JOURNAL OF LAW, INFORMATION & SCIENCE
ISSN 0729-1485• Vol. 4, Issue 1 (2026) • https://jlisjournal.com/

REVIEW ARTICLE Article ID: JLIS/2026/4/1/003

Digital Evidence and Cybercrime Prosecution: Legal Challenges in the Age of Encrypted and Distributed Technologies

Dr. Rohan Malhotra [1], Dr. Elena Brooks [2], Prof. Arvind Kapoor[3]

[1] *Faculty of Law and Cybersecurity, National Institute of Legal Studies, New Delhi, India.*
[2] *School of Law and Digital Justice, University of London, United Kingdom.*
[3] *Department of Legal Technology and Cybercrime Studies, International University of Technology, Singapore*

Received: 18 Oct 2025 **Revised:** 28 Nov 2026 **Accepted:** 28 Jan 2025 **Published:** 11 Feb 2026

ABSTRACT

The rapid expansion of digital technologies has transformed both the nature of criminal activity and the methods through which criminal investigations are conducted. Cybercrime investigations increasingly depend upon digital evidence obtained from computers, smartphones, cloud platforms, encrypted communications, online services, and distributed networks. Although digital evidence can provide valuable information for identifying offenders and reconstructing criminal events, its increasing complexity creates significant legal challenges concerning authenticity, integrity, admissibility, privacy, jurisdiction, and chain of custody. Encryption and decentralized technologies may further complicate the ability of investigators to obtain and verify relevant information. This article examines the principal legal challenges associated with the collection, preservation, authentication, and presentation of digital evidence in cybercrime prosecutions. It argues that conventional evidentiary principles require appropriate adaptation to address technologically complex forms of evidence without compromising fundamental procedural safeguards. The article proposes a framework emphasizing forensic integrity, documented chain of custody, judicial scrutiny, proportionality, and reliable authentication mechanisms. It concludes that effective cybercrime prosecution requires a balanced legal approach that strengthens investigative capabilities while protecting privacy, due process, and fair-trial rights.

Keywords: *Digital evidence; Cybercrime; Electronic evidence; Chain of custody; Evidence admissibility; Encryption; Cyber law.*

1. Introduction

The digital transformation of society has fundamentally changed the nature of criminal activity. Traditional crimes increasingly involve digital components, while entirely new categories of offences have emerged through computer networks, online platforms, mobile applications, and other technological infrastructures. Cyber fraud, identity theft, ransomware, unauthorized access, online harassment, financial crimes, and data theft are examples of offences in which digital information may constitute an important source of evidence.

Digital evidence can take numerous forms, including emails, instant messages, metadata, computer logs, browser histories, location information, digital photographs, transaction

records, cloud-storage information, and data recovered from electronic devices. Unlike traditional physical evidence, digital evidence can be copied, modified, deleted, encrypted, transmitted across jurisdictions, or automatically altered through routine system operations.

These characteristics create important legal questions. How can a court determine whether a digital file is authentic? How can investigators demonstrate that evidence has not been altered? What procedures should be followed when evidence is collected from a device containing both relevant and highly personal information? How should courts evaluate evidence obtained from foreign servers or encrypted platforms?

The increasing dependence on digital evidence therefore requires a careful interaction between technology and law. Investigators need sufficient powers and technical capabilities to identify and preserve electronic evidence, while individuals must remain protected against unreasonable searches, privacy violations, unreliable evidence, and procedural unfairness.

This article examines the major legal challenges surrounding digital evidence in cybercrime prosecutions. It focuses particularly on authenticity, integrity, chain of custody, encryption, privacy, jurisdiction, and judicial evaluation of technologically generated evidence.

2. Concept and Nature of Digital Evidence

Digital evidence may be understood as information stored, transmitted, or generated in digital form that has potential relevance to a legal proceeding. It may originate from personal devices, enterprise systems, telecommunications networks, cloud platforms, financial institutions, social media services, or other digital environments.

One important characteristic of digital evidence is its intangible nature. A physical object can often be directly examined, whereas digital information exists through electronic representations stored on physical or virtual infrastructure.

Digital evidence can also be highly volatile. Information stored in temporary memory may disappear when a device is switched off. Network logs may be overwritten after a particular period, while cloud-service providers may maintain data under retention policies that vary according to jurisdiction and service.

