INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

IJLAR

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

IJLAR

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

IJLAR

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

IJLAR

ROLE OF DIGITAL DATA PROTECTION MECHANISMS WITH SPECIAL REFERENCE TO FORENSIC LAWS

AUTHORED BY - ADWAIT PRATAP SINGH (UPSIFS, Lucknow)
CO-AUTHOR - CHANDRAYAN DAHARIA (NFSU, Delhi)
CO-AUTHOR 2 - SHASHANK KUMAR (Advocate, Ranchi Jharkhand)

1. Introduction

The growing digitalization of information has changed the methods of collection, storage, and analysis of information, which means the need for protection of information in the digital context is critical. Digital data protection is the collection of legal, technical, and administrative steps needed to safeguard data and protect personal and sensitive information from unauthorized access, abuse, or use, alteration, or disclosure[1]. Protection of digital information becomes more critical in forensic digital data and evidence because data drives criminal investigations and prosecutions. The rise in the use of digital communication devices has also increased the amount of information and data stored electronically that is used in legal proceedings. Therefore, the data must be preserved in a way that protects the data from unauthorized access, abuse, and manipulation, and in a way that protects the data from privacy violation. The integrity of the data must be maintained to ensure justice.

The conflicts in data breaches, cyber attacks, and violations of digital privacy continues to grow in complexity. Most forensic experts come to examine personal data held in electronic devices. This may provoke questions of consent and proportionality and the right to privacy. Most explosive consequences, it may affect not only the investigation at hand but also the rights of the person who is the object of the investigation. The data protection and forensic legislation overlap because in these cases law enforcement may need to act in the absence of legislation to provide the necessary constitutional protections.

Across the globe, the legal framework governing the law has started to include recognition of the importance of data protection[2]. This is evident in the European Union which has positioned

[1] Park S, Akatyev N, Jang Y, Hwang J, Kim D, Yu W, Shin H, Han C, Kim J. A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. Digital Investigation. 2018 Mar 1;24:S93-100.

[2] Mampilly AJ, Manda VK. Securing Digital Documents: Advanced Cybersecurity and Forensics Techniques for Data Protection. InCyber Security, Forensics and National Security 2026 (pp. 40-68). CRC Press.

the General Data Protection Regulations (GDPR) as the gold standard in the privacy protection law. This is due to the fact that the GDPR has principles of consent and accountability. The California Consumer Protection Act (CCPA) also gives people control over their data. In the Indian scenario, the 2000 Information Technology Act and presently the 2023 Digital Personal Data Protection Act also show the same positioning in data protection. All these legislations will act as important pillars in guiding the forensic data practices in the collection, analysis, and presentation of evidence.

This is to understand the working of digital data protection mechanisms within the forensic framework on a global and Indian scale.

2. Conceptual and Theoretical Framework

This study focuses on understanding the intersection of data protection and forensic and digital evidence. Data protection is a principle and practice approach to handling personal and sensitive information where lawfulness, fairness, and security must be observed. Forensic data constitutes information, digital, and telecommunication data and logs preserved for legal implications. In the legal sense, digital evidence is data contained in a physical storage facility or transmitted over a channel that is contemporaneously relevant to the litigation and is capable of proving or disproving a claim. Legally, intangible digital data must be preserved, authenticated, and rendered evidence while losing and modifying digital data is a reality.

Data protection theory rests on privacy, proportionality, and due process. In the context of the Indian Constitution, the 'right to privacy' as stated by Justice K. S. Puttaswamy v. Union of India (2017) must be the first step in addressing any state activity on data surveillance/seizure[3]. For proportionality, any restrictions on the right to privacy, particularly in forensic probing where digital data searches involve substantial personal space, must be lawful, necessary, and proportional to the objective at hand. Alongside the due process theory, the collection of evidence must be continuous, and state actions must consider individuals' interests and rights rationally, avoiding arbitrary action from the state.

