Research Article RJ-55

Researches on Multidisciplinary Approaches 2026 (3), 1-15 ISSN:2791-9099

Evidentiary Guarantorship of Trace Generation in Data Destruction Offences

Cüneyt Şamil Oğurlu / Ind. Res.
Istanbul Chamber of Commerce, Istanbul, Türkiye
csogurlu@gmail.com

Abstract

This study examines the evidentiary problem arising where data are lost or destroyed following unlawful access to an information system, through qualitative document analysis of legislation, case law, scholarship, conventions and technical standards. Its central claim is that the difficulties arising at the levels of typicity, attribution and the presumption of innocence are three manifestations of one structural problem, not separate defects: trace generation in digital environments is tied to no evidentiary guarantor independent of the parties to the proceedings. At the level of typicity, the feature warranting the graver characterisation is the very feature that makes proof impossible, and comparison with the case law on forgery of documents raises a question of coherence regarding the evidentiary value of secondary records. At the level of attribution, trace generation is a product of software design and therefore contingent, so a trace's absence cannot by itself establish the causal link on which culpability depends; digital traces are treated as natural indicia although, in their mode of formation, they answer to the definition of artificial indicia. At the level of the presumption of innocence, treating that absence as an indicium of intent risks inverting in dubio pro reo where doubt is greatest. The principal finding is that safeguards attach to the moment of the act for physical evidence but to the moment of intervention in digital environments. The same mismatch is embedded in the ISO/IEC standards.

Keywords: Evidentiary Guarantorship, Anti-Forensics, Data Interference, Digital Evidence, Presumption of Innocence.

JEL Codes: K14, K24, K42, K33

Highlights

- Recoverability decides both the graver charge and the impossibility of proof.
- Digital traces are design choices, so Locard holds as a default, not a law.
- Unless independent processes are excluded, a missing trace cannot prove causation.
- Treating absent traces as proof of intent risks inverting in dubio pro reo.
- Safeguards begin at seizure, not at the act, leaving no neutral guarantor.

Citation: Oğurlu, C. Ş. (2026). Evidentiary guarantorship of trace generation in data destruction offences. *Researches on Multidisciplinary Approaches (ROMAYA Journal)*, 2026(3), 1-15

Submission Date : 12.09.2026
Acceptance Date : 29.09.2026

1. Introduction

Article 243(3) of the Turkish Criminal Code (TCK) punishes an offender where data held in an information system are lost or altered as a result of his unlawfully accessing that system or remaining within it. Applying the provision depends on the court establishing which data were lost or altered; yet once the result described has occurred, the object that would make such a finding possible no longer exists. As drafted, the norm punishes conduct that simultaneously destroys the evidentiary condition of its own application. The same structure holds for Article 244(2) TCK, which lists destruction among the alternative modes of conduct. The core of the problem lies in what destruction means: where the statute speaks of damaging, altering and rendering inaccessible, ordinary access ceases but the data can as a rule be recovered, whereas destruction, on the definition adopted here, requires elimination beyond recovery.

The subject is therefore the loss of data provided for in Article 243(3) as an aggravated result, together with the act of destruction listed in Article 244(2); the other five modes of conduct serve as contrasting concepts fixing it negatively, since in all of them the object of proof survives and the difficulty is one of tools, methods and access (Alp, 2018, p. 56; Akbulut, 2016, pp. 32–37; Sarı, 2013, pp. 175–179; Tezcan et al., 2020, p. 1168). In destruction the act eliminates its own referent, the object of the offence and its sole item of evidence coinciding in one thing that no longer exists; Article 281 TCK differs in that the object destroyed is evidence of another offence, so an external referent survives. Anti-forensic techniques produce this feature systematically. Known in the Turkish literature as countermeasures, they are defined as methods preventing an investigation from achieving its purpose (Değirmenci, 2014, p. 162; Garfinkel, 2007, pp. 77–78), and decisive here is the classification accepting that an offender may also prevent evidence from arising at all (Peron & Legary, 2005; Conlan et al., 2016, p. S71).

The research is justified by the fact that data destruction has been examined as an epistemic question, whether tools can recover data, rather than an ontological one, whether data still exist, on which the normative consequences depend, and that anti-forensics is treated as a technical difficulty (Caloyannides et al., 2009, p. 16) rather than a problem of typicity and attribution, while the legal framework changes rapidly: the EU e-Evidence Regulation has been directly applicable since 18 August 2026 (Regulation (EU) 2023/1543; Espina Ramos, 2025, p. 216), and the Constitutional Court has annulled Article 134 of the Code of Criminal Procedure (CMK), which governs search, copying and seizure in computers, computer programs and records, with effect from 25 February 2027 (Constitutional Court, 12 February 2026, Merits No. 2023/128, Decision No. 2026/36, Official Gazette 25 May 2026, No. 33264). The study asks, first, in what modality Locard's principle holds in the digital environment and whether the absence of a trace can be attributed to the offender's act; second, which evidentiary proposition the safeguards actually answer, and where the period between act and seizure sits within them; third, whether adverse inference from a trace's absence is compatible with the presumption of innocence.

The thesis defended here concerns the evidentiary guarantorship of trace generation. Physical evidence may also degrade or be destroyed, and circumstantial proof has long served where the act consumes its own evidence, as in homicide without a body; the difference lies in the source of contingency. Physical trace generation is uncertain but exogenous: no party sets the rules by which traces form, and even the effort to destroy them leaves traces. Digital trace generation is endogenous: whether, in what detail and for how long an event is recorded is a configuration decision distributed among the offender, the system operator and the investigating authority, so a digital trace is no material necessity and no neutral guarantor exists. The difference is thus ontological: it concerns not how hard traces are to find but whether their formation is guaranteed at all. Guarantorship in this evidentiary sense denotes control over trace generation, not the guarantor position founding omission liability under Article 83 TCK; nor does it rival the doctrine of circumstantial evidence, naming instead why that doctrine's premises are unavailable here. The solution therefore lies not in prohibiting adverse inference but in tying trace generation to a neutral guarantee and disciplining the method of inference.

2. Conceptual and Theoretical Framework

2.1. The Statutory Rationales and the Problem of Interpretation

Article 243(1) TCK punishes unlawfully accessing an information system or remaining within it, and the third paragraph provides for the form aggravated by result (Apiş, 2018, p. 65; Aydın, 2022, pp. 92–93; Koca & Üzülmez, 2020, p. 896), while Article 244(2) punishes as an independent offence the damaging, destroying, altering or rendering inaccessible of data, the insertion of data into a system and the transmission of data elsewhere. The statutory rationales show the two diverging in three respects: Article 243(3) attaches an aggravating result to a basic offence whereas Article 244 establishes a self-standing wrong; the rationale of Article 243(3) posits the absence of intent directed at the graver result as a negative condition (Aydın, 2022, p. 93, n. 607; Mucuk, 2022, p. 29); and loss under Article 243(3) occurs independently of the offender's will, while destruction under Article 244 is the typical conduct itself. The rationale cited for Ar-

ticle 244, however, relates to the single-paragraph first version of the bill, the acts having been split at the plenary stage, so it is the rationale of a provision whose text was subsequently amended.

The provision rests on a magnetic storage architecture in which deleted data can as a rule be recovered, and no legislative will can be attributed as regards solid-state drives, cloud infrastructures, end-to-end encryption or tools operating solely in volatile memory. The rationales are therefore binding interpretative material in so far as they disclose the protective purpose of the norm, and no more than historical documents as to their technical assumptions; scholarship, indeed, draws the distinction between the two provisions from the scope of intent (Apiş, 2018, p. 65; Aydın, 2022, p. 93; Koca & Üzülmez, 2020, pp. 896, 905; Dülger, 2020, pp. 268, 291).

What matters here is which presupposition the debate on the mental element shares: rationales and scholarship alike assume that what the lost data were, and when they were lost, can be established, for the line between intent and negligence can be drawn only where there is knowledge of the result. The Guidelines explaining the Regulation show the same mismatch, defining overwriting by a seven-pass count specific to magnetic media although the method is acknowledged to fail on solid-state disks (Personal Data Protection Authority, 2025, pp. 19–20), a hardware-bound presupposition surviving in regulatory practice as recent as 2025.