Another important characteristic is replicability. Unlike many physical forms of evidence, digital information can be duplicated without necessarily changing its apparent content. However, this does not eliminate evidentiary concerns. Investigators must demonstrate that the copy presented before the court accurately represents the original evidence.

Consequently, legal systems require appropriate procedures for collection, preservation, verification, and presentation.

3. Authenticity of Digital Evidence

Authenticity is a fundamental requirement for evidentiary reliability. A court must be satisfied that the evidence presented is what the party claiming it to be.

In digital cases, authenticity may involve demonstrating the origin of a file, the identity of the device from which it was obtained, the account associated with the information, and the circumstances under which the data was collected.

For example, an electronic message may appear to originate from a particular account, but account credentials can be compromised or impersonated. Similarly, metadata may provide useful information but should not automatically be treated as conclusive proof of authorship.

Technical mechanisms such as cryptographic hash values can assist investigators in demonstrating that a forensic copy has remained unchanged after acquisition. However, technological verification should operate alongside proper procedural documentation.

Authentication should therefore be understood as a combined legal and technical process. Courts should evaluate not merely whether a digital record exists but also how it was obtained, preserved, attributed, and presented.

4. Integrity and Chain of Custody

The integrity of digital evidence is closely associated with the chain of custody. Chain of custody refers to the documented history of evidence from the moment it is collected until its presentation in court.

A reliable chain of custody should identify:

1. who collected the evidence;
2. when and where it was collected;
3. the method used for acquisition;
4. how the evidence was stored;
5. who subsequently accessed it;
6. whether forensic copies were created; and
7. whether any changes occurred during examination.

Weak documentation may create uncertainty regarding whether evidence was modified or improperly handled.

Digital forensic investigators commonly use specialized procedures to create forensic images and calculate cryptographic hash values. These mechanisms can provide technical evidence that the analyzed copy corresponds to the acquired data.

Nevertheless, technological tools cannot replace procedural discipline. A perfectly calculated hash value does not establish that the original evidence was lawfully obtained or correctly attributed. Thus, evidentiary integrity requires both technical safeguards and legally compliant procedures.

5. Encryption and Investigative Challenges

Encryption is an important component of modern cybersecurity because it protects information against unauthorized access. At the same time, strong encryption can create substantial challenges for criminal investigations.

Investigators may encounter encrypted smartphones, messaging applications, storage devices, or network communications. Even when authorities lawfully obtain a device, the relevant information may remain inaccessible without an appropriate key or authentication mechanism.

This creates a difficult legal balance. Investigative authorities may argue that access to encrypted information is necessary for preventing or prosecuting serious crimes. Conversely, weakening encryption mechanisms may expose millions of legitimate users to security risks.

The legal response should therefore avoid treating encryption itself as evidence of criminal conduct. Instead, investigative access should be governed by lawful authorization, proportionality, necessity, and appropriate judicial oversight.

Where compelled decryption or access to credentials is legally permitted, courts may need to consider constitutional protections, privilege, privacy, and the specific circumstances of the investigation.

6. Privacy and Digital Searches

Digital devices contain an extraordinary quantity of personal information. A single smartphone may contain photographs, financial records, private communications, medical information, location histories, employment information, and personal documents.

Consequently, digital searches can be significantly more intrusive than searches of many physical objects. An investigation targeting a particular offence may potentially expose information unrelated to the alleged crime.

This raises important questions concerning proportionality and scope. Investigative authorities should, where legally required, obtain appropriate authorization and limit searches to information reasonably connected with the investigation.

Courts should carefully examine whether evidence was collected through lawful procedures. The admissibility or evidentiary weight of improperly obtained digital evidence may depend on the applicable legal framework.

Privacy protection should not be viewed as an obstacle to cybercrime investigation. Rather, lawful and proportionate investigative procedures can strengthen the legitimacy and reliability of criminal justice processes.

7. Jurisdictional Problems

Cybercrime frequently crosses national borders. An offender may operate from one country, use infrastructure located in another, target victims in a third country, and store relevant evidence on cloud servers distributed across several jurisdictions.

This creates significant problems concerning investigative authority and access to evidence.

A domestic warrant or investigative authorization may not automatically provide authority to obtain information physically stored in another country. Investigators may therefore need to rely upon international cooperation mechanisms, mutual legal assistance procedures, cross-border agreements, or lawful requests to service providers.

Cloud computing further complicates the concept of physical location. Data may be dynamically distributed among multiple data centers, making it difficult to identify a single location associated with the evidence.

