organization in Brazil, represents a historical landmark of total importance, considering that, in addition to institutionalizing a new

doctrine to the organization and management of public safety in Brazil, it also stimulated the promulgation of a series of laws and regulations, as well as the use of cutting-edge technologies in this context, which experience high and continuous risks to their data security.

Based on this, the phenomenon of the challenges to the security of data of the CoC of criminalistic evidence, whether physical or digital or archival, i.e., that is to say that they comprise the CocPP, DCCPD and CCDA, particularly specified by Matida (2020), Motta (2022), Gava and Flores (2023), and Fischer (2025), represent a structured condition on a technical defense model in order to ensure its authenticity, integrity, reliability and sameness. These principles of the DPP and the CPP are essential to the expert analyses, as also defend the studies of Stecker and Damian (2021), Magno and Comploier (2021), Lima and Romanelli (2023), Souza (2022) and Ramalho et al. (2023), Marques and Barbosa (2025), Pereira and Torres (2025) and Silva and Lopes (2025).

With regard to these principles, it was clearly seen that the CoC is broad, complex and subject to numerous challenges, especially regarding the data security of cutting-edge technologies applicable to DCCPD and CCDA, as discussed by Stecker and Damian (2021), Motta (2022), Gava and Flores (2023) and Silva and Lopes (2025), among others. It was noted that it is common to the literature analyzed, confirming the growing need to implement this technological evolution to achieve the principles revealed above, these, guiding the ten stages given to criminal evidence custody chains, with emphasis on ICTs and cybersecurity devices.

Although the study has not deepened the technologies applicable to DCCDs and DCDCs, it was verified that Brazil has a diversity of laws and regulations in the regulation of procedures applicable to its structures, and that involve steps from identification to disposal of evidence in judgment. In this, art stands out. 4th LGPD (Brazil, 2018) that generated EC n. 115/22 (Brazil, 2022) based on three basic directs guaranteed to citizens by the FC of 88: the information self-determination that deals with the self-control of personal data to each Brazilian; the crime of invasion of a computer device that prevails by the previous law and; the requirement of specific law corresponding in this case, to EC 115/22.

These guarantees are also governed by Art. 154-A of the CP (Law No. 14,155/21) (Brazil, 2021), by Law No. 13,964/19 (Brazil, 2019), and other national and international legislation and standards relevant to the use of technologies in the DPP. In the conception of Abreu; Cardoso e Passos (2022), Santos (2022) and Pereira e Torres (2025), the promulgation of Law n. 13,964/19 is essential for minimizing and combating corruption in all its possibilities, modernizing the CPP and enhancing the DCCD and CCDA. One of the main points governed by this Law is associated with the lawfulness of evidence, that is, of its veracity and preservation

initiated in the environment of origin, traces of crime, collection, storage, transportation, cataloging and guarding. These steps are in line with what was summarized in Chart 2. Gathered together, they are crucial to expert results.

It was further verified that digital and digital archival custody chains are supported on specific theories that for Abreu; Cardoso and Passos (2022), involve the illegality or unlawfulness of the evidence; the occurrence of causality with it within the parameters governed by Law n. 11.690/08 and Art. 157 § 1st and 2nd of the CPP, and; the flexibility of illicit evidence sometimes inevitable. This reality marks state-of-the-art technologies as increasingly indispensable instruments for DCCD and DCDC.

In this theoretical-analytical process, the following aspects were identified:

action and expert responsibility; procedural fraud, breaches of secrecy; commitment of truth; guarantee of evidence preservation; archival recommendations, all relevant to the structure of the DCCPD and CCDA, which as systems that control the custody of criminal evidence in a digital way, need to act in accordance with the PDS and its management, as discussed by Gava and Flores (2023).

With regard to the breach of the chain of custody, authors such as Alves and Bezerra (2023), Fischer (2025) and Marques and Barbosa (2025) present and discuss resources and regimental aggravations of divergent jurisprudences of the STJ at the national level, exposing the divergences in the conception of the legal system on the legality and nullity of digital evidence focusing on the admission or not of their convalidations.

Generally, the Magistracy understands that the digital evidence of the CoC requires the records due conducted chronologically and responsible for the prosecution of criminal evidence. This legal condition involves a number of possibilities that open the gap to Law n. 13,964/19, identified in Chart 4 of this study, which were summarized in Chart 5, emphasizing the problems with data security.

