Knowledgeable Research (KR) 2026, Vol., (5):02
ISSN: 2583-6633, CODEN: KRABAU
International open-access peer-reviewed refereed monthly journal
https://knowledgeableresearch.com/index.php/1

भारतीय समाज में उभरते साइबर अपराध: स्वरूप, कारण एवं विधिक नियंत्रण की समीक्षा

[1]ऋषिकेश यादव (शोध छात्र)*
[2]डा निधि शर्मा, एसोसिएट प्रोफेसर
विधि संकाय, आगरा कालेज आगरा

Abstract

वर्तमान समय में डिजिटल तकनीक के व्यापक विस्तार ने भारतीय समाज की संरचना और कार्यप्रणाली में गहरा परिवर्तन किया है। इंटरनेट, मोबाइल फोन, ऑनलाइन लेन–देन और सोशल मीडिया के बढ़ते उपयोग ने जहाँ जीवन को अधिक सुविधाजनक बनाया है, वहीं साइबर अपराधों की समस्या को भी गंभीर रूप से बढ़ाया है। आज साइबर अपराध केवल तकनीकी समस्या नहीं रह गया है, बल्कि यह सामाजिक, आर्थिक और नैतिक आयामों से जुड़ी एक जटिल चुनौती बन चुका है।भारतीय परिप्रेक्ष्य में साइबर अपराध के विविध रूप देखने को मिलते हैं, जैसे ऑनलाइन ठगी, पहचान की चोरी, साइबर उत्पीड़न, फर्जी वेबसाइटों के माध्यम से धोखाधड़ी, डेटा की अवैध चोरी तथा अश्लील या आपत्तिजनक सामग्री का प्रसार। डिजिटल माध्यमों की आसान उपलब्धता और उपयोगकर्ताओं की असावधानी अपराधियों को अवसर प्रदान करती है। विशेष रूप से डिजिटल साक्षरता की कमी, तकनीकी जानकारी का अभाव, त्वरित आर्थिक लाभ की प्रवृत्ति और साइबर सुरक्षा उपायों की अनदेखी इन अपराधों को बढ़ावा देती है।

साइबर अपराधों का प्रभाव केवल व्यक्तिगत स्तर तक सीमित नहीं है, बल्कि यह सामाजिक विश्वास, आर्थिक स्थिरता और राष्ट्रीय सुरक्षा को भी प्रभावित करता है। ऑनलाइन बैंकिंग और डिजिटल भुगतान प्रणालियों में बढ़ती निर्भरता के कारण आर्थिक अपराधों की संभावना और अधिक बढ़ गई है। इसके अतिरिक्त, इंटरनेट की गुमनामी अपराधियों के लिए पहचान छिपाने का माध्यम बनती है, जिससे अपराध की जांच और नियंत्रण जटिल हो जाता है।विधिक नियंत्रण के संदर्भ में भारत में सूचना प्रौद्योगिकी संबंधी कानूनों तथा दंडात्मक प्रावधानों के माध्यम से साइबर अपराधों को नियंत्रित करने का प्रयास किया गया है। फिर भी, बदलती तकनीक और अपराध के नए स्वरूपों को देखते हुए कानूनों के प्रभावी क्रियान्वयन, जन-जागरूकता, डिजिटल साक्षरता और सुदृढ़ साइबर सुरक्षा तंत्र की आवश्यकता अत्यंत महत्वपूर्ण है।.

Keywords: *साइबर अपराध, डिजिटल साक्षरता, ऑनलाइन धोखाधड़ी, डेटा सुरक्षा, विधिक नियंत्रण।*

Received: 08/01/2026
Accepted: 26/02/2026
Published: 28/02/2026

***Corresponding Author:**
ऋषिकेश यादव (शोध छात्र)
Email: yadavr1399@gmail.com

प्रस्तावना

21वीं सदी को सूचना एवं संचार प्रौद्योगिकी के युग के रूप में जाना जाता है। इंटरनेट, कंप्यूटर, स्मार्टफोन और डिजिटल नेटवर्किंग के तीव्र विकास ने वैश्विक समाज की संरचना में व्यापक परिवर्तन किया है। भारत भी इस परिवर्तन से अछूता नहीं रहा। पिछले एक दशक में देश में डिजिटल सेवाओं का अभूतपूर्व विस्तार हुआ है, जिसके परिणामस्वरूप शासन, शिक्षा, व्यापार, बैंकिंग और सामाजिक संवाद के स्वरूप में आमूलचूल परिवर्तन देखने को मिला है। डिजिटल प्लेटफॉर्म और ऑनलाइन लेन–देन की बढ़ती प्रवृत्ति ने नागरिकों को त्वरित, पारदर्शी और सुलभ सेवाएँ प्रदान की हैं।

डिजिटल क्रांति के इस दौर में इंटरनेट की पहुँच ग्रामीण क्षेत्रों तक विस्तारित हुई है। सरकारी पहलों और तकनीकी नवाचारों ने नागरिकों को डिजिटल पहचान, ऑनलाइन बैंकिंग, ई–कॉमर्स और सामाजिक मीडिया के माध्यम से एक नई सामाजिक-आर्थिक

गतिशीलता प्रदान की है। विशेष रूप से 'डिजिटल इंडिया' कार्यक्रम[1] ने प्रशासनिक सेवाओं को ऑनलाइन माध्यम से उपलब्ध कराकर सुशासन को सुदृढ़ करने का प्रयास किया है। इसके परिणामस्वरूप आम नागरिक का जीवन अधिक सुविधाजनक और तीव्रगामी हुआ है।

किन्तु तकनीकी प्रगति के साथ-साथ साइबर अपराधों की समस्या भी गंभीर रूप से उभरी है। इंटरनेट और स्मार्टफोन की व्यापक उपलब्धता ने जहाँ एक ओर संचार को सरल बनाया है, वहीं दूसरी ओर अपराधियों को नए अवसर भी प्रदान किए हैं। हैकिंग, ऑनलाइन वित्तीय धोखाधड़ी, पहचान की चोरी, साइबर बुलिंग और डेटा उल्लंघन जैसी घटनाएँ निरंतर बढ़ रही हैं। सोशल मीडिया प्लेटफॉर्म जैसे Facebook और WhatsApp के माध्यम से गलत सूचनाओं का प्रसार, फर्जी प्रोफाइल बनाकर ठगी तथा व्यक्तिगत गोपनीयता का उल्लंघन आम होता जा रहा है।

