INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

DIGITAL EVIDENCE AND CYBER LAW INTEGRATIONS

AUTHORED BY - PRASOON RANJAN,
IIMT COLLEGE OF LAW

CO-AUTHOR - AVILIPSA PALTASINGH,
INDORE INSTITUTE OF LAW

Introduction

Digital evidence can be defined as incorporating any data that is electronic in nature and is admissible in a court of law. This covers email communication, messages in most forms of communication, documents in electronic form, posts on social sites, and information from computers or smartphones. Digital evidence is described as a rather extensive construct which entails files and content, data about data and activity that captures and documents users' action on the computer or a system.

On the other hand, cyber law is identified as the legal matters connected with application of information technology and the internet. The relation to cyber it comprises laws that regulate cyberspace, electronic business, and cyber criminality. Within its sphere of interest cyber law encompasses a vast array of legal fields that regulates the ownership of ideas, access to information, freedom of speech and privacy of data.

Cyber law gives legal guidelines for the prosecution of computer evidence, that is, this law sets the standards on how that evidence is going to be collected, held and produced in court. While more engagements shift to the digital domain, the utilization of digital evidence is increasingly evident in the judicial systems. Internet law determines how this evidence is dealt with, how citizens' rights are to be observed, and justice is to be served. Therefore, digital forensics is involved in the locating of all evidence to be used in court while cyber law is the law regulating all activities within the cyber space.

 ISSN: 2582-6433

Digital Trails

In the present society, use of digital evidence together with the cyber laws has been deemed a major factor in enhancement of deliverance of justice. Electronic data, also called digital data, which are data in electronic form, are also extensively used in civil and criminal inquiries and include emails, text messages and SMS, social network updates, files stored on a computer or a network, and logs. Digital profiling can be defined as the detailed track of a user's activities that may be traced with great ease in order to get some important information in the case. These are important digital trails in cyber law whereby crimes committed are beyond geographical regions and thus can hardly employ traditional crime detection methods of collecting physical evidence.

Law Enforced and Regulatory Agencies

The law enforcement agencies and other regulatory bodies such as the police and specialized cybercrime units have the responsibility of handling Cases of digital evidence and implementing cyber law to keep law and order maintained in society. To that extent, law enforcement officers, particularly the police and demarcated cybercrime investigation units, have the mandate to investigate cybercrimes and gather evidence in digital form and to ascertain the admissibility and reliability of the same. Most of them employs various forms of gadgets, applications, and tools that help them in tracking footprints, retrieval of deleted data and analysis of electronic devices for evidence.

The concepts of digital evidence and cyber law are the components of the legal framework especially with the increase in the rates of digital transactions and cyber activities. Therefore, documents sent by e-mail, posts on social networks, and other digital materials can be regarded as the key elements of civil and criminal cases. The Indian cyberspace and digital evidence are regulated by the Information Technology Act, 2000 commonly referred to as the IT Act. According the section 65B of the Indian Evidence Act, 1872 the digital evidence can be produced in the court if and only if the production and certification of the electronic record meets some conditions. This integration has been supported by several leading cases. The Social issue that we wish to address is the reliability and admissibility of Evidence through Video Conferencing in recording witness deposition which has been illustrated in the following case of State of Maharashtra vs Dr. Praful B. Desai (2003) where, the supreme court upheld the use of video conferencing techniques in recording the testimonies of witnesses as & tech is

 ISSN: 2582-6433

playing important role in Judicial System.

Another important case is Anvar P V v P. K. Basheer (2014) where Supreme court of India framed some main principles for the admissibility of electronic evidence, where without following the Section 65B of the act it was held that such electronic evidence cannot be admitted by any court of law.Latest, in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), the Supreme court restated that Section 65B certification is mandatory for the relevancy of the digital evidence. It has become evident from these cases that the integration of digital evidence is not a static process in India's legal framework and further proves how the judiciary is trying to maintain the proper use of technology and legal principles to authenticate the digital evidence.

Understanding Cyber Forensics and Information Security

To focus the inclusion of both the digital evidence and cyber law, it is essential to know about the cyber forensics and information security in India. Cyber forensics involves the recovery, identification, examination, and reporting of digital clues that are admissible in the legal procedures. Information security, on the other hand, is defined as the prevention of information from becoming available or reachable to an unauthorized individual or system in a form that is not reliable, usable or exploitable.