Table 5 - Main gaps in DCCD and CCDA that impact BP

Lacuna	Characterisation	Author/year
Archivistic frauds, confidentiality and data sharing	If not cleared in time, they modify the results of criminal proceedings. They affect the objectives of Law No. 13.964/19.	Stecker and Damian (2021); Santos (2022); Gava and Flores (2023); Lima and Romanelli (2023); Pereira and Torres (2025)
Proof production and its control by the DCCD and CCDA	There may be a break in this process, compromising the basic principles that guide the digital CDC as a whole.	Pereira and Torres (2025); Silva and Lopes (2025); Cavalcanti e Silva (2026)
Infrastructure and resource problems	Standardization of procedures; qualified human resources; tracking technologies; communication between sectors; socioeconomic differences between states and municipalities of the federation.	Gava e Flores (2023); Lima e Romanelli (2023); Pereira e Torres (2025); Silva e Lopes (2025); Cavalcanti e Silva (2026); Souza (2026)

Illegality of using screen prints	WhatsApp and social media, which hold controversial proof status.	Motta (2022); STJ (2024); STJ (2026)

Source: Adapted by the author (2026).

When discussing the visa in Chart 5, it was found that the frauds modify the authenticity of the proof, however, aspects such as irregular documentation and/or lack of expertise are validated, depending on the judge's understanding. In line with this reality, there are the confidentiality and data sharing factors, which require strategic procedures, previously postulated and standardized, whose internal and external procedures, should be carried out only with authorized and qualified personnel and between integrated departments.

In the legal understanding of Exmo. Minister Ribeiro Dantas of the STJ with the Appeal of Habeas Corpus RHC n. 77,836/2023, it is that the objective of the CoC to ensure the legal process and its resources related to any and all accused, as a tool of defense, contradictions and rights to the lawfulness of the proof to which it is widely fair, is supported in the scope of the institute by defending the proceedings “[...] until its analysis by the magistrate, being sure that any interference during the procedural procedure can result in its impresability” (STJ, 2023, p.1).

Digital evidence, in the conception of Stecker and Damian (2021, p.11), becomes essential since “[...] without an egalitarian technological power, between accusation and defense... criminal prosecution as fiction is a democratic emptying”. Therefore, the admission of the proof is questionable, considering its appreciation to the records. This is a common occurrence against the inadequacy of infrastructure resources and qualified human capital, which adds to the problems of geoeconomic disparities common to the Brazilian territory.

Lima and Romanelli (2023) defend the question of falsity of the source or its documentation, which must be treated as an incident with imputation of probatory burden to those entitled, therefore, this condition tends to affect the materiality of the trace. Documentary Irregularities of the CoC and/or absence of an expert do not affect factors of legality or legitimacy, but should be considered by the legal body so that there is probative and circumstantial force of proof. This is the case through its authentication that veracities from the beginning, and that only occurs by analyzing the set of items arranged in the records.

This being said, it is clarified that the production and examination of the evidence are essential elements to effectively confront the macrocrime currently in existence pursued by the provisions of the BP. In this perspective, Cavalcanti e Silva (2026) emphasize that the CoC only achieves its legal purposes effectively, by strictly following the stages set out in the article. 158-B of the CPP, reinforced by the arts. 158-A to 158-F of the Law. 13.964/19. This means that the process of identifying and collecting the evidence, must be conducted by a specialized

public agent, who verifies the potential of the element to be inserted in the CoC, since he is the professional who evaluates the direct relationship between trace and criminal offence. The STF Rule 361 (2026) makes it clear that: (i) application to Non-Official Experts – validity becomes null as Article 1. 159 of the Code of Criminal Procedure (CPP) when the absence of official expert; (ii) inapplicability to Official Experts (federal and state servants) – under the understanding that the signature of a single expert, characterizes the validity of the report; (iii) Impedition by Prior Participation: the original text aims to avoid conflicts of interest, preventing the same expert who acted in the seizure of the evidence (e.g. drug seizure) from being the only one to report the material, ensuring impartiality. Therefore, although the statement of the summary maintains the rule of nullity for examinations performed by a single expert, it is relativized to official experts, being the report signed by one of them considered valid.

Finally, regarding the illegality of the use of screen prints such as WhatsApp and social media, the discussions revolve around the legal understanding regarding the sending and exclusion of messages freely, by those who send and/or receive, without any trace or storage of them, which tends to invalidate their possibility of criminal evidence. The STJ (2023) does not admit any type of digital evidence without the proper record of the procedures adopted by the police, aiming to preserve the integrity, authenticity and reliability of the components in these conditions.

