The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 11 | November 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

साइबर कानून और डिजिटल फॉरेंसिक : अपराध अन्वेषण में तकनीकी साक्ष्यों की स्वीकार्यता

Ankita Keshri

(Research Scholar), Email: ankita.keshri24@gmail.com

Dr. Sayyad Ismail Nasir

Department of Law, NIILM University, Kaithal, Hariyana

DOI : https://doi.org/10.5281/zenodo.17922328

ARTICLE DETAILS

Research Paper

Accepted: 22-11-2025

Published: 10-12-2025

Keywords:

साइबर कानून, डिजिटल फॉरेंसिक, तकनीकी साक्ष्य, साइबर अपराध,

ABSTRACT

डिजिटल युग में अपराध का स्वरूप लगातार बदल रहा है। जहाँ एक ओर सूचना और संचार प्रौद्योगिकी (ICT) ने मानव जीवन को अभूतपूर्व गति और सुविधा प्रदान की है, वहीं दूसरी ओर साइबर अपराधों ने समाज और विधि-व्यवस्था के सामने गंभीर चुनौतियाँ उत्पन्न कर दी हैं। हैकिंग, डेटा चोरी, पहचान की चोरी, फिशिंग, साइबर आतंकवाद और ऑनलाइन धोखाधड़ी जैसे अपराध आज वैश्विक सुरक्षा और न्याय प्रणाली के लिए एक बड़ा खतरा बन चुके हैं। इन अपराधों की जाँच और अभियोजन के लिए पारंपरिक अन्वेषण पद्धतियाँ पर्याप्त नहीं रह गईं, जिसके परिणामस्वरूप डिजिटल फॉरेंसिक विज्ञान की महत्ता अत्यधिक बढ़ गई है। डिजिटल फॉरेंसिक अपराध अन्वेषण की वह प्रक्रिया है, जिसके अंतर्गत कंप्यूटर, मोबाइल, सर्वर, नेटवर्क और क्लाउड जैसे इलेक्ट्रॉनिक उपकरणों से अपराध संबंधी साक्ष्यों का वैज्ञानिक ढंग से संग्रह, संरक्षण, विश्लेषण और प्रस्तुतीकरण किया जाता है। यह प्रक्रिया न केवल अपराधियों की पहचान और दोष सिद्धि सुनिश्चित करती है, बल्कि न्यायालय को निष्पक्ष और विश्वसनीय साक्ष्य उपलब्ध कराकर न्याय प्रक्रिया को भी सुदृढ़ बनाती है। भारत में "सूचना प्रौद्योगिकी अधिनियम, 2000 तथा भारतीय साक्ष्य अधिनियम, 2023" ने इलेक्ट्रॉनिक साक्ष्यों को वैधानिक मान्यता प्रदान की है। विशेष रूप से, साक्ष्य अधिनियम, 2023 में इलेक्ट्रॉनिक रिकॉर्ड्स की स्वीकार्यता, उनकी प्रामाणिकता और सर्टिफिकेट संबंधी प्रावधान

न्यायालय में तकनीकी साक्ष्यों की वैधता को सुनिश्चित करते हैं। सर्वोच्च न्यायालय के अनवर *पी.वी. बनाम पी.के. बशीर* (2014) तथा *अर्जुन पंडित्राओ बनाम कैलाश कुशनराव* (2020) जैसे महत्वपूर्ण निर्णयों ने इस क्षेत्र को और अधिक स्पष्ट दिशा प्रदान की है। फिर भी, तकनीकी साक्ष्यों की स्वीकार्यता में कई व्यावहारिक चुनौतियाँ मौजूद हैं। इनमें चेन ऑफ कस्टडी (Chain of Custody) की शुद्धता बनाए रखना, डिजिटल डेटा में छेड़छाड़ रोकना, न्यायिक अधिकारियों और अन्वेषण एजेंसियों की तकनीकी विशेषज्ञता की कमी, तथा गोपनीयता एवं निजता से जुड़े प्रश्न प्रमुख हैं। इन चुनौतियों से निपटने के लिए आधुनिक डिजिटल फॉरेंसिक प्रयोगशालाओं की स्थापना, अन्वेषण अधिकारियों का प्रशिक्षण, और अंतरराष्ट्रीय सहयोग की आवश्यकता है। यह शोध-पत्र साइबर अपराधों की बढ़ती जटिलताओं, डिजिटल फॉरेंसिक की उपयोगिता, भारतीय विधिक ढाँचे और न्यायालयों के दृष्टिकोण का विश्लेषण करता है। इसके साथ ही यह शोध यह निष्कर्ष प्रस्तुत करता है कि तकनीकी साक्ष्यों की स्वीकार्यता न केवल अपराध अन्वेषण को प्रभावी बनाती है, बल्कि न्यायिक प्रक्रिया की पारदर्शिता और विश्वसनीयता को भी सुदृढ़ करती है।

परिचय (Introduction)

सूचना और संचार प्रौद्योगिकी (ICT) ने मानव जीवन के लगभग हर क्षेत्र में क्रांतिकारी परिवर्तन किए हैं। बैंकिंग, ई-गवर्नेंस, ऑनलाइन शिक्षा, सोशल मीडिया और डिजिटल लेन-देन जैसी सुविधाओं ने समाज को नई गति दी है। किंतु इस तकनीकी प्रगति के समानांतर साइबर अपराधों में भी अप्रत्याशित वृद्धि हुई है। हैकिंग, डेटा चोरी, साइबर धोखाधड़ी, पहचान की चोरी, साइबर आतंकवाद और ऑनलाइन वित्तीय अपराध आज के युग की गंभीर चुनौतियाँ बन चुकी हैं। पारंपरिक अपराध अन्वेषण पद्धतियाँ इन नए अपराधों के लिए अपर्याप्त सिद्ध हो रही हैं। यही कारण है कि डिजिटल फॉरेंसिक एक अनिवार्य उपकरण बनकर उभरा है। डिजिटल फॉरेंसिक वह वैज्ञानिक तकनीक है, जिसके द्वारा इलेक्ट्रॉनिक उपकरणों—जैसे कंप्यूटर, मोबाइल फोन, सर्वर, क्लाउड डेटा और नेटवर्क—से अपराध संबंधी साक्ष्यों का संग्रह, विश्लेषण और प्रस्तुतीकरण किया जाता है। यह प्रक्रिया न केवल अपराधियों की पहचान करने में सहायक होती है, बल्कि न्यायालय में अभियोजन (prosecution) की सफलता की आधारशिला भी रखती है।

भारत में "सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act, 2000) तथा भारतीय साक्ष्य अधिनियम**, 2023 (BSA 2023)"** ने इलेक्ट्रॉनिक साक्ष्यों को वैधानिक मान्यता दी। न्यायालयों ने भी समय-समय पर महत्वपूर्ण निर्णय देकर इलेक्ट्रॉनिक रिकॉर्ड्स की स्वीकार्यता को परिभाषित किया है। यद्यपि डिजिटल साक्ष्य अपराध अन्वेषण में अत्यधिक महत्वपूर्ण हैं, परंतु इनकी विश्वसनीयता, संग्रहण की शुद्धता, गोपनीयता की रक्षा तथा न्यायालयीन अधिकारियों की तकनीकी समझ जैसी चुनौतियाँ आज भी विद्यमान हैं। अतः आवश्यक है कि साइबर कानून और डिजिटल फॉरेंसिक के बीच संतुलन बनाकर एक ऐसा विधिक तंत्र विकसित किया जाए, जो अपराधियों पर कठोर कार्रवाई सुनिश्चित कर सके और निर्दोष व्यक्तियों के मौलिक अधिकारों की रक्षा भी कर सके।

इस शोध-पत्र का उद्देश्य साइबर अपराधों की बढ़ती जटिलताओं, डिजिटल फॉरेंसिक की भूमिका और तकनीकी साक्ष्यों की स्वीकार्यता के कानूनी पहलुओं का गहन अध्ययन करना है, जिससे भविष्य की विधिक और नीतिगत दिशा तय की जा सके।