The infusion of technology within the set scope of Constitutional and Human Rights Litigation has rapidly grown. Within the principles of consensual self-determination and autonomy, challenges arise from forensic investigations involving the analysis of metadata, the decryption

[3] Katkuri S. Securing the Digital Frontier: Legal Analysis of Cybersecurity, Data Privacy and Cyber Forensics in India. Indian Journal of Public Administration. 2025 Mar;71(1):75-91.

of devices, and pattern recognition algorithms[4]. Thus, forensic data practice must be anchored on the principles of human rights and constitutional fundamentals. This study combines legal theory and technology, the integration, within the scope of the study, centers on human dignity and procedural justice instead of merely cyber security, highlighting the reality of the present digital world.

3. Evolution of Data Protection Mechanisms

The growth of data protection legislation shows how privacy and the value of data as legal and fundamental concerns in the digital world have grown over the years. In India, the first step in legislation was the Information Technology Act of 2000 with the dealings of electronic data, digital evidence and cybercrime.In 2008 amendments to the IT Act, the 43A provision that enabled Data compensation and the 72A provision that punishes the wrongful disclosure of private data introduced the first building blocks of protection measures for data in the digital space. Aimed at the sheer exponential rise of data driven technologies, the cross border flow of data and the urgent need for targeted legislation, the Digital Personal Data Protection Act, 2023 (DPDP Act) finally came to be.

The DPDP Act has moved the paradigm from sector-specific legislation to a comprehensive legislation focused on rights[5]. It mandates data processing on the basis of consent, stipulates purpose limitation, and provides accountability on the part of data fiduciaries. However, data processing for national security, prevention, and investigation of crimes which entail powerful state action, are legal. In forensics, this means that lawful and necessary data collection has to be justified, as with the other broader principles laid down in Puttaswamy.

The General Data Protection Regulation (GDPR) implemented by the European Union in 2016 continues to be the most influential model worldwide, ensuring transparency, minimization of collection, and the rights of data subjects to erasure and rectification[6]. Likewise, the California Consumer Privacy Act of 2018 (CCPA) provides rights of access, deletion, and the ability to opt-out of sharing personal information. The OECD Privacy Guidelines additionally provides emphasis on the principles of fairness, security, and accountability as the baseline international standards. These global privacy frameworks continue to inspire national laws, including

[4] Horsman G. Defining principles for preserving privacy in digital forensic examinations. Forensic Science International: Digital Investigation. 2022 Mar 1;40:301350.
[5] Babikian J. Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era. Law Research Journal. 2023 Dec 31;1(2):91-101.
[6] Omeleze S, Venter HS. Digital forensic application requirements specification process. Australian Journal of Forensic Sciences. 2019 Jul 4;51(4):371-94.

privacy laws in India, to establish harmonized systems of privacy protection.

These laws directly impact the forensic sector in the way data is acquired, retained, and shared in an investigation. Authorization is required as per the law, the proper chain-of-custody, and the protection against unauthorized disclosure. The development of these mechanisms enables a critical change in the law—from inequitable, state-centric surveillance towards a dual focus: the need to preserve the integrity of an investigation and the need to protect an individual's privacy.

4. Forensic Laws and Digital Evidence

In digital forensic investigations, two main factors shape its course: the admissibility and the reliability of digital evidence. As far as the Evidence Act of 1872 is concerned, India, too, has legal and admissibility conditions for records and, specifically for electronic records, pillars 65 and 65B. As per pillar 65B, every electronic record submitted as evidence must come with a certificate of evidence describing the source, the device used, the method of transfer, and the manner of sealing evidence[7]. This provision seeks to ensure that the presented evidence is and remains authentic, as well as unaltered in its original form. In Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473, the Supreme Court canonized the principle that as of 65B every electronic record presented must have a certificate and for the first time underlined evidence procedural compliance in respect of tampering and fabrication.

To show compliance with regulations, certification, and documentation, and prove the legitimacy and reliability of digital evidence, the procedural framework in forensic practice must be followed.

