Abhi International Journal of
Humanities and Law
(A Peer Review Journal)
journal homepage: https://abhijournals.com/index.php/aijhl

Volume 1, Issue 4, October 2025 ISSN : 3107-6793

साइबर अपराध के संदर्भ में भारतीय दंड विधान और सूचना प्रौद्योगिकी अधिनियम का तुलनात्मक अध्ययन

प्रियंका पांडेय, डॉ. कमल सिंह धाकड़

शोधार्थिनी, स्कूल ऑफ लॉ एंड लीगल स्टडिज, संस्कृति विश्वविद्यालय, मथुरा (उत्तर प्रदेश)

सहायक प्रोफेसर, स्कूल ऑफ लॉ एंड लीगल स्टडिज, संस्कृति विश्वविद्यालय, मथुरा (उत्तर प्रदेश)

सार: प्रस्तुत शोधपत्र में साइबर अपराध के संदर्भ में भारतीय दंड विधान (आईपीसी/बीएनएस) तथा सूचना प्रौद्योगिकी अधिनियम, 2000 के प्रावधानों का तुलनात्मक विश्लेषण किया गया है। अध्ययन में साइबर अपराध की अवधारणा, उसके प्रकार, तकनीकी जटिलताओं, डिजिटल साक्ष्य, एन्क्रिप्शन, सीमा-पार अपराध तथा कृत्रिम बुद्धिमत्ता आधारित चुनौतियों का विस्तृत परीक्षण किया गया है। साथ ही यह स्पष्ट किया गया है कि जहाँ सूचना प्रौद्योगिकी अधिनियम तक नीकी-विशिष्ट अपराधों के लिए विशेष विधिक ढाँचा प्रदान करता है, वहीं भारतीय दंड विधान पारंपरिक आपराधिक सिद्धांतों के माध्यम से डिजिटल अपराधों को दंडित करने में सहायक भूमिका निभाता है। न्यायालयीन दृष्टिकोण, विशेषकर अभिव्यक्ति की स्वतंत्रता और डिजिटल साक्ष्य की स्वीकार्यता के संदर्भ में, इस क्षेत्र में संतुलन स्थापित करने का प्रयास करता है। अंततः शोध यह निष्कर्ष प्रस्तुत करता है कि साइबर अपराधों के प्रभावी नियंत्रण हेतु दोनों कानूनों के मध्य समन्वित और अद्यतन विधिक ढाँचे की आवश्यकता है।

1. भूमिका: डिजिटल प्रौद्योगिकी के तीव्र विकास ने मानव जीवन, शासन प्रणाली और आर्थिक गतिविधियों को व्यापक रूप से प्रभावित किया है, जिसके साथ ही अपराध का स्वरूप भी पारंपरिक सीमाओं से निकलकर आभासी क्षेत्र में परिवर्तित हो गया है। इंटरनेट, सामाजिक माध्यमों और ऑनलाइन लेन-देन की बढ़ती निर्भरता ने साइबर अपराधों को नई गति प्रदान की है, जिससे व्यक्तियों, संस्थानों तथा राष्ट्र की सुरक्षा पर गंभीर प्रभाव पड़ता है। इस परिप्रेक्ष्य में भारतीय दंड विधान तथा सूचना प्रौद्योगिकी अधिनियम की प्रासंगिकता और प्रभावशीलता का विश्लेषण आवश्यक हो जाता है। जहाँ एक ओर भारतीय दंड विधान सामान्य आपराधिक ढाँचा प्रदान करता है, वहीं सूचना प्रौद्योगिकी अधिनियम विशेष रूप से डिजिटल अपराधों के नियंत्रण के लिए निर्मित किया गया है। अतः इन दोनों विधिक व्यवस्थाओं के तुलनात्मक अध्ययन के माध्यम से यह समझना महत्वपूर्ण है कि वर्तमान कानूनी ढाँचा साइबर अपराधों की जटिलताओं का सामना किस सीमा तक कर पा रहा है और भविष्य में किन सुधारों की आवश्यकता है।

शर्मा, आर. के. (2015) ने सूचना प्रौद्योगिकी अधिनियम, 2000 का आलोचनात्मक अध्ययन प्रस्तुत करते हुए यह प्रतिपादित किया कि यह अधिनियम भारत में साइबर कानून की आधारशिला है, परंतु इसकी संरचना प्रारंभिक डिजिटल युग की आवश्यकताओं पर आधारित थी। उन्होंने विशेष रूप से धारा 43, 66 और 67 के प्रावधानों का विश्लेषण करते हुए यह स्पष्ट किया कि तकनीकी अपराधों की जटिलता को

