Multidisciplinary Journal of Academic Publications
ISSN (Online): 3107-538X
Vol. 02, Issue 01, January – February 2026

DIGITAL EVIDENCE IN CYBERCRIME INVESTIGATIONS: LEGAL, TECHNICAL, AND PROCEDURAL PERSPECTIVES

Suneeta Rathore[1], Prof (Dr.) Aryendu Dwivedi[2]

Research Scholar, Institute of Legal Studies, Shri Ramswaroop Memorial University Lucknow Deva Road Barabanki Uttar Pradesh[1]

Professor, Institute of Legal Studies, Shri Ramswaroop Memorial University Lucknow Deva Road Barabanki Uttar Pradesh[2]

Abstract

The rapid proliferation of digital technology has demon-kissed a new type of crime roughly dubbed cybercrime of late. The requirement to identify, seize, manage, and present digital evidence in the investigation of such offences presents legal, technical, and logistical challenges that are systematically different from other traditional evidential objects. In this paper, we refer to the digital evidence stemming from cybercrime investigations and discuss its admissibility under existing legal regimes. The main aims are to examine the legal criteria for digital evidence in different jurisdictions, and to assess the technical and procedural mechanisms that safeguard its forensic soundness. A doctrinal and analytical approach is applied, with references to statutory provisions, judicial pronouncements with due regard to international conventions and academic writings. The findings demonstrate the great degree of variation between legal standards, jurisdictional overreach, and the consistent difficulty of keeping chain of custody in digital forensic workflows. The dialogue addresses the challenges that such growth creates for lawmakers. Harmonised legal frameworks, standardised forensic procedures, and enhanced international cooperation are crucial for the successful prosecution of cybercrimes, the paper concludes.

Keywords: *Digital Evidence[1], Cybercrime[2], Digital Forensics[3], Admissibility[4], Chain of Custody[5].*

1. Introduction

Never before has digital technology become so embedded into our lives and activities since the turn of the twenty-first century. Although this shift has brought tremendous socio-economic progress, it has also enabled the criminal underbelly to flourish. Cybercrime broadly defined as crime that requires a computer, networked device, or a network to commit has become one of the greatest challenges faced by justice systems around the world.[1]US$ 8.15 trillion; by 2028, this number could reach a staggering USD 13.82 trillion, highlighting the TRUE scale of the problem.[2]US$ 8.15 trillion; by 2028, this number could reach a staggering USD 13.82

[1]Wall, D.S., *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, 2007, p. 10.
[2]Statista Research Department, "Estimated Cost of Cybercrime Worldwide 2018–2028," Statista, 2024.

trillion, highlighting the TRUE scale of the problem.[3]Digital evidence refers to any information that is stored or transmitted in digital form, and unlike traditional physical evidence, it is fragile, volatile, and easily tampered with, complicating the process of collecting, preserving, and presenting it as an admissible form of evidence in a court of law.[4]Legal systems worldwide have struggled to either rework or create entirely new evidentiary rules, which were primarily based on the use of physical objects and oral testimony, in order to account for this novel form of evidence.The Information Technology Act, 2000 (hereinafter referred to as "IT Act") is the enactment that represents central legislation in India with respect to e-commerce and cybercrimes.[5]Sections 65A and 65B were inserted in the Indian Evidence Act, 1872 by way of an amendment in 2000, allowing inclusion of electronic records under the purview of the Act.[6]Even though the Indian Evidence Act was repealed almost a century later by way of the BharatiyaSakshyaAdhiniyam, 2023 (BSA), the foundational idea of document evidences has been preserved and refined under sections 61 and 62 of the new Ac which has its effect from 01 July 2024.[7]At the international level, the only multilateral treaty that continues to hold importance in terms of procedural matters, including the collection of digital evidence, is the Convention of the Council of Europe on Cybercrime, 2001 (Budapest Convention).[8]However, all these legislative attempts, however needed, were not enough to change the status quo. The topics of admissibility, proving authenticity and integrity, and what procedural safeguards need to be in place to protect against tampering continue to elicit much litigation and academic thought. This problem is further exacerbated by the fact that the internet is a jurisdictional void, where cybercriminals commonly operate from the cover of a different nation-state, requiring international cooperation mechanisms that are slow and underwhelming. The paper presents a detailed discussion of digital evidence in terms of its legality, its technical aspects and its procedural approach in dealing with cybercrime investigations. It examines the legislative frameworks of digital evidence, the technical standards and forensic practices used in its collection and analysis, and the procedural mechanisms that guarantee its reliability and use in court.