In India for Cyber law, the Information Technology Act, 2000 is the main act that deals with the aspects of cyber law and encompasses topics such as, cyber trial, digital evidence etc. The Act enables the police and other security forces to investigate cybercrimes and requires the use of electronic evidence in court. One important legal precedent in this regard is State of Maharashtra vs Dr Praful B Desai (2003) where the Apex Court of India endorsed video conferencing reference for taking evidence which is the recognition of digital evidence.

Understanding Cyber Forensics and Information Security

To focus the inclusion of both the digital evidence and cyber law, it is essential to know about the cyber forensics and information security in India. Cyber forensics involves the recovery, identification, examination, and reporting of digital clues that are admissible in the legal procedures. Information security, on the other hand, is defined as the prevention of information from becoming available or reachable to an unauthorized individual or system in a form that is

 ISSN: 2582-6433

not reliable, usable or exploitable.

In India for Cyber law, the Information Technology Act, 2000 is the main act that deals with the aspects of cyber law and encompasses topics such as, cyber trial, digital evidence etc. The Act enables the police and other security forces to investigate cybercrimes and requires the use of electronic evidence in court. One important legal precedent in this regard is State of Maharashtra vs Dr Praful B Desai (2003) where the Apex Court of India endorsed video conferencing reference for taking evidence which is the recognition of digital evidence.

Another precedent is Shafhi Mohammad v. State of Himachal Pradesh (2018), wherein the Supreme Court of India held that electronic evidence shall be admissible even in the absence of a certificate in terms of Section 65B of the Indian Evidence Act if the said evidence is reliable and it serves the justice.

India has also witnessed the presence of Indian Computer Emergency Response Team (CERT-In) that works towards the improvement of the cyber security in India through reaction to the incidents of the cyber attacks and cyber security, through putting out advisories and promoting the practices. Cyber forensics and information security is well supported by such measures including the Digital India campaign which seeks to make India a digitally empowered society and a knowledge economy.

Cyber forensics can be explained with the help of an example – Mumbai's 26/11 attack case in which, VoIP calls and emails as the specimen of digital evidence turned to be very useful in identifying the criminal. Primarily, this case brings out the importance of sound cyber forensic and considerable information security to minimize or eliminate fabrication and doubts to the credibility of digital evidence in combating cybercrime.

Understanding Types of Digital Evidence

The various categories of digital evidence assist investigators and forensic experts in collection, analysis, archiving, and applying different techniques on digital evidence in criminal investigations to adequately meet the current world's complexity. The types of digital evidences are mentioned below: -

 ISSN: 2582-6433

- Logs – These are files containing descriptions of the events that occur in a computer system or a network. They are created by diverse computer applications and subsidiary equipment to measure and monitor use, entry, and treatment. One example of logs is web logs which is a record of all the requests made to a web server and system logs which record events concerning the operation being performed by the operating system for instance user log in, file access and errors. The first log is critical when reviewing or investigating a security breach or an intrusion attempt, because it supports the timeline of occurrence of activities when the intrusion was detected or before.
- Video Footage and Images – Tape recordings and still pictures mean motion pictures and photographs that can actually be used in law suits. These can be recorded either through other individuals, security cameras, mobile phones, surveillance systems or other gadgets. For example, video recorded by a security camera may depict a suspect in a crime scene and/or their movement, while a photo taken by a smart phone may depict an event or object related to the case. Any videos or images used as evidence have to be dealt with in a manner that does not alter their quality and that they remain entirely genuine.

  In a landmark case of State of Maharashtra v. Dr. Praful B. Desai (2003), Supreme Court allowed the use of video conferencing as a mechanism for recording evidence. The case involved a doctor who became a witness in the case however the said doctor happened to be in the United States. Therefore, the court noted that video conferencing was allowed under Indian law and evidence could be recorded through the means. The importance of this judgment can be expressly seen as it evidenced the changes in the technological progress and their acceptance within the judicial trials, which led to the usage of technology to obtain evidences remotely. Since this decision, the legal process has benefited as witnesses have been given the chance to provide their testimonies without having to be present in court, so makes the judicial system more flexible.
- Archives – Archives are areas that are comprised of records and documents in digital format, that is stored for long term usage. These may be emails, records of monetary transactions, database, other vital documents, or anything that is digital. Legal and regulatory compliance is the most common application of archives since key information gathered in the past is essential in the future. For example, an organization may need to keep emails after their specified periods to meet the set legal regulations and look for emails if they will be useful in case of a legal case.