2.2. The Meaning and Limits of the Act of Destruction

The definition widely adopted in the literature equates destruction with the cessation of ordinary access to data; but since that criterion also defines the alternative act of rendering inaccessible, it cannot distinguish the two (Alp, 2018, pp. 64, 67; Karagöz, 2019, p. 124; Akbulut, 2016, pp. 35–36; Kurt, 2005, p. 168), while defining destruction as putting an end to the existence of data merely restates the problem (Koca & Üzülmez, 2020, p. 872; Tezcan et al., 2020, p. 1168). The criterion of recoverability invoked to secure that demarcation rests on the assumption that data cannot technically be deleted irreversibly (Karagöz, 2019, pp. 123–124; Akbulut, 2016, p. 33). Overwriting weakens that assumption. Whereas in 1996 secure deletion was thought to require thirty-five passes, a single write now suffices for drives made after 2001, the thirty-five-pass method being deemed unsuited to modern drives (Garfinkel, 2007, pp. 77–78; González Arias et al., 2024, p. 7, Table 3); persistence is thus a hardware-dependent empirical matter, and the assumption historical rather than technical. Forensic computing theory distinguishes two forms of deletion: in the first and more common, only pointers are removed, the traces remain and recovery is often possible; in the second, the traces are overwritten and no longer exist in digital form (Cohen, 2013, p. 223). A further definition, treating as destruction a removal after which an access command returns no result (Özbek et al., 2019, p. 982; Tezcan et al., 2020, p. 1168), corresponds technically to the first form and so equates destruction with what is recoverable. The real difficulty is that the existence of data in an information system is not a single fact. Firmware, controller, storage medium, file system and operating system abstraction form relatively independent layers, so data may cease to be locatable by the operating system while persisting at hardware level, and the same act may count as destruction, alteration or rendering inaccessible depending on the layer taken as reference (Carrier, 2005, pp. 17–19, 132–133; Stoykova et al., 2022, pp. 2–3); with solid-state drives the difficulty deepens, since background operations on NAND memory both hamper complete removal and cause residual data to persist unpredictably (González Arias et al., 2024, p. 20). The minority view, adopted here, ties destruction to elimination beyond any possibility of return and observes that rendering inaccessible presupposes the data's continued presence (Karagöz, 2019, pp. 124–125; Mucuk, 2022, p. 123).

Articles 243 and 244 TCK attach typicity not to data in the abstract but expressly to a particular information system. The resulting criterion will be termed system-relative irreversibility: destruction is the elimination of data, in respect of the system forming the object of the offence, such that they cannot be regained through that system's ordinary or technical recovery facilities. Typicity is accordingly not made out where a copy remains within the same system (Akbulut, 2016, p. 33), whereas the presence of the same data on another device, in an institutional backup or with a service provider does not negate irreversibility in this sense. Where the boundary of the system lies in synchronised cloud and distributed architectures remains a problem in its own right.

Nor is the legislator unfamiliar with this proposition. The Regulation on the Deletion, Destruction or Anonymisation of Personal Data (Official Gazette, 28 October 2017, No. 30224) separates deletion from destruction along precisely the axis of the range of subjects for whom data become inaccessible (Arts. 4, 8, 9), that and the Guidelines record that several device categories have a delete command but no destruction capability (Personal Data Protection Authority, 2025, pp. 17–22). The normative functions of the two texts nevertheless differ, since the Regulation's absolute definition covers every medium under the controller's control whereas the criminal norm ties typicity to a particular system; transposed into the criminal norm, it would mean that a copy held anywhere negates typicity, so the offence would never in practice be completed. Because physical destruction and degaussing require material access to the medium, moreover, an offender acting through unlawful access is confined to logical methods

such as overwriting or cryptographic erasure, and in the Regulation's absolute sense the maximum result attainable is rendering the data inaccessible: the limit is set by the architecture of the target system before intent or criterion comes into play.

By treating conduct as rendering inaccessible where data have not been irreversibly deleted from the system in question, the criterion clarifies the boundary under Article 244(2) and forestalls a zone of impunity that a narrow reading would create; since Article 243(3) attaches the aggravated form only to loss and alteration, however, a result so characterised will not trigger it at all, and the solution holds only until the legislator takes account of the layered operation of information systems. A drawback should be conceded: where the offender acts with intent to destroy but the result cannot occur because of the system's backup architecture, the case approaches the debate on the inaptitude of the object under Article 35 TCK, so punishability depends on a configuration choice outside his knowledge and control. Punishability does not vanish, however: having entered the system unlawfully, the offender has completed the offence under Article 243(1) in any event, so the attempt under Article 244(2) either falls to be combined with it under the rules on concurrence or, if held unpunishable for inaptitude, leaves liability under Article 243(1) alone (Akkaş & Doğruoğlu, 2025, pp. 208–209).

It may be said that rendering inaccessible sometimes produces the same outcome as destruction; but data rendered inaccessible can be proved to exist by their location, volume and metadata, whereas in destruction the object of proof disappears. The difference arises not from the difficulty of proof but from the existence of the thing to be proved. The Explanatory Report to the Convention on Cybercrime accordingly treats deletion as equivalent to the destruction of a corporeal thing (Council of Europe, 2001, para. 61). A recent study takes the opposite path, holding destruction made out even where data could be retrieved by special devices and defining rendering inaccessible as eliminating the potential access of the person concerned (Akkaş & Doğruoğlu, 2025, pp. 203–204, 212); adopted together, those definitions strip recoverability of its function. Yet on any criterion the need to determine which data were lost remains: recoverability ties typicity to a technical feature outside the offender's control and requires it to be assessed against an object that no longer exists, while abandoning it erases the boundary of typicity altogether. Either way, characterisation depends on a fact outside the control of the adjudicating body; only the direction of dependence differs.

2.3. The Reliability Regime of Digital Evidence and the Theory of Traces

Digital evidence covers records created, altered or stored electronically and used in an investigation, and because it is produced in digital form it raises problems of reliability (Arslan, 2015, p. 254; Değirmenci, 2014, pp. 25–26; Sarsıkoğlu, 2015, p. 439). Its place within the traditional classification into documents, statements and indicia is contested (Saydam, 2023, pp. 53–54, 172; Değirmenci, 2014, pp. 124, 130), but here the controversy resolves itself: once the data are destroyed, the derivative records that remain are already indicia.

An indicium covers facts and traces assisting indirectly in proving the event to be established; and its weight has grown as criminal procedure has come to proceed from evidence to the accused (Öztürk et al., 2022, pp. 403–404). The distinction drawn within the category is decisive here. A natural indicium arises independently of the offender's will and in the nature of things, and proves although it was not created in order to prove; an artificial indicium is a man-made sign representing the event by convention. The consequence attaches to probative force: natural indicia are treated as objective, artificial indicia as having none on their own (Yenisey & Nuhoğlu, 2021, pp. 560–561). The theoretical claim of this study is that the distinction shifts in the digital environment. Data left in communication systems are counted among natural indicia (Yenisey & Nuhoğlu, 2021, p. 561), yet which events are recorded, and for how long, is a matter of software design: a digital trace is treated as a natural indicium while, in its mode of formation, it answers to the definition of an artificial one. The line is not strictly binary either: a system log is artificial in design yet arises, in relation to any particular act, without a will to prove, an intermediate position reflected in the three-fold distinction of Section 5.2. The thesis below follows out the consequences of that displacement.

Three further concepts must be separated. Integrity denotes that the object has remained unchanged after a determined moment; authenticity, that it existed in a particular system at a particular time; reliability, the capacity of the producing system to generate correct results (ISO/IEC 27037, 2012, Arts. 3.15, 3.16 and 5.2; Casey, 2011, pp. 20–23; Neale et al., 2022, p. 1; Christie, 2023). Turkish law gathers these under the soundness of evidence, and the consequence appears in the reference point of the safeguards: verification of integrity shows only that the evidence is unaltered since collection (Casey, 2011, p. 22), while a valid digital signature shows at most that the cor-

responding private key was used, forgery at bit level being indistinguishable (Cohen, 2013, pp. 117, 130). Nor is the distinction easily operated, since there is no defined formula for the level of confidence and classification depends on the examiner's experience (Çalışkan, 2013, pp. 116–117; Afandak, 2021, pp. 72–74, Casey, 2011, p. 70).

Standardisation supports the distinction. ISO/IEC 27043 lists relevance and authenticity separately among the conditions of admissibility (Art. 5.2), and under ISO/IEC 27042 potential digital evidence becomes digital evidence only once relevance is determined (Arts. 3.1, 3.5, 3.14, 3.15), a threshold destroyed data cannot reach, there being no object to which relevance could be applied. The case law points the same way, treating the obligation to hand a copy from the backup to the person concerned as a safeguard of the right to reliable evidence and of the rights of the defence (Constitutional Court, *Yankı Bağcıoğlu and Others*, App. No. 2014/253, 9 January 2015).