International cooperation and harmonization of procedural standards are therefore increasingly important for effective cybercrime enforcement.

8. Admissibility and Reliability

Admissibility determines whether evidence may be considered by a court, while reliability concerns the degree of confidence that should be placed in that evidence.

Digital evidence should not automatically receive greater evidentiary value merely because it appears technically sophisticated. Courts should consider the circumstances under which the evidence was created, collected, preserved, and attributed.

For automatically generated records, issues may include the reliability of the underlying system, accuracy of timestamps, integrity of databases, and reliability of the process through which the record was generated.

For user-generated content, courts may need to examine questions of authorship and account control. Screenshots, for example, may demonstrate that particular content existed but may not independently establish who created it or whether the displayed information was manipulated.

Judicial evaluation should therefore consider both technological reliability and the surrounding factual circumstances.

9. Artificial Intelligence and Digital Evidence

Artificial intelligence introduces a new dimension to digital evidence. AI systems may be used to analyze large quantities of seized data, identify patterns, classify files, detect suspicious activity, or assist investigators in prioritizing evidence.

While these capabilities may significantly improve investigative efficiency, reliance on AI-generated analysis creates additional legal questions.

If an AI system identifies a particular document or communication as relevant, investigators should be able to establish how that result was generated and how human investigators verified it.

AI-generated outputs should not automatically be treated as independent proof of criminal conduct. They may function as investigative tools that help identify potentially relevant evidence, but final legal conclusions should remain subject to appropriate human and judicial evaluation.

This distinction is important because statistical predictions can contain errors and may reflect limitations in the underlying datasets or models.

10. Challenges in Presenting Digital Evidence Before Courts

Digital evidence can be technically complex and difficult for judges, lawyers, and juries to understand. Specialized terminology relating to encryption, metadata, blockchain, cloud infrastructure, hashing, and forensic imaging may create communication barriers.

Expert testimony can assist courts in understanding technical matters. However, experts should distinguish between technical findings and ultimate legal conclusions.

Courts should also remain cautious about excessive dependence on technical expertise. The role of the expert is to explain relevant technological facts and methodologies, while the court retains responsibility for determining legal significance.

Effective presentation may therefore require simplified forensic reports, visual explanations, clearly documented acquisition procedures, and transparent descriptions of technical methodology.

11. Proposed Legal Framework

A comprehensive framework for digital evidence in cybercrime cases should incorporate several principles.

First, legality: Digital evidence should be obtained through legally authorized procedures.

Second, authenticity: Parties introducing digital evidence should establish its origin and relevance.

Third, integrity: Appropriate forensic procedures should demonstrate that evidence has not been improperly altered.

Fourth, documented custody: Every significant transfer or examination of evidence should be properly recorded.

Fifth, proportionality: Digital searches should be appropriately limited in relation to the investigative objective.

Sixth, technical competence: Investigators and judicial institutions should possess adequate technical expertise.

Seventh, judicial oversight: Significant investigative measures should remain subject to appropriate legal and judicial scrutiny.

Eighth, cross-border cooperation: International mechanisms should facilitate lawful access to evidence located outside the investigating jurisdiction.

This framework can help reconcile effective cybercrime investigation with fundamental procedural and privacy protections.

12. Future Legal Developments

The continuing evolution of technology will require courts and legislatures to reconsider traditional approaches to evidence. Emerging technologies such as decentralized networks, end-to-end encryption, artificial intelligence, Internet of Things devices, and blockchain-based systems may generate increasingly complex forms of digital evidence.

Future legislation should provide clear standards for forensic acquisition, authentication, preservation, expert testimony, and cross-border evidence collection.

Legal education should also incorporate basic technological concepts so that judges and legal practitioners can effectively evaluate technical evidence.

International cooperation should receive particular attention because cybercrime rarely respects territorial boundaries. Greater harmonization of procedural standards could reduce delays in obtaining evidence and improve the effectiveness of criminal investigations.

13. Conclusion

Digital evidence has become an essential component of contemporary cybercrime investigation and prosecution. Its ability to reveal communications, transactions, identities, locations, and patterns of activity provides law-enforcement authorities with powerful investigative capabilities. However, the technical nature of digital evidence also creates significant legal challenges concerning authenticity, integrity, chain of custody, privacy, encryption, jurisdiction, and admissibility.