 ISSN: 2582-6433

- Active Data – It is defined as data that is presently being used or data that is stored in any computer system. This covers the files, documents that any user may open and work on together with the applications and databases that are in a running state. It is readily available and can be obtained right from storage units of the data system. For example, an investigator may get active data out of a suspect's computer in a bid to unravel documentation or information of criminal acts.
- Metadata – It is the information about data and its properties and environment it originates from. Such metadata may include the author of a document, the time of their creation/last edit including year, month, day of the document and even the country/region where the photo was taken. Integrated metadata is very important in digital investigations since it holds useful information about the creation, history and possibly the credibility of the digital evidence. For example, the email headers can point out the IP address of the sender, thus, determine the source of the email.
- Residual Data – It is also referred as data remnant or data residue that remains on a storage device after an attempt to delete it. This can contain bits and pieces of files that have been deleted, files of programs that were uninstalled or data that is left in an unused disk space on the hard drive. Some other data may be found after cases, and their traces can be uncovered with the help of the so-called forensic applications, thus obtaining important evidence. For example, the investigators can obtain minor artifacts from a suspect's computer that got deleted containing important information.
- Volatile Data – It is a class of data that is stored in a computer's RAM commonly referred to as Random Access Memory that is cleared when the computer is shut down. This consists of details regarding the currently executing programs, open connections in the network, and other transient files. Volatile data may be necessary in such applications as real-time investigation of the environment, that is, searching for active malware or the system snapshot at a given time. For example, a forensic investigator might acquire volatile data from a suspect's computer to examine connections and processes that show activity of illicit actions.
- Replicant Data – It is a duplicate of the original data that can reside on another location or perhaps another device. This can mean backups, files that are kept in sync across devices, or copies made for the purpose of redundancy, or in case of a disaster. It guarantees that even if the original data input has been destroyed or is in the wrong format replicant data input will still be available.

 ISSN: 2582-6433

Collection and Preservation of Evidence

The process of searching, capturing and storing digital evidence points to the fact that the gathering of evidence requires attention to various small aspects and the reference to the legal and technical standards. In managing digital evidence its admissibility in the courts and has improved its reliability, especially during trial. Therefore, the approaches of digital evidence collection and preservation are still critical in any case solution to confirm the credibility and admissibility of electronic information in the court.

Collection

The collection is a concept understood to denote a procedure or process where different methods are used to gather information likely to be of importance in a court case or later investigation. This has to be done carefully so that the evidence itself is not altered in any way that makes it unreliable. Key steps involved in the collection of digital evidence are: -

- Identifying Sources – If there were a cyber incident, decide where potential digital evidence might be found. This ranges from computers, smart phones, servers, Cloud storage, emails, social media accounts and Internet of Thing's (IOT) devices.
- Using Appropriate Tools – Data extraction software and hardware are important to ensure that the data is retrieved with minimal manipulation of the raw results. Software that enables to make a duplication of data includes forensic imaging that allows the original data to be kept unchanged.
- Documenting the Process – The documentation process of collection has to be concise to ensure that each collection process is well recorded. This would contain information answering questions such as where the evidence was retrieved from, how and what kind of tools were used. That documentation is needed often for preservation of evidence and for the chain of custody.

Preservation

Preservation refers to the protection of the gathered evidence from changes or losses. To conserve its integrity from collection to court presentation, this is necessary. Some of these measures include:

- Maintaining Chain of Custody – Chain of custody indicates how evidence was handled right from when it was collected up to when it got into court. This involves who

 ISSN: 2582-6433

recovered it, who had control over it, and where and how it was kept and moved around. It helps to ascertain whether any tampering took place or not.

- Secure Storage: To ensure that no other person or process gains access to the evidence and alters it maliciously or destroys it, the evidences are required to be secured. Encryption of storage devices for example virtual private servers and physical security are used.
- Creating Forensic Copies: All digital evidences are duplicated with the use of forensic copies or images. These duplicates helps in analysis such that; the original evidence is preserved as an original version in case it is required later.
- Regular Audits and Checks: It is important also to check and audit the stored digital evidence on a regular basis to ensure its genuineness and safety. It helps in early detection of any possible challenges that might occur at that time and ensure that the articles themselves remain reliable before any mishap occurs.