The theoretical ground of the regime of safeguards is Locard's exchange principle, under which every contact entails a mutual transfer of material, so that an offender both leaves traces at a scene and carries traces away (Öztürk, 2006, pp. 36–37, 72); it lends proof a three-stage logic: if an act occurred it left a trace; traces can be collected; from traces one can work back to the act. Transposed to the digital environment, it becomes the assumption that activity leaves digital footprints from which acts and intentions can be inferred (Sommer, 2013, p. 15). Yet a digital trace may change, diminish or vanish between the act and its collection, and since volatile data cannot be recovered once the system is powered down, a trace cannot be assumed to have survived to the moment of intervention (Başlar, 2020, pp. 86–88).

In the physical world, leaving traces is not a choice but a consequence of matter being subject to the laws of physics. An offender cannot choose to leave none; he can only try to reduce them, and the attempt generates a fresh trace, which is why the effort to destroy indicia is itself treated as an indicium (Yenisey & Nuhoğlu, 2021, p. 560). In the digital environment, whether the effort generates a trace depends on the layer at which and the tool with which it is carried out, and controlled experiments confirm that live operating system distributions run in read-only mode leave no trace on the physical storage medium (Zdzichowski et al., 2015, pp. 8–9, 36). Trace formation here is a product of software design, not of physical law, and since which event a system records, in what detail and for how long is a configuration choice, disabling the logging function is nothing out of the ordinary (Conlan et al., 2016, p. S72; Garfinkel, 2007, p. 78). What changes is not the method of looking for traces but the mechanism guaranteeing their existence: physical laws lie beyond the control of investigator and offender alike, whereas programs are open to the intervention of both (Değirmenci, 2014, pp. 25, 168; see also Caloyannides et al., 2009, p. 16). That data are ultimately physical states changes nothing, since configuration decides whether an event is written at all. Locard's principle therefore operates here not as a law of nature but at most as a configuration default. Cohen treats digital evidence as trace evidence (Cohen, 2013, pp. 131, 134). The view taken here is that the characterisation is functional: within the classification into documents, statements and indicia noted above, data offered for what they say act as documents, and system-generated records offered for what they reveal about an event act as traces, the only capacity in which destroyed data leave anything to prove.

2.4. Anti-Forensics: Concept, Classification and its Counterpart in Turkish Law

Anti-forensics is the body of techniques that systematically instrumentalise the non-necessity of trace generation, and the field's most striking feature is the absence of any agreed definition. Harris (2006) understood the concept as any attempt compromising the availability or usefulness of evidence, while Conlan, Baggili and Breitinger (2016, pp. S67–S68) found the common denominator of existing definitions to be an adverse effect on the existence, quantity and quality of evidence. This multiplicity is not legally trivial: while the boundary of the concept remains unsettled, so does the question when a behaviour counts as unlawful interference with evidence and when as a legitimate privacy measure (Kessler, 2007; González Arias et al., 2024, p. 25). Detecting deliberately concealed content is in any event accepted to be insoluble in general, meaning being a function of the intent in the offender's mind and not present in the traces (Cohen, 2013, p. 222).

The widely adopted fourfold taxonomy divides techniques into data hiding, artefact wiping, trail obfuscation, and attacks against forensic tools and processes (Kessler, 2007; Schneider et al., 2026, p. 3; Okoye et al., 2026, p. 2), which Conlan and others (2016, p. S71) extend by classifying three hundred and eight tools; like rival classifications (Harris, 2006; González Arias et al., 2024, pp. 6–7), it classifies destruction by tool, not by whether data cease to exist. Two headings deserve legal attention: activities generating very few traces or none form a distinct sub-category, data contraception, concerned not with the later deletion of a trace but with its never coming into existence; and anti-forensic tools or their installation files found on a system are listed as possible indicators of anti-forensic activity. A heading serving as an aid to detection in forensic science carries, once transposed into criminal procedure, the risk of becoming an indicium of guilt, since between a tool's installation and the destruction of particular data by it at a particular moment lies a wide evidentiary gap. A caveat

should be entered here, for the fact that certain techniques break forensic acquisition tools shows that an intervention occurred (Zdzichowski et al., 2015, pp. 3, 7, 9): the absence of a trace is not equivocal in every case. Data contraception as such falls outside the material element of Articles 243(3) and 244(2), which presuppose existing data; where achieved by disabling logging in another's system, however, the change to configuration data may itself constitute alteration under Article 244(2), whereas running a read-only system on one's own device is not typical. Its significance here is evidentiary.

The second decisive distinction lies in the approach of Peron and Legary (2005), whose classification adds to destroying, hiding and manipulating evidence the category of preventing evidence from arising, which Harris (2006) calls evidence source elimination. The fourth differs in kind: hidden or manipulated evidence can be assessed if found, whereas evidence whose creation was prevented never existed. The standards point the same way, ISO/IEC 27042 defining obfuscation as an effect that may be deliberate or accidental (Arts. 3.8 and 3.19), so that the field's own consensus treats the link between a trace's disappearance and the offender's act as an independent proposition requiring separate proof.

In the Turkish literature the concept appears as a technical obstacle facing the investigator; within the literature reviewed for this study, no work was encountered treating anti-forensics as a problem of typicity, attribution or culpability, or as an object of classification.

2.5. Studies in the Field

The literature falls into four clusters, and the subject of this study lies where they do not intersect. The first is substantive criminal law scholarship, which frames the distinction between the two provisions in terms of culpability without asking how it is to be operated at the level of proof (Aydın, 2022; Apiş, 2018; Akbulut, 2016; Karagöz, 2019; Alp, 2018; Mucuk, 2022; Sarı, 2013). The second is the Turkish criminal procedure and forensic computing literature, which requires data to be sealed by imaging, hashing and time-stamping, develops a right to reliable evidence and advocates amending Article 134 CMK (Öztürk et al., 2022, pp. 457, 582; Saydam, 2023; Değirmenci, 2014; Başlar, 2020; Özen & Özocak, 2015; Arslan, 2015; Sarsıkoğlu, 2025; Sarsıkoğlu & Ergün, 2025; Dinç, 2026); what goes unquestioned there is the metaphor of the seal itself, for a seal protects only what comes after it. The third is the general literature on the law of proof, which examines evidentiary prohibitions, the object of proof and inner conviction without addressing problems specific to digital evidence (Roxin, 2005; Başlar, 2022; Turinay, 2026). The fourth comprises the reliability debate and forensic computing's internal critique, in which the presumption of proper functioning is shown to be incompatible with software engineering (Ladkin et al., 2020), the law is shown not to distinguish hardware, software and data reliability (Christie, 2023), the treatment of digital evidence as inherently reliable is exposed as a fallacy (Ryser et al., 2020, p. 1) and the verification of trust assumptions one by one is proposed (Neale et al., 2022).

3. Method

3.1. Research Approach, Data Sources and Analysis

The study adopts a qualitative research approach, since making the tensions between normative texts visible requires those texts to be analysed systematically. Document analysis was conducted through two operations: doctrinal analysis directed at the coherence of the norms, and case-law analysis aimed at the norm's applicability and the form it takes in practice. The data were drawn from five groups of sources: legislation in force; case law; Turkish and foreign scholarship together with graduate theses; international conventions, Union legislation, institutional reports and official guidelines; and international technical standards (ISO/IEC 27037, 27041, 27042 and 27043). The case-law survey covers decisions of the relevant criminal chambers of the Court of Cassation and of its Criminal General Assembly, together with the constitutionality review and individual application decisions of the Constitutional Court, for 2010–2026.

3.2. Limitations

The study has five limitations. There are no official statistics on how often Article 243(3) TCK is applied or in how many files the result could be proved, a gap identified at international level as well (Council of Europe T-CY, 2017). Since there is no settled case law, the prospective part is an assessment of adequacy rather than a prediction, and the finding on adverse inference, which does not appear explicitly in published reasons, is advanced as a structural risk rather than an empirical generalisation and is expressed conditionally throughout. The ISO/IEC standards are not binding and are used not as a source of norms but as documents of technical consensus evidencing professional due care. Finally, the technical propositions relied on are not original: that digital evidence is trace evidence, that trace generation is a product of software design, and that some traces originate in autonomous processes are all established in the forensic computing literature (Cohen, 2013; Farmer & Venema, 2005; Carrier, 2005).