Contextualizing with the above, both Agravos cited in the course of the theoretical foundation attest that the legal system in Brazil does not admit convictions supported by traces of unconfirmed and expert origin, once the guarantee of reliability of what is presented in court is mandatory. Thus, all the legal challenges and guarantees identified in this study reinforce the legal protection and the need for data security as a way to eliminate the need for undue violation of the security mechanism, expanding the legal coverage surrounding the DCCPD and the CCDA.

5. Final considerations

To answer the guiding problem of this literature review, asking about the structure and challenges of the DCCD and CCDA tangible to data security for the preservation of forensic evidence from related laws and, in particular, the provisions of Law n. 13,964/19, the theoretical analyses allow it to be stated that the hypotheses listed as their answers were right, because it

was clarified the extent and complexity that involves this phenomenon, both in legal terms and in resources so that the purposes of both the CdC and the AP are effectively achieved.

Therefore, the general and secondary objectives that aimed to address the characteristics, relevance and challenging aspects of data security of criminal evidence integrated into the custody chain of the DPP were achieved, in view of the knowledge gathered about principles, theories, stages, preservation and custody of their files and probable gaps left by Law n. 13.964/19.

It was possible to extend conceptual knowledge and applications of custody, where the legal guidelines governing the use of state-of-the-art technologies applicable to this DPP Institute were more comprehensive. The challenges hypothetically addressed in the introduction and involving the confidential factors, search and seizure of evidence, preservation/alteration of the object and the expert environment, legal rights and duties, structures of processes failures, fraud, illegality of evidence from screens without the proper police record or sufficient loyal basis and, everything that involves the breach of the digitized CdC, were analyzed and proven as possible elements of impact to forensic and legal results, adding the issue of fraud, breaches in custody and illegality of evidence.

The bibliographic study found no gaps in association with the challenges of data security in the digitalized CoC, but showed low production of academic-scientific research that presents the technologies in detail within the legal bias. Therefore, it is concluded that there is an immensity of legal knowledge involving the proposed theme, reaffirming its relevance, as well as the need to continue further studies, considering that the Anticrime Package is still a novelty, despite its 7 years of establishment. BP is faced daily with numerous obstacles, including what structure the digital and digital archival CdC, where the breach, fraud and secrecy of its files is essential to data security and the results of criminal cases.

References

ABREU, Lauro Pereira; CARDOSO, Jaqueline Ribeiro; PASSOS, Fábio Presoti. The analysis of the need to predict the figure of the judge contaminated in the legal system. In: Libertas Direito, Belo Horizonte, Vol. 3, n. 1, p. 1-33, Jan./Jul. 2022.https://periodicos.famig.edu.br/index.php/direito/article/view/209/136.Accessed on Apr 12. 2026.

ALVES, Ani H. da Silva; BEZERRA, Thiago J. de S. Lima. The production of evidence in the Brazilian criminal case: an analysis of the nullity by non-compliance with the rules of the chain of custody. In: RECIMA21 - Exact and Earth Sciences, Social, Health, Humanities and

Engineering/Technology. Vol. 4, n. 9, 2023.https://recima21.com.br/recima21/en/article/view/4033/2901.Access set 07. 2026.

BRAZIL. Law No. 3,689 of October 3, 1941: Code of Criminal Procedure. Rio de Janeiro: Presidency of the Republic. D.O.U. of 13.10.1941 and corrected on 24.10.1941.https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm.Accessed on April 20. 2026.

BRAZIL. Law No. 12,965 April 23, 2014: Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil. Brasília, DF: Presidency of the Republic.

D.O.U. of 24.4.2014.https://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm.Accessed on April 20. 2026.

BRAZIL. Law No. 13,709 of 14 August 2018: It provides for the protection of personal data and amends Law 12,965, of 23 April 2014 (Internet Civil Mark). General Law on the Protection of Personal Data (LGPD). Brasília, DF: Presidency of the Republic. D.O.U. of 15.8.2018, and partially republished on 15.8.2018 - Extra edition.https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.Access on 21 Apr. 2026.

BRAZIL. Law No. 13,964 of 24 December 2019: Improves criminal and procedural legislation. Brasília, DF: Presidency of the Republic. D.O.U. of 30.04.2021.http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.Accessed on Apr 03. 2026.

BRAZIL. Guide to ISO and NBR Standards for Information Security. (online), 2026.https://ufdpar.edu.br/ufdpar/guia-de-normas-iso-e-nbr-para-seguranca-dainformacao.Accessed on 22 Apr. 2026.