Evidence retention and interception obligations in the framework of the Information Technology Act of 2000 (Amended 2008) primarily focus on the data. Section 67C obliges intermediaries to retain and maintain data in a readily accessible format, for a reasonable time frame, and for legal or investigative purposes, data holders may be needed to reveal. Section 69 allows government authorities to intercept, monitor, or analyze data for purposes of national security, sovereignty, or public order, but only via a legal order[8]. Section 72A creates a confidentiality and privacy and imposes a criminal sanction for unauthorized disclosure of personal data. These sections guide the legislation regarding the collection, preservation, and

[7] Karagiannis C, Vergidis K. Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. Information. 2021 Apr 22;12(5):181.

[8] Ogunseyi TB, Adedayo OM. Cryptographic techniques for data privacy in digital forensics. IEEE Access. 2023 Dec 15;11:142392-410.

protection of digital evidence.

Issues of digital evidence preservation, integrity, and custody are still unsolved. Electronic evidence alters, and volatile data and the lack of proper preservation of metadata create a need for precise digital forensic techniques[9]. For a sequenced data collection, forensic examiners should ensure that the process in the creation of bit forensic images, hash value control, logging, and audit trail documentation is fully executed and the details are adequately and appropriately captured.

The absence of gapless, consistent standards of uniform certification and lab accreditation within the country, especially in India, increases the probabilities of contamination of the evidence. The challenges of encryption, proprietary tools, and verification in cloud computing exacerbate the issues[10]. For evidence to be of value and restore the confidence of the judiciary, the chain of custody must be unbroken from seizure to the point of court presentation. The legal framework of the Indian Evidence Act and the IT Act offers procedural safeguards, yet effective implementation of the law demands technical knowledge, institutional infrastructure, and regular updates of judicial education on digital forensic science to cope with the rapidly changing technology.

5. Constitutional Dimensions of Data Protection

The right to privacy is a fundamental right under Article 21 and is constitutionally protected in India. This was recognized in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1. The Supreme Court Decision held that privacy is one of the components of the right to life and personal liberty and extends to 'informational privacy' and protection from arbitrary state surveillance[11]. The decision also introduced a three-fold test of privacy for restrictions to be placed on an individual—legality, necessity, and proportionality. This now gives us a constitutional touchstone for all data protection and forensic practice.

Under this doctrine, any forensic investigation that deals with personal or digital data must be predicated on a legally justified. The purpose of the measure also needs to be a justified state aim like the prevention of crime and/or proportionality in the sense that the measure must be

[9] Funta R, Ondria P. Data Protection in Law Enforcement and Judicial Cooperation in Criminal Matters. TalTech Journal of European Studies. 2021 Sep 1;11(2).

[10] Jayasekara SD, Abeysekara I. Digital forensics and evolving cyber law: case of BIMSTEC countries. Journal of Money Laundering Control. 2019 Oct 7;22(4):744-52.

[11] Marquenie T. The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework. Computer Law & Security Review. 2017 Jun 1;33(3):324-40.

the least intrusive in achieving the aim[12]. This means that the constitutional guarantees cannot be sacrificed on the altar of assumed investigative efficiency. For example, continuous digital surveillance and mass data collection that is not focused on an individual is not justified.

Article 21's due process clause also requires that the mechanisms to obtain and process forensic data be fair, just, and non-arbitrary. To protect against misuse, there has to be judicial or independent oversight regarding cases of interception and seizure of data. Although the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, provide procedural safeguards, it must still be read along with Puttaswamy for compliance with the principles of privacy and proportionality.

Constitutionally, the challenge of balancing the claims of the state and the rights of the individual still remains unresolved. The state does have a forensic mandate, but it must always also provide and uphold the right of the citizen to privacy[13]. Any access to digital data for forensic purposes must, therefore, be specific to a purpose, limited in time, and conditioned with safeguards of transparency and accountability. Incorporating constitutional principles into the forensic law illustrates that the progress of technology used in investigations must meet the objectives of serving justice and upholding the constitutional values of individual liberty and the right to personal space.