The claim to originality lies instead in transposing the descriptive categories of forensic computing into those of substantive criminal law and the law of proof at five points: pairing the distinction betwe-

en archaeological and geological traces with that between natural and artificial indicia and proposing it as a criterion of causal attribution that precedes the assessment of fault; comparing the missing-object problem with the case law on forgery of documents, making visible a question of coherence concerning the evidentiary value of secondary records; confining the act of destruction, on the ontological plane, by the criterion of system-relative irreversibility, the claim concerning not the invention of the criterion but the confinement of its frame of reference to the information system named in the norm; comparing the blind-spot interval with the duty of preservation for physical evidence, a comparison drawn before (Yenisey & Nuhoğlu, 2021, p. 459) but treated here as a structural mismatch arising from the temporal starting point of the safeguards rather than a procedural lacuna; and showing that the same structure is embedded in the international standardisation order.

4. Findings

4.1. Disentangling the Evidentiary Propositions

Before Articles 243(3) and 244(2) TCK can be applied, a court must separately resolve four independent propositions: that particular data were in the system at the moment of the act (existence); what those data were (content); that the object examined is the object seized (identity); and that the loss is attributable to the offender's act (attribution). Attribution denotes here the causal and objective link between act and loss, which any assessment of intent or negligence presupposes. The distinction has a counterpart in scholarship, which divides the facts requiring proof into principal facts, indicia and auxiliary facts, the last underpinning the reliability of evidence (Öztürk et al., 2022, pp. 365–367): identity belongs to the auxiliary class, existence and content to the first two. The propositions are graduated, content presupposing existence and attribution presupposing both. Digital evidence does not by itself place a person at a given time and place; it shows only whether particular sequences of events are consistent with the traces available (Cohen, 2013, p. 131).

Where the data are gone, proof proceeds through derivative records: system and event logs, metadata, file-system and registry remnants, backup records and service-provider records. None of them discloses the content of the destroyed data, and each requires a step of inference (Singh & Singh, 2018, § 4.1). The freedom of evidence does not cure this. Article 217 CMK provides that the judge may found the decision only on evidence brought before the hearing and discussed in his presence, which he assesses freely by inner conviction, and that the charge may be proved by any lawfully obtained evidence (Yenisey & Nuhoğlu, 2021, p. 528; Roxin, 2005, p. 273; Özcan, 2023, pp. 7, 11; Turinay, 2026, pp. 353–355); but freedom of evidence concerns the means of proof, not its object, and where the object has disappeared it generates no means of showing what is not there. A means of proof qualifies as evidence, moreover, only if it represents the event, is reliable, and is accessible and extant (Yenisey & Nuhoğlu, 2021, pp. 531 ff.; Gökcen & Çakır, 2019, pp. 2913–2915). Destroyed data fail the last requirement by definition; and the principle of immediacy, already diluted for digital evidence because contact is mediated by tools and experts (Gökcen & Çakır, 2019, pp. 2930–2931), cannot operate at all.

4.2. The Scope of the Evidence-Gathering Regime

Search, copying and seizure in information systems are governed by Article 134 CMK, which provides for backing up the data, delivering a copy of the backup to the person concerned on request, and documenting the operation; under Article 17 of the Regulation on Judicial and Preventive Searches, examination is conducted on a forensic copy whose identity with the original is shown by hash values. Scholars treat back-up at seizure as a requirement of fair proceedings and stress that the image must cover both allocated and unallocated space (Öztürk et al., 2022, pp. 582–583), and the Criminal General Assembly of the Court of Cassation has accepted that imaging in the presence of the person concerned dispels any suspicion that data were planted (Court of Cassation, Criminal General Assembly, 25 February 2020, Merits No. 2016/544, Decision No. 2020/127).

The reference point of every safeguard is the moment of seizure or copying, so the system's starting point is the intervention, not the act. The hash value seals the state of affairs at that moment and yields no proposition about any earlier one; in the case law, too, the review of unlawfulness is built on imaging and hashing, that is, on integrity alone (Court of Cassation, 8th Criminal Chamber, 24 October 2013, Merits No. 2012/21817, Decision No. 2013/25428). The regime largely satisfies identity; even performed flawlessly, it leaves existence, content and attribution beyond its reach.

4.3. Annulment of the Statutory Basis and the Legislative Response

The Constitutional Court's annulment of Article 134 CMK deferred to 25 February 2027, rests not on legality, which the Court found satisfied, but on the disproportionality of the restriction imposed on the rights to respect for private life and to request the protection of personal data (Constitution, Arts. 13 and 20; Constitutional Court, 12 February 2026, Decision No. 2026/36). It creates a legislative timetable for the proposals below, and since its reasoning

turns on the absence of statutory safeguards for the retention and destruction of seized data, it points in the same direction as the findings here. The legislature's handling is nevertheless discouraging: a provision requiring the destruction of data obtained after a defined period appeared in the bill that became Law No. 7589, was removed at the plenary stage, and the law entered into force with that omission (Law No. 7589, Official Gazette 31 July 2026, No. 33326; Minutes of the Plenary of the Grand National Assembly, 16 July 2026). This confirms that the generation and retention of digital traces is not yet a matter of disciplined legal policy.

4.4. Cross-Border Access Regimes

The Budapest Convention and its Second Additional Protocol, the EU e-Evidence Regulation and the United States CLOUD Act all concern access to data already stored with a service provider (Daskal, 2018, pp. 221–225; Rojszczak, 2021); none compels production of data that no longer exist, since such orders function only where directed at an existing object (Internet & Jurisdiction Policy Network, 2021, pp. 4, 17), so the gap is ontological, not merely domestic.

4.5. Anti-Forensics in the Case Law

In the published higher-court decisions reviewed, no use of the terms anti-forensics or countermeasures as a legal category was found, although the phenomenon itself appears as data not being found, records not having been kept or examination not being possible. The finding is negative and does not extend to unpublished decisions; what it shows is that a trace's absence is treated as a problem of proof rather than a distinct problem of typicity and attribution.

5. Discussion

5.1. The First Manifestation: Typicity and the Missing-Object Problem

The mismatch found in Section 4.2 has its source in the structure of the offence type, for in the typical case the object of the offence and its evidence are separate things, whereas in the offences of destroying and altering data the object protected and the object that would show its violation are identical. The paradox arises when this meets the criterion proposed above: once the line between destruction and rendering inaccessible is drawn by system-relative irreversibility, the feature warranting the graver characterisation and the feature making it impossible to prove are one and the same, so that once the threshold is crossed the act attracts the graver characterisation, and the more sophisticated the anti-forensic technique employed, the fewer derivative traces survive to prove it. Nor does this depend on the choice between criteria: even where destruction is complete regardless of recoverability, the need to determine which data were destroyed remains, and only the centre of gravity shifts, from recoverability to content.

Anti-anti-forensic methods, which identify a deletion and even the tool used from change journals and deletion patterns, weaken the categorical claim that data destruction leaves no trace (Garfinkel, 2007, p. 78; Lees, 2013; Oh et al., 2020; Lee et al., 2023); yet a trace's existence varies with the tool, file system or version, and such analyses confirm only that a deletion occurred. The paradox is thus scale-dependent, its normative weight falling at the level of content.

That weight becomes visible once one asks how the same structural problem is resolved elsewhere in Turkish criminal law. In forgery of documents the object protected and the evidentiary object are likewise identical, and because the capacity to deceive is a constitutive element whose assessment requires examination of the document itself, both scholarship and the Court of Cassation conclude that where the original cannot be obtained, deceptiveness cannot be reviewed and typicity is not made out. This is a line of case law rather than a single decision, one being cited by way of illustration (Court of Cassation, 21st Criminal Chamber, 24 December 2015, Merits No. 2015/2901, Decision No. 2015/6657). Without the object the element cannot be reviewed, and failure of proof operates in the accused's favour. The comparison is confined to the evidentiary value of secondary records where the original is absent, not to the material elements of the two offences. In forgery the loss of the original is usually incidental, whereas in data destruction it is the act charged; yet the reliability of a copy as proof of the original's content does not depend on who caused the loss. The two bodies of case law therefore raise a question of coherence: in forgery the unavailability of the original leads to acquittal even where photocopies exist, whereas in data destruction the same gap may be filled with derivative records and presumptions. Lowering the standard of proof because loss is ordinary in digital environments would be reasoning in reverse, and the rule that no conviction may rest on secondary records alone where the original is missing should be carried over. That the rule may leave the most complete destruction unproved is not an objection to it but the paradox itself, which Section 5.4 locates upstream, in trace generation.

