Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 2 (2025)

LEGAL PERSPECTIVE OF DIGITAL EVIDENCES IN THE MODERN JUDICIAL PROCESS: OPPORTUNITIES AND HURDLES

Manish Tandon[1], Dr. Sapna Bansal[2], Dr. Kriti Kaushik[3]
[1]Ph.D Scholar, School of Law, G.D. Goenka University, Sohna, Gurugram, India
[2]Associate Professor, School of Law, G.D. Goenka University, Sohna, Gurugram, India
[3]Assistant Professor, School of Law, G.D. Goenka University, Sohna, Gurugram, India

Abstract
Evidence, whether digital or otherwise, plays a remarkable role in the judicial process for proving any crime. Now it is a pressing need for synchronization between new technology, the legal framework, the judicial process and digital evidence. In this paper attempt is made to probe and scrutinize the urgent need for strong legislative and legal framework to address and resolve the intricacies resulting from the technological development. Breach of right to Privacy (privacy) has the effect of jeopardizing judicial process. The Criminal Procedure (Identification) Act 2022 (TCPIA) is in violation of the law set by the Apex Court. Privacy violations could potentially undermine trust in law enforcement and legal processes. How the veracity and applicability of the digital evidence is examined and tested in court and how the police collect the digital evidences during investigation is the core area for the consideration. There is always a risk of tampering, data fabrication and manipulation, hacking with the digital evidences. The paper aims to propose pragmatic recommendations for bridging these gaps.

Keywords:
Digital Evidence, Privacy, Information Technology, Judicial Process, Investigation, Trial.

Introduction
Digital evidence is defined as the information and data which is kept or stored or received from or transferred by an electronic device. Digital evidence can be acquired when electronic devices such as mobiles, computers, laptops, electronic gadgets etc are confiscated by the prosecuting agencies during investigation and after scrutiny of devices evidences are extracted from these devices. Digital evidences include logs, video footage and images, archives, active data, metadata, residual data, volatile data, replicant data. These digital evidences are used and depended upon by the investigating agencies or parties or stakeholders in trial or court proceedings for proving or not proving any fact or relevant fact.[1] In cyber-crimes such as hacking, phishing, online fraud, cyberstalking, identity theft etc digital or cyber evidences plays a significant role in establishing the cyber-crimes.[2] With the advent of sophisticated technological advancement and information technology in the entire world the perspective, pattern, structure, character and quality of evidences has also undergone significant changes. In criminal investigation, investigating agencies are consistently using CCTV footage, mobile location,

Global Positioning Systems (GPS), Social Media, facial recognition technology (FRT)[3] etc. to locate criminals, crime scenes and documents such as emails, WhatsApp data, phone records as evidences against the criminals.[4] Mere collecting of these evidences by the investigating agencies does not per se proves the offence against an accused but has be proved and authenticated under section 65A and 65B of the I.E.A[5] as held in Anwar P.V v. P.K. Basheer & Ors.[6] The gap in the new laws and the evidences which have taken the new shape due to technological advancement subsist. Undoubtedly, these evidences, if proved by the police or defense or if they stand on their legs and believing these to be substantiated, conviction or acquittal of an accused will ultimately culminate in a fair trial against an accused without prejudicing the rights of an accused but the aforesaid is a big challenge in the present scenario qua digital evidences. There is gross abuse of power[7] leading to violation of privacy and ultimately rule of law is not sustained in the judicial process. It is an arduous task for the police force or CBI to balance the privacy interests and the enforcement of Law where crimes are of serious nature, crimes against National Security etc.[8] The authorities exceed their surveillance powers to collect the comprehensive evidences and data or conduct obtrusive investigations and encroach in to privacy of people. TCPIA[9] authorize police officers and prison officers to collect biometric data such as finger, palm, foot print impressions as mentioned in section 53 and 53A of CrPC[10] from convicted and arrested persons and the collection of the personal data is in violation of privacy and Article 21 of the COI[11]. Privacy is an inherent part of Article 21 as held in Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.[12]

Laws Relating To Digital Evidences In India

The various laws include substantive and procedural laws i.e. Constitution of India, IEA, BSA[13], CR.P.C, BNSS[14] BNS[15], IPC, DPDPA[16], ITA[17] TCPIA Information Technology (Reasonable Security Practices and Procedures & sensitive personal data information) rules, 2011 etc. As per Section 66E of the IT Act, 2000 an individual's privacy is considered to be violated if anyone captures, publishes or transmits the image of the individual's private body parts non consensually and liable for prison or fine or with both. Under Section 72A of the ITA, on disclosure of

personal information by any person or intermediary he shall be liable for prison or fine or with both.
The DPDP Act has been enacted for the protection and security of personal data of users. The act confers rights on the individuals to protect their personal data and obligations on the entities that process personal data. This act has replaced the information technology rules 2011 and Section 43A of the ITA. This act is still not in force.