6. Intersection of Forensic Investigation and Data Privacy

Emails, photographs, financial records, transaction histories, geolocation histories, and social records- these are examples of data records that could be examined in a forensic investigation. Some records might be sensitive and contain personal data that is not pertinent to the investigation. Therefore, such data records require the utmost consideration so as not to incur negative ramifications from misplaced care. Forensic investigators are obligated to adhere to the principles of purpose limitation and data minimization in the collection, processing, and storage of data.

One of the foremost concerns in privacy and data ethics is consent. The issue of statutory authorization and warrant use in forensic function creep settings has also given rise to similar concerns[14].Unquestioned access to sensitive data raises issues of informed consent and control.

[12] Chen L, Takabi H, Le-Khac NA, editors. Security, privacy, and digital forensics in the cloud. John Wiley & Sons; 2019 Apr 29.
[13] Seyyar MB, Geradts ZJ. Privacy impact assessment in large-scale digital forensic investigations. Forensic Science International: Digital Investigation. 2020 Jun 1;33:200906.
[14] Ramadani EW, Idham R, Fikri ZU, Ridwan MK. Legal Protection Framework for Digital Forensic Experts in The Society 5.0 Era. Walisongo Law Review (Walrev). 2025 Oct 23;7(2):130-42.

Furthermore, the consequences of tracking are always less significant than the ability to infer behavioral patterns, especially in circumstances such as profiling and prediction.

Reflection is necessary on the overlap between the misuse of surveillance practices and forensic tools. Surveillance tools and AI the Government agencies has designed are tailored for specific investigations and purposes. The potential for overreach when indenting the scope of an investigation prism and scope is concerning. Investigation Prism and scope is concerning. Retention *is* unconstitutional. Erosion of civic trust, as *is* the case with surveillance. Other parts of the world have experienced these problems and introduced restrictions, such as the EU's Tele2 decision, which regulates the retention of data for surveillance.

The 2001 Budapest Convention on Cybercrime is centered around cross-border evidence-sharing which is the root cause of unmatched complexity for investigative purposes with international relations and cybercrime integration[15]. The MLAT framework still allows for countries such as India which is not a signatory, to maintain sovereignty and private info protection while Germany to access cross border data. Cyber transformed crime policies and cooperative frameworks have had shifts with world crimes. New data privacy frameworks coupled with cross border challenges and localization laws are startling.

Instances of overreach or abuse of information collecting forensics systems continue to take place. With no judicial oversight, the retrieval of information from personal devices or clouds may result in an invasion of privacy. The more concise procedural policy provisions will need to address specifically the scope, duration, and entail regulation of the forensic data processing stages. The intermingling of principles of privacy and the demand of the forensic context will need the greatest attention in addressing the securing of balance in the service of the conflicting demand of privacy and justice.

7. Data Protection Mechanisms in Forensic Practice

The interplay between technology, management, and law determines the level of protective safeguards instituted. The safeguards of confidentiality and integrity of forensic data, as mentioned, incorporated encryption, anonymization, and access control. During storage and transmission, the data is encrypted, and even if it were to be intercepted, the data would be gibberish to any unauthorized user lacking the appropriate decryption keys[16]. Personally

[15] Ferrazzano M, Raffaella B. Digital forensics: best practices and perspective. COLLEZIONE DI GIUSTIZIA PENALE. 2021:13-48.

[16] Malik AW, Bhatti DS, Park TJ, Ishtiaq HU, Ryou JC, Kim KI. Cloud digital forensics: beyond tools, techniques, and challenges. Sensors. 2024 Jan 10;24(2):433.

identifiable information is removed from the records to allow the data to be used for analysis and to minimize the potential for tracing the individual, thus preventing unnecessary invasions of privacy. Control systems like multi-factor authentication, along with role-based access, ensure that only approved forensic specialists and investigators may access and use the data and conduct forensic analysis, thereby vastly decreasing the potential for internal abuse.

Another principle of protection data in forensic science is the digital chain of custody. This is the uninterrupted recording of the movement of digital evidence, starting from the initial acquisition to various layers of storage and concluding with court presentation. This is crucial in confirming the legality and the integrity of the evidence. Improvements in evidence management systems have enabled the adoption of blockchain technology. Each change to digital evidence is recorded in an unchangeable and distributed ledger.