5.2. The Second Manifestation: Attribution and the Types of Trace

Since Article 243(3) TCK creates an offence aggravated by its result, liability for that result requires, under Article 23 TCK, culpability at least at the level of negligence (Aydın, 2022, pp. 92–93; Koca & Üzülmez, 2021, pp. 242–244). Foreseeability under Artic-

le 22 concerns the type of result and the essential course of events, not the precise causal mechanism; the prior question, however, is whether the loss is causally attributable to the act at all, and fault can be debated only once that is proved. Farmer and Venema (2005, pp. 12–13) divide traces into archaeological traces, the direct result of user action, and geological traces, the result of the system's autonomous processes. Though developed as a technical description, the distinction can serve as a criterion of causal attribution once geological processes are divided in two. A trace eliminated directly by the offender's act is attributable to him. Where the act triggers an autonomous process that eliminates it, attribution remains possible and the ordinary assessment of intent, dolus eventualis or negligence follows. Where the process would have operated independently of the act, as with scheduled log rotation or retention policies, the loss does not realise the risk created by the access and cannot be attributed to it.

What makes the distinction hard to apply is that geological processes are the rule rather than the exception. TRIM and wear-levelling on solid-state drives clear blocks regarded as deleted without user intervention, and log rotation, backup retention periods and automated cloud lifecycle rules have the same effect (Carrier, 2005, pp. 132–133, 138–139; Farmer & Venema, 2005, pp. 13–14; Ryser et al., 2020, p. 1); the automatic purging of Prefetch records beyond a threshold ties a trace's lifespan to a configuration rule rather than the user's will (Singh & Singh, 2018, § 5). Attribution theory records the same difficulty, since the most an examiner can usually say is that there is no inconsistency indicating tampering (Cohen, 2013, pp. 365–366, 370). Hence the difficulty: distinguishing a triggered from an independent process requires reconstructing the sequence of events, and that requires examining the trace. Yet the trace is precisely what is missing, its absence carrying away the cause of that absence. Where the two cannot be told apart, the causal link on which liability under Article 243(3) depends remains unproved, and the doubt must operate in the accused's favour.

An extension appears in the law of concurrence. Article 281(1) TCK exempts from punishment an offender who destroys evidence of his own offence, reflecting the rationale of nemo tenetur, whereas Article 244(2) protects the integrity of data in another's information system; the difference in punishability follows from the different legal interests protected and is not in itself inconsistent, since destroying evidence embodied in another's property attracts liability for damage to property in the physical world as well. Its structural effect is nonetheless specific to the digital environment: because the traces of unlawful access are typically held in the victim's system, erasing them almost invariably satisfies Article 244(2), so the privilege of Article 281(1) is in practice unavailable to such offenders and the concealing act is punished more severely than the access itself. A recent study establishes concurrence separately for Articles 243, 245/A, 151 and 267–271 without discussing Article 281 (Akkaş & Doğruoğlu, 2025, pp. 208–209), and practice has met the problem only implicitly (Court of Cassation, 5th Criminal Chamber, 3 July 2014, Merits No. 2014/6872, Decision No. 2014/7366; 12 June 2014, Merits No. 2014/4793, Decision No. 2014/6553).

5.3. The Third Manifestation: The Presumption of Innocence and Adverse Inference

Where no trace is found and the cause of its absence cannot be determined, the proceedings may go one of two ways: the failure of proof is resolved in the accused's favour, or the absence is itself converted into an indicium. The second path rests on an inferential scheme by which the absence of logs, or the presence of cleaning tools, indicates a careful act of destruction. The scheme thereby converts a fact listed in the anti-forensic taxonomy as an aid to detection into an indicium of guilt.

Its first weakness is that it treats an unanswered proposition as answered. Moving from the absence of a trace to the act of destruction requires independent proof that the data said to have been destroyed were present at the moment of the act; yet the inference is deployed precisely where that cannot be proved, so their former existence is inferred backwards from their absence. Existence and attribution are thus derived from one and the same fact, and the reasoning generates its own premise from its own conclusion. The scheme also runs against the assumption adopted for scaling evidentiary value, since the scale transposed into the Turkish literature from Casey's places the case in which the image contains no trace whatever of the content alleged at the lowest level of confidence (Casey, 2011, p. 70; Çalışkan, 2013, pp. 117–118; Afandak, 2021, pp. 73–74): on the field's own scale the total absence of a trace is the zero point of evidentiary value, and the scheme places it at the top.

Structurally, although there is no burden of proof in the technical sense in criminal procedure (Yenisey & Nuhoğlu, 2021, p. 530), the accused would be left having to explain why no trace exists of an act he did not commit. Scholarship recognises shifts of the burden (Yenisey & Nuhoğlu, 2021, p. 531), but the criterion legitimating one, that the knowledge capable of explaining the event is concentrated in a single actor, is not met here. It is expressly accepted that an accused's inability to prove a defence cannot be used as an indicium of guilt (Yenisey & Nuhoğlu, 2021, p. 562) and that traces acquire meaning only when supported by other evidence (Öztürk et al., 2022, p. 404); if even an existing trace will not alone found a judgment, drawing a conclusion from one

that does not exist is a fortiori unacceptable. The inference also engages Article 6(2) of the Convention. Although the Court has not addressed trace-absence inference as such, the structural analogy is close. The inference functions as a presumption of fact, and such presumptions must be confined within reasonable limits that take account of what is at stake and maintain the rights of the defence (ECtHR, Salabiaku v. France, 7 October 1988, App. No. 10519/83, § 28). Its final step requires the accused to explain an absence, and a conviction founded on the failure to explain, in place of a prima facie case, breaches the presumption of innocence (ECtHR, Telfner v. Austria, 20 March 2001, App. No. 33501/96, §§ 15, 18); adverse inferences from silence are admissible only where the prosecution case already calls for an explanation (ECtHR, John Murray v. the United Kingdom [GC], 8 February 1996, App. No. 18731/91, §§ 47, 51, 54). Where drawn, the inference would thus operate where the prosecution case is weakest. Closest of all, the Court has held incompatible with Article 7 a practice attaching liability almost automatically to a technical indicator without individually establishing the mental element (ECtHR, Yüksel Yalçınkaya v. Türkiye [GC], 26 September 2023, §§ 264-266); inferring intent from a trace's absence shares that structure.

The same Court treats keeping the reliability of digital evidence open to challenge as a requirement of the right to a fair trial, and regards equality of arms as impaired where raw data are withheld and the source of the evidence cannot be tested (ECtHR, *Yüksel Yalçınkaya v. Türkiye* [GC], 26 September 2023, §§ 334–335; ECtHR, *Sigurður Einarsson and Others v. Iceland*, 4 June 2019, §§ 90–93); such review presupposes an object to be tested. In forensic computing theory, by contrast, the absence of traces that ought ordinarily to be present is treated as consistent with the event not having occurred (Cohen, 2013, pp. 317, 417). Converting a trace's absence into an indicium of guilt would also exert de facto pressure to produce on the accused, the only person able to explain the situation; such pressure would arise not from the statute but from evidentiary practice, and would erode the principle that a person must not be made the sole instrument of his own conviction.

The paradox deepens where in dubio pro reo would be inverted at the point of greatest doubt. Contrary to the prevailing view that the digitalisation of criminal procedure does not impair that principle (Öztürk et al., 2022, p. 129), it is exposed to impairment in the limited class of offences in which the act itself eliminates the object of proof. Two objections must be met. The first is that doubt must rest on the evidence in the file rather than an abstract hypothesis (Yenisey & Nuhoğlu, 2021, p. 527); that is sound as a general rule, but an independent geological process is not a hypothesis, but the documented configuration default of the system. The second is that intent is ordinarily inferred from facts manifested in the external world. This is untenable on three grounds: an inference from positive conduct is not equivalent to one from an absence; alternatives such as autonomous processes and third-party intervention cannot be eliminated; and the distance between a program's presence on a system and the destruction of specific data at a specific moment precludes founding a conviction on such inferences. Nor does encryption turn characterisation into a premium for surrendering the key, since Turkish secondary legislation already treats irreversible encryption as destruction (Personal Data Protection Authority, 2025, pp. 22–23).

The field's own standards address the methodological weakness. ISO/IEC 27042 requires facts found to be separated from information inferred, the supporting facts to be verified, the chain of inference to be reproducible, and competing interpretations to be presented with probability values (Arts. 5.5, 8.2 and 8.3), while ISO/IEC 27043 requires that, where no clear conclusion is possible, the report state its assumptions and hypothetical character (Art. 10.5). The scheme departs from all three: the supporting existence proposition is unverified, alternative explanations are not eliminated, and maximum certainty is attributed to the inference where the evidence is thinnest.