CAVALCANTI, Douglas Rodrigues; SILVA, Thiago Henrique Costa. Breaking the chain of custody and the consequence for due process: a literature review. In: Atatot - Interdisciplinary Human Rights Magazine of the UEG. Vol. 7, n. 1, 2026.https://revista.ueg.br/index.php/atatot/article/view/16405.Access in 22 Apr. 2026.

NATIONAL ARCHIVE COUNCIL. Resolution n. 51 of 21 August 2023: It has on the "Directs for the Implementation of Confidential Digital Archivistic Repositories" – Version 2. Brasília, DF: Ministry of Management and Innovation in Public Services – CONARQ. 2023.https://www.gov.br/conarq/pt-br/legislacaoarquivistica/resolucoes-do-conarq/resolucao-conarq-no-51-de-25-de-agosto-de-2023.Access 12 o'clock. 2026.

NATIONAL COUNCIL OF JUSTICE – CNJ. Custody hearings complete 10 years with unpublished data. (online) Feb 24. 2025.https://www.cnj.jus.br/audiencias-de-custodia-completam-10-anos-com-dados-ineditos/.Accessed on Apr 12. 2026.

FISCHER, Douglas. The chain of custody involves measuring the sameness or reliability of the proof, not its invalidity/nullity. (online), 11 set. 2025.https://temasjuridicospdf.com/acadeia-de-custodia-envolve-a-afericao-da-mesmidade-ou-fiabilidade-da-prova-nao-a-suainvalidade-nulidade/.Access set 05. 2026.

GAVA, Tânia Barbosa Salles; FLORES, Daniel. Problematizing Post-Custody with the contemporaneity of the Digital Custody Chain shared and distributed in Systemic Digital Preservation. In: InCID - Rev. Scient. Inf. and Doc. Ribeirão Preto, Vol.13, n. 2, p. 222-243, set. 2022/feb. 2023.https://www.academia.edu/95019816/Problematizando_a_P%C3%B3s_Cust%C3%B3dia com a contemporaneity da Cadeia de Cust%C3%B3dia Digital File%C3% ADstic share and

distribute%C3%ADda na Preservation%C3%A7%C3%A3o Dig ital Sist%C3%Aemic. Access on 21 Apr. 2026.

HENRIQUES, Antonio; MEDEIROS, João Bosco. Scientific Methodology of Legal Research. 9th Ed. Ebook Kindle. São Paulo: Atlas, 2017, 2.9 MB, 413 p.

LIMA, Paulo Guilherme Carolis; ROMANELLI, Leonardo Leonel. The custody chain from the reform of the CPP: probatory activity of second degree. In: Journal of the Military Public Ministry. Vol. 48, n. 34, p. 1-38, 2023.https://revsita.mpm.mp.br/rmpm/article/view/81/75.Access on 21 Apr. 2026.

LUCAS, Thiago José; FIGUEIREDO, Inês S. de; TOJEIRO, Carlos; ALMEIDA, Alex

M.G. de. A Comprehensive Survey on Ensemble Learning-Based Intrusion Detection Approaches in Computer Networks. ==References== Vol. 11, p. 122638-676, Jan. 2023.https://www.researchgate.net/publication/375103711_A_Comprehensive_Survey_on_E == sync, corrected by elderman == @elder man

MAGNO, Levy E; COMPLOIER, Mylene. Prison of custody of criminal evidence. In: Legal notebooks. São Paulo, Year 22, no 57, p. 195-219, Jan./Mar.2021.https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/cj_n57_10_cadeia%20%20cost%C3%B3day.pdf?d=637437206976264894. Access set 05. 2026.

MARQUES, Thaysa Mendes; BARBOSA, Karlos Alves. Chain of custody of digital evidence in criminal proceedings. 2021, 18 P. Article of Course Completion (Bablished in Law). Law school. Federal University of Uberlandia. 2021.https://repositorio.ufu.br/bitstream/123456789/47148/2/Cadeiadecust%C3%B3dia.pdf.Access on Sep 04. 2026.

KILLED, Janaina. The chain of custody is a necessary condition for reducing the risk of convictions of innocents. In: Newsletter. Year 28, n.331, jun. 2020.https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/541/61.Access set 05. 2026.