This occurs whenever evidence is incorporated into a transaction within the chain of custody, serving as a record against evidence being modified without access. Innovations such as these are expected to change the field of digital forensics by providing reliable and audit-able systems for evidence traceability.

The safeguards put in place in various organizations are just as necessary during the forensic investigation processes[17]. Take Indian Computer Emergency Response Team (CERT-In) as an example. It, like other national agencies relating to oversight of cybersecurity incident response, offers guidance on the secure handling of potentially breachable data as well as recommendations for breach mitigation. Cyber forensic labs, whether accredited to central or state agencies, are also required to follow standard protocols when acquiring, analyzing, and preserving data. With the Unveiling of the Digital Personal Data Protection Act, 2023, the requirement of accountability within the fiduciary principle in data processing introduces an obligation of forensic institutions, and all other organizations as data handlers, to process personal data that is in scope, consented to, and lawful and addresses the responsible data processing issue raised in previous sections.

The rationale also lies in the requirement to ensure robust audit trails and other accountability frameworks. Corrective action to streamline processes is made easier due to automated systems as internal and external audits are performed to establish systems for regular adherence[18]. Public accountability over forensic processes paired with the required judicial oversight

[17] Arshad H, Jantan AB, Abiodun OI. Digital forensics: Review of issues in scientific validation of digital evidence. Journal of Information Processing Systems. 2018 Apr 1;14(2).

[18] Goldstraw-White J. LEGAL AND POLICY FRAMEWORK FOR DIGITAL FORENSICS: A RESOURCE FOR PRACTITIONERS.

provides the necessary mandate on restraint relative to the intrusive investigations. The use of appropriate technology, ethics, and internal systems to adhere to standards creates safe conditions under which data can be obtained, processed, and stored.

8. Comparative Legal Perspective

Many international models stem from the principles of legally processing forensic information while upholding rights of privacy and human rights[19]. The European Union's General Data Protection Regulation (GDPR), introduced in 2016 and still the most complete framework for the regulation of personal data processing, exercises lawfulness, purpose limitation, data minimization, and storage limitation. As for the forensic aspects, Article 22 of the GDPR discusses the restriction of automated decision processing and mandates human involvement in such decisions if they are legally binding. GDPR also states that data processing concerning the prevention of a crime must be proportionate, transparent, and accountable, in essence, investigative necessity must respect fundamental rights.

The 2018 United States Clarifying Lawful Overseas Use of Data (CLOUD) Act permits cross-border access to electronic evidence stored by U.S. service providers and permits U.S. law enforcement agencies to compel service providers to hand over data, regardless of where that data is stored, provided there is a bilateral executive agreement[20]. The Act seeks to boost international collaborative digital investigations, however, it also poses questions on extraterritorial jurisdiction and incompatibility with data protection laws from other nations, particularly the EU and India.

At the EU regional level, the body responsible for cybersecurity, ENISA, issued comprehensive guidelines for AI and cybersecurity that prioritize secure design, auditability, and explainability for forensic tools. Including risk assessments, default encryption, and thorough documentation of forensic data collection helps ensure accountability and transparency in technology.

In comparison to global benchmarks, as well as India’s own cybersecurity and data protection legislation—the IT Act (2000), Indian Evidence Act (1872) and lately, the Digital Personal Data Protection Act (2023) —India’s legal framework still seems to be in the process of full interoperability[21]. The DPDP Act does seem to align with the concepts of the GDPR in relation

[19] Fakhouri HN, AlSharaiah MA, Alkalaileh M, Dweikat FF. Overview of challenges faced by digital forensic. In2024 2nd International Conference on Cyber Resilience (ICCR) 2024 Feb 26 (pp. 1-8). IEEE.
[20] Casey E, Biasiotti M, Turchi F. Using standardization and ontology to enhance data protection and intelligent analysis of electronic evidence. InDiscovery of Electronically Stored Information Workshop 2017.
[21] Kazemi SS, Heidari S. Digital forensics and its role in promoting criminal prosecution. Revista Eletrônica em Gestão, Educação e Tecnologia Ambiental. 2021 Jan 1;25:5.

to consent, purpose limitation, and accountability, but also carries significant state exemptions for investigative purposes which may diminish privacy protections. Differing definitions of "personal data," "lawful processing," and "judicial oversight" only compound interoperability issues.