2. Objectives

1. To critically analyse the legal frameworks governing the admissibility, authentication, and reliability of digital evidence in cybercrime investigations across key jurisdictions, with particular emphasis on Indian statutory provisions and landmark judicial pronouncements.
2. To evaluate the technical standards, forensic methodologies, and procedural safeguards essential for the proper identification, collection, preservation, and presentation of digital evidence, and to identify gaps and challenges that hinder the effective prosecution of cybercrimes.

3. Research Methodology

This paper uses a doctrinal and critical research technique. It will be based on primary sources such as the statutory enactments like the Information Technology Act, 2000, the BharatiyaSakshyaAdhiniyam, 2023, and the Computer Fraud and Abuse Act, 1986 (United States) as well as the Council of Europe Convention on Cybercrime, 2001. Cases of the Indian courts, especially the Supreme Court of India and a few foreign cases

[3]Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd edn., Academic Press, 2011, p. 7.
[4]Mason, S., *Electronic Evidence*, 4th edn., LexisNexis Butterworths, 2017, p. 35.
[5]The Information Technology Act, 2000 (Act No. 21 of 2000), Parliament of India.
[6]The Indian Evidence Act, 1872 (Act No. 1 of 1872), Sections 65A and 65B, inserted by the Information Technology Act, 2000.
[7]The BharatiyaSakshyaAdhiniyam, 2023 (Act No. 47 of 2023), Sections 61 and 62.
[8]Council of Europe, Convention on Cybercrime, CETS No. 185, Budapest, 23 November 2001.

have been considered with the aim of tracking the development of judicial standards concerning digital evidence. Peer-reviewed journal articles, reports issued by international organisations such as, INTERpol and the United Nations office on drugs and crime (UNODC) as well as authoritative textbooks on digital forensics and cyber law have been consulted as secondary sources. This is mostly a qualitative analysis though it incorporates comparative legal analysis in establishing similarities and differences across the jurisdictions.

4. Conceptual Framework: Understanding Digital Evidence

Digital evidence can be described as any probative information that is represented in binary form or transferred.[9]Scientific Working Group on Digital Evidence (SWGDE) defines it as information that has probative value, and that information is stored or transmitted in digital format."[10]This is a broad collection of data forms containing emails, text messaging, social media interactions, web browsing history, metadata, server logs, and digital photographs, GPS location information, and data that was stored in the services of cloud storage.Digital evidence also has some unique features that set it apart compared to traditional physical evidence. First, it is latent in that it can not be detected by human senses without the help of technological equipment.[11]Second, it is volatile and can be easily modified or deleted or even corrupted either deliberately or accidentally. Third, digital evidence can be replicated in an exact copy and the copy is identical to the original and can be distinguished.[12]Fourth, it can be large; millions of potentially relevant files can be stored in one storage. Lastly, the digital evidence often crosses geographical lines, as it may be generated by computer (and therefore should be considered as computer-generated evidence) or it can be created by people (and therefore should be computer-stored evidence) and a combination of both (and therefore should be considered as a hybrid evidence).In general, the digital evidence can be classified into: (a) computer-generated evidence, which is framed by the work of automated processes of a computer; (b) computer-stored evidence, which is created through the work of humans and is stored digitally; and (c) hybrid evidence.[13]This categorization has direct bearing on the legal requirements of admissibility since various categories could be subject to various evidentiary rules in accordance with the jurisdiction.