साइबर अपराध : अवधारणा और प्रकार

सूचना और संचार प्रौद्योगिकी के व्यापक प्रसार ने समाज को डिजिटल रूप से परिवर्तित कर दिया है। जहाँ एक ओर इंटरनेट ने जीवन को सरल और गतिशील बनाया है, वहीं दूसरी ओर अपराधियों ने भी तकनीक को अपने अपराधों के नए साधन के रूप में अपनाया है। इस परिप्रेक्ष्य में "साइबर अपराध" शब्द का प्रयोग उन सभी अवैध गतिविधियों के लिए किया जाता है, जो कंप्यूटर, इंटरनेट, नेटवर्क, मोबाइल या अन्य डिजिटल उपकरणों के माध्यम से संपन्न की जाती हैं।

साइबर अपराध की अवधारणा केवल वित्तीय या तकनीकी क्षेत्र तक सीमित नहीं है, बल्कि यह व्यक्तिगत निजता, सामाजिक सुरक्षा और राष्ट्रीय हितों तक को प्रभावित करती है। यह अपराध कभी व्यक्तिगत स्तर पर हानिकारक हो सकता है, जैसे किसी के सोशल मीडिया अकाउंट को हैक करना, तो कभी अंतरराष्ट्रीय स्तर पर खतरनाक, जैसे साइबर आतंकवाद या संवेदनशील सरकारी डेटा की चोरी।

साइबर अपराध के प्रमुख प्रकार इस प्रकार हैं:

1. **हैकिंग) Hacking):** अनधिकृत तरीके से कंप्यूटर सिस्टम या नेटवर्क में प्रवेश कर डेटा की चोरी, परिवर्तन या नष्ट करना।
2. **साइबर धोखाधड़ी) Cyber Fraud):** ऑनलाइन माध्यम से वित्तीय लेन-देन में धोखाधड़ी, जैसे फिशिंग ईमेल या नकली वेबसाइट।

3. **पहचान की चोरी) Identity Theft):** किसी व्यक्ति की व्यक्तिगत जानकारी) जैसे आधार, पैन, बैंक विवरण (का अवैध उपयोग।

4. **साइबर आतंकवाद) Cyber Terrorism):** डिजिटल माध्यम से किसी राष्ट्र की सुरक्षा व्यवस्था, बैंकिंग सिस्टम या संचार नेटवर्क पर हमला।

5. **ऑनलाइन अश्लीलता) Cyber Pornography):** इंटरनेट पर अवैध और आपत्तिजनक सामग्री का प्रसार।

6. **साइबर स्टॉकिंग और बुलिंग:** डिजिटल प्लेटफॉर्म पर किसी को लगातार परेशान करना या डराना।

7. **डाटा चोरी) Data Theft):** संगठनों या व्यक्तियों के संवेदनशील डाटा को चुराना और उसे काले बाजार में बेचना।

8. **रैनसमवेयर और मैलवेयर हमले:** किसी कंप्यूटर सिस्टम को लॉक करके उससे फिरौती माँगना।

इस प्रकार, साइबर अपराध न केवल व्यक्तिगत अधिकारों और आर्थिक सुरक्षा को प्रभावित करते हैं, बल्कि राष्ट्र की आंतरिक एवं बाहरी सुरक्षा के लिए भी गंभीर खतरा उत्पन्न करते हैं।

साइबर कानून का विकास

सूचना प्रौद्योगिकी और इंटरनेट के तीव्र विकास ने समाज को डिजिटल अर्थव्यवस्था, ई-गवर्नेंस और वैश्विक संपर्क की दिशा में अग्रसर किया, किंतु इसके साथ ही नए प्रकार के अपराधों ने भी जन्म लिया। पारंपरिक आपराधिक कानून इन जटिल साइबर अपराधों से निपटने में पर्याप्त नहीं थे, इसलिए भारत सहित विश्व के अनेक देशों ने साइबर अपराधों को नियंत्रित करने हेतु विशेष कानून बनाए। भारत में साइबर कानून की यात्रा वर्ष 2000 में "**सूचना प्रौद्योगिकी अधिनियम) IT Act, 2000)**" से शुरू होती है। यह अधिनियम इलेक्ट्रॉनिक वाणिज्य) E-commerce) और इलेक्ट्रॉनिक रिकॉर्ड्स को वैधानिक मान्यता देने के साथ-साथ साइबर अपराधों को नियंत्रित करने का पहला व्यापक प्रयास था। इसमें कंप्यूटर से छेड़छाड़, अनधिकृत प्रवेश) हैकिंग(, डिजिटल हस्ताक्षर की सुरक्षा, और साइबर धोखाधड़ी जैसे अपराधों के लिए दंडात्मक प्रावधान किए गए।

बढ़ते अपराधों की जटिलता को देखते हुए **2008 में IT अधिनियम में संशोधन** किया गया। इस संशोधन ने साइबर आतंकवाद, डेटा चोरी, साइबर स्टॉकिंग, बाल अश्लीलता) child pornography), और ऑनलाइन धोखाधड़ी जैसे गंभीर अपराधों को स्पष्ट रूप से अपराध की श्रेणी में रखा। इसके अतिरिक्त, संवेदनशील व्यक्तिगत डेटा की सुरक्षा तथा कंपनियों पर उत्तरदायित्व) corporate liability) से संबंधित प्रावधान भी जोड़े गए। इस संशोधन ने भारत में साइबर अपराधों की परिभाषा को और व्यापक बनाया तथा दंडात्मक प्रावधानों को कठोर किया। सिर्फ आपराधिक

पहलू ही नहीं, बल्कि **तकनीकी साक्ष्यों की स्वीकार्यता** भी एक बड़ा प्रश्न था। प्रारंभिक वर्षों में न्यायालय इलेक्ट्रॉनिक रिकॉर्ड्स को लेकर असमंजस में थे, लेकिन बाद में विधिक ढाँचे को और स्पष्ट किया गया। इसी उद्देश्य से हाल ही में लागू **भारतीय साक्ष्य अधिनियम, 2023** (BSA 2023) ने इलेक्ट्रॉनिक रिकॉर्ड्स की प्रमाणिकता और उनकी न्यायालय में स्वीकार्यता को विधिक मान्यता दी। इसमें सर्टिफिकेट और प्रामाणिकता से संबंधित प्रावधानों ने अपराध अन्वेषण और अभियोजन को नई दिशा दी है।

अंतरराष्ट्रीय स्तर पर भी साइबर कानून का विकास समानांतर रूप से हुआ है। **बुडापेस्ट कन्वेंशन) 2001)** को विश्व का पहला और सबसे महत्वपूर्ण अंतरराष्ट्रीय समझौता माना जाता है, जिसने सदस्य देशों को साइबर अपराधों से निपटने के लिए सहयोग और एक समान कानूनी ढाँचा तैयार करने पर बल दिया। इसके अतिरिक्त, **यूरोपीय संघ का जीडीपीआर) GDPR, 2018)** डेटा सुरक्षा और गोपनीयता के लिए महत्वपूर्ण मील का पत्थर है। संयुक्त राष्ट्र और अन्य अंतरराष्ट्रीय संगठन भी साइबर अपराध नियंत्रण हेतु दिशा-निर्देश प्रदान कर रहे हैं।

डिजिटल फॉरेंसिक की भूमिका

डिजिटल युग में अपराध की प्रकृति पारंपरिक सीमाओं से परे होकर आभासी) virtual) दुनिया तक पहुँच चुकी है। आज अपराधी अपने उद्देश्यों की पूर्ति के लिए कंप्यूटर, मोबाइल फोन, नेटवर्क, क्लाउड सेवाओं और अन्य इलेक्ट्रॉनिक उपकरणों का उपयोग करते हैं। ऐसे में अपराध अन्वेषण के लिए पारंपरिक पुलिसिंग और जांच पद्धतियाँ अपर्याप्त सिद्ध हो रही हैं। यही कारण है कि **डिजिटल फॉरेंसिक** एक अनिवार्य उपकरण बनकर उभरा है। डिजिटल फॉरेंसिक न केवल अपराधी की पहचान और दोषसिद्धि सुनिश्चित करता है, बल्कि न्यायालय को तकनीकी दृष्टि से विश्वसनीय और प्रमाणिक साक्ष्य भी उपलब्ध कराता है।