देखते हुए दंडात्मक एवं प्रक्रिया संबंधी प्रावधानों में अधिक स्पष्टता अपेक्षित है। लेखक ने यह भी संकेत किया कि अधिनियम में अभिव्यक्ति की स्वतंत्रता और साइबर नियंत्रण के मध्य संतुलन आवश्यक है। वर्मा, एस. (2016) ने साइबर अपराधों के संदर्भ में भारतीय दंड संहिता की प्रासंगिकता का विश्लेषण करते हुए यह दर्शाया कि यद्यपि दंड संहिता पारंपरिक अपराधों के लिए निर्मित थी, फिर भी उसकी अनेक धाराएँ—जैसे धोखाधड़ी, जालसाजी और मानहानि—डिजिटल माध्यम से किए गए अपराधों पर समान रूप से लागू होती हैं। उन्होंने यह निष्कर्ष निकाला कि साइबर अपराधों के प्रभावी नियंत्रण हेतु पारंपरिक और विशेष कानूनों के समन्वय की आवश्यकता है। तिवारी, म. एवं सिंह, पी. (2017) ने डिजिटल साक्ष्य की स्वीकार्यता के संदर्भ में भारतीय साक्ष्य अधिनियम की धारा 65बी के महत्व पर बल दिया। उन्होंने न्यायालयीन प्रवृत्तियों का अध्ययन कर यह स्पष्ट किया कि इलेक्ट्रॉनिक अभिलेखों की प्रमाणिकता सुनिश्चित करने के लिए प्रमाण-पत्र की अनिवार्यता और तकनीकी अखंडता अत्यंत आवश्यक है। लेख में यह भी बताया गया कि प्रक्रिया संबंधी त्रुटियाँ अभियोजन की सफलता को प्रभावित कर सकती हैं। चौधरी, डी. (2018) ने साइबर स्टॉकिंग और महिलाओं की विधिक सुरक्षा पर प्रकाश डालते हुए बताया कि डिजिटल माध्यम से उत्पीड़न के मामलों में धारा 354D सहित अन्य प्रावधानों का महत्व बढ़ गया है। उन्होंने यह तर्क दिया कि साइबर स्टॉकिंग केवल तकनीकी अपराध नहीं, बल्कि लैंगिक न्याय और निजता के अधिकार से जुड़ा गंभीर सामाजिक प्रश्न है। यादव, के. (2018) ने ऑनलाइन धोखाधड़ी के बढ़ते स्वरूप का विश्लेषण करते हुए यह बताया कि ई-कॉमर्स, बैंकिंग फ्रॉड और निवेश घोटालों के मामलों में दंड विधान की पारंपरिक धाराओं का विस्तार आवश्यक हो गया है। उन्होंने सुझाव दिया कि तकनीकी विशेषज्ञता और त्वरित न्यायिक प्रक्रिया के अभाव में पीड़ितों को पर्याप्त न्याय नहीं मिल पाता। मिश्रा, ए. (2019) ने सूचना प्रौद्योगिकी अधिनियम में 2008 संशोधन और न्यायालयीन दृष्टिकोण का विश्लेषण करते हुए यह प्रतिपादित किया कि संशोधन ने साइबर आतंकवाद, पहचान चोरी और डेटा संरक्षण जैसे नए आयाम जोड़े। साथ ही उन्होंने धारा 66ए के निरस्तीकरण को अभिव्यक्ति की स्वतंत्रता के संरक्षण की दिशा में महत्वपूर्ण कदम बताया। गुप्ता, वी. एवं सक्सेना, एल. (2019) ने फिशिंग और हैकिंग जैसे अपराधों की तकनीकी प्रकृति पर चर्चा करते हुए यह कहा कि अपराधी सोशल इंजीनियरिंग तकनीकों का उपयोग कर विधिक तंत्र को चुनौती देते हैं। उन्होंने साइबर सुरक्षा जागरूकता, तकनीकी प्रशिक्षण और विधिक अद्यतन को आवश्यक सुधार के रूप में रेखांकित किया। जोशी, न. (2020) ने साइबर आतंकवाद को राष्ट्रीय सुरक्षा के संदर्भ में विश्लेषित करते हुए यह स्पष्ट किया कि महत्वपूर्ण अवसंरचना पर साइबर हमले राज्य की संप्रभुता को प्रभावित कर सकते हैं। उन्होंने अंतरराष्ट्रीय सहयोग और कठोर दंडात्मक प्रावधानों की आवश्यकता पर बल दिया। सिंह, आर. (2020) ने सीमा-पार साइबर अपराधों में क्षेत्राधिकार की समस्या का विस्तृत अध्ययन किया। उन्होंने यह बताया कि जब अपराधी, सर्वर और पीड़ित अलग-अलग देशों में हों, तब विधिक प्रक्रिया जटिल हो जाती है। लेखक ने पारस्परिक विधिक सहायता संधियों के महत्व को रेखांकित किया। कुमारी, अ. (2021) ने डिजिटल गोपनीयता और अभिव्यक्ति की स्वतंत्रता के मध्य संतुलन पर विचार करते हुए धारा 66ए के संदर्भ में न्यायालयीन निर्णयों का विश्लेषण किया। उन्होंने यह निष्कर्ष निकाला कि साइबर नियमन के नाम पर मौलिक अधिकारों का अतिक्रमण नहीं होना चाहिए। पांडेय, ह. (2021) ने इलेक्ट्रॉनिक अभिलेखों की प्रमाणिकता पर न्यायालयीन प्रवृत्ति का विश्लेषण करते हुए बताया कि तकनीकी मानकों का पालन न करने पर साक्ष्य अस्वीकार्य हो सकते हैं। उन्होंने डिजिटल फॉरेंसिक क्षमता के विकास की आवश्यकता को रेखांकित किया। श्रीवास्तव, जी. (2022) ने साइबर अपराधों के वर्गीकरण और विधिक ढाँचे का विश्लेषण करते हुए यह स्पष्ट किया कि व्यक्ति, संपत्ति और राज्य के विरुद्ध अपराधों का पृथक अध्ययन आवश्यक है। उन्होंने सुझाव दिया कि विधिक संरचना को तकनीकी परिवर्तनों के अनुरूप अद्यतन किया जाना चाहिए। अग्रवाल, पी. (2023) ने कृत्रिम

बुद्धिमत्ता आधारित अपराधों, विशेषकर डीपफेक और स्वचालित फिशिंग बॉट्स, की कानूनी चुनौतियों का विश्लेषण किया। उन्होंने यह प्रतिपादित किया कि वर्तमान कानून इन उभरते अपराधों से पूर्णतः निपटने में सक्षम नहीं हैं और विशेष प्रावधानों की आवश्यकता है। त्रिपाठी, एस. एवं दुबे, आर. (2024) ने भारतीय न्याय संहिता में साइबर अपराधों के पुनर्संगठन का अध्ययन करते हुए बताया कि नई संहिता ने पारंपरिक अपराधों को आधुनिक डिजिटल संदर्भ में पुनर्परिभाषित करने का प्रयास किया है। उन्होंने इसे विधिक आधुनिकीकरण की दिशा में महत्वपूर्ण कदम माना। भारद्वाज, न. (2025) ने भारतीय दंड विधान और सूचना प्रौद्योगिकी अधिनियम के तुलनात्मक अध्ययन के माध्यम से यह निष्कर्ष निकाला कि दोनों कानून परस्पर पूरक हैं। उन्होंने यह सुझाव दिया कि समन्वित विधिक ढाँचा, विशेष साइबर न्यायालय और तकनीकी क्षमता निर्माण के माध्यम से साइबर अपराधों का प्रभावी नियंत्रण संभव है।