A technologically advanced investigation cannot be considered legally sufficient merely because investigators possess sophisticated forensic tools. Evidence must also be collected through lawful procedures, preserved reliably, attributed appropriately, and presented transparently before the court.

The proposed legal framework emphasizes legality, authenticity, integrity, proportionality, judicial oversight, technical competence, and international cooperation. These principles can help ensure that the fight against cybercrime does not undermine the fundamental guarantees of due process and fair trial.

Ultimately, the future of cybercrime prosecution depends upon creating a balance between technological capability and legal accountability. Digital evidence should be powerful enough to assist investigators but sufficiently regulated to preserve the integrity of the justice system. As technology continues to evolve, legal institutions must develop equally sophisticated mechanisms for ensuring that digital evidence remains reliable, lawful, and capable of supporting just outcomes.

1. Introduction

The digital transformation of society has fundamentally changed the nature of criminal activity. Traditional crimes increasingly involve digital components, while entirely new categories of offences have emerged through computer networks, online platforms, mobile applications, and other technological infrastructures. Cyber fraud, identity theft, ransomware, unauthorized access, online harassment, financial crimes, and data theft are examples of offences in which digital information may constitute an important source of evidence.

Digital evidence can take numerous forms, including emails, instant messages, metadata, computer logs, browser histories, location information, digital photographs, transaction records, cloud-storage information, and data recovered from electronic devices. Unlike traditional physical evidence, digital evidence can be copied, modified, deleted, encrypted, transmitted across jurisdictions, or automatically altered through routine system operations.

These characteristics create important legal questions. How can a court determine whether a digital file is authentic? How can investigators demonstrate that evidence has not been altered? What procedures should be followed when evidence is collected from a device containing both relevant and highly personal information? How should courts evaluate evidence obtained from foreign servers or encrypted platforms?

The increasing dependence on digital evidence therefore requires a careful interaction between technology and law. Investigators need sufficient powers and technical capabilities to identify and preserve electronic evidence, while individuals must remain protected against unreasonable searches, privacy violations, unreliable evidence, and procedural unfairness.

This article examines the major legal challenges surrounding digital evidence in cybercrime prosecutions. It focuses particularly on authenticity, integrity, chain of custody, encryption, privacy, jurisdiction, and judicial evaluation of technologically generated evidence.

2. Concept and Nature of Digital Evidence

Digital evidence may be understood as information stored, transmitted, or generated in digital form that has potential relevance to a legal proceeding. It may originate from personal devices, enterprise systems, telecommunications networks, cloud platforms, financial institutions, social media services, or other digital environments.

One important characteristic of digital evidence is its intangible nature. A physical object can often be directly examined, whereas digital information exists through electronic representations stored on physical or virtual infrastructure.

Digital evidence can also be highly volatile. Information stored in temporary memory may disappear when a device is switched off. Network logs may be overwritten after a particular period, while cloud-service providers may maintain data under retention policies that vary according to jurisdiction and service.

Another important characteristic is replicability. Unlike many physical forms of evidence, digital information can be duplicated without necessarily changing its apparent content. However, this does not eliminate evidentiary concerns. Investigators must demonstrate that the copy presented before the court accurately represents the original evidence.

Consequently, legal systems require appropriate procedures for collection, preservation, verification, and presentation.

3. Authenticity of Digital Evidence

Authenticity is a fundamental requirement for evidentiary reliability. A court must be satisfied that the evidence presented is what the party claiming it to be.

In digital cases, authenticity may involve demonstrating the origin of a file, the identity of the device from which it was obtained, the account associated with the information, and the circumstances under which the data was collected.

For example, an electronic message may appear to originate from a particular account, but account credentials can be compromised or impersonated. Similarly, metadata may provide useful information but should not automatically be treated as conclusive proof of authorship.

Technical mechanisms such as cryptographic hash values can assist investigators in demonstrating that a forensic copy has remained unchanged after acquisition. However, technological verification should operate alongside proper procedural documentation.

Authentication should therefore be understood as a combined legal and technical process. Courts should evaluate not merely whether a digital record exists but also how it was obtained, preserved, attributed, and presented.

4. Integrity and Chain of Custody

The integrity of digital evidence is closely associated with the chain of custody. Chain of custody refers to the documented history of evidence from the moment it is collected until its presentation in court.