Best privacy-preserving lawful evidence collection practices involves the adoption of GDPR principles of necessity and proportionality, prior judicial approval for data seizure, and the use of data minimization techniques, encryption to conceal data[22], and differential privacy. Potential to strengthen policies and laws is in establishing independent oversight of digital forensics, greater alignment of domestic legislation with the global south, greater harmonization of laws to international standards on privacy, and improved transparency on cross-border data flows.

9. Challenges and Ethical Concerns

There are still unanswered questions, and problems remain to be solved, in digital forensics, despite advancements in the law and technology. One such problem involves the misuse of data. Sensitive personal and business data, acquired during the course of forensic investigations, can be leaked, mishandled, and kept for extended periods. No minimum or maximum periods for holding such data[23], and the lack of supervision and data retention policies result in data over retention to the violation of privacy of the innocent. Innocent people can face the consequences of 'no data retention' policies infringing on their privacy rights. The lack of consent when large personal devices and personal cloud data are seized and analyzed raises ethical issues regarding the practice of forensic professionals.

Concerns regarding the ethical use of technology in digital forensics, particularly the use artificial intelligence for facial and voice recognition and predictive analytics, are on the rise. Potential discrimination through the use of AI is a significant social concern, especially when the AI is applied uncritically and the training data has hidden biases and public trust in forensic outcomes is lost[24]. Accordingly, ethical digital forensics must entail the elimination of bias and unambiguous evidence of fairness, through accountable and transparent governance of the

[22] Ledbetter EM. *Facing the Challenge: Protecting Data Privacy During Forensic Investigations* (Master's thesis, Utica College).

[23] Scheibner J, Ienca M, Kechagia S, Troncoso-Pastoriza JR, Raisaro JL, Hubaux JP, Fellay J, Vayena E. Data protection and ethics requirements for multisite research with health data: a comparative examination of legislative governance frameworks and the role of data protection technologies. Journal of Law and the Biosciences. 2020 Jan;7(1):lsaa010.

[24] KAUR G, DHAWAN A. Laws of electronic evidence and digital forensics. PHI Learning Pvt. Ltd.; 2024 Apr 15.

forensic AI tools and processes, is a mandatory requirement.

Another major issue is secrecy and transparency. Transparency about methods and evidence integrity drives forensic accountability. However, excessive transparency might expose sensitive data, harm procedures, and violate non-disclosure agreements. Keeping trust and operating efficiency in balance is crucial. Courts have used restricted disclosures, in-camera case file review, and referral to outside experts to protect privacy in the adjudicative process.

Finally, the disparity between modern technology and human rights abuse is concerning. Abuse of modern technology in forensic investigations and monitoring could turn a justice system into a surveillance system. The practice of forensic science ethically will always depend on the moral values of justice, accountability, and respect for a person's dignity. For this reason, forensic institutions should have, as a matter of priority, the presence of ethical review committees, appointed Data Protection Officers, and periodic transparency audits.

10. Policy and Legal Recommendations

For digital data protection measures to be effectively integrated into forensic practices, comprehensive policy reforms, and institutional safeguards will have to be set into place first. The first step is the creation of comprehensive and uniform forensic data handling protocols that will be adopted by all the investigative and adjudicative bodies[25]. These protocols must outline the lawful processes via which digital forensic evidence will be acquired, secured, and stored, and the processes via which evidence will be destroyed post-judicial use and preserved, and how and when a digital forensic files will be deleted. This uniformity will address the differences that currently exist among forensic laboratories, and increase the strength of the digital materials evidence that is submitted during court proceedings, thus reinforcing the evidentiary value that the materials possess[26].