Though many scholarly articles, papers and blogs have written and research has been conducted on the present topic and different facets of the theme but they overlooked the process of courts to deal with the digital evidences in the various judgments and proceedings. The settled law on diverse perspectives of digital evidences, legal provisions qua admissibility, mode as laid down by the Courts through various judgments and court proceedings is the research gap attempted and highlighted herein with its relation and impact on the Privacy.

Judicial Pronouncements

In Arjun Panditrao Khotkar v. Kailash Kushan Rao Gorantyal and Others,[18] court has overruled Tomaso Bruno v. State of UP,[19] Shafhi Mohammad v. The State of Himachal Pradesh,[20] and judgment dated 03.04.2018 as Shafhi Mohammad v. The State of Himachal Pradesh,[21] passed in ignorance of Law and also ruled that the law promulgated in Anwar P.V v. P.K Basheer, as clarified in this judgment is fixed on section 65B. It was observed and suggested by the apex court that the most of the nations of the world have tuned and amended their legislations in consonance with the upgraded and developed technological advancement in the domain of information and technology to mitigate disputes. Hence, it is imperative and inevitable that section 65B be revisited in view of the developed technological advancement in the domain of information and technology and to keep pace with developed technological advancement. Section 65B of IEA was introduced twenty years back, by the IT A[22] and from inception there is a judicial confusion qua this section and law has been fluctuating from State (NCT of Delhi) v. Navjot Sandhu[23] to Sonu v. State of Haryana[24].

The legislative evolution in USA, United Kingdom and Canada qua admissibility of digital evidences is at much more pace than in India. In USA under the FRE[25] there is recognition of several alternatives to produce an electronic record. There is provision to either follow the rule 901 or rule of self-authentication under rule 902 followed by certificate of authenticity. In case titled as Lorraine v. Markel American Insurance Co.[26] in which when facing the problem of admissibility of emails, the court conferred trust on the said rules and amendment under sub−rules.

In an article[27] distinct methods and rules of authentication of ESI[28] are elucidated.

I. E.A was enacted in 1872 where as FRE was adopted in 1972. In U.S, after enactment of the rules in 1975 various modifications were made periodically caused by inadequacy of the rules to address the developing circumstances. Consequent of aforesaid amendments choices are available to the litigants who are relying upon the ESI and sub rule (13) and (14) of FRE, 902. This expansion in U.S proves that in U.S evidence law has a balance with technology but in India the same has not happened.

II.

In Arjun Panditrao Khotkar case, following directions were issued by the Apex Court:

a. For the mobile carrier companies to maintain the call detail record and other records for the concerned period, which are captured during investigation by the investigating authorities. Such records could be summoned during trial. The aforesaid directions are applicable till provisions are not made under section 67C of the IT act.

b. When the original document is produced certificate[29] is not required.

c. For safeguarding the digital record produced in the criminal trial, appeals desired provisions may be framed.

It was ruled that certificate can be produced during the trial. Section 65B is a self-contained Code and being special provision the general law on secondary evidence under section 63 and 65 of the I.E.A shall not be admissible unless the required procedure of section 65B are complied with.
The court also held that the CCTV Footage unreliable due to deficiency in the investigation, as the source of the CCTV footage and its creation was doubtful, the witness who recorded the CCTV footage failed to provide consistent source of obtaining video and further transferring it from mobile to CD, CD was not sent to the CFSL for verification and certificate was prepared by an unnamed police official.

In Mohd. Arif Alias Ashfaq v. State (NCT of Delhi),[30] the ruling in Supra Note 18 and 6 has been reaffirmed. The admittance of electronic evidence i.e CDR (Call detail record) was in controversy. The Court had ruled that without appropriate certificate the electronic evidence i.e CDR is not admissible and must be eschewed.

In P. Gopalkrishnan @ Dileep v. The State of Kerala and Anr.[31] The internal strife of fundamental rights emerging from Article 21 i.e. right to fair trial of the accused and privacy of the victim (in present case of rape) was in dispute and court directed that:

(i) in such situation the court has to harmonize both sides to elevate Rule of Law.

(ii) electronic record i.e. contents of the memory card/pen-drive (video footage/clipping contained therein) are evidence as per section 3 of the I.E.A, Section 29 of the IPC and document under section 2 (1) (t) of the IT Act.