डिजिटल फॉरेंसिक की परिभाषा और उद्देश्य

डिजिटल फॉरेंसिक को सामान्यतः इस प्रकार परिभाषित किया जा सकता है—
"डिजिटल फॉरेंसिक वह वैज्ञानिक प्रक्रिया है जिसके अंतर्गत डिजिटल उपकरणों) जैसे कंप्यूटर, मोबाइल, हार्ड डिस्क, नेटवर्क या क्लाउड (से अपराध संबंधी साक्ष्यों का संग्रह, संरक्षण, विश्लेषण और प्रस्तुतीकरण न्यायालयीन मानकों के अनुरूप किया जाता है।"

इसका प्रमुख उद्देश्य निम्नलिखित हैं:

1. अपराध से संबंधित डिजिटल साक्ष्य का **संग्रह और संरक्षा**।
2. साक्ष्य की **प्रामाणिकता और विश्वसनीयता** बनाए रखना।

3. अपराधी की **पहचान और गतिविधियों का पुनर्निर्माण**।
4. न्यायालय के समक्ष **वैधानिक रूप से स्वीकार्य साक्ष्य** प्रस्तुत करना।
5. अपराध की रोकथाम हेतु डिजिटल सुरक्षा मानकों में सुधार करना।

डिजिटल फॉरेंसिक की प्रमुख शाखाएँ

डिजिटल फॉरेंसिक की विभिन्न शाखाएँ अपराध अन्वेषण में अत्यंत महत्वपूर्ण भूमिका निभाती हैं क्योंकि हर प्रकार के अपराध का स्वरूप और उसमें प्रयुक्त तकनीक भिन्न हो सकती है। सबसे पहली और प्रमुख शाखा **कंप्यूटर फॉरेंसिक** है, जिसके अंतर्गत कंप्यूटर सिस्टम, लैपटॉप, हार्ड डिस्क, पेन ड्राइव और अन्य डिजिटल स्टोरेज डिवाइस से अपराध संबंधी जानकारी प्राप्त की जाती है। इसमें डिलीट की गई फाइलों की रिकवरी, ब्राउज़िंग हिस्ट्री का अध्ययन, सिस्टम लॉग्स का विश्लेषण और मैलवेयर की पहचान जैसी प्रक्रियाएँ शामिल होती हैं। यह शाखा हैकिंग, वित्तीय धोखाधड़ी, कॉर्पोरेट जासूसी और आतंकवादी गतिविधियों में निर्णायक साक्ष्य उपलब्ध कराती है। इसके बाद **मोबाइल फॉरेंसिक** एक अत्यधिक उपयोगी शाखा है क्योंकि आज मोबाइल फोन प्रत्येक व्यक्ति की डिजिटल पहचान का सबसे महत्वपूर्ण स्रोत है। अपराधी अक्सर मोबाइल एप्स, कॉल्स और लोकेशन सेवाओं का उपयोग करते हैं। मोबाइल फॉरेंसिक के माध्यम से कॉल डिटेल रिकॉर्ड्स, व्हाट्सएप और टेलीग्राम जैसी मैसेजिंग सेवाओं के चैट्स, जीपीएस लोकेशन और क्लाउड बैकअप्स से प्राप्त डेटा का विश्लेषण किया जाता है। हत्या, अपहरण, साइबर स्टॉकिंग और धोखाधड़ी जैसे मामलों में मोबाइल फॉरेंसिक निर्णायक साबित होता है।

इसी तरह **नेटवर्क फॉरेंसिक** भी अपराध जाँच में अत्यंत आवश्यक है। चूँकि अधिकांश साइबर अपराध नेटवर्क स्तर पर होते हैं, इसलिए नेटवर्क ट्रैफिक, पैकेट डेटा और सर्वर लॉग्स का विश्लेषण करके यह पता लगाया जाता है कि अपराध कब और किस स्रोत से हुआ। यह शाखा डिनायल ऑफ सर्विस) DoS), डेटा चोरी, हैकिंग और फ़ायरवॉल बायपासिंग जैसी गतिविधियों का पर्दाफाश करने में उपयोगी है। कॉर्पोरेट संगठनों, वित्तीय संस्थानों और सरकारी विभागों के नेटवर्क सुरक्षा के लिए यह अनिवार्य माना जाता है। डिजिटल अपराधों की बढ़ती जटिलता को देखते हुए **क्लाउड फॉरेंसिक** का महत्व भी बढ़ गया है। अपराधी अक्सर डेटा को क्लाउड स्टोरेज जैसे गूगल ड्राइव, ड्रॉपबॉक्स या iCloud में छिपाते हैं। क्लाउड फॉरेंसिक के माध्यम से इन सेवाओं से डिजिटल साक्ष्य एकत्र किए जाते हैं, लेकिन इसमें सबसे बड़ी चुनौती यह होती है कि डेटा विभिन्न देशों में संग्रहीत हो सकता है और अधिकार क्षेत्र संबंधी समस्याएँ उत्पन्न होती हैं। इसके बावजूद साइबर आतंकवाद, वित्तीय धोखाधड़ी और अंतरराष्ट्रीय स्तर के अपराधों की जाँच में क्लाउड फॉरेंसिक एक अनिवार्य शाखा बन चुकी है।

ईमेल फॉरेंसिक भी डिजिटल अपराधों की जाँच में अत्यधिक महत्त्वपूर्ण है क्योंकि आधिकारिक संचार का सबसे प्रमुख माध्यम ईमेल है। इस शाखा में ईमेल हैडर का विश्लेषण कर प्रेषक का आईपी एड्रेस पता लगाया जाता है, मेटाडेटा का अध्ययन कर ईमेल की प्रामाणिकता सिद्ध की जाती है और फिशिंग या स्पैमिंग के जरिए किए गए अपराधों की पहचान की जाती है। वित्तीय धोखाधड़ी, कॉर्पोरेट घोटाले और ब्लैकमेलिंग जैसे मामलों में ईमेल फॉरेंसिक निर्णायक भूमिका निभाता है। आजकल अपराधी वीडियो, ऑडियो और फोटो सामग्री का भी दुरुपयोग करते हैं, इसलिए **मल्टीमीडिया फॉरेंसिक** की आवश्यकता होती है। यह शाखा एडिटेड इमेज, मॉर्फ्ड फोटो, डीपफेक वीडियो और ऑडियो क्लिप की प्रामाणिकता की जाँच करती है। साइबर बुलिंग, अश्लील सामग्री के प्रसार और राजनीतिक प्रचार में इसका महत्व तेजी से बढ़ रहा है।

नई तकनीकों के विकास के साथ **इंटरनेट ऑफ थिंग्स) IoT) फॉरेंसिक** का क्षेत्र भी सामने आया है। आज स्मार्ट वॉच, सीसीटीवी कैमरा, स्मार्ट डोर लॉक और होम ऑटोमेशन सिस्टम व्यापक रूप से प्रयोग हो रहे हैं। अपराध की स्थिति में इन डिवाइसों से प्राप्त डेटा जैसे लोकेशन ट्रैकिंग, वीडियो फुटेज और वॉयस कमांड्स को साक्ष्य के रूप में प्रस्तुत किया जा सकता है। हत्या, चोरी या घरेलू हिंसा जैसे मामलों में यह शाखा अत्यंत उपयोगी सिद्ध हो रही है। इसी तरह **डेटाबेस फॉरेंसिक** का क्षेत्र भी महत्त्वपूर्ण है क्योंकि बड़े संगठनों और सरकारी विभागों में विशाल डेटाबेस का उपयोग होता है। इसमें डेटाबेस से अनधिकृत परिवर्तन, छेड़छाड़ या अवैध डेटा एंट्री का पता लगाया जाता है। कॉर्पोरेट धोखाधड़ी, वित्तीय घोटाले और भ्रष्टाचार की जाँच में यह शाखा विशेष महत्त्व रखती है।