5. Legal Perspectives on Digital Evidence

The Indian Legal Framework

The law of admissibility of digital evidence in India is largely controlled by the Information Technology Act, 2000, and the body of proof contained in the Indian Evidence Act, 1872 (and currently in the BharatiyaSakshyaAdhiniyam, 2023). According to section 2(1)(t) of the IT Act, an electronic record is the data, record or data created, image or sound stored, received or sent in electronic mode, or micro film or computer generated micro fiche.[14]Information Technology (Amendment) Act, 2000 came up with a regime regarding the admissibility of electronic records, with the introduction of the former Section 65A and 65B of the Indian Evidence Act. Section 65B was that any information in an electronic record which is created, copied, or recorded on paper, or stored, copied, or recorded in optical or magnetic means, produced by a computer, shall be

[9]SWGDE, "Digital and Multimedia Evidence Glossary," Scientific Working Group on Digital Evidence, Version 3.0, 2016.
[10]*Ibid.*
[11]Carrier, B., *File System Forensic Analysis*, Addison-Wesley, 2005, p. 3.
[12]Casey, E., *supra* note 3, p. 14.
[13]Law Commission of India, Report No. 185, *Review of the Indian Evidence Act, 1872*, 2003, Chapter VIII.
[14]The Information Technology Act, 2000, Section 2(1)(t).

considered to be a document and shall be admissible in court, on condition that some requirements are met.[15]As stated in these conditions, the computer had to be in constant operation, the information had to enter the computer as part of the usual business of running the device in question and that a certificate existed under Section 65B(4) by a person who was in a position of responsibility with regard to the operation of the concerned device.[16]

The need of Section 65B(4) certificate certificate was discussed in a row of landmark decisions by the Supreme Court of India. The Court in **Anvar P.V. v. P.K. Basheer(2014)** ruled that electronic evidence is mandatory as in the certificate in Section 65B(4), which reversed the previous position adopted in the case State (NCT of Delhi) v. This had been a more lenient approach taken by Navjot Sandhu (2005).[17]The Court stated that secondary electronic evidence in the shape of CDs, DVDs, or pen drives cannot be admitted without the necessary certificate. The Supreme Court reiterated that the certificate of Section 65B(4) is mandatory, but noted that where an original electronic device is manufactured prior to the court, there is no need to have the certificate requirement because the original document itself is the primary evidence (KailashKushanraoGorantyal, 2020).[18]The ruling eliminated a lot of ambiguity in the judiciary and provided a clear direction to the lower courts.

The admissibility of electronic or digital records is defined in Section 61 of the BharatiyaSakshyaAdhiniyam, 2023, whereas Section 62 sets the circumstances of admissibility of electronic records, such as the certificate requirement, in a substantially similar fashion to the previous Section 65B framework but adapting it to the current technological reality.[19]The IT Act also identifies different cybercrimes in the form of Sections 43, 65, 66, 66A-66F, 67, 67A, 67B and so on providing punishments to computer-related fraud, identity theft, cyber terrorism and publishing of obscene contents in electronic forms.[20]It is relevant to mention that the supreme court invalidated Section 66A of the communication acts of sending offensive messages in the year 2012 in Shreya Singhal v. As unconstitutional because it infringed Art 19(1)(a) of the Constitution.[21]

International Legal Frameworks

The international treaty on cybercrime is named the first and most comprehensive, which is the Council of Europe Convention on Cybercrime (Budapest Convention, 2001). It also demands signatory States to adopt legislations to expedited preservation of computer data stored (Article 16), expedited preservation and partial disclosure of traffic data (Article 17), production orders (Article 18), search and seizure of stored computer data (Article 19) and real-time collection of traffic data (Article 20).[22]In the United States, digital evidence is admissible under the Federal Rules of Evidence, specifically, Rules 901 and 902 that provide the admissibility criteria of an evidence in terms of its authentication and self-authentication.India does not have a signature on the Budapest Convention, as well as, but has taken part in the proceedings of the Cybercrime Convention Committee.[23]Stored Communications Act, 18 U.S.C. 27012712, governs the situations in which law enforcement agencies may require service providers to reveal electronic communications that are stored.[24]The

[15]The Indian Evidence Act, 1872, Section 65B(1).
[16]*Id.*, Section 65B(4).
[17]*Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (Supreme Court of India).
[18]*Arjun PanditraoKhotkar v. KailashKushanraoGorantyal*, (2020) 7 SCC 1 (Supreme Court of India).
[19]The BharatiyaSakshyaAdhiniyam, 2023, Sections 61 and 62.
[20]The Information Technology Act, 2000, Sections 43, 65, 66, 66A–66F, 67, 67A, and 67B.
[21]*Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (Supreme Court of India).
[22]Council of Europe, Convention on Cybercrime, *supra* note 8, Articles 16–21.
[23]Federal Rules of Evidence, Rules 901(b)(9) and 902(13)–(14), United States.
[24]Stored Communications Act, 18 U.S.C. §§ 2701–2712 (United States).