While collecting and also storing the evidence, one has to fullfill the legal requirements and regulations so that the evidence becomes admissible in court. This includes the following: -

- Adherence to Legal Protocols – As per the guidelines and the certain processes mentioned in the Information Technology of India Act or other legal documents that talks and prescribes about the Electronic Evidence, rules must be followed during collection and preservation of digital evidences.
- Obtaining Necessary Warrants – The collection of any digital evidence should be done in compliance with the provisions of the law unlike breaking the constitutional provisions.
- Respecting Privacy and Data Protection Laws – This is adhering to the legal requirements of the GDPR (General Data Protection Regulation). For instance, as it safeguards the privacy rights of individuals within the process of collection and handling of digital evidence.

In the case of Arjun Pandit Rao Khotkar v. Kailash Kushanrao Gorantyal (2020), the Supreme Court explained the missing ingredients of Section 65B of the Indian Evidence Act. It made a ruling declaring that compliance with the requirement of a certificate is essential for the admittance of electronic records. This decision emphasizes the need for proper authentication of electronic evidence to ensure that only acceptable substantive and admissible evidence is

 ISSN: 2582-6433

admitted in the court. It also assists in escaping the abuse of digital evidence and therefore assists to retain integrity in the judicial system as it embraces modern technology.

Analysis and Examination of Digital Evidence

Digital evidences are analysed and examined in the following ways: -

Forensic Analysis

Cyber law involves use of digital forensics as in light of examining and or analysing digital evidence. Forensic analysts or digital forensic experts are skilled people who manage to collect and oversee the details of the computer-based evidence within court sentences. They use several forms of forensic science and equipment to investigate chips, computers, and networks. Some of the widely used methods of forensic analysis include data acquisition, which involves making an exact duplicate copy of a storage media to ascertain its property without any possible change to the data within the storage device. Two well established tools used by analysts to analyse the digital evidence include EnCase and FTK (Forensic Toolkit). Another challenge is the modification of data, such as encrypted and deleted information, which is crucial in the forensic investigation process. Encryption as a security measure might render certain data unavailable to the case investigation team. Therefore, digital forensics investigators rely on special software and methods to crack encrypted information and also recover accidentally erased files and messages

Legal and Ethical Considerations

It is common acknowledged that in every case of digital investigation, the legal and ethical issues need to be taken into account in order to be certain of the admissibility of the digital evidence in court. Ethical considerations involve privacy as press time gathers and analyse the digital evidences. Also, in the process may access the individual's personal data in the electronic gadgets or online profile. Legal guidelines governing the examination of computers set legal requirements for how evidence in computers is to be identified, retrieved, and processed to meet the evidentiary requirements in court. Some of these standards inevitably differ across jurisdiction and depend on the specifics of a case, yet they demand lawful and fair means of evidence collection. There are several ethical practices in digital forensic that include impartiality, confidentiality, and appropriate utilization of the tools and software involved in the process. In a similar manner, ethicality principles call for the forensic analyst to be ethical in handling of digital evidence to ensure the evidence is accurate and the justice system is not

 ISSN: 2582-6433

unfair. Therefore, it can be said that digital forensics outlines the proper ways that can be used to obtain and analyse the digital evidence in a legal and ethical manner which will have respect to the privacy of individuals involved.

How Digital Evidence Is Different From Physical Evidence

Digital evidence and physical evidence can be classified as fundamentally differing in terms of the distinctiveness of their collection, analysis, and admissibility as well as in the context of their use in legal trials and cases. Digital evidence refers to any information in the form of data whether stored or transferred in a digital format including emails, computer files, posts in the social media, and networking logs among others. However, physical evidence entails any items in the crime scene entailing documents, fingerprints and footprints on the crime scene, weapons, and even body fluids.

The major difference between these two pertains to the nature and stability of the objects. Computer-related evidence is by its nature difficult to render tangible and can be modified, copied, or deleted with a minimum of effort. For instance, a single stroke of a key in typing can wipe out a whole string or email thread or change text in a document. This nature requires strict measures in the collection, storage and documentation process in order to protect its genuineness and legibility in the court. On the other hand, physical evidence is normally subjected to relatively simpler methods of preservation and identification since it is easily quantifiable in terms of physical characteristics.