MOTTA, Eduardo Titão. Chain of custody of digital evidence and illegal use of prints as evidence in criminal proceedings. In: Library of the Brazilian Institute of Economic Criminal Law – IBDPE. May 31st. 2022.https://ibdpe.com.br/cadeia-de-custodia-da-prova-digital-e-a-ilegalidade-do-uso-deprints-de-tela-como-elementos-de-prova-no-processo-penal/.Accessed on Apr 12. 2026.

PEREIRA, Leticia Rodrigues; TORRES, Leonardo Guimarães. Law 13.964/2019 and the chain of custody: advances and challenges in the preservation of criminal evidence. In: Ibero-American Journal of Humanities, Sciences and Education. Vol.11, n.10, p. 4487–4497, 2025.https://periodicorease.pro.br/rease/article/view/21714.Accessed April 16th. 2026.

RAMALHO, Thales Novais et al. The importance of the chain of custody in Brazilian justice: the guarantee of the integrity of the evidence and the decisive role in the conduct of judicial proceedings. In: Ibero-American Journal of Humanities, Sciences and Education. São Paulo, v.9.n.02. Feb. 2023.https://periodicorease.pro.br/rease/article/view/8412.Access on Sep 04. 2026.

SANTOS, Damian of Sousa. Law No. 13.964/2019 – Brazil Anticrime Package. In: Education, Health and Society: research, challenges and future perspectives. 1 ed. Chapter 4. Rio de Janeiro: Epitaya, p. 85 – 118,

2022.https://portal.epitaya.com.br/index.php/ebooks/article/view/514/395.Accessed: Apr 19. 2026.

SILVA, Cristiane V. da; LOPES, José A. Bezerra. The use of digital evidence in criminal proceedings. In: Ibero-American Journal of Humanities, Sciences and Education. São Paulo, v. 11. Five, May. 2025.https://periodicorease.pro.br/rease/article/view/19071.Access on Sep 04. 2026.

SOUZA, Ricardo Calmona. Constitutional Amendment No 115 and the right of data protection in criminal prosecution: the (un)concern with the need for a "criminal LGPD". In: DOUTRINA - Revista de Direito da Defensoria Pública do Estado do Rio de Janeiro. 32, 2022.https://defensoria.rj.def.br/uploads/imagens/97f7a07e38234ad09e7c42a5292a0432.pdf. Access set 05. 2026.

STECKER, Matias Hillesheim; DAMIAN, Felipe Bochi. Chain of custody of digital trace: technology as defensive power. 2021, 13 p. Article (Master of Criminal Sciences and Specialization in Penal Sciences). Pontifical Catholic University of Rio Grande do Sul – PUV/RS. Porto Alegre, RS, 2021.https://editora.pucrs.br/anais/congresso-internacional-de-cienciascriminais/assets/edicoes/2021/arquivos/40.pdf.Accessed on Apr 12. 2026.

Supreme Court of Justice. Special Appeal Abuse No. 1,847,296-PR (2021/0049381-6). Brasília, DF: Rapporteur: Minister Reynaldo Soares da Fonseca. 2021.https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&seqUncial=2073099&num registration=202100493816&data=20210628&petition number=22100584037&format=PDF. Access on Sep 04. 2026.

STJ. The chain of custody in criminal proceedings: from the Anticrime Package to the case law of STJ. (online), 23 Apr. 2023.https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/23042023-Acadeia-de-custodia-no-processo-penal-do-Pacote-Anticrime-a-jurisprudencia-doSTJ.aspx.Accessed on Apr 12. 2026.

STJ. AgRg no HC No 828054 - RN (2023/0189615-0). Mr Ilan Paciornik. Apr. 2024.https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento type=integrate&document sequential=242041837&registration number=20230189615 0&petition number=202300906480&publication data=2040429&format=PDF. Access set 06. 2026.

STJ. AgRg no HC 1014212 / ES Agravo Regimental no Habeas Corpus 2025/0231341-3. VITA, ES: Minister Carlos Pires Brandão. Feb. 2026.https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%28%28AGRHC+INPATH%28CLAS%29+OR+%22AgRg+no+HC%22+INPATH%28CLAP%29%29+AND+1014212+INPATH%28NUM%29%29+OR+%28NEAR%28%28%28AGRHC+OR+%22AgRg+no+HC%22%29%2C1014212%29%2C0%2CTRUE%29+INPATH%28SUCE%29%29. Access set 06. 2026.

Supreme Court – Supreme Court. Application of Summary number 361. Brasília, DF. 2026.https://portal.stf.jus.br/jurisprudencia/sumariosumulas.asp?base=30&sumula=2737.Access on 21 Apr. 2026.