साइबर अपराधों की वृद्धि के पीछे कई कारण उत्तरदायी हैं। डिजिटल साक्षरता की कमी, साइबर सुरक्षा उपायों के प्रति लापरवाही, बेरोजगारी, त्वरित आर्थिक लाभ की मानसिकता तथा इंटरनेट की गुमनामी अपराधियों को प्रोत्साहित करती है। इसके अतिरिक्त, तकनीकी विकास की गति कानूनों और नियामक व्यवस्थाओं की तुलना में अधिक तेज है, जिसके कारण अपराध नियंत्रण की प्रक्रिया जटिल हो जाती है।

भारतीय विधि व्यवस्था ने साइबर अपराधों की रोकथाम हेतु महत्वपूर्ण कदम उठाए हैं। सूचना प्रौद्योगिकी अधिनियम, 2000 के माध्यम से साइबर अपराधों को परिभाषित कर उनके लिए दंडात्मक प्रावधान निर्धारित किए गए हैं। साथ ही, भारतीय न्याय संहिता के अंतर्गत भी कई अपराधों को साइबर माध्यम से किए जाने पर लागू किया जाता है[2]। तथापि, बदलते तकनीकी परिदृश्य में केवल विधिक प्रावधान पर्याप्त नहीं हैं; इसके लिए जन-जागरूकता, तकनीकी दक्षता और संस्थागत सुदृढ़ीकरण भी आवश्यक है।

21वीं सदी में डिजिटल सशक्तिकरण और साइबर अपराध एक साथ उभरती हुई वास्तविकताएँ हैं। जहाँ डिजिटल तकनीक ने भारतीय समाज को नई दिशा प्रदान की है, वहीं साइबर अपराधों ने सामाजिक सुरक्षा, आर्थिक स्थिरता और विधिक व्यवस्था के समक्ष गंभीर चुनौती प्रस्तुत की है। इस संदर्भ में साइबर अपराधों के स्वरूप, कारणों और विधिक नियंत्रण की सम्यक समीक्षा अत्यंत आवश्यक हो जाती है।

2. साइबर अपराध का स्वरूप

साइबर अपराध वे अपराध हैं जो कंप्यूटर, इंटरनेट या अन्य डिजिटल माध्यमों के द्वारा किए जाते हैं। भारतीय समाज में इनके विविध स्वरूप देखने को मिलते हैं। प्रमुख प्रकारों का संक्षिप्त विवरण निम्नलिखित है—

i. हैकिंग एवं डाटा चोरी

हैकिंग वह प्रक्रिया है जिसके माध्यम से कोई व्यक्ति अनधिकृत रूप से किसी कंप्यूटर प्रणाली, सर्वर या नेटवर्क में प्रवेश कर संवेदनशील सूचनाओं तक पहुँच प्राप्त करता है। डाटा चोरी में व्यक्तिगत, वित्तीय या सरकारी गोपनीय सूचनाओं को अवैध रूप से प्राप्त कर उनका दुरुपयोग किया जाता है। आज के डिजिटल युग में बैंकिंग विवरण, आधार संख्या, पासवर्ड और आधिकारिक दस्तावेज साइबर अपराधियों के प्रमुख लक्ष्य बन चुके हैं। कई बार सरकारी वेबसाइटों या निजी कंपनियों के सर्वर पर हमला कर बड़ी मात्रा में डेटा चुराया जाता है, जिससे राष्ट्रीय सुरक्षा और नागरिकों की गोपनीयता प्रभावित होती है। हैकिंग की घटनाएँ न केवल आर्थिक हानि पहुँचाती हैं, बल्कि संस्थागत विश्वसनीयता को भी कमजोर करती हैं। ऐसे अपराधों के नियंत्रण हेतु सूचना प्रौद्योगिकी अधिनियम, 2000 में दंडात्मक प्रावधान किए गए हैं।[3]

ii. ऑनलाइन वित्तीय धोखाधड़ी

[1] भारत सरकार, डिजिटल इंडिया कार्यक्रम, 2015.

[2] भारतीय न्याय संहिता, 2023 की प्रासंगिक धाराएँ।

[3] सूचना प्रौद्योगिकी अधिनियम, 2000, धारा 43 एवं 66।

ऑनलाइन वित्तीय धोखाधड़ी वर्तमान समय का सबसे सामान्य साइबर अपराध है। डिजिटल भुगतान प्रणाली, नेट बैंकिंग, यूपीआई और क्रेडिट/डेबिट कार्ड के बढ़ते उपयोग ने सुविधा तो प्रदान की है, परंतु जोखिम भी बढ़ाया है। अपराधी फर्जी कॉल, मैसेज या लिंक के माध्यम से बैंक विवरण और ओटीपी प्राप्त कर धन की अवैध निकासी करते हैं। कई मामलों में नकली ग्राहक सेवा प्रतिनिधि बनकर लोगों को भ्रमित किया जाता है। डिजिटल लेन-देन में असावधानी और साइबर सुरक्षा के प्रति जागरूकता की कमी ऐसे अपराधों को बढ़ावा देती है। इन धोखाधड़ियों से न केवल व्यक्ति को आर्थिक क्षति होती है, बल्कि डिजिटल बैंकिंग प्रणाली पर विश्वास भी कम होता है। इस प्रकार के अपराधों पर नियंत्रण हेतु भारतीय न्याय संहिता और सूचना प्रौद्योगिकी संबंधी कानून लागू होते हैं।[4]