डिजिटल अपराधों के विस्तार के साथ **सोशल मीडिया फॉरेंसिक** भी नई शाखा के रूप में उभरकर सामने आई है। फेसबुक, ट्विटर, इंस्टाग्राम, व्हाट्सएप और टेलीग्राम जैसे प्लेटफॉर्म अपराधियों के लिए प्रचार और गुप्त संचार का साधन बन चुके हैं। सोशल मीडिया फॉरेंसिक के माध्यम से संदिग्ध अकाउंट्स की गतिविधियों का अध्ययन, हेट स्पीच और अफवाहों की पहचान तथा सामुदायिक तनाव फैलाने वाले कंटेंट का पता लगाया जाता है। इस शाखा का महत्त्व राजनीतिक अपराधों, सांप्रदायिक हिंसा और साइबर बुलिंग की जाँच में अत्यधिक बढ़ गया है।

अतः यह स्पष्ट है कि डिजिटल फॉरेंसिक की प्रत्येक शाखा अपराध अन्वेषण के विभिन्न पहलुओं को संबोधित करती है। कंप्यूटर और मोबाइल फॉरेंसिक अपराधी के व्यक्तिगत उपकरणों से साक्ष्य जुटाती है, नेटवर्क और क्लाउड फॉरेंसिक तकनीकी बुनियादी ढांचे पर हुए अपराधों का विश्लेषण करती है, वहीं ईमेल, मल्टीमीडिया और सोशल मीडिया फॉरेंसिक संचार माध्यमों से अपराध की जाँच को सुनिश्चित करते हैं। IoT और डेटाबेस फॉरेंसिक जैसी नई शाखाएँ इस क्षेत्र को और अधिक व्यापक बना रही हैं। भारतीय संदर्भ में, जहाँ इंटरनेट उपयोगकर्ता करोड़ों की संख्या में हैं और साइबर अपराधों की दर तेजी से बढ़ रही है, वहाँ इन सभी शाखाओं का विकास न्यायिक प्रक्रिया की विश्वसनीयता और अपराध रोकथाम दोनों के लिए अपरिहार्य है।

डिजिटल फॉरेंसिक की अपराध अन्वेषण में भूमिका

21वीं सदी में तकनीक और इंटरनेट का विस्तार अभूतपूर्व रहा है। सूचना और संचार प्रौद्योगिकी ने समाज को अनेक सुविधाएँ प्रदान कीं, परंतु इसके साथ ही अपराध की प्रकृति भी बदली। अपराध अब केवल भौतिक दुनिया तक सीमित नहीं रहे, बल्कि वर्चुअल और डिजिटल दुनिया तक फैल चुके हैं। **साइबर अपराध, आर्थिक धोखाधड़ी, डिजिटल आतंकवाद, सोशल मीडिया दुरुपयोग और ऑनलाइन शोषण** आज गंभीर चुनौतियाँ हैं।

ऐसे अपराधों की जाँच पारंपरिक पुलिस पद्धतियों से संभव नहीं, क्योंकि इनका मूल साक्ष्य "डिजिटल" होता है। यहाँ **डिजिटल फॉरेंसिक** (Digital Forensics) की भूमिका अत्यंत महत्वपूर्ण हो जाती है। यह वह विज्ञान है जो इलेक्ट्रॉनिक उपकरणों और डिजिटल डेटा से साक्ष्य एकत्रित, सुरक्षित, विश्लेषित और प्रस्तुत करता है, ताकि अपराध की सत्यता सामने आ सके और न्यायालय में यह साक्ष्य स्वीकार्य हो।

(1) **साक्ष्य का वैज्ञानिक संग्रहण:** किसी भी अपराध अन्वेषण में पहला कदम साक्ष्य एकत्र करना होता है। डिजिटल अपराधों में यह प्रक्रिया विशेष रूप से महत्वपूर्ण है क्योंकि इलेक्ट्रॉनिक उपकरणों से निकला डेटा बेहद नाजुक और परिवर्तनीय होता है। डिजिटल फॉरेंसिक विशेषज्ञ **Write Blocker** जैसे टूल्स का उपयोग करते हैं जिससे डेटा में कोई बदलाव न हो।

(2) **साक्ष्य का संरक्षण**: डिजिटल साक्ष्य का महत्व तभी है जब यह "अपरिवर्तित" हो। इसके लिए "चेन ऑफ कस्टडी" बनाई जाती है जिसमें यह दर्ज होता है कि किस समय किस अधिकारी ने साक्ष्य को प्राप्त, संग्रहीत या प्रस्तुत किया। यह न्यायालय को आश्वस्त करता है कि डेटा में छेड़छाड़ नहीं हुई।

(3) **अपराध की पुनर्निर्मिति:** डिजिटल फॉरेंसिक अपराध के घटनाक्रम को पुनर्निर्मित करने में मदद करता है। **CCTV फुटेज, मोबाइल कॉल रिकॉर्ड,** और **GPS लोकेशन** के माध्यम से यह समझा जा सकता है कि अपराधी किस समय कहाँ मौजूद था और उसने किन गतिविधियों को अंजाम दिया।

(4) **अपराधी की पहचान:** अपराधी चाहे नकली प्रोफाइल या फर्जी ईमेल का उपयोग करे, डिजिटल दुनिया में उसके पीछे हमेशा कोई न कोई निशान रह जाता है। **IP Address ट्रैकिंग, MAC Address, डिवाइस आईडी और डिजिटल फिंगरप्रिंट्स** अपराधी की वास्तविक पहचान उजागर करते हैं।

(5) **न्यायालयीन स्वीकार्यता:** भारत में डिजिटल साक्ष्य की स्वीकार्यता का आधार है "**भारतीय साक्ष्य अधिनियम, 1872 की धारा 65B**। सुप्रीम कोर्ट ने *अनवर पी.वी .बनाम पी.के .बशीर) 2014)* और *अर्जुन पंडित्राव बनाम कैलाश कुशनराव) 2020")* जैसे मामलों में स्पष्ट किया है कि डिजिटल साक्ष्य तभी मान्य होगा जब उसका विधिसम्मत प्रमाणपत्र प्रस्तुत किया जाए।

(6) **वित्तीय अपराधों की जाँच:** आजकल ऑनलाइन बैंकिंग, UPI और क्रिप्टोकरेंसी के माध्यम से बड़े पैमाने पर धोखाधड़ी हो रही है। डिजिटल फॉरेंसिक **ट्रांजेक्शन लॉग्स, ईमेल्स और पेमेंट गेटवे रिकॉर्ड्स** का विश्लेषण कर यह पता लगाता है कि धन का प्रवाह किस दिशा में गया।

(7) **आतंकवाद और राष्ट्रीय सुरक्षा:** आतंकी संगठन अब डिजिटल माध्यमों से संवाद और फंडिंग करते हैं। वे **एन्क्रिप्टेड चैट्स, डार्क वेब और क्रिप्टोकरेंसी** का उपयोग करते हैं। डिजिटल फॉरेंसिक इन चैनलों की निगरानी कर सुरक्षा एजेंसियों को अपराध रोकने में मदद करता है।

(8) **सामाजिक अपराध:** सोशल मीडिया पर **फेक न्यूज, हेट स्पीच और साइबर बुलिंग** समाज में अशांति फैला सकते हैं। डिजिटल फॉरेंसिक यह साबित करने में मदद करता है कि किस व्यक्ति या समूह ने ऐसा संदेश डाला और उसके परिणामस्वरूप क्या प्रभाव पड़ा।

(9) **छिपाए गए साक्ष्यों की खोज:** अपराधी अक्सर फाइलें डिलीट कर देते हैं या डेटा छुपा देते हैं। लेकिन डिजिटल फॉरेंसिक तकनीक से **डिलीटेड फाइल्स, रिकवर किए गए चैट्स और क्लाउड बैकअप्स** से वास्तविक साक्ष्य प्राप्त किए जा सकते हैं।

(10) **अंतरराष्ट्रीय सहयोग:** कई बार सर्वर विदेशों में होते हैं या अपराधी किसी और देश में बैठा होता है। ऐसे मामलों में डिजिटल फॉरेंसिक एजेंसियाँ **इंटरपोल और विदेशी न्यायिक संस्थाओं** के साथ मिलकर साक्ष्य प्राप्त करती हैं।