A reliable chain of custody should identify:

1. who collected the evidence;
2. when and where it was collected;
3. the method used for acquisition;
4. how the evidence was stored;
5. who subsequently accessed it;
6. whether forensic copies were created; and
7. whether any changes occurred during examination.

Weak documentation may create uncertainty regarding whether evidence was modified or improperly handled.

Digital forensic investigators commonly use specialized procedures to create forensic images and calculate cryptographic hash values. These mechanisms can provide technical evidence that the analyzed copy corresponds to the acquired data.

Nevertheless, technological tools cannot replace procedural discipline. A perfectly calculated hash value does not establish that the original evidence was lawfully obtained or correctly attributed. Thus, evidentiary integrity requires both technical safeguards and legally compliant procedures.

5. Encryption and Investigative Challenges

Encryption is an important component of modern cybersecurity because it protects information against unauthorized access. At the same time, strong encryption can create substantial challenges for criminal investigations.

Investigators may encounter encrypted smartphones, messaging applications, storage devices, or network communications. Even when authorities lawfully obtain a device, the relevant information may remain inaccessible without an appropriate key or authentication mechanism.

This creates a difficult legal balance. Investigative authorities may argue that access to encrypted information is necessary for preventing or prosecuting serious crimes. Conversely, weakening encryption mechanisms may expose millions of legitimate users to security risks.

The legal response should therefore avoid treating encryption itself as evidence of criminal conduct. Instead, investigative access should be governed by lawful authorization, proportionality, necessity, and appropriate judicial oversight.

Where compelled decryption or access to credentials is legally permitted, courts may need to consider constitutional protections, privilege, privacy, and the specific circumstances of the investigation.

6. Privacy and Digital Searches

Digital devices contain an extraordinary quantity of personal information. A single smartphone may contain photographs, financial records, private communications, medical information, location histories, employment information, and personal documents.

Consequently, digital searches can be significantly more intrusive than searches of many physical objects. An investigation targeting a particular offence may potentially expose information unrelated to the alleged crime.

This raises important questions concerning proportionality and scope. Investigative authorities should, where legally required, obtain appropriate authorization and limit searches to information reasonably connected with the investigation.

Courts should carefully examine whether evidence was collected through lawful procedures. The admissibility or evidentiary weight of improperly obtained digital evidence may depend on the applicable legal framework.

Privacy protection should not be viewed as an obstacle to cybercrime investigation. Rather, lawful and proportionate investigative procedures can strengthen the legitimacy and reliability of criminal justice processes.

7. Jurisdictional Problems

Cybercrime frequently crosses national borders. An offender may operate from one country, use infrastructure located in another, target victims in a third country, and store relevant evidence on cloud servers distributed across several jurisdictions.

This creates significant problems concerning investigative authority and access to evidence.

A domestic warrant or investigative authorization may not automatically provide authority to obtain information physically stored in another country. Investigators may therefore need to

rely upon international cooperation mechanisms, mutual legal assistance procedures, cross-border agreements, or lawful requests to service providers.

Cloud computing further complicates the concept of physical location. Data may be dynamically distributed among multiple data centers, making it difficult to identify a single location associated with the evidence.

International cooperation and harmonization of procedural standards are therefore increasingly important for effective cybercrime enforcement.

8. Admissibility and Reliability

Admissibility determines whether evidence may be considered by a court, while reliability concerns the degree of confidence that should be placed in that evidence.

Digital evidence should not automatically receive greater evidentiary value merely because it appears technically sophisticated. Courts should consider the circumstances under which the evidence was created, collected, preserved, and attributed.

For automatically generated records, issues may include the reliability of the underlying system, accuracy of timestamps, integrity of databases, and reliability of the process through which the record was generated.

For user-generated content, courts may need to examine questions of authorship and account control. Screenshots, for example, may demonstrate that particular content existed but may not independently establish who created it or whether the displayed information was manipulated.

Judicial evaluation should therefore consider both technological reliability and the surrounding factual circumstances.

9. Artificial Intelligence and Digital Evidence

Artificial intelligence introduces a new dimension to digital evidence. AI systems may be used to analyze large quantities of seized data, identify patterns, classify files, detect suspicious activity, or assist investigators in prioritizing evidence.

While these capabilities may significantly improve investigative efficiency, reliance on AI-generated analysis creates additional legal questions.

If an AI system identifies a particular document or communication as relevant, investigators should be able to establish how that result was generated and how human investigators verified it.