2. साइबर अपराध की अवधारणा एवं वर्गीकरण: साइबर अपराध से अभिप्राय उन अवैध कृत्यों से है जो कंप्यूटर, इंटरनेट, डिजिटल नेटवर्क या इलेक्ट्रॉनिक उपकरणों के माध्यम से किए जाते हैं, जहाँ कंप्यूटर स्वयं अपराध का साधन, लक्ष्य या दोनों हो सकता है। डिजिटल प्रौद्योगिकी के तीव्र विस्तार के साथ अपराध का स्वरूप पारंपरिक भौतिक सीमाओं से हटकर आभासी (Virtual) क्षेत्र में परिवर्तित हो गया है, जिससे पहचान छिपाना, त्वरित संचार और सीमा-पार संचालन संभव हो गया है। साइबर अपराध का वर्गीकरण सामान्यतः तीन आधारों पर किया जाता है—(1) व्यक्ति के विरुद्ध अपराध, जैसे साइबर स्टॉकिंग, ऑनलाइन मानहानि, पहचान चोरी और अश्लील सामग्री का प्रसारण; (2) संपत्ति के विरुद्ध अपराध, जैसे हैकिंग, डेटा चोरी, फिशिंग, ऑनलाइन धोखाधड़ी और रैनसमवेयर आक्रमण; तथा (3) राज्य या समाज के विरुद्ध अपराध, जैसे साइबर आतंकवाद, वेबसाइट डिफेसमेंट, महत्वपूर्ण अवसंरचना पर हमले और दुष्प्रचार अभियान। इसके अतिरिक्त तकनीकी आधार पर भी इन्हें वर्गीकृत किया जाता है, जैसे मैलवेयर आधारित अपराध, सोशल इंजीनियरिंग अपराध, नेटवर्क घुसपैठ, तथा कृत्रिम बुद्धिमत्ता आधारित अपराध (डीपफेक आदि)। इस प्रकार साइबर अपराध की अवधारणा केवल तकनीकी अनधिकृत प्रवेश तक सीमित नहीं है, बल्कि यह डिजिटल परिवेश में मानव व्यवहार, गोपनीयता, डेटा सुरक्षा और राष्ट्रीय सुरक्षा से जुड़े व्यापक विधिक एवं सामाजिक आयामों को समाहित करती है।

(i) साइबर अपराध की परिभाषा: साइबर अपराध वह अवैध कृत्य है जो कंप्यूटर, कंप्यूटर प्रणाली, नेटवर्क, इंटरनेट या किसी अन्य डिजिटल माध्यम के द्वारा किया जाता है, जिसमें डिजिटल उपकरण अपराध करने का साधन, लक्ष्य अथवा दोनों के रूप में प्रयुक्त होते हैं। सरल शब्दों में, जब कोई व्यक्ति सूचना प्रौद्योगिकी का उपयोग कर डेटा की चोरी, अनधिकृत प्रवेश (हैकिंग), ऑनलाइन धोखाधड़ी, पहचान की चोरी, साइबर स्टॉकिंग, अश्लील सामग्री का प्रसारण या किसी डिजिटल प्रणाली को क्षति पहुँचाने जैसे कार्य करता है, तो वह साइबर अपराध की श्रेणी में आता है। विधिक दृष्टि से, यह ऐसे अपराधों का समूह है जो सूचना एवं संचार प्रौद्योगिकी के दुरुपयोग से संबंधित हैं और जिनके नियंत्रण एवं दंड के लिए विशेष प्रावधान बनाए गए हैं।

(ii) प्रमुख प्रकार: साइबर अपराधों के प्रमुख प्रकारों में हैकिंग, फिशिंग, पहचान चोरी, साइबर स्टॉकिंग और ऑनलाइन धोखाधड़ी विशेष रूप से उल्लेखनीय हैं। हैकिंग में किसी कंप्यूटर प्रणाली, सर्वर या नेटवर्क में अनधिकृत प्रवेश कर डेटा चुराना, बदलना या नष्ट करना शामिल होता है। फिशिंग एक सामाजिक अभियांत्रिकी तकनीक है, जिसमें अपराधी नकली ई-मेल, संदेश या वेबसाइट के माध्यम से उपयोगकर्ता से गोपनीय जानकारी जैसे पासवर्ड, बैंक विवरण या ओटीपी प्राप्त कर लेते हैं। पहचान चोरी में किसी व्यक्ति की व्यक्तिगत जानकारी—जैसे आधार

संख्या, पैन, बैंक खाता या सोशल मीडिया प्रोफ़ाइल—का दुरुपयोग कर आर्थिक या सामाजिक नुकसान पहुँचाया जाता है। साइबर स्टॉकिंग के अंतर्गत किसी व्यक्ति को इंटरनेट या सोशल मीडिया के माध्यम से लगातार परेशान करना, धमकी देना या निगरानी करना शामिल है, जो उसकी निजता और मानसिक शांति का उल्लंघन करता है। वहीं ऑनलाइन धोखाधड़ी में ई-कॉमर्स ठगी, निवेश घोटाले, लॉटरी स्कैम या फर्जी कॉल के माध्यम से आर्थिक लाभ प्राप्त करने के अवैध प्रयास किए जाते हैं। ये सभी अपराध डिजिटल माध्यम की गोपनीयता और तकनीकी जटिलताओं का दुरुपयोग कर तेजी से बढ़ रहे हैं और विधिक नियंत्रण के लिए गंभीर चुनौती प्रस्तुत करते हैं।