(11) **अपराध रोकथाम**: डिजिटल फॉरेंसिक केवल अपराध की जाँच ही नहीं करता, बल्कि यह बताता है कि अपराध किस तकनीकी कमजोरी का फायदा उठाकर किया गया। इससे **साइबर सुरक्षा सुधार** संभव होता है और भविष्य में ऐसे अपराधों की रोकथाम की जा सकती है।

भारतीय साक्ष्य अधिनियम, 2023 एवं तकनीकी साक्ष्य की स्वीकार्यता

न्यायिक प्रक्रिया में साक्ष्य) Evidence) का स्थान अत्यंत महत्वपूर्ण होता है। न्यायालय किसी भी अपराध या विवाद पर निर्णय देते समय केवल भावनाओं या धारणाओं पर नहीं, बल्कि प्रमाणित साक्ष्यों पर निर्भर करता है। बदलते समय में अपराधों की प्रकृति पारंपरिक से हटकर तकनीकी रूप ले चुकी है। आज के युग में अधिकांश अपराधों में प्रत्यक्षदर्शी गवाह से अधिक महत्व **डिजिटल और इलेक्ट्रॉनिक साक्ष्यों** का होता है। भारत में लंबे समय तक **Indian Evidence Act, 1872** लागू रहा। लेकिन 150 वर्षों से अधिक पुराने इस कानून में डिजिटल युग की चुनौतियों का पर्याप्त समाधान नहीं था। इस कमी को दूर करने के लिए भारत सरकार ने नया कानून – **भारतीय साक्ष्य अधिनियम, 2023 (Bharatiya Sakshya Adhiniyam – BSA 2023)** लागू किया। इसका सबसे बड़ा

योगदान यह है कि इसमें **तकनीकी और इलेक्ट्रॉनिक साक्ष्यों की स्वीकार्यता) Admissibility)** को विधिक रूप से स्पष्ट किया गया है।

तकनीकी साक्ष्य का अर्थ

तकनीकी या डिजिटल साक्ष्य का अभिप्राय उन सभी साक्ष्यों से है जो **कंप्यूटर, मोबाइल, नेटवर्क, क्लाउड, सोशल मीडिया, डिजिटल डिवाइस** या अन्य इलेक्ट्रॉनिक माध्यम से उत्पन्न, संग्रहित या संप्रेषित होते हैं। इसमें शामिल हैं –

- ईमेल, व्हाट्सएप/टेलीग्राम जैसे मैसेज
- कॉल डिटेल रिकॉर्ड्स और मोबाइल लोकेशन
- सीसीटीवी फुटेज और अन्य वीडियो रिकॉर्डिंग
- डिजिटल हस्ताक्षर और इलेक्ट्रॉनिक प्रमाणपत्र
- ऑनलाइन ट्रांजेक्शन और बैंकिंग रिकॉर्ड
- क्लाउड स्टोरेज डेटा और सर्वर लॉग्स
- सोशल मीडिया पोस्ट और वेबसाइट कंटेंट

इन साक्ष्यों का महत्व इसलिए है क्योंकि आधुनिक अपराधों का अधिकांश भाग इन्हीं माध्यमों से किया जाता है।

BSA 2023 में तकनीकी साक्ष्य से संबंधित प्रमुख प्रावधान

(1) दस्तावेज़ की परिभाषा का विस्तार

1872 के कानून में दस्तावेज़ का अर्थ मुख्यतः लिखित या मुद्रित सामग्री तक सीमित था। BSA 2023 ने दस्तावेज़ की परिभाषा में स्पष्ट किया कि **कोई भी इलेक्ट्रॉनिक रिकॉर्ड भी दस्तावेज़ है।** इसका अर्थ है कि अब ईमेल, मैसेज या डिजिटल फाइल भी वैध कानूनी दस्तावेज़ माने जाएंगे।

(2) इलेक्ट्रॉनिक रिकॉर्ड्स की स्वीकार्यता

नए अधिनियम में यह प्रावधान है कि **इलेक्ट्रॉनिक रिकॉर्ड्स को उसी प्रकार स्वीकार किया जाएगा जैसे भौतिक दस्तावेज़ों को**। अंतर केवल यह है कि उनकी **प्रामाणिकता) Authenticity) और अखंडता) Integrity)** को प्रमाणित करना आवश्यक है।

धारा 63 के अनुसार, यदि इलेक्ट्रॉनिक रिकॉर्ड्स निम्नलिखित शर्तों को पूरा करते हैं, तो उन्हें प्रमाण के रूप में स्वीकार किया जाएगा:

- रिकॉर्ड को नियमित रूप से उपयोग किए गए कंप्यूटर या डिवाइस द्वारा उत्पन्न किया गया हो।
- रिकॉर्ड में जानकारी नियमित रूप से कंप्यूटर या डिवाइस में डाली गई हो।
- कंप्यूटर या डिवाइस पूरी अवधि के दौरान सही तरीके से कार्य कर रहा हो।
- रिकॉर्ड की जानकारी सही तरीके से पुन :उत्पन्न की जा सकती हो।

इसके अतिरिक्त, इलेक्ट्रॉनिक रिकॉर्ड्स के साथ एक प्रमाणपत्र प्रस्तुत करना आवश्यक है, जिसमें रिकॉर्ड के उत्पत्ति, निर्माण की प्रक्रिया, और उसकी सत्यता का विवरण हो

(3) प्रमाणन और सत्यापन

इलेक्ट्रॉनिक साक्ष्य को न्यायालय में प्रस्तुत करते समय यह आवश्यक होगा कि –

- यह बताया जाए कि डेटा किस माध्यम से प्राप्त किया गया।
- उसकी कॉपी और मूल में कोई अंतर नहीं है।
- डेटा को सुरक्षित तरीके से संरक्षित किया गया।
- आवश्यक होने पर तकनीकी विशेषज्ञ की राय भी प्रस्तुत की जाए।

(4) डिजिटल हस्ताक्षर और ई-प्रमाणपत्र

BSA 2023 में **डिजिटल सिग्नेचर, ई-सर्टिफिकेट और इलेक्ट्रॉनिक प्रमाणीकरण** को कानूनी मान्यता दी गई है। इससे ई-गवर्नेंस, ऑनलाइन कॉन्ट्रैक्ट और डिजिटल लेन-देन को मजबूत आधार मिला है।

- **धारा 66**: डिजिटल हस्ताक्षर की प्रमाणिकता सुनिश्चित करने के लिए, यह साबित करना आवश्यक है कि हस्ताक्षर उस व्यक्ति का है जिसने उसे लगाया है।

- **धारा 73**: कोर्ट को यह अधिकार है कि वह डिजिटल हस्ताक्षर प्रमाणपत्र की प्रस्तुति की मांग कर सकता है या सार्वजनिक कुंजी प्रमाणीकरण विधियों का उपयोग करके हस्ताक्षर की प्रमाणिकता की जांच कर सकता है।

- **धारा 87**: यदि कोई इलेक्ट्रॉनिक संदेश पांच वर्ष पुराना है और उचित रूप से संग्रहित है, तो कोर्ट यह मान सकता है कि संदेश की जानकारी सही है, लेकिन भेजने वाले की पहचान के बारे में कोई पूर्वधारणा नहीं बनाई जा सकती।

- **धारा 90**: इलेक्ट्रॉनिक संदेश की जानकारी को सही मानने के लिए, यह आवश्यक है कि संदेश को भेजने के समय में सही तरीके से इनपुट किया गया हो।

(5) डेटा संरक्षण और चेन ऑफ कस्टडी

किसी भी इलेक्ट्रॉनिक साक्ष्य को तब तक वैध नहीं माना जाएगा जब तक उसकी **चेन ऑफ कस्टडी** सुरक्षित न हो। इसका अर्थ है कि साक्ष्य एकत्र करने से लेकर अदालत में पेश करने तक हर चरण का रिकॉर्ड रखा जाएगा ताकि उसमें छेड़छाड़ की संभावना न हो।