(iii) If the investigating authority is relying upon the electronic record against accused, accused must be provided with the replica of the same in compliance to Section 207 and 173 of the Cr.PC to allow him to present his defence .

(iv) that instead of providing the replica of the memory card/pen-drive the court had allowed only inspection thereof to the accused/lawyer or expert for their defence and that accused can also ensure about its reliability by taking second expert opinion from an independent agency i.e Central Forensic Science Laboratory (CFSL) as State FSL had also given its first opinion.

(v) For keeping the second opinion confidential by not allowing the access to any other agency or person till the final outcome of the case.

In Taqdir v. State of Haryana,[32] The involvement, culpability, conviction and sentence of life imprisonment under section 302/120-B/149 of IPC was affirmed. It was affirmed that courts below had rightly depended upon the electronic evidences i.e CCTV Camera Footages, Hard-disk, Compact Disc, pen drive and requisite certification as they were completely supported by the requirements and could be read as evidence on record.

In Ravinder Singh alia Kaku v. State of Punjab,[33] the substantive question of law was if the oral evidence instead of certificate regarding call records is admissible as evidence. Relying upon the settled law in Supra Note 10 and 13 it was ruled that for admissibility of call records certificate is obligatory in Law and oral evidence for such certificate regarding call records would be inadmissible. The High Court order and conviction of A2 under section 302 and 364 of the IPC was overruled. The acquittal of A1 and A3 was upheld.

In Union of India and others v. CDR Ravindra V. Desai,[34] it was held that:
(i) report of call data record submitted with certificate is reliable.
(ii) non production of the certificate on an earlier occasion is a curable defect.
In State by Karnataka Lokayukta, Police Station Bengaluru v. M.R.Hiremath,[35] It was held that:
(i) Certificate should also be produced during trial with the electronic record.
(ii) Court was mistaken in inferring that the default to produce a certificate with the chargesheet (i.e when chargesheet was filed) was disastrous.

In Smriti Madaan Kansagra v. Perry Kansagra,[36] The certificate filed under Section 65B (4) in respect of the emails did not certify the source of the messages allegedly received and therefore certificate was not genuine, authentic and as per Law
In William Stephen v. The State of Tamil Nadu and Anr,[37] The record relating to the call details has been discarded by the Court due to lack of certificate. Since, the Investigating officer (IO)

had no understanding of the procedure for obtaining certificate so it was not filed and not responsible as proper training was not imparted to him. Hence, it was directed to government to impart proper training to the Police officers qua obtaining and filing of certificate.

In State of Maharashtra v. Dr. Praful B. Desai,[38] it was held that evidence can be recorded in criminal case through electronic records such as video conferencing. As such the evidence so recorded is being recorded in the presence of accused as per the requirement and procedure of section 273 of Cr.PC. Evidence of a witness can be recorded by video conferencing as per section 274 Cr.PC and is permissible only if the witness is in a country which has extradition treaty with India and under the laws of such country contempt of court and perjury are also punishable. Commission can be issued under section 284 Cr.PC for evidence recording through video conferencing where witness presence cannot be procured and he belongs to other countries.

In State of Karnataka v. T. Naseer @Naseer Thandiantavida Naseer @ Umarhazi @ Hazi & Ors.[39] During investigation certain electronic devices such as laptop, external hard disc, pendrives floppies, Compact Disc (CDs), Sim cards, mobile phones, memory card and digital cameras were seized and original electronic devices were submitted before the court along with additional charge sheet. The court had passed the order that the CFSL report of electronic devices was not admissible in evidence without certificate. When said certificate was produced trial court ruled that the certificate was inadmissible in evidence. Thereafter, an application under section 311 of the Cr.p.c was filed before the trial court to allow the prosecution to produce certificate. The application was rejected by the court due to delay in filing the same. Trial Court order was upheld by the High Court. The apex Court ruled that the courts below had erred in concluding that there was delay of six years in producing the certificate. Further, the trial was still pending when the said application was filed to produce certificate. The certificate endeavored is not evidence created now but of earlier act and will not result in irreparable loss to the accused. Application was allowed reversing the courts below.