The courts should be in charge of all steps of collecting and analysing digital proof. It should be up to courts to issue subpoenas, make sure that digital searches and analyses are fair, and even watch over the analysis of private, sensitive information. A warrant system that is overseen by judges over complex chains of custody should be put in place to cut down on illegal access and overreach.

[25] Kasper A, Laurits E. Challenges in collecting digital evidence: a legal perspective. InThe future of law and eTechnologies 2016 Feb 23 (pp. 195-233). Cham: Springer International Publishing.

[26] Singh, R. K., & Singh, V. (2024). Beyond Consent: Ensuring Meaningful Protection of Genetic Data Under India's Digital Personal Data Protection Act, 2023. *Journal of Indian Academy of Forensic Medicine*, *46*(4), 562-567.

The Digital Personal Data Protection Act of 2023 says that the plan for an independent Data Protection Authority (DPA) and independent control of forensic data processing are both big changes that need to be made. It should be possible for the DPA to look at both public and private records, look into claims of data abuse, and check to see if organisations are following the rules for data security. If there was this kind of oversight, the DPA would be more likely to take stronger actions, which would make investigative data more accountable in general. Without a doubt, investigative systems that use AI must be checked out and given a seal of approval. The main thing that independent assessors should do is check the algorithmic techniques used in forensic credit-worthy persuasive technologies, like real-time face recognition, data-linking, and pattern analysis, for bias, equality, legality, and bias neutrality. Authorised evaluators who do forensic investigations make it less likely that assistive technologies will be misused, make sure that they work, and keep evaluators from misusing their position to make money.

11. Conclusion

Another novel characteristic of justice in the age of technology is the introduction of privacy barriers in forensic law. Along with the rise of forensic technologies, the infringement of privacy rights and the violation of personal rights becomes more prevalent. Overregulation and underregulation of forensic technologies bring about paradoxical legal and ethical issues. When the justice system employs privacy-invading digital technologies as forensic tools, the inevitable paradox is the need to balance the rights of the individuals with the privacy of fundamental rights.

In considering the safe and legal use of digital evidence, foundational laws such as the IT Act (2000), the Indian Evidence Act (1872) and most recently the Digital Personal Data Protection Act (2023) encapsulate India's stance. Concern should be raised about the lack of doctrinal and practical coherence in these laws, the rapidly evolving technologies, and the world as a digital borderless environment. The functions of digital justice ought to be assistive, not coercive. The coercive nature of digital justice points to a breakdown in systemic trust, which must be rebuilt through institutional capacity, accountability through ethical and technological audits, and adequate judicial oversight.

With advancements in AI, future research and policy should consider the impact of AI-assisted forensic technologies, especially the privacy-preserving techniques of evidence collection. With regards to the balance between innovation and the safeguarding of rights, the main

challenges will be in privacy-preserving computing, blockchain evidence validation, and explainable AI. The advanced forensic ecosystems of the future should prioritize responsibility and transparency, and the inherent dignity of all persons. Technology should serve justice, not the other way around.

Reference

1. Park S, Akatyev N, Jang Y, Hwang J, Kim D, Yu W, Shin H, Han C, Kim J. A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. Digital Investigation. 2018 Mar 1;24:S93-100.
2. Mampilly AJ, Manda VK. Securing Digital Documents: Advanced Cybersecurity and Forensics Techniques for Data Protection. InCyber Security, Forensics and National Security 2026 (pp. 40-68). CRC Press.
3. Katkuri S. Securing the Digital Frontier: Legal Analysis of Cybersecurity, Data Privacy and Cyber Forensics in India. Indian Journal of Public Administration. 2025 Mar;71(1):75-91.
4. Horsman G. Defining principles for preserving privacy in digital forensic examinations. Forensic Science International: Digital Investigation. 2022 Mar 1;40:301350.
5. Babikian J. Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era. Law Research Journal. 2023 Dec 31;1(2):91-101.
6. Omeleze S, Venter HS. Digital forensic application requirements specification process. Australian Journal of Forensic Sciences. 2019 Jul 4;51(4):371-94.
7. Karagiannis C, Vergidis K. Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. Information. 2021 Apr 22;12(5):181.
8. Ogunseyi TB, Adedayo OM. Cryptographic techniques for data privacy in digital forensics. IEEE Access. 2023 Dec 15;11:142392-410.
9. Funta R, Ondria P. Data Protection in Law Enforcement and Judicial Cooperation in Criminal Matters. TalTech Journal of European Studies. 2021 Sep 1;11(2).
10. Jayasekara SD, Abeysekara I. Digital forensics and evolving cyber law: case of BIMSTEC countries. Journal of Money Laundering Control. 2019 Oct 7;22(4):744-52.
11. Marquenie T. The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework. Computer Law & Security Review. 2017 Jun 1;33(3):324-40.