सूचना प्रौद्योगिकी अधिनियम, 2000(IT Act, 2000): साइबर कानून और डिजिटल फॉरेंसिक

डिजिटल तकनीक के बढ़ते उपयोग ने अपराध अन्वेषण के तरीके बदल दिए हैं। कंप्यूटर, स्मार्टफोन, सर्वर और अन्य डिजिटल उपकरण अब अपराध के महत्वपूर्ण स्रोत बन गए हैं। अपराध अन्वेषण में तकनीकी साक्ष्य जैसे ई-मेल, डिजिटल दस्तावेज़, चैट रिकॉर्ड्स और डेटा लॉग्स की मान्यता न्यायालय में निर्णायक साबित होती है। भारत में सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act, 2000) ने इलेक्ट्रॉनिक साक्ष्यों की कानूनी मान्यता और प्रमाणिकता को स्पष्ट किया है।

मुख्य प्रावधान

तकनीकी साक्ष्य की परिभाषा और स्वीकार्यता

इलेक्ट्रॉनिक रिकॉर्ड्स, डिजिटल दस्तावेज़, ई-मेल, मैसेज और डेटा लॉग्स तकनीकी साक्ष्य माने जाते हैं।

- धारा 65A के अनुसार इलेक्ट्रॉनिक रिकॉर्ड्स को कानूनी साक्ष्य के रूप में प्रस्तुत किया जा सकता है।
- धारा 65B प्रमाणिकता और सत्यापन की प्रक्रिया को सुनिश्चित करती है, जिसमें प्रमाणपत्र) Certificate of Authenticity) प्रस्तुत करना आवश्यक है।
- प्रमाणपत्र यह दर्शाता है कि रिकॉर्ड की उत्पत्ति, संग्रहण और संग्रह प्रक्रिया सही तरीके से हुई।

डिजिटल फॉरेंसिक की भूमिका

- डिजिटल फॉरेंसिक का उद्देश्य अपराध के डिजिटल साक्ष्यों का सुरक्षित संग्रह, विश्लेषण और प्रस्तुति करना है।
- चेन ऑफ कस्टडी) Chain of Custody) का पालन अनिवार्य है, ताकि यह सुनिश्चित किया जा सके कि साक्ष्य में कोई छेड़छाड़ नहीं हुई।
- डेटा की शुद्धता और डिजिटल हस्ताक्षर/ई-प्रमाणपत्र की पुष्टि न्यायालय में स्वीकार्यता के लिए आवश्यक है।

अन्य महत्वपूर्ण प्रावधान

- धारा 65- कंप्यूटर सिस्टम या डेटा के विनाश, बदलाव या अवरोध को अपराध मानती है।
- धारा 65A- इलेक्ट्रॉनिक रिकॉर्ड्स को प्रमाण के रूप में प्रस्तुत किया जा सकता है।
- धारा 65B- इलेक्ट्रॉनिक रिकॉर्ड की प्रमाणिकता और सत्यापन के लिए प्रमाणपत्र आवश्यक।
- धारा 66- कंप्यूटर अपराध जैसे हैकिंग, डेटा चोरी, धोखाधड़ी।
- धारा 66C- डिजिटल पहचान की चोरी।
- धारा 66D- कंप्यूटर धोखाधड़ी।
- धारा 67- इलेक्ट्रॉनिक माध्यम से आपत्तिजनक सामग्री का प्रसार।

प्रमाणन और न्यायालय में स्वीकार्यता

- इलेक्ट्रॉनिक रिकॉर्ड के साथ प्रमाणपत्र प्रस्तुत करना अनिवार्य है।
- कोर्ट इलेक्ट्रॉनिक रिकॉर्ड्स और डिजिटल प्रमाणों की विश्वसनीयता की जांच कर सकता है।
- सही तरीके से प्रमाणित तकनीकी साक्ष्य न्यायालय में स्वीकार्य होते हैं और अपराधियों के विरुद्ध निर्णायक भूमिका निभाते हैं।

साक्ष्यों की सुरक्षा और चेन ऑफ कस्टडी

- डिजिटल साक्ष्य संग्रह के समय, स्थान और प्रक्रिया का रिकॉर्ड रखा जाता है।
- प्रत्येक ट्रांसफर और एक्सेस का विवरण सुनिश्चित करता है कि साक्ष्य में कोई बदलाव नहीं हुआ।
- यह प्रक्रिया डिजिटल साक्ष्य को न्यायालय में प्रभावी और स्वीकार्य बनाती है।

न्यायिक उपयोगिता के विभिन्न आयाम

1. अपराध की सटीक पहचान

तकनीकी साक्ष्य अपराधी और अपराध स्थल की सही पहचान करने में सहायक है। उदाहरण के लिए, **फिंगरप्रिंट स्कैनिंग, DNA टेस्ट और CCTV फुटेज** से यह स्पष्ट किया जा सकता है कि घटना में वास्तव में कौन शामिल था।

2. अपराध की परिस्थितियों का पुनर्निर्माण

डिजिटल और तकनीकी साधनों के माध्यम से घटना की वास्तविक परिस्थितियों का पुनर्निर्माण किया जा सकता है। जैसे कि ब्लैक बॉक्स रिकॉर्डर) एविएशन मामलों में(, लोकेशन ट्रैकिंग) मोबाइल डेटा के माध्यम से (और साइबर लॉग्स) ऑनलाइन अपराधों में(।

3. गवाह की कमी को पूरा करना

कई बार किसी अपराध का प्रत्यक्षदर्शी गवाह नहीं होता, या गवाह पक्षपाती हो सकता है। ऐसी स्थिति में तकनीकी साक्ष्य जैसे वीडियो रिकॉर्डिंग या इलेक्ट्रॉनिक दस्तावेज़ गवाह की तरह कार्य करते हैं और न्यायालय को निष्पक्ष प्रमाण उपलब्ध कराते हैं।

4. डिजिटल अपराधों में अनिवार्य

साइबर अपराध जैसे **हैकिंग, ऑनलाइन फ्रॉड, ई-मेल स्पूफिंग, डेटा चोरी, और क्रिप्टोकरेंसी घोटाले** में तकनीकी साक्ष्य ही एकमात्र साधन होते हैं। बिना इनके न्यायालय में अपराध सिद्ध करना असंभव हो जाता है।

5. त्वरित और विश्वसनीय निर्णय

तकनीकी साक्ष्य न्यायालय को शीघ्र और सटीक निर्णय लेने में मदद करते हैं। उदाहरणस्वरूप DNA टेस्ट से यह तुरंत तय हो जाता है कि आरोपी अपराध स्थल पर मौजूद था या नहीं। इससे न्यायिक प्रक्रिया लंबी बहसों और अनिश्चितताओं से बचती है।

6. आर्थिक अपराधों का पर्दाफाश

आजकल आर्थिक अपराध) Financial Crimes) ऑनलाइन लेन-देन के माध्यम से किए जाते हैं। **बैंकिंग ट्रांजेक्शन लॉग, UPI रिकॉर्ड और डिजिटल हस्ताक्षर** ऐसे मामलों में अपराध की सच्चाई सामने लाते हैं और आरोपी को दोषी ठहराने में निर्णायक भूमिका निभाते हैं।

7. राष्ट्रीय सुरक्षा और आतंकवाद विरोधी मामलों में

आतंकी संगठन एन्क्रिप्टेड मैसेजिंग ऐप, डार्क वेब और डिजिटल नेटवर्क का उपयोग करते हैं। न्यायालय में प्रस्तुत तकनीकी साक्ष्य जैसे सर्वर लॉग्स, IP एड्रेस और डेटा पैटर्न से उनके नेटवर्क का पता लगाया जा सकता है। यह राष्ट्रीय सुरक्षा के लिए अत्यंत आवश्यक है।

8. न्यायिक पारदर्शिता और विश्वास

तकनीकी साक्ष्य वस्तुनिष्ठ) Objective) और वैज्ञानिक होते हैं। इनमें मानवीय पक्षपात) Bias) की संभावना कम होती है। इससे न्यायालय के निर्णय पर जनता का विश्वास बढ़ता है और न्यायिक प्रक्रिया पारदर्शी प्रतीत होती है।