The collection and the flow of the electronic evidence are also quite distinct. Digital evidence is difficult to capture, store and analyse without distorting the material and this is why special tools and methods have to be employed. Also, the digital forensic professional has to see whether the data is altered or not. On the other hand, physical evidence is dealt with using seals, bags, and proper recordation of everyone who comes into contact with the physical item.

As a matter of law, digital evidence always requires different rules and concerns with regard to the admissibility of the evidence. Judiciary systems inevitably get faced by cases where the underlying digital evidence may be fake, exaggerated, outdated or irrelevant, in areas where digital evidence is abundant it is easy for it to be forged and therefore the judiciary assesses the credibility of the evidence. In India, the Indian Evidence Act, 1872 incorporated provisions regarding digital evidence called as Section 65B that is related to circumstances where

 ISSN: 2582-6433

electronic records are considered admissible.

A precedent Anvar P. V. v. P. K. Basheer (2014) is an case concerning the Supreme Court's affirmation of the need to comply with Section 65B standards for electronic evidence. This is a message to the common practice of the court of using electronic evidence without the necessary certificate as provided under section 65B and making it clear that electronic evidence needs to be accompanied by proper legal procedures.

Therefore, there is a clear fact that both digital and physical evidence are vital tools that are utilized in a legal proceeding, however they are different in ways. The fusion of digital evidence and cyber law requires detailed processes of addressing the evidence by law enforcement agencies and a profound understanding of the legal requirements concerning the electronic records.

Hurdles In The Integration Of Digital Evidence And Cyber Laws

The field of digital evidence and cyber law encompasses complexities of jurisdiction, technicalities, legal gray areas, privacy, and the dynamic and evolving nature of cyber threats. Solving these issues calls for collaboration of policy makers, police forces, legal adviser's international organizations and researchers on framing effective, flexible and integrated measures that can have corresponding pace with the technological advances and can ensure safety and liberty to the society. These challenges are mentioned below: -

- Jurisdictional Challenges

  An issue as basic as jurisdiction is perhaps one of the most critical issues in digital evidence and cyber law. Most cyber criminals target, from, and utilize resources in at least two nations. This gives rise to major legal concerns regarding the definition and jurisdiction of the law in the countries that encompass the internet as a means of carrying out various cyber crimes due to the differences in law and due process that different countries have when it comes to handling digital evidence and prosecuting the individuals involved in cyber crimes. For instance, in India, what is legal may be considered illegal in another country, making the laws and the judicial system to be diametrically opposed. This has led to the difficulties in taking action against offenders, obtaining evidence, transferring suspects, and even executing legal decisions within the cyberspace, thus, has made the fight against cybercrime a difficult task.

 ISSN: 2582-6433

- Technical Challenges

  Digital evidence involves great technicalities associated with digitization and the fact that it is dynamic due to advancement in technology. Problems arise from the complexity and propriety of linguistic and mathematical structures such as encryption and secure communication channels where messages might require decryption keys to gain access. Moreover, digital evidence is an extremely volatile category because the object of interest can be easily altered. Also, digital evidence requires specific instruments and knowledge on how to work with materials or otherwise a minor violation of the procedure would prevent the data from being used as evidence in court. It is for this reason that the use of technology is ever changing and universally accepted, and so the police and other legal individuals must further their education to handle such important evidence.

- Legal Challenges

  The laws relating to electronic evidence remain rather weak and generally underdeveloped, and often the laws frequently fail to keep up with the present technological trends. Another significant issue has been the absence of clear rules and procedures for the acquisition, storage, and dissemination of both digital proof and digital trails. Furthermore, there could be a cumulative failure in providing adequate coverage for new forms of digital evidence or cybercrimes where existing laws may fail to fully satisfy the requirements of society necessitating enhancements and changes in the laws.

  One more problem is the protection from individual liberties violation, or being more specific – privacy. This is easily explained when taking into account the legal frameworks that regulate data processing and utilization, such as the General Data Protection Regulation (GDPR), which presents strict limitations to data collection and usage in contrast with the demands that investigative agencies have concerning digital evidence. However, there is always a problem of ensuring that the law enforcement agencies in every country do their work effectively while at the same time protecting the rights of every person.