सूचना प्रौद्योगिकी अधिनियम, 2000 के अंतर्गत साइबर अपराधों से निपटने हेतु विभिन्न धाराएँ निर्धारित की गई हैं, जिनमें धारा 43, धारा 66 और धारा 67 विशेष रूप से महत्वपूर्ण हैं। धारा 43 अनधिकृत प्रवेश (Unauthorized Access), डेटा की चोरी, डाउनलोडिंग, कॉपी करना, वायरस या मैलवेयर के माध्यम से कंप्यूटर प्रणाली को क्षति पहुँचाने जैसे कृत्यों के लिए दायित्व और क्षतिपूर्ति का प्रावधान करती है; यह मुख्यतः नागरिक दायित्व (Civil Liability) से संबंधित है। धारा 66, धारा 43 में वर्णित कृत्यों को यदि दुर्भावनापूर्ण या धोखाधड़ी की मंशा से किया जाए तो उन्हें आपराधिक अपराध घोषित करती है और इसके लिए कारावास तथा जुर्माने का प्रावधान करती है, जिससे यह साइबर अपराधों के दंडात्मक पहलू को सुदृढ़ बनाती है। वहीं धारा 67 इलेक्ट्रॉनिक माध्यम से अश्लील सामग्री के प्रकाशन या प्रसारण को दंडनीय बनाती है और डिजिटल प्लेटफॉर्म पर अशोभनीय या अनैतिक सामग्री के प्रसार को नियंत्रित करने का प्रयास करती है। इन धाराओं के माध्यम से अधिनियम ने अनधिकृत तकनीकी हस्तक्षेप, कंप्यूटर-संबंधित अपराधों और डिजिटल अश्लीलता जैसे प्रमुख साइबर अपराधों को विधिक दायरे में लाकर उनके नियंत्रण की व्यवस्था की है।

3. भारतीय दंड विधान (IPC / BNS) के अंतर्गत साइबर अपराध: भारतीय दंड विधान के अंतर्गत साइबर अपराधों का प्रत्यक्ष उल्लेख प्रारंभिक रूप से नहीं था, क्योंकि Indian Penal Code उस समय बनाया गया था जब डिजिटल तकनीक का अस्तित्व नहीं था, फिर भी इसकी अनेक धाराएँ ऑनलाइन माध्यम से किए गए अपराधों पर लागू होती रही हैं, जैसे धारा 419 और 420 (ऑनलाइन धोखाधड़ी), धारा 463–471 (इलेक्ट्रॉनिक जालसाजी), धारा 499–500 (ऑनलाइन मानहानि) तथा धारा 354D (साइबर स्टॉकिंग)। वर्तमान में Bharatiya Nyaya Sanhita ने IPC का स्थान लेकर पारंपरिक अपराधों को आधुनिक संदर्भ में पुनर्संगठित किया है, जिससे डिजिटल माध्यम से किए गए कृत्यों—जैसे पहचान की चोरी, वित्तीय ठगी, साइबर उत्पीड़न और अश्लील सामग्री का प्रसारण—को अधिक स्पष्ट रूप से समाहित किया जा सके। यद्यपि साइबर अपराधों के लिए विशेष अधिनियम के रूप में सूचना प्रौद्योगिकी अधिनियम प्रभावी है, फिर भी IPC/BNS के सामान्य आपराधिक प्रावधान डिजिटल अपराधों के दंड निर्धारण, मंशा (Mens Rea) की व्याख्या और न्यायिक प्रक्रिया में महत्वपूर्ण भूमिका निभाते हैं, जिससे पारंपरिक आपराधिक कानून और आधुनिक साइबर विधि के बीच एक समन्वित विधिक ढाँचा निर्मित होता है।

भारतीय दंड विधान के अंतर्गत कई धाराएँ ऐसी हैं जो डिजिटल माध्यम से किए गए अपराधों पर भी समान रूप से लागू होती हैं। धारा 420 के अंतर्गत धोखाधड़ी और बेईमानी से संपत्ति या धन की प्राप्ति को दंडनीय माना गया है, जो ऑनलाइन ठगी, फर्जी निवेश योजनाओं या बैंकिंग फ्रॉड जैसे साइबर अपराधों में प्रासंगिक होती है। धारा 463 से 471 तक जालसाजी और कूटरचना से संबंधित प्रावधान हैं, जिनका उपयोग फर्जी डिजिटल दस्तावेज, नकली ई-मेल, इलेक्ट्रॉनिक हस्ताक्षर या ऑनलाइन प्रमाणपत्रों के दुरुपयोग के मामलों में किया जाता है। धारा 499 मानहानि से संबंधित है, जिसके अंतर्गत सोशल मीडिया

या डिजिटल प्लेटफॉर्म पर किसी व्यक्ति की प्रतिष्ठा को हानि पहुँचाने वाले कथनों को अपराध की श्रेणी में रखा गया है। वहीं धारा 354D, जिसे साइबर स्टॉकिंग के संदर्भ में विशेष महत्व प्राप्त है, किसी महिला का ऑनलाइन माध्यम से पीछा करने, बार-बार संपर्क करने या उसकी ऑनलाइन गतिविधियों की निगरानी करने को दंडनीय बनाती है। इस प्रकार ये धाराएँ पारंपरिक आपराधिक कानून के अंतर्गत होते हुए भी आधुनिक साइबर अपराधों के विरुद्ध प्रभावी विधिक आधार प्रदान करती हैं।

4. सूचना प्रौद्योगिकी अधिनियम 2000 का विश्लेषण: सूचना प्रौद्योगिकी अधिनियम का अधिनियम भारत में साइबर कानून का मूल आधार है, जिसे ई–गवर्नेंस को वैधानिक मान्यता प्रदान करने, इलेक्ट्रॉनिक अभिलेखों एवं डिजिटल हस्ताक्षरों को कानूनी वैधता देने तथा साइबर अपराधों को नियंत्रित करने के उद्देश्य से लागू किया गया था। इस अधिनियम ने अनधिकृत प्रवेश, डेटा क्षति, हैकिंग, पहचान चोरी, साइबर आतंकवाद तथा अश्लील सामग्री के प्रकाशन जैसे अपराधों के लिए दंडात्मक प्रावधान स्थापित किए और साथ ही मध्यस्थ की उत्तरदायित्व सीमा भी निर्धारित की। वर्ष 2008 के संशोधन द्वारा इसमें महत्वपूर्ण परिवर्तन किए गए, जिनमें इलेक्ट्रॉनिक साक्ष्य, साइबर सुरक्षा और डेटा संरक्षण से जुड़े प्रावधानों को सुदृढ़ किया गया, यद्यपि धारा 66A को बाद में सर्वोच्च न्यायालय द्वारा असंवैधानिक घोषित कर दिया गया। विश्लेषणात्मक दृष्टि से यह अधिनियम तकनीकी अपराधों से निपटने हेतु विशेष और आधुनिक ढाँचा प्रदान करता है, परंतु तीव्र तकनीकी विकास, कृत्रिम बुद्धिमत्ता आधारित अपराधों और सीमा-पार साइबर हमलों की चुनौतियों के संदर्भ में इसकी प्रभावशीलता निरंतर अद्यतन एवं सुधार की अपेक्षा रखती है।