12. Chen L, Takabi H, Le-Khac NA, editors. Security, privacy, and digital forensics in the cloud. John Wiley & Sons; 2019 Apr 29.
13. Seyyar MB, Geradts ZJ. Privacy impact assessment in large-scale digital forensic investigations. Forensic Science International: Digital Investigation. 2020 Jun 1;33:200906.
14. Ramadani EW, Idham R, Fikri ZU, Ridwan MK. Legal Protection Framework for Digital Forensic Experts in The Society 5.0 Era. Walisongo Law Review (Walrev). 2025 Oct 23;7(2):130-42.
15. Ferrazzano M, Raffaella B. Digital forensics: best practices and perspective. COLLEZIONE DI GIUSTIZIA PENALE. 2021:13-48.
16. Malik AW, Bhatti DS, Park TJ, Ishtiaq HU, Ryou JC, Kim KI. Cloud digital forensics: beyond tools, techniques, and challenges. Sensors. 2024 Jan 10;24(2):433.
17. Arshad H, Jantan AB, Abiodun OI. Digital forensics: Review of issues in scientific validation of digital evidence. Journal of Information Processing Systems. 2018 Apr 1;14(2).
18. Goldstraw-White J. LEGAL AND POLICY FRAMEWORK FOR DIGITAL FORENSICS: A RESOURCE FOR PRACTITIONERS.
19. Fakhouri HN, AlSharaiah MA, Alkalaileh M, Dweikat FF. Overview of challenges faced by digital forensic. In2024 2nd International Conference on Cyber Resilience (ICCR) 2024 Feb 26 (pp. 1-8). IEEE.
20. Casey E, Biasiotti M, Turchi F. Using standardization and ontology to enhance data protection and intelligent analysis of electronic evidence. InDiscovery of Electronically Stored Information Workshop 2017.
21. Kazemi SS, Heidari S. Digital forensics and its role in promoting criminal prosecution. Revista Eletrônica em Gestão, Educação e Tecnologia Ambiental. 2021 Jan 1;25:5.
22. Ledbetter EM. *Facing the Challenge: Protecting Data Privacy During Forensic Investigations* (Master's thesis, Utica College).
23. Scheibner J, Ienca M, Kechagia S, Troncoso-Pastoriza JR, Raisaro JL, Hubaux JP, Fellay J, Vayena E. Data protection and ethics requirements for multisite research with health data: a comparative examination of legislative governance frameworks and the role of data protection technologies. Journal of Law and the Biosciences. 2020 Jan;7(1):lsaa010.

24. KAUR G, DHAWAN A. Laws of electronic evidence and digital forensics. PHI Learning Pvt. Ltd.; 2024 Apr 15.
25. Kasper A, Laurits E. Challenges in collecting digital evidence: a legal perspective. InThe future of law and eTechnologies 2016 Feb 23 (pp. 195-233). Cham: Springer International Publishing.
26. Singh, R. K., & Singh, V. (2024). Beyond Consent: Ensuring Meaningful Protection of Genetic Data Under India's Digital Personal Data Protection Act, 2023. *Journal of Indian Academy of Forensic Medicine*, *46*(4), 562-567.

IJLAR