The debate over the presumption of proper functioning confirms that the problem is structural rather than technical. The presumption that computers operate correctly has been criticised as incompatible with software engineering (Ladkin et al., 2020, p. 5), its consequences emerging when hundreds of post office officials were convicted on faulty software data (Marshall, 2020; Christie, 2020, 2023), and the standards confirm that all tools carry an error rate (ISO/IEC 27041, 2015, Arts. 5.6.3, 5.7.2). The scheme examined here builds the same presumption in reverse: there the system is assumed to have functioned correctly, here to have kept records, and in both an unverified technical assumption grounds the judgment.

5.4. The Blind-Spot Interval and the Absence of a Neutral Guarantor

The common root of the three manifestations is that the safeguards begin at the moment of intervention rather than the moment of the act. The period between the act and the beginning of seizure or copying is termed here the blind-spot interval, and what distinguishes it is not that it is legally undefined but that no safeguard whatever is provided for it: hash values, time stamps and the chain of custody cover only what follows their own starting points, although scholarship lists them together as the guarantee of the lawfulness of evidence (Öztürk et al., 2022, p. 461). The loss of volatile data at power-down (Başlar, 2020, pp. 87–88; Caloyannides et al., 2009, p. 16) forms the material basis of the interval, identified within the field as the failure to verify the

assumptions of trust on which an investigation rests (Neale et al., 2022).

That the interval is not wholly foreign to the legal order becomes apparent on comparison with the regime for physical evidence, where the duty of preservation begins from the moment the offence begins to be committed and safeguards run from protection of the scene to sealing. That the same instruments list traces, marks and indications as items distinct from evidence shows that Turkish law protects a physical trace before it becomes evidence, whereas in the digital domain protection attaches only to what follows the intervention (Regulation on Judicial and Preventive Searches, Art. 4; PAGY, Arts. 5, 13–18; Gökcen & Çakır, 2019, pp. 2920–2923). Scholarship defines the principal duty of the judicial police as preventing indicia from changing and notes the need for similar rules for the seizure of computers (Yenisey & Nuhoğlu, 2021, pp. 459, 561). Tying the starting point of safeguards to the moment of the act is therefore not foreign to Turkish law, yet no regime performing that function exists for the digital environment. It may be objected that in homicide without a body or in arson the act also consumes its evidence, yet circumstantial proof suffices. That proof rests on three premises: the prior existence of the victim or object is established independently of the act; its disappearance departs from the ordinary course of events; and the circumstantial facts arise through processes no party controls. In data destruction, prior existence is often provable only through the system destroyed, disappearance is the ordinary product of autonomous processes, and derivative records depend on configuration, so whether a trace was ever formed is independent of when the police arrive. The doctrine's method of excluding alternative hypotheses can be carried over, as the third and fourth proposals below do; its premises cannot. Anti-forensics prevents traces from forming by the offender's will; the blind-spot interval, by the legal order's own omission, makes it impossible to verify whether they formed at all.

That the gap is not merely a domestic shortcoming is clear from the international standardisation order. ISO/IEC 27043 runs the chain of custody from the moment the incident is detected (Arts. 11.5 and 11.6), treats pre-incident readiness as optional and within the organisation's discretion (Art. 7.1), and records that practitioners cannot guarantee such preparation on every system (Art. 8.2), while ISO/IEC 27042 applies only to the investigative process class (Art. 6.2). That safeguards begin at the intervention is thus a structural feature of the field's international design, anti-forensic threat modelling likewise entering only with the forensic process (Hoelz & Maues, 2017, p. 169; González Arias et al., 2024, p. 7), and the only regime covering the earlier period is left, voluntarily, to one of the potential parties, the organisation operating the system. Standardisation therefore does not close the neutral-guarantor gap but converts it into an assumption, independence being recognised at the level of method validation (ISO/IEC 27041, 2015, Art. 7.2) and not of trace generation.

The control constituting the evidentiary guarantor position is distributed among three actors: the offender can prevent a trace from arising; the system operator generates or withholds traces according to his own purposes; the investigating authority fixes the moment at which safeguards begin. Widen the perspective and much of that control rests with actors beyond the parties' reach altogether, since cloud providers, operating system designers and hardware suppliers determine which events are recorded and for how long. Narrowly viewed, the absence of a neutral guarantor produces a problem of proof; widely viewed, a problem of authority, which this study does no more than name.

The normative consequence is that the solution lies neither in prohibiting adverse inference outright nor in leaving it unregulated, but in transferring trace generation to a neutral guarantor. The extremes appear opposed yet produce the same outcome: under prohibition, the offender who eliminates traces most completely becomes the most protected; under free rein, an accused for whom no records were ever kept must explain why no trace exists of an act he did not commit. At both, technical competence becomes the measure of criminal liability. The third path is to remove the existence of traces from the control of offender and investigating authority alike and tie it to a predetermined, auditable and unalterable recording regime.

5.5. Legal Policy Proposals

Four proposals are advanced to close the gap, connected directly to the legislative work that must be completed before the annulment of Article 134 CMK takes effect.

The first is to extend the temporal scope of the safeguards to the period between the act and the intervention; otherwise the seal will continue to operate as though it protected a period it does not. Since the duty of preservation already runs from the moment of the act for physical evidence, this asks not for a new logic of safeguards but for the existing one to be carried into the digital environment, and it can proceed incrementally: under Article 134 CMK the record could state whether any logging existed for the period preceding seizure; assessment of logging adequacy could become a mandatory heading of examination for the judicial police and court-appointed experts; and immutable logging with independent time-stamping, already implemented at storage level (Soriano-Salvador & Guardiola-Múzquiz, 2021), could be prescribed for defined categories of data.

The second is that a minimum logging standard be laid down by statute for critical systems. The obligation is not foreign to Turkish law, since Law No. 5651 already requires hosting and access providers to retain traffic data and ensure its accuracy and integrity; the shortcoming lies in its confinement to communications traffic rather than changes to data within a system. Unless which events are recorded, in what detail and for what minimum period ceases to be a configuration choice, the contingency of trace generation will remain beyond legal scrutiny. The technical content is not new either, such logging being listed among pre-incident data-gathering processes in the standard (ISO/IEC 27043, 2015, Art. 7.9). Because logs contain personal data, the obligation must be reconciled with data minimisation and storage limitation under Article 4(2) of Law No. 6698 (KVKK). Four conditions would secure that: a statutory basis within Article 5(2); confinement to integrity events, recording which object was altered or erased, when and by which account, rather than content; purpose limitation with access control; and a retention period fixed by statute, as Article 4(2)(d) contemplates. Logging so designed is itself a data-protection safeguard, as Article 25 of Directive (EU) 2016/680 shows, and its natural vehicle would be secondary legislation implementing Law No. 7545 on Cybersecurity (Art. 7).

The third is to discipline, as a matter of interpretative method, the inference drawn from a trace's absence, conditioning its validity on the elimination by expert examination of alternative explanations, in particular autonomous system processes and third-party intervention, so that absence does not by itself count as an indicium of intent. This asks that the standard already requiring facts to be separated from inferences and competing interpretations to be reported with probability values (ISO/IEC 27042, 2015, Arts. 8.2 and 8.3) be made binding for criminal procedure. It also has a basis in existing law: since the public prosecutor must investigate exculpatory evidence (Art. 160(2) CMK; Yenisey & Nuhoğlu, 2021, p. 530), asking whether an absence originates in an independent geological process is the digital counterpart of an existing duty, so the proposal calls for a standard of practice before legislative amendment.

The fourth is to make the distinction between archaeological, triggered geological and independent geological traces a mandatory heading in expert reports, so that the report categorises the probable cause of a trace's absence rather than merely recording it. Its basis in scholarship is that indicia acquire meaning only through expert examination (Yenisey & Nuhoğlu, 2021, p. 562), and in the standards the requirement that reports state the limits of the analysis and any incomplete data sets (ISO/IEC 27042, 2015, Art. 9.2; Bollé et al., 2020, pp. 6, 12).

The obvious alternative on the criminal law alternative, extending Article 245/A TCK to possession of anti-forensic tools, appears closed for four reasons. The requirement that the device be designed exclusively for committing offences turns dual use into a condition of typicity, which overwriting, encryption and read-only distributions do not satisfy (Conlan et al., 2016, pp. S67–S68). More decisively, since secondary legislation describes lawful destruction by reference to these very tools (Personal Data Protection Authority, 2025), a data controller applying the required method would become liable for possessing a prohibited program. The extension would also punish at the preparatory stage conduct whose completion Article 281(1) leaves unpunished under nemo tenetur, where the tools eliminate evidence of the possessor's own offence; and relaxing exclusivity would produce a typicity unreviewable under legality, the Convention likewise protecting authorised uses (Council of Europe, 2001). The solution lies only in a positive recording obligation.