landmark Carpenter v. The ruling of the United States (2018) of the U.S Supreme Court declared that the purchase of cell-site location information is a Fourth Amendment search, which must be warranted with probable cause.[25]TThe General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a model that influences the framework of the European Union and places serious requirements on processing personal data, including during criminal investigations.[26]The proposed e-Evidence Regulation aims to put in place a framework of European Production Orders and European Preservation Orders of electronic evidence in criminal proceedings, as well as to make authorities in one Member State have the possibility of a direct request of the service providers in another country.[27]

6. Technical Perspectives on Digital Evidence

Digital Forensic Process

Digital evidence is technically handled in a systematic forensic procedure that is vital in the predilection of integrity and admissibility. The National Institute of Standards and Technology (NIST) Special Publication 800-86 is a guide to integrating forensic techniques into incident response, which involves a four-phase approach, namely, collection, examination, analysis, and reporting.[28]Collection phase entails identification and acquisition of the possible sources of digital evidence. The best practices require generating a bit-to-bit copy of the original storage medium by forensic image development using write-blocking technology to ensure that the original data are never changed.[29]EnCase, FTK (Forensic Toolkit), and open-source systems like Autopsy are commonly used in that purpose.The stage of examination presupposes the usage of forensic techniques to render the data visible and extract valuable information. This involves file carving, key-word searching, timeline analysis, registry analysis as well as metadata analysis.[30]The analysis phase entails interpretation of the extracted information with reference to the investigation and coming up with conclusions on the activities of the user, the timelines, and the relevance of the evidence generated as far as the case under the spotlight is concerned.At this stage, the forensic examiner is expected to document all the processes including tools and techniques used, results and findings, and how the identified evidence may be relevant to the case under the investigation in a manner that is understandable to the legal community, as well as the court.

Integrity Verification: Hash Values

The integrity of digital evidence is checked by cryptographic hash functions. A hash value is an alpha-numeric and fixed size value that is a result of a mathematical algorithm used on a data set. MD5 (Message Digest Algorithm 5) and SHA-256 (Secure Hash Algorithm 256-bit) are the most popular algorithms.[31]Any change made to the data in any form, however, slight, will lead to a totally different hash value and hence a solid way of identifying tampering. Forensic examiners also produce hash values when acquiring evidence and later when

[25]*Carpenter v. United States*, 585 U.S. 296 (2018) (Supreme Court of the United States).
[26]Regulation (EU) 2016/679 (General Data Protection Regulation), European Parliament and Council, 27 April 2016.
[27]European Commission, Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17 April 2018.
[28]Kent, K., Chevalier, S., Grance, T. & Dang, H., NIST Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, National Institute of Standards and Technology, 2006.
[29]*Ibid.*, pp. 3-1 to 3-8.
[30]Nelson, B., Phillips, A. &Steuart, C., *Guide to Computer Forensics and Investigations*, 6th edn.,Cengage Learning, 2019, Chapter 7.
[31]NIST, "Secure Hash Standard (SHS)," FIPS PUB 180-4, National Institute of Standards and Technology, August 2015.

preparing it to be analyzed and presented, this is to ensure that no alterations have been made on the evidence at any point.

Challenges in Cloud Computing and Encryption

The spread of the cloud computing has posed serious technical challenges. The information in cloud facilities can be spread across various computers in various jurisdictions and therefore is not easy to acquire both technically and legally.[32]Moreover, it is possible that cloud service providers use encryption both at rest and in transit, and the end-user implements their own encryption layer, providing an additional barrier to legal access to the contents of the communications transmitted.End-to-end encryption in like messaging systems e.g. WhatsApp and Signal is an especially acute problem, where neither the service provider nor the law enforcement can access the contents of communications without the user holding the decryption key.[33]It has spawned the current encryption debate, in which law enforcement agencies are demanding the creation of mechanisms by which access can be made lawful, and privacy advocates and technologists concerned about the creation of systemic vulnerabilities.