In Central Bureau of Investigation v. R. Vasudevan & Ors,[40] Hard discs were seized by the CBI during investigation and before filing of the chargesheet, but were neither deposited to the Trial Court/Magistrate nor the same constituted the chargesheet in compliance to section 102 of the Cr.PC. CBI had filed an application under section 91 of the Cr.PC when the case was fixed for pronouncement of judgment for placing on record hard disks as additional documents and it was dismissed vide order dated 13.05.2022 but was challenged by CBI. High Court while dismissing the said petition of the CBI had held that CBI had not filed the Hard Disks due to inadvertent mistake or oversight or unavailability with the CBI while filing final report (S-173 Cr.PC) before the commencement of trial. Therefore, test to produce additional documents i.e Hard disks is not satisfied. If the CBI is allowed to place on record the Hard Disks than it will violate the constitutional guarantee of speedy trial of accused under Article 21 and will cause grave prejudice to the accused who have disclosed and revealed their entire defence. Since the delay in the trial is caused by CBI and at the point trial has just concluded and fixed for pronouncement of

judgment, therefore court did not allow the additional documents/Hard Disks due to the lack of promptitude and alertness of CBI which is amenable for this situation.

In Supra Note [41] as evidence of the calls made and received on a particular telephone number print out of the telephone call made on mobile number was taken. It was ruled "where a machine observes a fact and records it, that record states a fact. It is evidence of what the machine recorded and this was printed out. The record was not the fact but the evidence of the fact".

The corresponding section of section 65A & 65B of the I.E.A is section 62 & 63 of the Bhartiya Sakshya Adhiniyam 2023 having same title without any change. On comparison of the same provisions of the old and the new act it is clear that slight variation has been brought by the legislature in section 62 & 63 of the Bhartiya Sakshya Adhiniyam 2023 (BSA). In comparison to the advancement in U.S, sections 62 & 63 of the BSA have not been refined in accordance with developed countries.

The conception of privacy includes within its scope inherent rights of a person to have control over his or their personal information, activities without any interference or violation or intervention by an individual or agency or entity qua those privacy rights and specially the Government.[42] The significance of private rights gets escalated amid investigation of crimes since the investigating agencies encroach in the personal affairs for collecting the personal data and thereby violates the privacy. It is not the unrestricted right of neither the investigating agencies to encroach in to the privacy during investigation nor of a person to abstain from providing the requisite information required for fair investigation but nevertheless a balanced approach is inevitable to protect the privacy while implementing efficacious law enforcement. If we examine the historical development of privacy rights in the USA, we will find in the fourth amendment of the charter which aimed at protecting the individuals from indefensible governmental invasion and the same is protected in the Bill of Rights. This right protects the individuals from unreasonable searches and seizures, safeguard and secure in persons, houses and effects etc. In Katz Versus United States (1967)[43] this right had achieved new dimensions and also broadened the gamut of fourth amendment by allowing the privacy in public spaces. This decision had emphasized that it extends beyond physical spaces which has implications on electronic privacy and supervision.

In Supra Note 12 it was concluded that "privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, and procreation, the home and sexual orientation. Privacy also connotes a right to be left alone.

Interpretation

It is evident that in present time digital and electronics evidences are key component of the judicial process whether it is civil cases or criminal cases or otherwise. It is demonstrated by the various Court judgments that all the participants of the system whether it is police or lawyers or

judges or litigants have to handle the digital evidences. Despite being various laws in our country it remains a hurdle for the investigating authorities to collect and prove successfully the digital evidences. From the above judgments it is evident that many times attributable to fine technicality of law or lack of proper training to deal with the digital evidences etc. the electronic evidences produced by the prosecution have not stood on their legs before the courts. At present Indian statutory provisions or Laws available for proving digital evidences are not developed to such extent as in USA or other developed countries. Even in other countries such as Canada and United Kingdom law has developed at much faster pace than in India. The privileges of digital evidences have helped in discovering the hidden crimes but it has far reaching negative ramifications in infringing the Privacy of the Individuals. In handling digital evidences courts have secured that fair trial of an accused is not infringed.

Conclusion

The TCPIA has been approved by the parliament and consent of the President was given on 18th April 2022 or become law and came in to force on 4th day of August 2022. This act has replaced the IPA[44] which was the law enacted by the Britishers. TCPIR[45] were notified on September 19, 2022. TCPIA has come before BSA, BNSS, BNS and the word 'criminal procedure' is not erased from the name of this Act nevertheless, Cr.p.c, has been repealed and replaced by BNSS hence TCPIA should also be amended at various places, including, where ever reference is made in the act to the Cr.p.c it should be in consonance with the BNSS. The TCPIA has been enacted to authorize the police or prison officer to take the "measurements" of the prisoners etc for investigation, identification, preserving records in crimes. The word "measurements" under section 2 (1)(b) include various kinds of human impressions, samples of body parts and prints etc and those under section 53 or 53A of the Cr.PC. As mentioned above and also reiterated that the collection of the personal data is in violation of privacy which is integral part of Article 21 and also in violation of Supra Note 12. The impact of such enactment is that there will be no personal room for the people and the authorities may misuse the power for corrupt purposes. The word used in section 3 i.e 'shall' indicate that criminal or under trial shall be compulsorily required to provide the private information to the police or prison officer and will give non consensually.[46]

Indian data protection and privacy laws are not strict. They are at the initial stage and still evolving.