प्रमुख न्यायिक निर्णय

तकनीकी साक्ष्य) Technical / Electronic Evidence) आधुनिक न्यायिक प्रक्रिया का मूल स्तंभ बन चुका है। न्यायालय अब केवल प्रत्यक्षदर्शी गवाह या पारंपरिक दस्तावेज़ पर निर्भर नहीं रहते, बल्कि डिजिटल रिकॉर्ड, सीसीटीवी, मोबाइल डेटा, ई-मेल और कंप्यूटर प्रिंटआउट को भी समान रूप से महत्व देते हैं। भारतीय न्यायपालिका ने कई महत्वपूर्ण निर्णयों में यह स्पष्ट किया है कि तकनीकी साक्ष्य यदि उचित प्रमाणन और सुरक्षा के साथ प्रस्तुत किए जाएँ, तो वे पूर्णतः स्वीकार्य हैं।

1. *स्टेट) (एनसीटी ऑफ दिल्ली) बनाम नवजोत संधू2005)* – संसद हमला मामला

इस मामले में सर्वोच्च न्यायालय ने माना कि टेलीफोन कॉल रिकॉर्डिंग और मोबाइल कॉल डिटेल्स) CDRs) इलेक्ट्रॉनिक साक्ष्य के रूप में स्वीकार्य हो सकते हैं। हालाँकि, इसमें यह भी कहा गया कि यदि धारा 65B (Indian Evidence Act, 1872) का अनुपालन न हो, तब भी मौखिक साक्ष्य के आधार पर इन्हें स्वीकारा जा सकता है।

3. *अनवर पी.वी. बनाम पी.के. बशीयर*

यह एक ऐतिहासिक फैसला है। सुप्रीम कोर्ट ने स्पष्ट कर दिया कि **किसी भी इलेक्ट्रॉनिक रिकॉर्ड को साक्ष्य के रूप में स्वीकार करने के लिए धारा 65B का पालन अनिवार्य है**। इसका अर्थ यह है कि केवल इलेक्ट्रॉनिक रिकॉर्ड की

प्रिंटआउट कॉपी या सीडी प्रस्तुत करने से काम नहीं चलेगा, बल्कि उसे धारा 65B(4) के अंतर्गत विधिवत प्रमाणपत्र)Certificate) के साथ पेश करना आवश्यक है।

3. *शफी मोहम्मद बनाम हिमाचल प्रदेश राज्य*

सुप्रीम कोर्ट ने यह कहा कि यदि किसी पक्षकार के पास 65B प्रमाणपत्र उपलब्ध नहीं है, परन्तु इलेक्ट्रॉनिक रिकॉर्ड अन्य स्रोत से प्राप्त है, तो न्यायालय परिस्थितियों को देखते हुए उसे स्वीकार कर सकता है। यह निर्णय Anvar P.V. केस में दिए गए सख्त नियम को कुछ हद तक लचीला बनाता है।

4. *अर्जुन पंडितराव खोतकर बनाम कैलाश कुशनराव गोरंट्याल*

यह निर्णय Anvar और Shafhi Mohammad के बीच के भ्रम को दूर करता है। सुप्रीम कोर्ट ने स्पष्ट कर दिया कि –

- **65B प्रमाणपत्र इलेक्ट्रॉनिक साक्ष्य की अनिवार्य शर्त है।**
- यदि प्रमाणपत्र उपलब्ध नहीं कराया जाता, तो साक्ष्य को स्वीकार नहीं किया जा सकता।
- केवल उन्हीं मामलों में अपवाद होगा जहाँ मूल उपकरण) जैसे मोबाइल या सर्वर (न्यायालय के सामने प्रस्तुत किया जाए।

5. *टोमासो ब्रूनो बनाम उत्तर प्रदेश राज्य*

सुप्रीम कोर्ट ने कहा कि **CCTV फुटेज और अन्य इलेक्ट्रॉनिक रिकॉर्ड को नज़रअंदाज़ करना न्यायिक त्रुटि होगी**। न्यायालय ने माना कि आधुनिक युग में इलेक्ट्रॉनिक साक्ष्य अपराध की सच्चाई सामने लाने का सबसे महत्वपूर्ण साधन है।

6. *के. रामज्यम बनाम पुलिस निरीक्षक*

इस मामले में इलेक्ट्रॉनिक रिकॉर्ड की प्रामाणिकता पर बल दिया गया। सुप्रीम कोर्ट ने कहा कि डिजिटल साक्ष्य तभी स्वीकार्य होगा जब यह सुनिश्चित किया जाए कि उसमें किसी प्रकार की छेड़छाड़ नहीं हुई है।

7. *जगदेव सिंह बनाम राज्य (एनसीटी ऑफ दिल्ली सरकार)*

दिल्ली हाई कोर्ट ने कहा कि कॉल डिटेल रिकॉर्ड्स) CDRs) और अन्य इलेक्ट्रॉनिक डेटा को तभी स्वीकार किया जाएगा जब उनके साथ 65B प्रमाणपत्र प्रस्तुत किया जाए।

8. *बोडाला मुरली कृष्ण बनाम स्मt. बोडाला प्रतिमा*

हाई कोर्ट ने माना कि ई-मेल, चैट रिकॉर्ड और कंप्यूटर प्रिंटआउट को वैध साक्ष्य तभी माना जाएगा जब उन्हें सही तरीके से प्रमाणित किया जाए।

तकनीकी साक्ष्य: चुनौतियाँ, संभावनाएँ और सुधार की दिशा

चुनौतियाँ

1. डेटा में छेड़छाड़ की संभावना: डिजिटल साक्ष्य आसानी से बदला, मिटाया या छेड़छाड़ किया जा सकता है। यदि साक्ष्य की सुरक्षा पर्याप्त रूप से सुनिश्चित नहीं की गई, तो अदालत में उसकी विश्वसनीयता कम हो जाती है।

2. प्रमाणन और वैधता का जटिलता: भारत में इलेक्ट्रॉनिक साक्ष्य की स्वीकार्यता के लिए धारा 65B का पालन आवश्यक है। सही प्रमाणपत्र (Certificate) के बिना, इलेक्ट्रॉनिक डेटा अदालत में मान्य नहीं माना जाता। कई बार यह प्रक्रिया जटिल और समय-सापेक्ष हो सकती है।

3. तकनीकी विशेषज्ञता का अभाव: पुलिस, अभियोजक और न्यायिक अधिकारी सभी मामलों में तकनीकी ज्ञान से लैस नहीं होते। तकनीकी साक्ष्य को सही तरीके से जाँचने और प्रस्तुत करने के लिए विशेषज्ञों की आवश्यकता होती है।

4. गोपनीयता और निजता के अधिकार: डिजिटल डेटा एकत्र करते समय व्यक्तिगत गोपनीयता का उल्लंघन होने का खतरा रहता है। न्यायालय को यह सुनिश्चित करना होता है कि साक्ष्य संग्रहण में निजता और सुरक्षा अधिकारों का उल्लंघन न हो।

5. अंतरराष्ट्रीय सीमाओं में समस्या: कई बार इलेक्ट्रॉनिक साक्ष्य विदेश में स्थित सर्वर या क्लाउड पर होता है। इस स्थिति में अधिकार क्षेत्र, न्याय सहयोग और डेटा एक्सेस की समस्याएँ उत्पन्न होती हैं।

6. डाटा संरक्षण और संग्रहण की चुनौती: साक्ष्य का संग्रहण और संरक्षा (Chain of Custody) न्यायिक प्रक्रिया की विश्वसनीयता के लिए अनिवार्य है। यदि डेटा असुरक्षित तरीके से संग्रहित हुआ, तो उसका प्रमाणिक होना संदेहास्पद हो सकता है।

सुधार की दिशा

1. विशेष डिजिटल फॉरेंसिक प्रयोगशालाएँ: सभी न्यायालयों और पुलिस विभागों में डिजिटल फॉरेंसिक लैब स्थापित की जानी चाहिए। इससे इलेक्ट्रॉनिक साक्ष्य की त्वरित और सुरक्षित जाँच संभव होगी।