7. Procedural Perspectives on Digital Evidence

Chain of Custody

Chain of custody is the time-based records of the objects, their possession, use, and disposition of physical or digital evidence.[34]The chain of custody in the digital world is especially difficult to maintain because electronic data can be copied and downloaded anywhere and therefore, it is intangible and easily duplicable. All access, transfer or analysis of digital evidence should be carefully documented such as the name of the individual handling the evidence, date and time of each action, tools and methods used.[35]The inability to provide a continuous chain of custody may lead to the exclusion of the evidence, and this may jeopardise the whole prosecution.Failure to provide a continuous chain of custody has been highlighted by the Supreme Court of India in handling electronic evidence. In **Tomaso Bruno v. According to the Court, in State of U.P. (2015),** electronic evidence should be treated with identical precautions as traditional evidence, and that any lapse in chain of custody will create a presumption of tampering.[36]

Standard Operating Procedures and Guidelines

A number of national and international organizations have come up with the standard operating procedures (SOPs) and rules of managing digital evidence. The **ISO/IEC 27037:2012** standard offers some guidelines that one uses in identifying, collecting, acquiring, and preserving digital evidence.[37]It sets out principles that are to be applied during all phases of the digital evidence handling procedure, such as reducing the amount of manipulation of the original digital device, considering the alterations made to the evidence, and adherence to local regulations and legislation.The Cyber Crime Investigation Manual released by the Bureau of Police Research and Development (BPR&D) specifies procedural guidelines of handling officers involved in the

[32]Ruan, K., *Cybercrime and Cloud Forensics: Applications for Investigation Processes*, IGI Global, 2013, p. 45.
[33]Koops, B.J. &Kosta, E., "Looking for Some Light Through the Lens of 'Crypto War' History," *Stanford Technology Law Review*, Vol. 21, 2018, pp. 318–372.
[34]NIST SP 800-86, *supra* note 28, p. 3-4.
[35]ISO/IEC 27037:2012, *Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, International Organization for Standardization, 2012.
[36]*Tomaso Bruno v. State of U.P.*, (2015) 7 SCC 178 (Supreme Court of India).
[37]ISO/IEC 27037:2012, *supra* note 35.

cybercrime cases in India.[38]Indian Computer Emergency Response Team (CERT-In) is a nodal agency in responding to cybersecurity-related incidents and can issue advisories and guidelines with regards to the forensic research of digital evidence under the IT Act Section 70B.[39]In the United Kingdom, digital evidence is subject to four principles prescribed by the Association of Chief Police Officers (ACPO) Guidelines (since renamed the National Police Chiefs' Council or NPCC Guidelines), namely that no steps taken to alter data on a digital device which is in turn to be relied upon in a court of law; that, where it is necessary to access original data, the individual should be competent to do so and be capable of giving evidence as to the nature and consequence of the actions taken; that an audit trail must be established and maintained; and that the overall responsibility of the person.[40]

Mutual Legal Assistance and Cross-Border Challenges

Since cybercrime has no borders, there should be cross-border collaboration in digital evidence collection and sharing. The main form of cooperation is the process of mutual legal assistance that is a system of formal government-to-government requests of legal assistance (Mutual Legal Assistance Treaty).[41]Nevertheless, the MLAT process is commonly criticized as being too slow, and may require months or even years to provide results a timeframe that, simply, does not suit the nature of digital evidence in any way.[42]India has signed MLATs as well as bilateral treaties with a number of nations in order to cooperate with them on criminal issues of which cybercrime is part.[43]In response to much of the limitations of the traditional MLAT process, the Second Additional Protocol to the Budapest Convention in 2021 proposes mechanisms of direct cooperation with service providers in other jurisdictions, swift disclosure of subscriber information, joint investigation teams, and so forth.[44]