iii. फिशिंग एवं स्पूफिंग

फिशिंग एक ऐसी विधि है जिसमें अपराधी नकली ईमेल, वेबसाइट या संदेश के माध्यम से उपयोगकर्ता को भ्रमित कर उसकी गोपनीय जानकारी प्राप्त करता है। स्पूफिंग में अपराधी किसी विश्वसनीय संस्था या व्यक्ति की पहचान का दुरुपयोग कर धोखाधड़ी करता है। उदाहरणस्वरूप, बैंक या सरकारी विभाग के नाम से फर्जी ईमेल भेजकर पासवर्ड और बैंक विवरण माँगे जाते हैं। कई बार नकली वेबसाइट वास्तविक वेबसाइट की तरह ही दिखाई देती है, जिससे आम व्यक्ति धोखे में आ जाता है। इन अपराधों की सफलता का मुख्य कारण तकनीकी जागरूकता का अभाव है। फिशिंग और स्पूफिंग के मामलों में साइबर सुरक्षा तंत्र और उपयोगकर्ता सतर्कता अत्यंत आवश्यक है।

iv. साइबर बुलिंग एवं ट्रोलिंग

साइबर बुलिंग और ट्रोलिंग मुख्यतः सोशल मीडिया प्लेटफॉर्म के माध्यम से की जाने वाली मानसिक उत्पीड़न की गतिविधियाँ हैं। Facebook, Instagram और WhatsApp जैसे मंचों पर अपमानजनक टिप्पणी, धमकी, अफवाह या चरित्र हनन की घटनाएँ बढ़ रही हैं। विशेष रूप से महिलाएँ और किशोर वर्ग इसका अधिक शिकार होते हैं। यह अपराध मानसिक तनाव, अवसाद और सामाजिक अलगाव जैसी गंभीर समस्याओं को जन्म देता है। कई बार यह उत्पीड़न आत्मसम्मान को गहरी चोट पहुँचाता है। साइबर बुलिंग से निपटने के लिए कानूनी प्रावधानों के साथ-साथ सामाजिक जागरूकता और डिजिटल नैतिकता की आवश्यकता है।[5]

v. रैनसमवेयर हमले

रैनसमवेयर एक प्रकार का दुर्भावनापूर्ण सॉफ्टवेयर (मैलवेयर) है जो कंप्यूटर या नेटवर्क के डेटा को एन्क्रिप्ट कर उसे लॉक कर देता है। इसके बाद अपराधी डेटा को पुनः उपलब्ध कराने के लिए फिरौती की मांग करता है। यह हमला व्यक्तिगत उपयोगकर्ताओं के साथ-साथ सरकारी संस्थानों और बड़ी कंपनियों को भी प्रभावित करता है। रैनसमवेयर हमले से महत्वपूर्ण दस्तावेज और सेवाएँ बाधित हो जाती हैं, जिससे आर्थिक और प्रशासनिक संकट उत्पन्न होता है। कई बार अंतरराष्ट्रीय स्तर पर संचालित गिरोह इन हमलों को अंजाम देते हैं, जिससे जांच प्रक्रिया जटिल हो जाती है। साइबर सुरक्षा उपायों, नियमित बैकअप और मजबूत एंटीवायरस प्रणाली से इस प्रकार के हमलों की रोकथाम संभव है।

vi. पहचान की चोरी

पहचान की चोरी में अपराधी किसी व्यक्ति की व्यक्तिगत जानकारी—जैसे आधार संख्या, पैन कार्ड, बैंक विवरण या सोशल मीडिया प्रोफाइल—का दुरुपयोग कर स्वयं को उस व्यक्ति के रूप में प्रस्तुत करता है। इसके माध्यम से वित्तीय लेन-देन, फर्जी खाते खोलना या आपराधिक गतिविधियाँ की जाती हैं। डिजिटल युग में व्यक्तिगत जानकारी का अत्यधिक ऑनलाइन साझा किया जाना इस अपराध को बढ़ावा देता है।

[4] भारतीय न्याय संहिता, 2023 की प्रासंगिक धाराएँ (धोखाधड़ी संबंधी)।

[5] सूचना प्रौद्योगिकी अधिनियम, 2000 तथा अन्य दंडात्मक प्रावधान।

पहचान की चोरी से व्यक्ति की प्रतिष्ठा और आर्थिक स्थिति दोनों प्रभावित हो सकती हैं। इस प्रकार के अपराधों की रोकथाम हेतु डेटा सुरक्षा, मजबूत पासवर्ड और दो-स्तरीय प्रमाणीकरण (Two-Factor Authentication) जैसे उपाय आवश्यक हैं।

3. साइबर अपराध के कारण

i. डिजिटल साक्षरता की कमी

डिजिटल साक्षरता का तात्पर्य कंप्यूटर, इंटरनेट और ऑनलाइन सेवाओं के सुरक्षित एवं प्रभावी उपयोग की समझ से है। भारत में इंटरनेट उपयोगकर्ताओं की संख्या तेजी से बढ़ी है, किंतु इसके अनुपात में साइबर सुरक्षा संबंधी जागरूकता का स्तर पर्याप्त नहीं है। ग्रामीण क्षेत्रों के साथ-साथ शहरी क्षेत्रों में भी अनेक लोग फर्जी लिंक, संदिग्ध कॉल और नकली वेबसाइटों की पहचान नहीं कर पाते। परिणामस्वरूप वे आसानी से ऑनलाइन ठगी और फिशिंग का शिकार बन जाते हैं। डिजिटल भुगतान प्रणालियों के प्रसार के बावजूद सुरक्षित लेन–देन के मूलभूत नियमों की जानकारी का अभाव गंभीर समस्या है। इस स्थिति से साइबर अपराधियों को अवसर मिलता है। अतः डिजिटल साक्षरता अभियान और साइबर जागरूकता कार्यक्रमों का व्यापक प्रसार अत्यंत आवश्यक है।[6]