2. तकनीकी प्रशिक्षण और क्षमता निर्माण: न्यायिक अधिकारियों, अभियोजकों और पुलिस कर्मियों के लिए नियमित प्रशिक्षण कार्यक्रम आयोजित किए जाने चाहिए, ताकि वे डिजिटल साक्ष्यों का सही मूल्यांकन कर सकें।

3. स्पष्ट कानूनी दिशा-निर्देश: साक्ष्य संग्रहण, प्रमाणन, संरक्षा और अदालत में प्रस्तुति के लिए स्पष्ट दिशा-निर्देश बनाए जाने चाहिए। इससे न्यायिक प्रक्रिया में पारदर्शिता और विश्वसनीयता बढ़ेगी।

4. डाटा संरक्षण कानून का सुदृढ़ीकरण: डिजिटल साक्ष्यों की सुरक्षा और व्यक्तिगत गोपनीयता सुनिश्चित करने के लिए डाटा संरक्षण कानून को मजबूत करना आवश्यक है।

5. अंतरराष्ट्रीय सहयोग और समझौते: विदेश में स्थित डिजिटल डेटा को एक्सेस करने और अपराधियों को न्यायिक प्रक्रिया में लाने के लिए अंतरराष्ट्रीय सहयोग और समझौते की आवश्यकता है।

6. तकनीकी उपकरण और सॉफ्टवेयर में नवाचार: अपराध अन्वेषण और साक्ष्य विश्लेषण में नवीन तकनीकी उपकरण और सॉफ्टवेयर का विकास न्यायिक प्रक्रिया को और अधिक प्रभावी बना सकता है।

निष्कर्ष

तकनीकी साक्ष्य और डिजिटल फॉरेंसिक आज की न्यायिक प्रक्रिया का अभिन्न हिस्सा बन चुके हैं। जैसे-जैसे अपराध और विवाद डिजिटल माध्यमों पर आधारित होते जा रहे हैं, न्यायपालिका ने पारंपरिक साक्ष्यों के साथ-साथ तकनीकी और इलेक्ट्रॉनिक साक्ष्यों को भी समान रूप से महत्व देना शुरू कर दिया है। तकनीकी साक्ष्य न केवल अपराध की सटीक पहचान में सहायक हैं, बल्कि घटना के समय, स्थान और परिस्थितियों का वास्तविक चित्र प्रस्तुत करके न्यायिक निर्णयों की विश्वसनीयता को भी बढ़ाते हैं। डिजिटल फॉरेंसिक की शाखाएँ जैसे कंप्यूटर फॉरेंसिक, मोबाइल फॉरेंसिक, नेटवर्क फॉरेंसिक और मल्टीमीडिया फॉरेंसिक, अपराधों के विविध पहलुओं का विश्लेषण करने में महत्वपूर्ण भूमिका निभाती हैं। न्यायालयों ने तकनीकी साक्ष्य के प्रति समय के साथ संतुलित और वैज्ञानिक दृष्टिकोण अपनाया है। हालाँकि, तकनीकी साक्ष्य के उपयोग में चुनौतियाँ भी हैं। इनमें डेटा की छेड़छाड़, प्रमाणन की जटिलता, विशेषज्ञता की कमी, गोपनीयता और निजता से जुड़े मुद्दे, और अंतरराष्ट्रीय स्तर पर डेटा की उपलब्धता शामिल हैं। इन चुनौतियों का समाधान डिजिटल फॉरेंसिक लैब्स का निर्माण, न्यायिक अधिकारियों और पुलिस कर्मियों का तकनीकी प्रशिक्षण, स्पष्ट कानूनी दिशा-निर्देश और अंतरराष्ट्रीय सहयोग के माध्यम से किया जा सकता है। इसके साथ ही नवाचार और उन्नत तकनीकी उपकरणों का उपयोग न्यायिक प्रक्रिया को और प्रभावी बना सकता है।

अंततः कहा जा सकता है कि तकनीकी साक्ष्य केवल सहायक साधन नहीं हैं, बल्कि आधुनिक न्यायपालिका में निर्णय की गुणवत्ता, सटीकता और निष्पक्षता सुनिश्चित करने वाले प्रमुख घटक बन गए हैं। यह अपराध अन्वेषण को वैज्ञानिक और तर्कसंगत बनाते हैं और समाज में न्याय व्यवस्था के प्रति विश्वास को मजबूत करते हैं। यदि कानूनी सुधार, प्रशिक्षण और तकनीकी अवसंरचना में लगातार सुधार किया जाता रहा, तो तकनीकी साक्ष्य न केवल वर्तमान अपराधों के समाधान में सहायक होंगे, बल्कि भविष्य के डिजिटल और साइबर अपराधों से निपटने के लिए न्याय प्रणाली की क्षमता को भी बढ़ाएंगे।

संदर्भग्रंथ सूची (Bibliography)

- राजाराम यादव, भारतीय साक्ष्य अधिनियम, 2023 (सेंट्रल लॉ एजेंसी, 2025)
- बसंतलाल बबेल, भारतीय साक्ष्य अधिनियम, 2023 (यूनिवर्सिटी बुक हाउस, 2024)
- कर्णिका सेठ, साइबर कानून: सिद्धांत और अभ्यास (LexisNexis, 2019)
- स्विगर्ट, के और कोट्ज़, एच, एन इंट्रोडक्शन टू कम्पेरेटिव लॉ (टोनी वीयर अनुवाद, 3rd संस्करण, ऑक्सफोर्ड यूनिवर्सिटी प्रेस 1998)
- डॉ. मोहन सिंह, डिजिटल साक्ष्य और भारतीय न्यायपालिका (LexisNexis, 2022)
- राहुल देव, 'डिजिटल साक्ष्य और उनकी कानूनी स्थिति' (2026) 10 Journal of Cyber Evidence 168
- साक्षी मल्होत्रा, 'डिजिटल फॉरेंसिक उपकरणों का न्यायिक परीक्षण' (2024) 8 Journal of Forensic Sciences 145
- डॉ. नीलम शर्मा, डिजिटल साक्ष्य: कानूनी और तकनीकी दृष्टिकोण (Eastern Book Company, 2021)
- रोस, फ्रांसिस, 'द इवोल्यूशन ऑफ द स्पीशीज़' एंड्रयू बुरोज और एलेन रॉडगर (संपादक), मैपिंग द लॉ: एसेज़ इन मेमोरी ऑफ पीटर बिर्क्स (ऑक्सफोर्ड यूनिवर्सिटी प्रेस 2006)
- क्रेग, पॉल, 'थ्योरी, 'प्योर थ्योरी' और पब्लिक लॉ में वैल्यूज़' [2005] पब्लिक लॉ 440
- बटुक लाल, भारतीय साक्ष्य अधिनियम, 2023 (एबीसी वेबस्टोर, 2025)

- ग्रीनलीफ, जी, 'फ्री एक्सेस टू लीगल इंफॉर्मेशन का वैश्विक विकास' (2010) 1(1) यूरोपीय जर्नल ऑफ लीगल टेक्नोलॉजी http://ejlt.org//article/view/17
- क्लार्कसन, सीएमवी, क्रिमिनल लॉ: टेक्स्ट एंड मटेरियल्स (7वीं संस्करण, स्वीट एंड मैक्सवेल 2010)
- न्यूवर्क, एफएच, 'न्यूसेंस की सीमाएँ' (1949) 65 लॉ क्वार्टरली रिव्यू 480
- किडनर, रिचर्ड, 'न्यूसेंस और प्रॉपर्टी के अधिकार' [1998] कान्वेन्स 267
- ओलिफेंट, के, 'न्यूसेंस की सीमाओं को अस्पष्ट करना' (1998) 6 टॉर्ट लॉ रिव्यू 21
- गिलिकर, पाउला, 'हंटर बनाम कैनरी व्हार्फ में मुकदमा करने के अधिकार पर प्रतिबंधों के प्रभाव' (1999) 7 टॉर्ट्स लॉ जर्नल 155
- डॉ. राकेश कुमार यादव, सूचना प्रौद्योगिकी अधिनियम और डिजिटल साक्ष्य (Central Law Publications, 2020)