AI-generated outputs should not automatically be treated as independent proof of criminal conduct. They may function as investigative tools that help identify potentially relevant evidence, but final legal conclusions should remain subject to appropriate human and judicial evaluation.

This distinction is important because statistical predictions can contain errors and may reflect limitations in the underlying datasets or models.

10. Challenges in Presenting Digital Evidence Before Courts

Digital evidence can be technically complex and difficult for judges, lawyers, and juries to understand. Specialized terminology relating to encryption, metadata, blockchain, cloud infrastructure, hashing, and forensic imaging may create communication barriers.

Expert testimony can assist courts in understanding technical matters. However, experts should distinguish between technical findings and ultimate legal conclusions.

Courts should also remain cautious about excessive dependence on technical expertise. The role of the expert is to explain relevant technological facts and methodologies, while the court retains responsibility for determining legal significance.

Effective presentation may therefore require simplified forensic reports, visual explanations, clearly documented acquisition procedures, and transparent descriptions of technical methodology.

11. Proposed Legal Framework

A comprehensive framework for digital evidence in cybercrime cases should incorporate several principles.

First, legality: Digital evidence should be obtained through legally authorized procedures.

Second, authenticity: Parties introducing digital evidence should establish its origin and relevance.

Third, integrity: Appropriate forensic procedures should demonstrate that evidence has not been improperly altered.

Fourth, documented custody: Every significant transfer or examination of evidence should be properly recorded.

Fifth, proportionality: Digital searches should be appropriately limited in relation to the investigative objective.

Sixth, technical competence: Investigators and judicial institutions should possess adequate technical expertise.

Seventh, judicial oversight: Significant investigative measures should remain subject to appropriate legal and judicial scrutiny.

Eighth, cross-border cooperation: International mechanisms should facilitate lawful access to evidence located outside the investigating jurisdiction.

This framework can help reconcile effective cybercrime investigation with fundamental procedural and privacy protections.

12. Future Legal Developments

The continuing evolution of technology will require courts and legislatures to reconsider traditional approaches to evidence. Emerging technologies such as decentralized networks, end-to-end encryption, artificial intelligence, Internet of Things devices, and blockchain-based systems may generate increasingly complex forms of digital evidence.

Future legislation should provide clear standards for forensic acquisition, authentication, preservation, expert testimony, and cross-border evidence collection.

Legal education should also incorporate basic technological concepts so that judges and legal practitioners can effectively evaluate technical evidence.

International cooperation should receive particular attention because cybercrime rarely respects territorial boundaries. Greater harmonization of procedural standards could reduce delays in obtaining evidence and improve the effectiveness of criminal investigations.

13. Conclusion

Digital evidence has become an essential component of contemporary cybercrime investigation and prosecution. Its ability to reveal communications, transactions, identities, locations, and patterns of activity provides law-enforcement authorities with powerful investigative capabilities. However, the technical nature of digital evidence also creates significant legal challenges concerning authenticity, integrity, chain of custody, privacy, encryption, jurisdiction, and admissibility.

A technologically advanced investigation cannot be considered legally sufficient merely because investigators possess sophisticated forensic tools. Evidence must also be collected through lawful procedures, preserved reliably, attributed appropriately, and presented transparently before the court.

The proposed legal framework emphasizes legality, authenticity, integrity, proportionality, judicial oversight, technical competence, and international cooperation. These principles can help ensure that the fight against cybercrime does not undermine the fundamental guarantees of due process and fair trial.

Ultimately, the future of cybercrime prosecution depends upon creating a balance between technological capability and legal accountability. Digital evidence should be powerful enough to assist investigators but sufficiently regulated to preserve the integrity of the justice system. As technology continues to evolve, legal institutions must develop equally sophisticated mechanisms for ensuring that digital evidence remains reliable, lawful, and capable of supporting just outcomes.

Declarations

Conflict of interest: The authors declare that they have no conflict of interest.

Funding: This review received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Ethical approval: Not applicable. This article is a review of published literature and did not involve human participants or animal subjects.

Data availability: No new data were generated or analyzed in support of this review. All sources relied upon are cited in the References.

Use of AI tools: No generative artificial intelligence tool was used in the conception, drafting or analysis of this article. The authors take full responsibility for the content.

Author contributions: Author contributed to the conception of the review, the survey of the literature, and the drafting and revision of the manuscript. Author read and approved the final version.