ii. तकनीकी विकास की तीव्र गति

तकनीकी विकास अत्यंत तीव्र गति से हो रहा है, जबकि कानूनों और नियामक व्यवस्थाओं का संशोधन अपेक्षाकृत धीमा होता है। नई-नई डिजिटल तकनीकें, कृत्रिम बुद्धिमत्ता, क्लाउड कंप्यूटिंग और एन्क्रिप्शन प्रणालियाँ लगातार विकसित हो रही हैं, जिनका दुरुपयोग अपराधी नए तरीकों से करते हैं। कई बार विधिक प्रावधान पुराने पड़ जाते हैं और उभरते साइबर अपराधों को समुचित रूप से परिभाषित नहीं कर पाते। इस अंतर के कारण अपराधियों को कानूनी खामियों का लाभ उठाने का अवसर मिलता है। साथ ही, जांच एजेंसियों के पास पर्याप्त तकनीकी संसाधन और विशेषज्ञता का अभाव भी समस्या को जटिल बनाता है। अतः कानून और तकनीक के बीच संतुलन स्थापित करना आवश्यक है।[7]

iii. आर्थिक लालच एवं बेरोजगारी

साइबर अपराध के पीछे आर्थिक लाभ की प्रवृत्ति एक प्रमुख कारण है। बेरोजगारी और त्वरित धन अर्जित करने की मानसिकता युवाओं को गलत दिशा में प्रेरित कर सकती है। इंटरनेट के माध्यम से कम जोखिम में अधिक धन कमाने की संभावना अपराधियों को आकर्षित करती है। कई बार संगठित गिरोह युवाओं को तकनीकी कौशल का दुरुपयोग कर ऑनलाइन धोखाधड़ी, हैकिंग या डेटा चोरी जैसे अपराधों में शामिल करते हैं। आर्थिक असमानता और सामाजिक दबाव भी इस प्रवृत्ति को बढ़ावा देते हैं। इस समस्या के समाधान के लिए रोजगार सृजन, कौशल विकास और नैतिक शिक्षा की आवश्यकता है, ताकि युवा वर्ग अपनी तकनीकी क्षमता का सकारात्मक उपयोग कर सके।[8]

vi. सुरक्षा उपायों की कमी

अनेक उपयोगकर्ता मजबूत पासवर्ड, दो-स्तरीय प्रमाणीकरण और एंटीवायरस सुरक्षा जैसे बुनियादी उपायों को अपनाने में लापरवाही करते हैं। सार्वजनिक वाई-फाई नेटवर्क का असुरक्षित उपयोग, संदिग्ध ऐप डाउनलोड करना तथा समय-समय पर सॉफ्टवेयर अपडेट न करना साइबर हमलों की संभावना बढ़ाता है। संस्थागत स्तर पर भी कई बार डेटा सुरक्षा नीतियों और साइबर सुरक्षा ढांचे में कमियाँ पाई जाती हैं। कमजोर सुरक्षा तंत्र अपराधियों के लिए आसान लक्ष्य सिद्ध होता है। यदि व्यक्ति और संस्थाएँ बुनियादी साइबर सुरक्षा मानकों का पालन करें, तो

[6] सूचना प्रौद्योगिकी अधिनियम, 2000 की प्रासंगिक धाराएँ।

[7] भारत सरकार द्वारा समय-समय पर जारी साइबर सुरक्षा दिशा-निर्देश।

[8] भारतीय न्याय संहिता, 2023 की प्रासंगिक धाराएँ।

कई अपराधों को रोका जा सकता है। इसलिए तकनीकी सुरक्षा उपायों को सुदृढ़ करना अत्यंत आवश्यक है।[9]

v. गोपनीयता के प्रति लापरवाही

डिजिटल युग में लोग सोशल मीडिया और अन्य ऑनलाइन प्लेटफॉर्म पर अपनी व्यक्तिगत जानकारी खुलकर साझा करते हैं। जन्मतिथि, पता, फोन नंबर, बैंक संबंधी विवरण या यात्रा संबंधी जानकारी सार्वजनिक करना अपराधियों को पहचान की चोरी और धोखाधड़ी का अवसर प्रदान करता है। कई बार उपयोगकर्ता गोपनीयता सेटिंग्स का सही उपयोग नहीं करते, जिससे उनकी निजी जानकारी असुरक्षित हो जाती है। इस प्रकार की लापरवाही साइबर अपराधों को बढ़ावा देती है। व्यक्तिगत डेटा की सुरक्षा के प्रति जागरूकता और सावधानी बरतना अत्यंत आवश्यक है। डिजिटल गोपनीयता के संरक्षण हेतु कानूनी प्रावधानों के साथ-साथ व्यक्तिगत जिम्मेदारी भी महत्वपूर्ण है।[10]

4. विधिक नियंत्रण एवं प्रावधान

i. सूचना प्रौद्योगिकी अधिनियम, 2000

सूचना प्रौद्योगिकी अधिनियम, 2000 भारत में साइबर अपराधों से निपटने के लिए बनाया गया प्रमुख कानून है। इस अधिनियम के माध्यम से इलेक्ट्रॉनिक अभिलेखों और डिजिटल हस्ताक्षरों को वैधानिक मान्यता प्रदान की गई तथा कंप्यूटर संसाधनों के दुरुपयोग को दंडनीय बनाया गया। अधिनियम की धारा 43 और 66 में हैकिंग, डाटा चोरी और अनधिकृत प्रवेश जैसे अपराधों के लिए दंड का प्रावधान है। इसके अतिरिक्त, अश्लील सामग्री के प्रकाशन, पहचान की चोरी और साइबर आतंकवाद से संबंधित प्रावधान भी इसमें सम्मिलित हैं। यह अधिनियम ई–कॉमर्स और ई–गवर्नेंस को कानूनी आधार प्रदान करता है। समय-समय पर इसमें संशोधन कर इसे अधिक प्रभावी बनाने का प्रयास किया गया है, ताकि बदलती तकनीक के अनुरूप साइबर अपराधों पर नियंत्रण स्थापित किया जा सके।[11]