- Privacy Concerns and Data Sheets

  Cognitive evidence is typically made of personal and sensitive data and, therefore, raises concerns on users' privacy. In any process that involves the collection and analysis of digital evidence, there are provisions held in the law concerning data privacy. Such laws, including the GDPR in India, lay down high standards on how

 ISSN: 2582-6433

consent is to be obtained, how data should be processed and used and how organizations and institutions must be transparent as they process the personal information of individuals. However, satisfying them may cause some hindrance to the way and manner with which law enforcement agencies can acquire important evidence for use in court. Also, there is likely to be tampering with people's data and breaches in the legal system that can lead to the leakage of private details to the public, damaging the trust between people and the law. Striking the right balance on privacy concerns while at the other end demanding for enforcement of law is a complex and perpetual issue in the field of digital evidence and cyber law.

In the case of K.S. Puttaswamy v. Union of India (2017), also known as the 'Right to Privacy case', a judgment delivered by the supreme Court of India, wherein the Supreme Court recognized the right to privacy as a fundamental right under the Indian Constitution. The case is connected with controversies regarding Aadhaar scheme that was collecting and preserving the biometric database of Indians. The court concluded that although, the government was free to gather data for some rightly praiseworthy public ends, it also had to safeguard the rights to privacy of the various individuals concerned. This judgment is also relevant to digital evidence as it sets rules and procedures of how a person's data should be collected, stored or used because this determines how that information would be treated if it counts as digital evidence for the protection of an individual's rights.

- Evolving nature of cyber threats

  In present times, the risks in the cyber world are very high, and the hackers become more and more creative to enter into the businesses. This situation is not favorable for establishing legal system that would seek to prevent or respond to the incidences of cybercrimes. Law enforcement agencies and legal professions need to keep updated with the trends, achieve continuous knowledge enhancement, spend substantial amounts on better technology, and work with partners all over the world. New trends of crimes in the cyberspace appear regularly, they range from simple payoff attacks to wiretapping, which requires modernisation of existing legislation and adoption of new legal norms. These are significant concerns that require prompt responses when they occur hence the need to be able to adapt to these changes in order to fight cyber crime.

 ISSN: 2582-6433

Conclusion

Given the increasingly digital world, the link between cyber law and digital evidence is of utmost importance due to the role that electronic data plays in legal and investigative processes. Digital evidence covers all types of electronics that means the scope of this type of evidence extends quite broadly. To sum up, merging digital evidence with cyber law is essential if justice is to be delivered effectively in the information age. Legal frameworks must continue changing as technology advances to regulate changes in internet communications and handling of electronic records for example where there may be need for widespread use of electronic signatures. Therefore, it is important to have dynamic relationship between technology, society and the rule of law in our contemporary world which is characterized by rising technological advancements on daily basis.

Cases cited

- State of Maharashtra v. Prafulla B. Desai (Dr.) (2003) 4 SCC 601
- Anvar P.V v. P.K. Basheer & Ors (2014 10 SCC 473)
- Justice K.S. Puttaswamy (Retd.) & Anr. Vs. Union of India & Ors (2017) 10 SCC 1
- Arjun Panditrao Khotkar v/s Kailash Kushanrao Gorantyal: Civil Appeals 20825-20826 of 2017

Reference

- https://vipslawblog.wordpress.com/2022/02/28/digital-evidence-and-cyber-forensics/
- https://www.slideshare.net/slideshow/digital-evidence-239809320/239809320
- https://www.researchgate.net/publication/378197719_Cybercrime_and_the_Law_Addressing_the_Challenges_of_Digital_Forensics_in_Criminal_Investigations
- https://www.slideshare.net/slideshow/electronic-evidence-digital-evidence-in-india/26311682
- https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools
- https://www.salvationdata.com/knowledge/8-types-of-digital-evidence/
- https://www.drishtijudiciary.com/indian-evidence-act/State%20of%20Maharashtra%20v.%20Prafulla%20B.%20Desai%20(Dr.)%20(2003)%204%20SCC%20601

 ISSN: 2582-6433

- https://www.linkedin.com/pulse/case-study-anvar-pv-v-pk-basheer-ors-2014-10-scc-473-chare/
- https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors#:~:text=Case%20Brief&text=The%20nine%20Judge%20Bench%20in,of%20dignity%2C%20autonomy%20and%20liberty
- https://www.legalserviceindia.com/legal/article-10539-arjun-panditrao-khotkar-v-s-kailash-kushanrao-gorantyal-civil-appeals-20825-20826-of-2017.html#google_vignette