(i) उद्देश्य: सूचना प्रौद्योगिकी अधिनियम, 2000 का प्रमुख उद्देश्य डिजिटल युग की आवश्यकताओं के अनुरूप विधिक ढाँचा स्थापित करना है, जिसके अंतर्गत सबसे पहले ई-गवर्नेंस को कानूनी मान्यता प्रदान की गई ताकि सरकारी अभिलेख, आवेदन, लाइसेंस, कर विवरण तथा अन्य आधिकारिक प्रक्रियाएँ इलेक्ट्रॉनिक माध्यम से वैध रूप से संपन्न की जा सकें। इसके साथ ही अधिनियम ने डिजिटल हस्ताक्षर (Digital Signature) और इलेक्ट्रॉनिक अभिलेखों को विधिक मान्यता देकर ऑनलाइन लेन-देन, अनुबंध और प्रमाणन प्रक्रियाओं को सुरक्षित तथा प्रमाणिक बनाने का आधार तैयार किया। इसके अतिरिक्त साइबर अपराधों के नियंत्रण हेतु दंडात्मक प्रावधान निर्धारित किए गए, जिनके माध्यम से अनधिकृत प्रवेश, डेटा क्षति, पहचान चोरी, साइबर आतंकवाद और अश्लील सामग्री के प्रसारण जैसे अपराधों को दंडनीय बनाया गया। इस प्रकार अधिनियम का उद्देश्य न केवल डिजिटल लेन-देन को वैधानिक संरक्षण देना है, बल्कि साइबर स्पेस में सुरक्षा, विश्वसनीयता और उत्तरदायित्व सुनिश्चित करना भी है।

(ii) संशोधन: सूचना प्रौद्योगिकी अधिनियम में वर्ष 2008 का संशोधन अत्यंत महत्वपूर्ण माना जाता है, क्योंकि इसने साइबर अपराधों की बदलती प्रकृति को ध्यान में रखते हुए अधिनियम के दायरे को विस्तृत और सुदृढ़ किया। इस संशोधन के माध्यम से साइबर आतंकवाद, पहचान की चोरी, धोखाधड़ी, डेटा संरक्षण तथा मध्यस्थों) की जिम्मेदारी से संबंधित नए प्रावधान जोड़े गए और इलेक्ट्रॉनिक साक्ष्य तथा साइबर सुरक्षा से जुड़े नियमों को अधिक स्पष्ट किया गया। इसी संशोधन के तहत धारा 66A जोड़ी गई थी, जिसके अंतर्गत आपत्तिजनक या आक्रामक संदेशों के ऑनलाइन प्रसारण को दंडनीय बनाया गया था; किन्तु इस धारा को अभिव्यक्ति की स्वतंत्रता के विरुद्ध मानते हुए सर्वोच्च न्यायालय ने 2015 में इसे असंवैधानिक घोषित कर निरस्त कर दिया। इस प्रकार 2008 का संशोधन साइबर कानून को आधुनिक स्वरूप देने का

प्रयास था, जबकि धारा 66A का निरस्तीकरण मौलिक अधिकारों और डिजिटल स्वतंत्रता के संतुलन की दिशा में एक महत्वपूर्ण न्यायिक हस्तक्षेप सिद्ध हुआ।

5. तुलनात्मक अध्ययन: तालिका 1 यह स्पष्ट करती है कि दोनों विधिक ढाँचे साइबर अपराधों के संदर्भ में भिन्न प्रकृति और उद्देश्य रखते हैं। प्रकृति के आधार पर भारतीय दंड विधान पारंपरिक अपराधों पर केंद्रित है, जिसमें धोखाधड़ी, जालसाजी, मानहानि और उत्पीड़न जैसे अपराध सम्मिलित हैं, जबकि सूचना प्रौद्योगिकी अधिनियम विशेष रूप से तकनीकी और डिजिटल माध्यम से किए गए अपराधों को लक्षित करता है। अधिकार क्षेत्र की दृष्टि से आईपीसी/बीएनएस के अंतर्गत सामान्य आपराधिक न्यायालय मामलों की सुनवाई करते हैं, जबकि सूचना प्रौद्योगिकी अधिनियम में साइबर अपराधों हेतु विशेष प्रावधान और कुछ मामलों में विशेष प्राधिकरणों की व्यवस्था की गई है। दंड के संदर्भ में आईपीसी/बीएनएस अपेक्षाकृत कठोर दंड प्रदान करता है, वहीं सूचना प्रौद्योगिकी अधिनियम तकनीकी प्रकृति और अपराध की गंभीरता के अनुसार दंड निर्धारित करता है। तकनीकी साक्ष्य के मामले में आईपीसी/बीएनएस में सीमित उल्लेख है, जबकि सूचना प्रौद्योगिकी अधिनियम डिजिटल साक्ष्य और इलेक्ट्रॉनिक अभिलेखों को विशेष मान्यता देता है। इस प्रकार तालिका यह दर्शाती है कि दोनों कानूनों की भूमिका परस्पर पूरक है, परंतु प्रभावी साइबर नियंत्रण के लिए इनके बीच समन्वित और स्पष्ट विधिक तंत्र की आवश्यकता है।

तालिका 1: भारतीय दंड विधान (आईपीसी/बीएनएस) एवं सूचना प्रौद्योगिकी अधिनियम के प्रमुख प्रावधानों का तुलनात्मक सार

आधार	IPC / BNS	IT Act
प्रकृति	पारंपरिक अपराध	तकनीकी-विशिष्ट अपराध
अधिकार क्षेत्र	सामान्य आपराधिक न्यायालय	विशेष साइबर प्रावधान
दंड	अपेक्षाकृत कठोर	तकनीकी प्रकृति अनुसार
तकनीकी साक्ष्य	सीमित उल्लेख	डिजिटल साक्ष्य का विशेष प्रावधान