ii. भारतीय न्याय संहिता, 2023

भारतीय न्याय संहिता, 2023 पारंपरिक आपराधिक कानून है, किंतु इसके कई प्रावधान साइबर अपराधों पर भी लागू होते हैं। धोखाधड़ी, जालसाजी, मानहानि, आपराधिक धमकी और विश्वासघात जैसे अपराध यदि डिजिटल माध्यम से किए जाते हैं, तो संबंधित धाराएँ लागू की जाती हैं। उदाहरणस्वरूप, ऑनलाइन वित्तीय धोखाधड़ी के मामलों में धोखाधड़ी से संबंधित धाराएँ प्रयोज्य होती हैं। इसी प्रकार, सोशल मीडिया के माध्यम से मानहानि या धमकी देने पर भी दंडात्मक कार्रवाई की जा सकती है। यद्यपि यह संहिता मूलतः पारंपरिक अपराधों को ध्यान में रखकर बनाई गई थी, फिर भी इसकी व्यापक परिभाषाएँ साइबर अपराधों को भी आच्छादित करती हैं। सूचना प्रौद्योगिकी अधिनियम के साथ मिलकर यह साइबर अपराध नियंत्रण की विधिक संरचना को सुदृढ़ बनाती है।[12]

iii. आईटी (संशोधन) अधिनियम, 2008

सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 के माध्यम से मूल अधिनियम में महत्वपूर्ण परिवर्तन किए गए। इस संशोधन ने डेटा सुरक्षा, गोपनीयता संरक्षण और साइबर आतंकवाद जैसे गंभीर अपराधों को स्पष्ट रूप से परिभाषित किया। धारा 66एफ के अंतर्गत साइबर आतंकवाद को दंडनीय अपराध घोषित किया गया। इसके अतिरिक्त, मध्यस्थों (Intermediaries) की जिम्मेदारी निर्धारित की गई, जिससे सोशल मीडिया और अन्य डिजिटल प्लेटफॉर्म को आपत्तिजनक सामग्री के नियंत्रण हेतु उत्तरदायी बनाया गया। इस संशोधन का उद्देश्य तेजी से बदलते डिजिटल परिवेश के अनुरूप कानूनी ढांचे को सशक्त करना था।

[9] सूचना प्रौद्योगिकी अधिनियम, 2000 की प्रासंगिक धाराएँ।

[10] भारत सरकार द्वारा समय-समय पर जारी साइबर सुरक्षा दिशा-निर्देश।

[11] सूचना प्रौद्योगिकी अधिनियम, 2000 एवं उसका संशोधन अधिनियम, 2008।

[12] "सोशल मीडिया में साइबर अपराध के रुझान।" *साइबरसिक्योरिटी रिसर्च जर्नल*, खंड 4, अंक 2, 2021, पृष्ठ 50–68।

यह अधिनियम साइबर अपराधों की प्रकृति और जटिलता को ध्यान में रखते हुए व्यापक दंडात्मक प्रावधान प्रदान करता है।[13]

iv. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

साइबर अपराधों की शिकायतों के त्वरित निवारण हेतु भारत सरकार ने राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल की स्थापना की है। इस ऑनलाइन मंच के माध्यम से नागरिक घर बैठे साइबर अपराधों की शिकायत दर्ज कर सकते हैं। विशेष रूप से महिलाओं और बच्चों के विरुद्ध ऑनलाइन अपराधों की रिपोर्टिंग के लिए यह पोर्टल उपयोगी सिद्ध हुआ है। शिकायत दर्ज होने के पश्चात संबंधित राज्य की कानून प्रवर्तन एजेंसी को जांच के लिए प्रेषित किया जाता है। यह पहल साइबर अपराध नियंत्रण में पारदर्शिता और त्वरित कार्रवाई सुनिश्चित करने का प्रयास है। डिजिटल प्लेटफॉर्म के माध्यम से शिकायत प्रक्रिया को सरल बनाकर सरकार ने नागरिक सहभागिता को प्रोत्साहित किया है।[14]

v. CERT-In की भूमिका

CERT-In (Computer Emergency Response Team–India) भारत की राष्ट्रीय साइबर सुरक्षा एजेंसी है। इसका मुख्य कार्य साइबर सुरक्षा घटनाओं की निगरानी, विश्लेषण और समाधान प्रदान करना है। यह संस्था विभिन्न संगठनों को सुरक्षा दिशा-निर्देश जारी करती है तथा साइबर हमलों के प्रति सतर्क रहने की सलाह देती है। बड़े पैमाने पर होने वाले डेटा उल्लंघन या रैनसमवेयर हमलों की स्थिति में CERT-In तकनीकी सहायता और समन्वय प्रदान करता है। यह एजेंसी साइबर सुरक्षा ढांचे को सुदृढ़ बनाने और राष्ट्रीय स्तर पर त्वरित प्रतिक्रिया सुनिश्चित करने में महत्वपूर्ण भूमिका निभाती है।[15]

5. प्रमुख न्यायिक निर्णय

i. तमिलनाडु राज्य बनाम सुहास कत्ती

यह भारत का पहला चर्चित साइबर अपराध मामला माना जाता है, जिसमें अभियुक्त ने एक महिला के नाम से फर्जी ईमेल और संदेश प्रसारित कर उसकी मानहानि की। न्यायालय ने सूचना प्रौद्योगिकी अधिनियम, 2000 और भारतीय न्याय संहिता की प्रासंगिक धाराओं के अंतर्गत दोषसिद्धि दी। यह मामला इस दृष्टि से महत्वपूर्ण है कि इसमें डिजिटल साक्ष्यों को स्वीकार कर त्वरित निर्णय दिया गया। इस निर्णय ने स्पष्ट किया कि ऑनलाइन मानहानि और उत्पीड़न भी दंडनीय अपराध हैं।[16]

ii. श्रेया सिंघल बनाम यूनियन आफ इण्डिया

इस ऐतिहासिक मामले में सर्वोच्च न्यायालय ने सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 66A को असंवैधानिक घोषित कर दिया। न्यायालय ने माना कि यह प्रावधान अभिव्यक्ति की स्वतंत्रता का उल्लंघन करता है। यह निर्णय साइबर कानून और मौलिक अधिकारों के संतुलन की दृष्टि से अत्यंत महत्वपूर्ण है। इससे यह सिद्ध हुआ कि साइबर स्पेस में भी संवैधानिक मूल्यों की रक्षा आवश्यक है।[17]