6. Conclusion

This study has concluded that the evidentiary problem arising where data are lost or destroyed following unlawful access to an information system stems not from an isolated failure of application but from a difference in scope between the system of safeguards and the propositions requiring proof: the existing system largely satisfies identity, while existence, content and attribution fall outside it. The central claim is that the difficulties this difference produces at the levels of typicity, attribution and the presumption of innocence are three manifestations of a single structural problem rather than separate defects. At the level of typicity, the feature warranting the graver characterisation is the same feature that makes proof impossible, and comparison with the case law on forgery of documents raises a question of coherence concerning the evidentiary value of secondary records. At the level of attribution, the causal link requires distinguishing triggered from independent autonomous processes, while a trace's absence carries away with it the cause of that absence; in the law of concurrence, the privilege of Article 281(1) proves structurally unavailable to such offenders. At the level of the presumption of innocence, the gap is exposed to being filled by treating that absence as an indicium of intent, which would subject the accused to de facto pressure to produce. The three are not independent: the second arises in the gap left by the first, the third in the way the first two are filled.

Their common root is the absence of any evidentiary guarantor of trace generation independent of the parties; in the physical world generation is exogenous and preservation with the act; in the digital environment control is distributed among the offender, system operator and the investigating authority, and safeguards operate only from the intervention. The solution lies in transferring trace generation to

a neutral guarantor and disciplining inferences, for which the Constitutional Court's annulment opens a legislative window. Three questions remain: whether, under system-relative irreversibility, recoverability is determined at the moment of the act, of examination or of judgment; the liability gap arising from the transfer of guarantorship to cloud providers and operating system and hardware manufacturers; and the reconciliation of statutory logging with privacy law.

Ethics Statement

This study is based on document analysis and involves no human or animal participants; it therefore requires no ethics committee approval.

Conflict of Interest Statement

The author declares that there is no conflict of interest.

Funding Statement

The study received no financial support from any institution or organisation.

Artificial Intelligence Use Statemen

During the preparation of the final version of this article, Claude AI was used for language and style refinement, formatting the text to align with the journal's guidelines, and language checking of translated content.

References

Afandak, K. (2021). Ceza muhakemesinde dijital deliller [Doctoral dissertation]. Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Akbulut, B. (2016). Sistemi engelleme, bozma, verileri yok etme veya değiştirme. Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 24(2), 7–55. https://doi.org/10.15337/SUH.2017.0

Akkaş, A. H., & Doğruoğlu, M. Ş. (2025). Türk Ceza Kanunu'nda düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları (TCK m. 244/1-2). Erciyes Üniversitesi Hukuk Fakültesi Dergisi, 20(1), 185–216. https://doi.org/10.58820/eruhfd.1683052

Alp, B. E. (2018). 5237 sayılı Türk Ceza Kanununda bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçu [Master's thesis]. Çankaya Üniversitesi Sosyal Bilimler Enstitüsü.

Apiş, Ö. (2018). Bilişim sistemine girme suçu bakımından bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama, elkoyma koruma tedbiri. Yasama Dergisi, 37, 49–86.

Arslan, Ç. (2015). Dijital delil ve iletişimin denetlenmesi. Ceza Hukuku ve Kriminoloji Dergisi, 3(2), 253–266.

Aydın, A. A. (2022). Türk ceza hukukunda bilişim sistemine girme suçu [Master's thesis]. Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü.

Başlar, Y. (2020). Elektronik delilin toplanması ve muhafazası. Hacettepe Hukuk Fakültesi Dergisi, 10(1), 77–107. https://doi.org/10.32957/hacettepehdf.690592

Başlar, Y. (2022). Ceza muhakemesinde ispat. Hacettepe Hukuk Fakültesi Dergisi, 12(2), 1383–1399. https://doi.org/10.32957/hacettepehdf.1106041

Bollé, T., Casey, E., & Jacquet, M. (2020). The role of evaluations in reaching decisions using automated systems supporting forensic analysis. Forensic Science International: Digital Investigation, 34, 301016. https://doi.org/10.1016/j.fsidi.2020.301016

Çalışkan, E. (2013). Zararlı yazılımların etkisinde dijital adli delillerin güvenilirliği [Master's thesis]. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü.

Caloyannides, M. A., Memon, N., & Venema, W. (2009). Digital forensics. IEEE Security & Privacy, 7(2), 16–17.

Carrier, B. (2005). File system forensic analysis. Addison-Wesley.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

Christie, J. (2020). The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence. Digital Evidence and Electronic Signature Law Review, 17, 49–70. https://doi.org/10.14296/deeslr.v17i0.5226

Christie, J. (2023). The Law Commission and section 69 of the Police and Criminal Evidence Act 1984. Digital Evidence and Electronic Signature Law Review, 20, 62–95. https://doi.org/10.14296/deeslr.v20i.5642

Cohen, F. (2013). Digital forensic evidence examination (5th ed.). Fred Cohen & Associates.

Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation, 18(Supp.), S66–S75. https://doi.org/10.1016/j.diin.2016.04.006

Constitutional Court, 12 February 2026, Merits No. 2023/128, Decision No. 2026/36 (Official Gazette, 25 May 2026, No. 33264).

Constitutional Court, [Grand Chamber], 9 January 2015, App. No. 2014/253 (Yankı Bağcıoğlu and Others).

Council of Europe T-CY. (2017). Implementation of Article 13 Budapest Convention by Parties and Observers: Assessment report (T-CY(2016)25). https://rm.coe.int/t-cy-2015-18-implementation-of-article-13-budapest-convention-by-parti/1680724ca4

Council of Europe. (2001). Explanatory report to the Convention on Cybercrime (ETS No. 185). https://rm.coe.int/16800cce5b

Court of Cassation, 21st Criminal Chamber, 24 December 2015, Merits No. 2015/2901, Decision No. 2015/6657.

Court of Cassation, 5th Criminal Chamber, 12 June 2014, Merits No. 2014/4793, Decision No. 2014/6553.

Court of Cassation, 5th Criminal Chamber, 3 July 2014, Merits No. 2014/6872, Decision No. 2014/7366.

Court of Cassation, 8th Criminal Chamber, 24 October 2013, Merits No. 2012/21817, Decision No. 2013/25428.

Court of Cassation, Criminal General Assembly, 25 February 2020, Merits No. 2016/544, Decision No. 2020/127.

Daskal, J. (2018). Unpacking the CLOUD Act. eucrim, 13/4, 220–225. https://doi.org/10.30709/eucrim-2018-022

Değirmenci, O. (2014). Ceza muhakemesinde sayısal (dijital) delil. Seçkin Yayıncılık.

Dinç, A. (2026). Ceza muhakemesinde dijital delillerin özel hayatın gizliliği kapsamında değerlendirilmesi [Doctoral dissertation]. Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü.

Dülger, M. V. (2020). Bilişim suçları ve internet iletişim hukuku (8th ed.). Seçkin Yayıncılık.

ECtHR, Grand Chamber, 8 February 1996, App. No. 18731/91 (John Murray v. the United Kingdom).

ECtHR, Chamber, 7 October 1988, App. No. 10519/83 (Salabiaku v. France).

ECtHR, Chamber, 4 June 2019, App. No. 39757/15 (Sigurður Einarsson and Others v. Iceland).

ECtHR, Chamber, 20 March 2001, App. No. 33501/96 (Telfner v. Austria).

ECtHR, Grand Chamber, 26 September 2023, App. No. 15669/20 (Yüksel Yalçınkaya v. Türkiye).

Ramos, J. Á. E. (2025). European preservation and production orders: a non-exclusive approach to E-Evidence within the EU: implications of the union legislator's choice to derogate from the precedence of union law in the E-Evidence regulation. Eucrim: the European Criminal Law Associations' fórum, (3), 216-220. https://doi.org/10.30709/eucrim-2025-018

Farmer, D., & Venema, W. (2005). Forensic discovery. Addison-Wesley Professional.

Garfinkel, S. (2007). Anti-forensics: Techniques, detection and countermeasures. 2nd International Conference on i-Warfare and Security (ICIW 2007), 77–84.

Gökcen, A., & Çakır, K. (2019). Ceza muhakemesinde delil, delillerin muhafazası, toplanması, değerlendirilmesi ve delil yasakları. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş Tezcan'a Armağan, 21(Special Issue), 2911–2951.