6. तकनीकी मुद्दे: साइबर अपराधों के संदर्भ में तकनीकी मुद्दे अत्यंत महत्वपूर्ण हैं, क्योंकि इन अपराधों की प्रकृति पारंपरिक अपराधों से भिन्न और अधिक जटिल होती है। डिजिटल साक्ष्य का संकलन, संरक्षण और प्रस्तुतीकरण एक प्रमुख चुनौती है, क्योंकि इसमें मेटाडाटा की सत्यता, साक्ष्य की अभिरक्षा श्रृंखला तथा फॉरेंसिक परीक्षण की शुद्धता सुनिश्चित करना आवश्यक होता है। एन्क्रिप्शन तकनीक, गोपनीयता संरक्षण और संचार की सुरक्षित प्रणालियाँ जाँच एजेंसियों के लिए बाधा उत्पन्न कर सकती हैं, जिससे अपराधी तक पहुँचना कठिन हो जाता है। इसके अतिरिक्त सीमा-पार अपराधों में अधिकार क्षेत्र निर्धारण और अंतरराष्ट्रीय सहयोग की आवश्यकता एक गंभीर विधिक जटिलता उत्पन्न करती है। कृत्रिम बुद्धिमत्ता, डीपफेक, स्वचालित बॉट और मैलवेयर जैसे उन्नत तकनीकी साधनों के कारण अपराध की पहचान और रोकथाम और भी चुनौतीपूर्ण हो गई है। अतः प्रभावी साइबर

नियंत्रण के लिए तकनीकी दक्षता, आधुनिक फॉरेंसिक प्रयोगशालाएँ, प्रशिक्षित मानव संसाधन और अद्यतन विधिक ढाँचे का समन्वय अत्यावश्यक है।

(i) डिजिटल साक्ष्य: डिजिटल साक्ष्य साइबर अपराधों की जाँच और न्यायिक प्रक्रिया में अत्यंत महत्वपूर्ण भूमिका निभाते हैं, किन्तु इनके साथ कई तकनीकी चुनौतियाँ जुड़ी होती हैं। मेटाडाटा में छेड़छाड़ एक गंभीर समस्या है, क्योंकि फाइल के निर्माण समय, संशोधन तिथि, स्थान अथवा स्रोत से संबंधित सूचनाएँ परिवर्तित की जा सकती हैं, जिससे साक्ष्य की प्रामाणिकता पर प्रश्न उठता है। इसी प्रकार अभिरक्षा श्रृंखला का निर्वहन आवश्यक है, अर्थात् साक्ष्य के संग्रहण से लेकर न्यायालय में प्रस्तुत करने तक प्रत्येक चरण का स्पष्ट और सुरक्षित अभिलेखन हो, ताकि यह सिद्ध किया जा सके कि साक्ष्य में कोई परिवर्तन नहीं हुआ। फॉरेंसिक अखंडता भी अनिवार्य है, जिसके अंतर्गत वैज्ञानिक परीक्षण, प्रमाणित उपकरणों का उपयोग और मानकीकृत प्रक्रिया का पालन सुनिश्चित किया जाता है। यदि इन तत्वों का समुचित पालन न किया जाए तो डिजिटल साक्ष्य न्यायालय में अविश्वसनीय माने जा सकते हैं, जिससे अभियोजन की सफलता प्रभावित हो सकती है।

(ii) एन्क्रिप्शन और गोपनीयता: एन्क्रिप्शन और गोपनीयता साइबर सुरक्षा के मूल स्तंभ हैं, किन्तु ये जाँच और प्रवर्तन की दृष्टि से जटिल प्रश्न भी उत्पन्न करते हैं। अंत से अंत तक कूटलेखन की तकनीक में संदेश प्रेषक और प्राप्तकर्ता के अतिरिक्त कोई तीसरा पक्ष सामग्री को पढ़ नहीं सकता, जिससे उपयोगकर्ताओं की निजता और संचार की सुरक्षा सुदृढ़ होती है; परंतु इसी कारण कानून प्रवर्तन एजेंसियों के लिए अपराध की जाँच में कठिनाई उत्पन्न हो सकती है। दूसरी ओर, डेटा अवरोधन की वैधता का प्रश्न भी महत्वपूर्ण है, क्योंकि राज्य को राष्ट्रीय सुरक्षा और सार्वजनिक व्यवस्था की रक्षा हेतु सीमित परिस्थितियों में संचार की निगरानी का अधिकार दिया गया है, किंतु यह अधिकार विधिक प्रावधानों, न्यायिक अनुमोदन और अनुपातिकता के सिद्धांतों के अधीन होना चाहिए। इस प्रकार एन्क्रिप्शन और गोपनीयता के संरक्षण तथा अपराध नियंत्रण के बीच संतुलन स्थापित करना आधुनिक साइबर विधि की प्रमुख चुनौती है।

(iii) सीमा-पार अपराध: सीमा-पार साइबर अपराध आधुनिक विधिक व्यवस्था के लिए एक जटिल चुनौती प्रस्तुत करते हैं, क्योंकि ऐसे अपराधों में अपराधी, पीड़ित और सर्वर अलग-अलग देशों में स्थित हो सकते हैं। सूचना प्रौद्योगिकी अधिनियम की धारा 75 के अनुसार इस अधिनियम का प्रभाव क्षेत्र भारत की सीमाओं से बाहर भी लागू हो सकता है, यदि अपराध का प्रभाव भारत में उत्पन्न होता है या किसी भारतीय कंप्यूटर संसाधन को प्रभावित करता है; इसे विधि का क्षेत्रातीत अनुप्रयोग कहा जाता है। तथापि व्यवहारिक स्तर पर अपराधी की पहचान, गिरफ्तारी तथा साक्ष्य संग्रहण के लिए अंतरराष्ट्रीय सहयोग आवश्यक होता है, जिसके लिए पारस्परिक विधिक सहायता संधियाँ महत्वपूर्ण भूमिका निभाती हैं। इन संधियों के माध्यम से देश एक-दूसरे को साक्ष्य प्राप्त करने, आरोपियों की जानकारी साझा करने तथा न्यायिक प्रक्रिया में सहयोग प्रदान करते हैं। फिर भी प्रक्रिया की जटिलता, समय की देरी और विधिक मानकों में भिन्नता के कारण सीमा-पार साइबर अपराधों का प्रभावी निवारण अभी भी एक महत्वपूर्ण चुनौती बना हुआ है।