iii. अनवर पी.वी. बनाम पी.के. बशीर

इस मामले में सर्वोच्च न्यायालय ने इलेक्ट्रॉनिक साक्ष्य की स्वीकार्यता के संबंध में महत्वपूर्ण दिशा-निर्देश दिए। न्यायालय ने कहा कि इलेक्ट्रॉनिक रिकॉर्ड को साक्ष्य के रूप में प्रस्तुत करने हेतु भारतीय साक्ष्य अधिनियम की धारा 65B के अंतर्गत प्रमाणपत्र आवश्यक है। यह निर्णय साइबर अपराध मामलों में डिजिटल साक्ष्य की वैधानिकता सुनिश्चित करने में मील का पत्थर सिद्ध हुआ।[18]

iv. के.एस. पुत्तस्वामी बनाम भारत संघ

[13] भारतीय न्याय संहिता, 2023 की प्रासंगिक धाराएँ तथा भारत सरकार की आधिकारिक अधिसूचनाएँ।

[14] "भारत में साइबर अपराध: समस्याएँ और चुनौतियाँ।" *जर्नल ऑफ़ लॉ एंड टेक्नोलॉजी*, खंड 12, अंक 3, 2018, पृष्ठ 45–62।

[15] कुमार, राकेश. *साइबर क्राइम एंड लॉ*. नई दिल्ली: लॉ पब्लिकेशन, 2019.

[16] AIR 2004 Mad 135

[17] AIR 2015 SC 1523

[18] AIR 2014 SC 2435

इस ऐतिहासिक निर्णय में सर्वोच्च न्यायालय ने निजता के अधिकार को संविधान के अनुच्छेद 21 के अंतर्गत मौलिक अधिकार घोषित किया। यद्यपि यह मामला सीधे साइबर अपराध से संबंधित नहीं था, परंतु डिजिटल डेटा सुरक्षा और गोपनीयता संरक्षण के संदर्भ में इसका अत्यधिक महत्व है। इस निर्णय ने व्यक्तिगत डेटा के दुरुपयोग के विरुद्ध कानूनी संरक्षण को सुदृढ़ किया।[19]

v. अवनीश बजाज बनाम राज्य (दिल्ली राष्ट्रीय राजधानी क्षेत्र)

यह मामला ऑनलाइन प्लेटफॉर्म की उत्तरदायित्व (Liability) से संबंधित था। बाजी.कॉम वेबसाइट पर आपत्तिजनक सामग्री की बिक्री के कारण प्रबंध निदेशक पर अभियोग लगाया गया। न्यायालय ने मध्यस्थों (Intermediaries) की जिम्मेदारी और दायित्व की सीमा स्पष्ट की। यह निर्णय ई–कॉमर्स प्लेटफॉर्म और सोशल मीडिया कंपनियों की कानूनी जवाबदेही के निर्धारण में महत्वपूर्ण सिद्ध हुआ।[20]

6. साइबर अपराध से संबंधित चनुौतियाँ

i. अपराधियों की पहचान में कठिनाई (गुमनामी)

साइबर अपराधों की सबसे बड़ी चुनौती अपराधियों की पहचान स्थापित करना है। डिजिटल माध्यमों में गुमनामी (Anonymity) की सुविधा अपराधियों को अपनी वास्तविक पहचान छिपाने का अवसर प्रदान करती है। वे फर्जी ईमेल आईडी, आभासी निजी नेटवर्क (VPN), प्रॉक्सी सर्वर और नकली सोशल मीडिया प्रोफाइल का उपयोग कर अपराध को अंजाम देते हैं। कई मामलों में आईपी एड्रेस भी भ्रामक या परिवर्तित होता है, जिससे जांच एजेंसियों को वास्तविक स्रोत तक पहुँचने में कठिनाई होती है। इसके अतिरिक्त, साइबर अपराधों में डिजिटल साक्ष्य (Electronic Evidence) को सुरक्षित रखना और न्यायालय में प्रमाणित करना भी जटिल प्रक्रिया है। साक्ष्यों के साथ छेड़छाड़ या डेटा को शीघ्र नष्ट कर देने की संभावना जांच को और कठिन बना देती है। परिणामस्वरूप अपराधी अक्सर कानून की पकड़ से बच निकलते हैं। अतः उन्नत तकनीकी साधनों और प्रशिक्षित विशेषज्ञों की आवश्यकता अत्यंत महत्वपूर्ण हो जाती है।[21]

ii. अंतरराष्ट्रीय स्तर पर अपराध का संचालन

साइबर अपराधों की प्रकृति सीमा-रहित (Borderless) होती है। अपराधी एक देश में बैठकर दूसरे देश के नागरिकों या संस्थाओं को निशाना बना सकते हैं। इस अंतरराष्ट्रीय स्वरूप के कारण जांच और अभियोजन की प्रक्रिया अत्यंत जटिल हो जाती है। विभिन्न देशों के कानून, न्यायिक प्रक्रियाएँ और प्रत्यर्पण संबंधी नियम अलग-अलग होते हैं, जिससे अपराधियों को पकड़ना कठिन हो जाता है। कई बार अपराधी ऐसे देशों में सक्रिय होते हैं जहाँ साइबर कानून कमजोर हैं या सहयोग की प्रक्रिया धीमी है। अंतरराष्ट्रीय सहयोग और सूचना आदान-प्रदान की कमी भी एक बड़ी बाधा है। वैश्विक स्तर पर साइबर अपराधों से निपटने के लिए देशों के बीच समन्वय, पारस्परिक कानूनी सहायता संधियाँ और तकनीकी सहयोग आवश्यक हैं। बिना अंतरराष्ट्रीय सहयोग के साइबर अपराधों पर प्रभावी नियंत्रण संभव नहीं है।[22]

iii. न्यायिक प्रक्रिया में तकनीकी विशेषज्ञता की कमी

साइबर अपराधों के प्रभावी निपटान के लिए न्यायिक प्रणाली में तकनीकी समझ और विशेषज्ञता का होना आवश्यक है। किंतु अनेक मामलों में न्यायिक अधिकारियों, वकीलों और पुलिस कर्मियों को उन्नत साइबर तकनीकों की पर्याप्त जानकारी नहीं होती। डिजिटल साक्ष्यों की प्रकृति जटिल होती है, जैसे सर्वर लॉग, एन्क्रिप्टेड डेटा और डिजिटल