8. Results and Discussion

The review brings out some important results. To begin with, even though the legal regimes concerning digital evidence have become much more liberal and advanced over the last twenty years, it still has a lot of gaps and inconsistencies. The obligatory certificate requirement provided by Section 65B of the Indian Evidence Act (now Section 62 of BSA) has had a repetitive litigation history, and despite these clarifications being provided in Arjun PanditraoKhotkar there are still practical challenges in enforcing these standards, especially relating to the size of the electronic records or data stored by a third party service provider. There is a chronic lack of certified digital forensic specialists, insufficient lab facilities, and the rate of technological evolution is a challenge. The rise of anti-forensic techniques methods that are intentionally used by criminals to undermine forensic examination such as wiping of data, steganography and encrypting also makes the landscape of investigation more complicated.[45] Third, the mechanisms of cross-border cooperation are not sufficient in terms

[38]Bureau of Police Research and Development (BPR&D), *Cyber Crime Investigation Manual*, Ministry of Home Affairs, Government of India, 2016.
[39]The Information Technology Act, 2000, Section 70B.
[40]Association of Chief Police Officers (ACPO), *Good Practice Guide for Digital Evidence*, Version 5, 2012.
[41]UNODC, *Manual on Mutual Legal Assistance and Extradition*, United Nations Office on Drugs and Crime, 2012.
[42]*Ibid.*, pp. 15–17.
[43]Ministry of Home Affairs, Government of India, "Bilateral Agreements on Mutual Legal Assistance in Criminal Matters."
[44]Council of Europe, Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, CETS No. 224, 2021
[45]Harris, R., "Arriving at an Anti-Forensics Consensus: Examining How to Define and Control the Anti-Forensics Problem," *Digital Investigation*, Vol. 3, 2006, pp. 44–49.

of the magnitude and pace of transnational cybercrime. The MLAT model, developed in a pre-digital time, is ineffective to the demands of cybercrime investigations in which the evidence can be deleted or altered at all within hours.

The pattern of India not being a party to the Budapest Convention restricts its ability to access the cooperative mechanisms provided under the convention though bilateral agreements and informal channels of cooperation are partial substitutes. The decision in Carpenter v. The American case of United States and the right to privacy in K.S. Puttaswamy v being acknowledged as a fundamental right by the Supreme Court of India. Union of India (2017),[46]have set constitutional standards that any system of gathering digital evidence should meet. Finding a balance between the legitimate demands of criminal investigation and the basic rights of the individuals is an issue that is still going on and must be addressed with subtle legislative and judicial formula. Although these technologies may significantly expedite and increase the accuracy of evidence analysis, especially in situations where the data works with large amounts of data, they are also associated with transparency, bias, and the capacity of the courts to question the methods through which AI-generated conclusions are achieved.[47]

9. Conclusion

Digital evidence is now essential in investigation and prosecution of cybercrime and its relevance will only increase as the society relies more on digital technology. On the legal front, as illustrated in this paper, the efficient use of digital evidence demands a concerted effort to establish harmonised standards of admissibility that are sensitive to the specifics of digital evidence and that do not compromise the basic tenets of fairness and reliability upon which the law of evidence is built.On the technical side, more concerted effort is needed to find a way of resolving the issues of standardisation of admissibility that would be sensitive to the peculiarities of digital evidence and that would not affect the basic principles of fairness and reliability on which the law of evidence is established. On the On the technical front, the shift in Indian Evidence Act to the BharatiyaSakshyaAdhiniyam is a move in the right direction, though the actual success will be the practicality of the provisions and the juridical tradition that will be developed around it. Current issues of encryption and anti-forensic technologies require new investigations and advancement of the forensic methods. The procedural level of need is possibly the most pressing one, and it is the reform of cross-border cooperation mechanisms. India must give a serious thought to joining the Budapest Convention and the Second Additional Protocol in order to enjoy the smooth cooperation processes these two provide. At the same time, the domestic procedural systems should be revised to make sure that the chain of custody requirements of the digital evidence should be well-defined, utilized consistently, and properly feasible.Finally, the credibility of the criminal justice system in combating cybercrime means updating it to fit the digital age. This is not only necessitated by legislative reform but also judicial education, institutional capacity development and long-term international partnership. The issue is daunting, although the necessity of the integrity of the rule of law in the digital age requires nothing less than an all-encompassing and long-term response.

[46]*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (Supreme Court of India).
[47]Europol, *Artificial Intelligence and Law Enforcement: Opportunities and Challenges*, European Union Agency for Law Enforcement Cooperation, 2020.