(iv) कृत्रिम बुद्धिमत्ता (**Artificial Intelligence**) **आधारित अपराध:** कृत्रिम बुद्धिमत्ता आधारित अपराध साइबर जगत में उभरती हुई गंभीर चुनौती के रूप में सामने आए हैं, जिनमें डीपफेक और स्वचालित फ़िशिंग बॉट प्रमुख हैं। डीपफेक तकनीक के माध्यम से कृत्रिम बुद्धिमत्ता का उपयोग कर किसी व्यक्ति की आवाज़, चेहरे या वीडियो को इस प्रकार परिवर्तित या निर्मित किया जाता है कि वह वास्तविक

प्रतीत हो, जिससे मानहानि, धोखाधड़ी, राजनीतिक दुष्प्रचार या ब्लैकमेल जैसी गतिविधियाँ संभव हो जाती हैं। इसी प्रकार स्वचालित फ़िशिंग बॉट बड़ी संख्या में भ्रामक संदेश या ईमेल भेजकर उपयोगकर्ताओं से गोपनीय जानकारी प्राप्त करने का प्रयास करते हैं, जिससे वित्तीय और व्यक्तिगत क्षति होती है। इन अपराधों की जटिलता इस तथ्य में निहित है कि इन्हें पहचानना कठिन होता जा रहा है और पारंपरिक सुरक्षा उपाय इनके सामने अपर्याप्त सिद्ध हो सकते हैं। इस संदर्भ में यह कथन अत्यंत सार्थक है कि "Cybersecurity is much more than a matter of IT." – Stephane Nappo, जो संकेत करता है कि साइबर सुरक्षा केवल तकनीकी विषय नहीं, बल्कि विधिक, नैतिक और सामाजिक उत्तरदायित्व का भी प्रश्न है।

7. न्यायालयीन दृष्टिकोण: साइबर अपराधों के संदर्भ में न्यायालयीन दृष्टिकोण ने विधिक संतुलन स्थापित करने में महत्वपूर्ण भूमिका निभाई है। सर्वोच्च न्यायालय ने Information Technology Act की धारा 66ए को असंवैधानिक घोषित करते हुए यह स्पष्ट किया कि अस्पष्ट और व्यापक शब्दावली के आधार पर अभिव्यक्ति की स्वतंत्रता पर अनुचित प्रतिबंध नहीं लगाया जा सकता, जिससे संविधान प्रदत्त विचार और अभिव्यक्ति की स्वतंत्रता को संरक्षण मिला। इस निर्णय ने यह सिद्ध किया कि साइबर नियंत्रण की आवश्यकता होते हुए भी राज्य को मौलिक अधिकारों के साथ संतुलन बनाए रखना होगा। साथ ही डिजिटल साक्ष्य की स्वीकार्यता के संदर्भ में Indian Evidence Act की धारा 65बी के अंतर्गत इलेक्ट्रॉनिक अभिलेखों को प्रमाण के रूप में स्वीकार करने हेतु विधिक प्रक्रिया निर्धारित की गई है, जिसमें प्रमाण-पत्र की अनिवार्यता और तकनीकी प्रामाणिकता सुनिश्चित करना आवश्यक है। इस प्रकार न्यायालयों ने एक ओर साइबर अपराध नियंत्रण को मान्यता दी है, तो दूसरी ओर नागरिक स्वतंत्रताओं और विधिक प्रक्रिया की शुचिता को भी समान महत्व प्रदान किया है।

8. सीमाएँ: साइबर अपराधों के प्रभावी नियंत्रण में कई संरचनात्मक सीमाएँ दृष्टिगत होती हैं, जिनमें प्रमुख रूप से भारतीय दंड विधान और सूचना प्रौद्योगिकी अधिनियम के बीच समुचित समन्वय का अभाव शामिल है, जिससे अनेक मामलों में प्रावधानों का आच्छादन, व्याख्यात्मक भ्रम और प्रक्रिया संबंधी जटिलताएँ उत्पन्न होती हैं। इसके अतिरिक्त प्रवर्तन एजेंसियों में उन्नत तकनीकी संसाधनों और उपकरणों की कमी जाँच प्रक्रिया को प्रभावित करती है, विशेषकर तब जब अपराधी अत्याधुनिक तकनीकों का उपयोग करते हैं। डिजिटल साक्ष्य के संकलन, संरक्षण और विश्लेषण के लिए आवश्यक विशेषज्ञता का अभाव भी एक गंभीर चुनौती है, क्योंकि बिना वैज्ञानिक और प्रमाणिक पद्धति के साक्ष्य न्यायालय में टिक नहीं पाते। साथ ही साइबर पुलिसिंग के क्षेत्र में समुचित प्रशिक्षण, अद्यतन ज्ञान और सतत कौशल विकास की कमी के कारण कानून के प्रभावी क्रियान्वयन में बाधाएँ आती हैं। इन सीमाओं के कारण साइबर अपराधों से निपटने के लिए विधिक ढाँचे के साथ-साथ संस्थागत क्षमता निर्माण की भी आवश्यकता स्पष्ट रूप से अनुभव की जाती है।

9. सुधार एवं सुझाव: साइबर अपराधों के प्रभावी नियंत्रण हेतु व्यापक सुधारों की आवश्यकता है, जिनमें सर्वप्रथम विशेष साइबर न्यायालयों की स्थापना महत्वपूर्ण है, ताकि तकनीकी जटिलताओं वाले मामलों का त्वरित और विशेषज्ञतापूर्ण निपटारा सुनिश्चित किया जा सके। इसके साथ ही डिजिटल फॉरेंसिक प्रयोगशालाओं का विस्तार तथा उन्हें आधुनिक उपकरणों और प्रशिक्षित विशेषज्ञों से सुसज्जित