[19] AIR 2017 SC 4161

[20] AIR 2008 Del 164

[21] "भारत में साइबर अपराध: समस्याएँ और चुनौतियाँ।" *जर्नल ऑफ़ लॉ एंड टेक्नोलॉजी*, खंड 12, अंक 3, 2018, पृष्ठ 45–62।

[22] "भारत में साइबर अपराध का कानूनी ढांचा।" *इंडियन जर्नल ऑफ़ साइबर लॉ*, खंड 5, अंक 2, 2019, पृष्ठ 23–41।

हस्ताक्षर, जिनकी व्याख्या विशेष तकनीकी ज्ञान की मांग करती है। यदि जांच और सुनवाई के दौरान तकनीकी पहलुओं को सही ढंग से प्रस्तुत नहीं किया जाता, तो अभियोजन कमजोर पड़ सकता है। इसके अतिरिक्त, साइबर अपराधों की संख्या बढ़ने के बावजूद विशेष साइबर न्यायालयों और प्रशिक्षित विशेषज्ञों की कमी न्यायिक प्रक्रिया को धीमा कर देती है। इसलिए न्यायपालिका और कानून प्रवर्तन एजेंसियों के लिए नियमित प्रशिक्षण और तकनीकी उन्नयन आवश्यक है।[23]

iv. कानूनों के प्रभावी क्रियान्वयन में बाधाएँ

यद्यपि भारत में साइबर अपराधों से निपटने के लिए विधिक प्रावधान मौजूद हैं, तथापि उनके प्रभावी क्रियान्वयन में अनेक बाधाएँ सामने आती हैं। संसाधनों की कमी, तकनीकी अवसंरचना का अभाव और प्रशिक्षित मानवबल की सीमित उपलब्धता प्रमुख समस्याएँ हैं। ग्रामीण और दूरस्थ क्षेत्रों में साइबर अपराधों की शिकायत दर्ज कराने तथा जांच की प्रक्रिया अपेक्षाकृत कमजोर है। इसके अतिरिक्त, कानूनों के प्रति जन-जागरूकता का अभाव भी अपराध नियंत्रण में बाधक है। कई पीड़ित सामाजिक संकोच या जानकारी के अभाव में शिकायत दर्ज नहीं कराते। न्यायिक प्रक्रिया की धीमी गति भी अपराधियों के मनोबल को कम करने में असफल रहती है। अतः केवल कानून बनाना पर्याप्त नहीं है; उनके प्रभावी और त्वरित क्रियान्वयन के लिए संस्थागत सुदृढ़ीकरण, तकनीकी संसाधन और जन-जागरूकता अत्यंत आवश्यक हैं।[24]

7. निष्कर्ष

21वीं सदी में सूचना एवं संचार प्रौद्योगिकी के तीव्र विकास ने भारत को डिजिटल रूप से सशक्त समाज के रूप में बदल दिया है। इंटरनेट, स्मार्टफोन, सोशल मीडिया और ऑनलाइन लेन–देन की सुविधा ने लोगों के जीवन को अधिक सरल, तेज और पारदर्शी बनाया है। डिजिटल शिक्षा, ई–गवर्नेंस और ई–कॉमर्स के माध्यम से नागरिकों को लाभ पहुँचाने के साथ-साथ प्रशासन और व्यापार में दक्षता भी बढ़ी है। डिजिटल इंडिया जैसे सरकारी कार्यक्रमों ने न केवल नागरिकों को डिजिटल सेवाओं तक पहुँच प्रदान की, बल्कि समाज के डिजिटल साक्षरता स्तर को भी सुधारने का प्रयास किया। इस संदर्भ में तकनीकी प्रगति ने समाज की संरचना और आर्थिक गतिविधियों में अभूतपूर्व परिवर्तन किए हैं।

किंतु डिजिटल युग में साइबर अपराध एक गंभीर सामाजिक, आर्थिक और कानूनी चुनौती के रूप में उभरा है। भारतीय समाज में साइबर अपराध के स्वरूप विविध हैं, जैसे हैकिंग, डाटा चोरी, ऑनलाइन वित्तीय धोखाधड़ी, फिशिंग, रैनसमवेयर हमले, साइबर बुलिंग और पहचान की चोरी। अपराधियों ने तकनीकी नवाचारों का दुरुपयोग कर नागरिकों, संस्थाओं और सरकारी तंत्र को निशाना बनाया है। इसके पीछे मुख्य कारण डिजिटल साक्षरता की कमी, तकनीकी जागरूकता का अभाव, आर्थिक लालच, बेरोजगारी और सुरक्षा उपायों की अनदेखी हैं। इसके अतिरिक्त, व्यक्तिगत डेटा का असुरक्षित साझा करना और गोपनीयता के प्रति लापरवाही साइबर अपराधों को बढ़ावा देते हैं। यह स्पष्ट है कि तकनीकी लाभ और जोखिम एक साथ मौजूद हैं, और डिजिटल क्रांति केवल सुविधाओं तक सीमित नहीं रह सकती; इसके लिए सुरक्षित और उत्तरदायी उपयोग आवश्यक है।

विधिक नियंत्रण और कानूनी ढांचे ने साइबर अपराधों की रोकथाम में महत्वपूर्ण भूमिका निभाई है। सूचना प्रौद्योगिकी अधिनियम, 2000 और उसका संशोधन अधिनियम, 2008 साइबर अपराधों के दंडात्मक प्रावधान प्रदान करते हैं। इसके साथ ही भारतीय न्याय संहिता की प्रासंगिक धाराएँ डिजिटल अपराधों पर लागू होती हैं। CERT-In जैसी संस्थाएँ साइबर सुरक्षा घटनाओं की निगरानी और तकनीकी सहायता