González Arias, R., Bermejo Higuera, J., Rainer Granados, J. J., Bermejo Higuera, J. R., & Sicilia Montalvo, J. A. (2024). Systematic review: Anti-forensic computer techniques. Applied Sciences, 14(12), 5302. https://doi.org/10.3390/app14125302

Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. Digital Investigation, 3(Supp.), 44–49. https://doi.org/10.1016/j.diin.2006.06.005

Hoelz, B., & Maues, M. (2017). Anti-forensic threat modeling. In G. Peterson & S. Shenoi (Eds.), Advances in digital forensics XIII (pp. 169–183). Springer. https://doi.org/10.1007/978-3-319-67208-3_10

Internet & Jurisdiction Policy Network. (2021). Cross-border access to electronic evidence: Toolkit (Ref. 21-103).

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

ISO/IEC 27041. (2015). Guidance on assuring suitability and adequacy of incident investigative method (ISO/IEC 27041:2015). ISO.

ISO/IEC 27042. (2015). Guidelines for the analysis and interpretation of digital evidence (ISO/IEC 27042:2015). ISO.

ISO/IEC 27043. (2015). Incident investigation principles and processes (ISO/IEC 27043:2015). ISO.

Karagöz, M. C. (2019). Bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçu (TCK m. 244) [Master's thesis]. Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü.

Kessler, G. C. (2007). Anti-forensics and the digital investigator. Proceedings of the 5th Australian Digital Forensics Conference, 1–7.

Koca, M., & Üzülmez, İ. (2020). Türk ceza hukuku özel hükümler (7th ed.). Adalet Yayınevi.

Koca, M., & Üzülmez, İ. (2021). Türk ceza hukuku genel hükümler (14th ed.). Seçkin Yayıncılık.

Kurt, L. (2005). Açıklamalı-içtihatlı tüm yönleriyle bilişim suçları ve Türk Ceza Kanunu'ndaki uygulaması. Seçkin Yayıncılık.

Ladkin, P. B., Littlewood, B., Thimbleby, H., & Thomas, M. (2020). The Law Commission presumption concerning the dependability of computer evidence. Digital Evidence and Electronic Signature Law Review, 17, 1–14. https://doi.org/10.14296/deeslr.v17i0.5143

Lee, E. J., Lee, S. Y., Kwon, H., Lee, S. J., & Kim, G. B. (2023). Identification of data wiping tools based on deletion patterns in ReFS $Logfile. Forensic Science International: Digital Investigation, 46, 301607. https://doi.org/10.1016/j.fsidi.2023.301607

Lees, C. (2013). Determining removal of forensic artefacts using the USN change journal. Digital Investigation, 10(4), 300–310. https://doi.org/10.1016/j.diin.2013.10.002

Marshall, P. (2020). The harm that judges do - Misunderstanding computer evidence: Mr Castleton's story 'an affront to the public conscience'. Digital Evidence and Electronic Signature Law Review, 17, 25–48. https://doi.org/10.14296/deeslr.v17i0.5172

Mucuk, M. H. (2022). Bilişim sistemine girme (TCK 243) ve sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK 244) suçları [Master's thesis]. Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Neale, C., Kennedy, I., Price, B., Yu, Y., & Nuseibeh, B. (2022). The case for Zero Trust Digital Forensics. Forensic Science International: Digital Investigation, 40, 301352. https://doi.org/10.1016/j.fsidi.2022.301352

Oh, D. B., Park, K. H., & Kim, H. K. (2020). De-Wipimization: Detection of data wiping traces for investigating NTFS file system. Computers & Security, 99, 102034. https://doi.org/10.1016/j.cose.2020.102034

Okoye, U., Karim, R., Onik, A., & Baggili, I. (2026). SoK: Anti-forensics evolution, platform coverage, and mobile residual evidence. Forensic Science International: Digital Investigation, 57, 302127. https://doi.org/10.1016/j.fsidi.2026.302127

Özbek, V. Ö., Doğan, K., & Bacaksız, P. (2019). Türk ceza hukuku özel hükümler (14th ed.). Seçkin Yayıncılık.

Özcan, F. B. (2023). Elektronik delillerin ceza muhakemesi bakımından ispat değeri [Master's thesis]. Hasan Kalyoncu Üniversitesi Lisansüstü Eğitim Enstitüsü.

Özen, M., & Özocak, G. (2015). Adli bilişim, elektronik deliller ve bilgisayarlarda arama ve elkoyma tedbirinin hukuki rejimi (CMK m. 134). Ankara Barosu Dergisi, 2015(1), 41–77.

Öztürk, B., Tezcan, D., & Erdem, M. R. (Eds.). (2022). Dijital ceza muhakemesi hukuku (2nd ed.). Seçkin Yayıncılık.

Öztürk, C. (2006). Ceza muhakemesinde iz bilimi-kriminalistik gerçeği. Seçkin Yayıncılık.

Peron, C. S. J., & Legary, M. (2005). Digital anti-forensics: Emerging trends in data transformation techniques. E-Crime and Computer Evidence Conference (ECCE 2005), Monte Carlo, Monaco, 28–30 March 2005.

Personal Data Protection Authority. (2025). Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi rehberi (KVKK Publications No. 71). https://kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf

Rojszczak, M. (2021). CLOUD Act agreements from an EU perspective. Computer Law & Security Review, 41, 105548. https://doi.org/10.1016/j.clsr.2021.105548

Roxin, C. (2005). İspat hukukunun esasları (Y. Ünver, Trans.). İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 4(8), 265–289.

Ryser, É., Spichiger, H., & Casey, E. (2020). Structured decision making in investigations involving digital and multimedia evidence. Forensic Science International: Digital Investigation, 34, 301015. https://doi.org/10.1016/j.fsidi.2020.301015

Sarı, O. (2013). Uluslararası hukuk ve Türk ceza hukuku bağlamında siber güvenlik ve bilişim sistemine yönelik suçlar [Master's thesis]. Harp Akademileri Stratejik Araştırmalar Enstitüsü.

Sarsıkoğlu, Ş. (2015). Ceza muhakemesinde delil ve ispat hukuku açısından elektronik delil (e-delil) kavramı. Türkiye Adalet Akademisi Dergisi, 6(22), 427–454.

Sarsıkoğlu, Ş. (2025). Bilişim sistemlerinden delil elde edilmesine yönelik işlemler (CMK m. 134) hakkında bir değerlendirme. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 12(1), 283–317.

Sarsıkoğlu, Ş., & Ergün, K. K. (2025). Dijital çağda Türk ceza muhakemesi: Siber suçlar özelinde koruma tedbirlerinin genel teorisi. Hacettepe Hukuk Fakültesi Dergisi, 15(2), 576–618. https://doi.org/10.32957/hacettepehdf.1706831

Saydam, M. (2023). Ceza muhakemesinde belge delili. Adalet Yayınevi.

Schneider, J., Ramming, F., Eichhorn, M., Pugliese, G., Hargreaves, C., Gruber, J., Schilling, J., Geus, J., Mayer, K., Uhlenbrock, L., Voigt, L., & Breitinger, F. (2026). SoK: Understanding anti-forensics concepts and research practices across forensic subdomains. arXiv:2604.05770. https://doi.org/10.48550/arXiv.2604.05770

Singh, B., & Singh, U. (2018). Program execution analysis in Windows: A study of data sources, their format and comparison of forensic capability. Computers & Security, 74, 94–114. https://doi.org/10.1016/j.cose.2018.01.006

Sommer, P. (2013). Digital evidence, digital investigations and e-disclosure: A guide to forensic readiness for organisations, security advisers and lawyers (4th ed.). Information Assurance Advisory Council.

Soriano-Salvador, E., & Guardiola-Múzquiz, G. (2021). SealFS: Storage-based tamper-evident logging. Computers & Security, 108, 102325. https://doi.org/10.1016/j.cose.2021.102325

Stoykova, R., Nordvik, R., Ahmed, M., Franke, K., Axelsson, S., & Toolan, F. (2022). Legal and technical questions of file system reverse engineering. Computer Law & Security Review, 46, 105725. https://doi.org/10.1016/j.clsr.2022.105725

Tezcan, D., Erdem, M. R., & Önok, R. M. (2020). Teorik ve pratik ceza özel hukuku. Seçkin Yayıncılık.

Turinay, F. Y. (2026). Ceza muhakemesinde vicdani kanaat ve delillerin serbestçe takdiri sistemi üzerine bir inceleme. İstanbul Hukuk Mecmuası, 84(1), 326–363. https://doi.org/10.26650/mecmua.2026.84.1.0003

Yenisey, F., & Nuhoğlu, A. (2021). Ceza muhakemesi hukuku (9th updated ed.). Seçkin Yayıncılık.

Zdzichowski, P., Sadlon, M., Väisänen, T. U., Botas Munoz, A., & Filipczak, K. (2015). Anti-forensic study. NATO Cooperative Cyber Defence Centre of Excellence.