करना आवश्यक है, जिससे इलेक्ट्रॉनिक साक्ष्यों का वैज्ञानिक और विश्वसनीय विश्लेषण संभव हो सके। विधिक स्तर पर भारतीय दंड विधान और सूचना प्रौद्योगिकी अधिनियम के बीच स्पष्ट समन्वय स्थापित कर प्रावधानों का एकीकृत और सुसंगत ढाँचा विकसित किया जाना चाहिए, ताकि आच्छादन और व्याख्यात्मक भ्रम दूर हो सकें। साथ ही कृत्रिम बुद्धिमत्ता आधारित अपराधों, जैसे डीपफेक, स्वचालित ठगी और एल्गोरिदमिक दुरुपयोग, को ध्यान में रखते हुए कानून में समयानुकूल संशोधन आवश्यक हैं। इन सुधारों के माध्यम से साइबर स्पेस में सुरक्षा, उत्तरदायित्व और न्यायिक प्रभावशीलता को सुदृढ़ किया जा सकता है।

10. निष्कर्ष: सूचना प्रौद्योगिकी अधिनियम साइबर अपराधों से निपटने के लिए एक विशिष्ट और उद्देश्यपरक कानून है, जिसने डिजिटल लेन-देन, इलेक्ट्रॉनिक अभिलेखों तथा कंप्यूटर-संबंधित अपराधों को विधिक मान्यता और दंडात्मक आधार प्रदान किया है; तथापि तीव्र तकनीकी विकास, कृत्रिम बुद्धिमत्ता आधारित अपराधों और जटिल सीमा-पार चुनौतियों के संदर्भ में यह अधूरा प्रतीत होता है। दूसरी ओर भारतीय दंड विधान व्यापक और सुदृढ़ आपराधिक ढाँचा प्रदान करता है, जो धोखाधड़ी, जालसाजी, मानहानि और उत्पीड़न जैसे अपराधों को समाहित करता है, परंतु इसकी संरचना पारंपरिक अपराधों पर आधारित होने के कारण यह तकनीकी विशिष्टताओं को पूर्णतः संबोधित नहीं कर पाता। इसलिए आवश्यक है कि दोनों कानूनों के बीच स्पष्ट समन्वय स्थापित कर एक समन्वित विधिक ढाँचा विकसित किया जाए, जो पारंपरिक आपराधिक सिद्धांतों और आधुनिक डिजिटल वास्तविकताओं का संतुलित समावेश कर सके तथा साइबर अपराधों के प्रभावी नियंत्रण को सुनिश्चित कर सके।

संदर्भ

1. अग्रवाल, पी. (2023). कृत्रिम बुद्धिमत्ता आधारित अपराध और भारतीय कानून. साइबर विधि अनुसंधान पत्रिका, खंड 2, अंक 2, पृ. 50–72.
2. कुमारी, अ. (2021). डिजिटल गोपनीयता बनाम अभिव्यक्ति की स्वतंत्रता: धारा 66ए के परिप्रेक्ष्य में. भारतीय संवैधानिक अध्ययन, खंड 9, अंक 2, पृ. 66–84.
3. गुप्ता, वी. एवं सक्सेना, एल. (2019). फिशिंग, हैकिंग और विधिक नियंत्रण की चुनौतियाँ. भारतीय साइबर सुरक्षा जर्नल, खंड 3, अंक 2, पृ. 21–39.
4. चौधरी, डी. (2018). साइबर स्टॉकिंग और महिलाओं की विधिक सुरक्षा. भारतीय अपराध विज्ञान पत्रिका, खंड 10, अंक 2, पृ. 75–92.
5. जोशी, न. (2020). साइबर आतंकवाद और राष्ट्रीय सुरक्षा का प्रश्न. राष्ट्रीय सुरक्षा एवं विधि पत्रिका, खंड 2, अंक 1, पृ. 101–118.
6. तिवारी, म. एवं सिंह, पी. (2017). डिजिटल साक्ष्य की स्वीकार्यता और धारा 65बी का महत्व. विधि एवं न्याय जर्नल, खंड 5, अंक 3, पृ. 120–138.

7. त्रिपाठी, एस. एवं दुबे, आर. (2024). भारतीय न्याय संहिता में साइबर अपराध का पुनर्संगठन. विधि शोध पत्रिका, खंड 14, अंक 1, पृ. 30–49.

8. पांडेय, ह. (2021). इलेक्ट्रॉनिक अभिलेखों की प्रमाणिकता और न्यायिक प्रवृत्ति. विधिक परिप्रेक्ष्य, खंड 6, अंक 1, पृ. 140–158.

9. भारद्वाज, न. (2025). भारतीय दंड विधान और सूचना प्रौद्योगिकी अधिनियम का तुलनात्मक अध्ययन. समकालीन भारतीय विधि जर्नल, खंड 10, अंक 2, पृ. 170–189.

10. मिश्रा, ए. (2019). सूचना प्रौद्योगिकी अधिनियम में संशोधन और न्यायालयीन दृष्टिकोण. विधि दर्शन पत्रिका, खंड 11, अंक 1, पृ. 52–70.

11. यादव, के. (2018). ऑनलाइन धोखाधड़ी और दंड विधान का विस्तार. समकालीन विधि विमर्श, खंड 7, अंक 4, पृ. 134–150.

12. वर्मा, एस. (2016). साइबर अपराध और भारतीय दंड संहिता: एक विधिक विश्लेषण. राष्ट्रीय विधि पत्रिका, खंड 12, अंक 1, पृ. 88–104.

13. शर्मा, आर. के. (2015). सूचना प्रौद्योगिकी अधिनियम, 2000 का आलोचनात्मक अध्ययन. भारतीय विधि समीक्षा, खंड 8, अंक 2, पृ. 45–60.

14. श्रीवास्तव, जी. (2022). साइबर अपराधों का वर्गीकरण और विधिक ढाँचा. आधुनिक विधि अध्ययन, खंड 8, अंक 3, पृ. 55–73.

15. सिंह, आर. (2020). सीमा-पार साइबर अपराध और क्षेत्राधिकार की समस्या. अंतरराष्ट्रीय विधि समीक्षा (हिंदी), खंड 4, अंक 3, पृ. 200–219.