[23] "सोशल मीडिया में साइबर अपराध के रुझान।" *साइबरसिक्योरिटी रिसर्च जर्नल*, खंड 4, अंक 2, 2021, पृष्ठ 50–68।

[24] "डिजिटल गोपनीयता और साइबर सुरक्षा।" *इंटरनेशनल जर्नल ऑफ़ लॉ एंड आईटी*, खंड 8, अंक 1, 2020, पृष्ठ 12–30।

प्रदान करती हैं। राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल ने नागरिकों को अपराध की त्वरित रिपोर्टिंग का साधन उपलब्ध कराया है। हालांकि कानून मौजूद है, किंतु बदलते तकनीकी परिवेश और अंतरराष्ट्रीय साइबर अपराधों के कारण उनका प्रभावी क्रियान्वयन चुनौतियों के साथ आता है। अपराधियों की गुमनामी, अंतरराष्ट्रीय स्तर पर अपराध संचालन, न्यायिक प्रणाली में तकनीकी विशेषज्ञता की कमी और कानूनों के प्रभावी कार्यान्वयन में बाधाएँ प्रमुख समस्याएँ हैं।

इसके अतिरिक्त, न्यायिक निर्णयों ने साइबर अपराध नियंत्रण और डेटा सुरक्षा की दिशा में महत्वपूर्ण मार्गदर्शन प्रदान किया है। जैसे श्रीय सिंगलाल बनाम भारत संघ मामले में अभिव्यक्ति की स्वतंत्रता और धारा 66A का संतुलन स्थापित किया गया, जबकि अनवर पी.वी. बनाम पी.के. बशीर मामले ने इलेक्ट्रॉनिक साक्ष्यों की वैधता स्पष्ट की। K.S. Puttaswamy मामले ने निजता के अधिकार को मौलिक अधिकार घोषित कर डिजिटल डेटा सुरक्षा को कानूनी आधार दिया। ये उदाहरण स्पष्ट करते हैं कि साइबर अपराध नियंत्रण केवल कानून बनाकर संभव नहीं है, बल्कि न्यायिक व्याख्या, तकनीकी विशेषज्ञता और नागरिक जागरूकता की भी आवश्यकता है।

अतः निष्कर्षतः यह कहा जा सकता है कि भारतीय समाज में डिजिटल सशक्तिकरण और साइबर अपराध दोनों ही यथार्थ हैं। डिजिटल क्रांति ने सामाजिक और आर्थिक विकास को बढ़ावा दिया है, किंतु इसके साथ ही साइबर अपराध एक गंभीर चुनौती के रूप में उपस्थित हैं। इनके प्रभावी नियंत्रण हेतु कठोर कानूनी प्रावधान, तकनीकी सुरक्षा उपायों का पालन, डिजिटल साक्षरता का प्रसार, न्यायिक प्रणाली की दक्षता और अंतरराष्ट्रीय सहयोग आवश्यक हैं। केवल इन उपायों के माध्यम से ही नागरिकों की सुरक्षा, डेटा गोपनीयता और समाज में विश्वास स्थापित किया जा सकता है। डिजिटल युग की प्रगति तभी सफल होगी जब तकनीक का लाभ सुरक्षित, जिम्मेदार और सतर्क उपयोग के माध्यम से प्राप्त किया जाए।

संदर्भ सूची

पुस्तकें

1. कुमार, राकेश. *साइबर क्राइम एंड लॉ*. नई दिल्ली: लॉ पब्लिकेशन, 2019.
2. गुप्ता, सुमित. *इन्फॉर्मेशन टेक्नोलॉजी लॉ*. दिल्ली: टेक्नोलॉजी पब्लिकेशन, 2018.
3. मिश्रा, अनिल. *साइबर सिक्योरिटी एंड प्रिवेंशन*. मुंबई: साइबर लॉ पब्लिकेशन, 2020.
4. अग्रवाल, पायल. *कंप्यूटर लॉ एंड एथिक्स*. नई दिल्ली: लॉ पब्लिशर्स, 2017.
5. चौहान, विकास. *डिजिटल इंडिया एंड साइबर लॉ*. जयपुर: इनोवेटिव पब्लिकेशन, 2021.

लेख

1. "भारत में साइबर अपराध: समस्याएँ और चुनौतियाँ।" *जर्नल ऑफ़ लॉ एंड टेक्नोलॉजी*, खंड 12, अंक 3, 2018, पृष्ठ 45–62।
2. "भारत में साइबर अपराध का कानूनी ढांचा।" *इंडियन जर्नल ऑफ़ साइबर लॉ*, खंड 5, अंक 2, 2019, पृष्ठ 23–41।
3. "डिजिटल गोपनीयता और साइबर सुरक्षा।" *इंटरनेशनल जर्नल ऑफ़ लॉ एंड आईटी*, खंड 8, अंक 1, 2020, पृष्ठ 12–30।
4. "सोशल मीडिया में साइबर अपराध के रुझान।" *साइबरसिक्योरिटी रिसर्च जर्नल*, खंड 4, अंक 2, 2021, पृष्ठ 50–68।

5. "ई–गवर्नेंस और साइबर अपराध की रोकथाम।" *जर्नल ऑफ़ इंडियन पब्लिक पॉलिसी*, खंड 10, अंक 1, 2017, पृष्ठ 15–33।

वेबसाइट्स

1. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल. *Government of India*, https://cybercrime.gov.in. Accessed 25 Feb. 2026.

2. CERT-In. *Indian Computer Emergency Response Team*, https://www.cert-in.org.in. Accessed 25 Feb. 2026.

3. भारत सरकार, डिजिटल इंडिया. https://www.digitalindia.gov.in. Accessed 25 Feb. 2026.

4. Ministry of Electronics and IT (MeitY). https://meity.gov.in. Accessed 25 Feb. 2026.

5. Indian Cyber Crime Portal – Guidelines. Ministry of Electronics and IT, https://www.meity.gov.in/content/cybercrime-guidelines. Accessed 25 Feb. 2026.