From the aforesaid, it is also ostensible that notwithstanding that there are penal provisions (Section 66E and 72A) in the Laws but still a dire need to balance the possibilities and confrontations, while dealing with the digital evidences.

Suggestions

(i) Laws relating to admissibility of electronic or digital evidences should be at par with the Laws of other developed countries such as USA or UK or Canada etc and in tune with developed technological advancement so that there is recognition and availability of more than one option while seeking to produce an electronic record.

(ii) Section 62 & 63 of the BSA 2023 be revisited.
(iii) For protecting the Privacy Rights strict provisions should be made, adhered and complied.
(iv) Investigating agencies should also be liable for breach of Privacy and strict penal provisions should be made and implemented for the same.

Reference

1. *Casey, E. (2011).* Digital evidence and computer crime: Forensic science, computers, and the internet *(3rd ed.). Academic Press.*
2. *Kesan, J. P., & Hayes, C. M. (2012). Mitigative counterstriking: Self-defense and deterrence in cyberspace.* Harvard Journal of Law & Technology, 25*(2), 429–484.*
3. *Kerr, O. S. (2005). Searches and seizures in a digital world.* Harvard Law Review, 119*(2), 531–585.*
4. *Volonino, L., & Anzaldua, J. (2008).* Computer forensics: Principles and practices. *Pearson Prentice Hall.*
5. *Brenner, S. W., & Goodman, M. D. (2002). The emerging consensus on criminal conduct in cyberspace.* International Journal of Law and Information Technology, 10*(2), 139–223. https://doi.org/10.1093/ijlit/10.2.139*
6. *Wall, D. S. (2007).* Cybercrime: The transformation of crime in the information age. *Polity Press.*
7. *Solove, D. J. (2006). A taxonomy of privacy.* University of Pennsylvania Law Review, 154*(3), 477–560. https://doi.org/10.2307/40041279*
8. *Rogers, M. K. (2006). A two-dimensional circumplex approach to digital forensic examination processes.* Digital Investigation, 3*(3), 137–147. https://doi.org/10.1016/j.diin.2006.06.003*
9. *Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions.* Computers & Security, 30*(8), 719–731. https://doi.org/10.1016/j.cose.2011.08.004*
10. *Sharma, R. S., & Sharma, M. (2025). Hydropower in South Asia: Challenges, resilience, and sustainable development in the face of climate change and socio-political dynamics. American Journal of Climate Change, 14(2), Article 142016. https://doi.org/10.4236/ajcc.2025.142016*
11. *National Institute of Standards and Technology. (2006).* Guide to Integrating Forensic Techniques into Incident Response *(SP 800-86). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf*
12. *Jaishankar, K. (Ed.). (2011).* Cyber criminology: Exploring internet crimes and criminal behavior. *CRC Press.*
13. *Cohen, F. (2010).* Digital evidence and computer crime. *Aspatore Books.*
14. *Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015).* Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence. *RAND Corporation. https://doi.org/10.7249/RR890*
15. *Bharadwaj, A., & Lalitha, S. (2020). Admissibility of digital evidence in Indian courts: An overview.* International Journal of Law Management & Humanities, 3*(4), 1366–1373.*
16. *Singh, P. (2019). Legal challenges in digital evidence: A study on Indian evidence act.* International Journal of Advanced Research in Law and Social Science, 1*(2), 25–31.*

17. *Kapoor, R., & Sharma, D. (2021). Digital evidence in the legal process: Issues and challenges.* International Journal of Legal Developments and Allied Issues, *7(3), 220–235.*
18. *Sharma, A. (2018). Digital forensics and its relevance in criminal justice system.* Indian Journal of Law and Justice, *9(2), 91–103.*
19. *McKemmish, R. (1999). What is forensic computing?* Trends & Issues in Crime and Criminal Justice, 118, *1–6. https://www.ojp.gov/ncjrs/virtual-library/abstracts/what-forensic-computing*
20. *United Nations Office on Drugs and Crime (UNODC). (2019).* Practical Guide for Requesting Electronic Evidence Across Borders. *https://www.unodc.org/documents/organized-crime/UNODC_Practical_Guide_Requesting_Electronic_Evidence_Cross_Border.pdf*
21. *European Union Agency for Cybersecurity (ENISA). (2021).* Challenges of the digital evidence chain of custody. *https://www.enisa.europa.eu/publications/challenges-of-the-digital-evidence-chain-of-custody*