IMPACT FACTOR 5.397 (SJIF USA)
BIHAR SHODH SAMAAGAM
Multidisciplinary, Multi-Lingual, Peer Reviewed /Refereed Open Access Journal
Vol. 4, Issue 1, January-March, 2026
Available online : https://www.biharshodhsamaagam.com/
ISSN : 3048-6971

भारत में साइबर अपराध की बढ़ती प्रवृत्ति: एक विश्लेषणात्मक अध्ययन

RAJESH KUMAR ACHARYA
RESEARCH SCHOLAR [LAW]
RNB GLOBAL UNIVERSITY, BIKANER
RAJESHKUMARACHARYA1371992@GMAIL.COM

सारांश (Abstract)

यह शोध पत्र भारत में तेजी से बढ़ते साइबर अपराधों की प्रकृति, कारणों और उनके समाज पर पड़ने वाले प्रभावों का विश्लेषण करता है। पिछले एक दशक में 'डिजिटल इंडिया' अभियान के प्रस्तुत तहत इंटरनेट उपयोगकर्ताओं की संख्या में अभूतपूर्व वृद्धि हुई है, लेकिन इसके समानांतर साइबर सुरक्षा की चुनौतियां भी बढ़ी हैं। यह अध्ययन राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (NCRB) के आंकड़ों, हालिया वित्तीय धोखाधड़ी के मामलों और कानूनी ढांचे (IT Act 2000) की प्रभावशीलता की समीक्षा करता है। निष्कर्ष बताते हैं कि तकनीकी जागरूकता की कमी और साइबर कानूनों के क्रियान्वयन में जटिलताएं इस वृद्धि के मुख्य कारक हैं। वर्तमान में भारत में डिजिटलकरण की तेज वृद्धि के साथ साइबर अपराधों में अभूतपूर्व वृद्धि देखी जा रही है। हालिया एनसीआरबी रिपोर्ट के अनुसार 2022 में दर्ज 65,983 मामलों से 2023 में यह बढ़कर 86,420 हो गए, अर्थात् 31% की वृद्धि। इनमें से लगभग 68.9% (59,526) मामले भोले-भाले लोगों को ठगने के उद्देश्य से थे, जबकि शेष में यौन शोषण, फिरौती, राजनीतिक प्रेरणा आदि शामिल हैं।

बीज शब्द:- साइबर अपराध, डिजिटल इंडिया, वित्तीय धोखाधड़ी, डेटा संरक्षण, साइबर सेल

प्रस्तावना (Introduction)

21वीं सदी सूचना प्रौद्योगिकी की सदी है। भारत, जो विश्व की सबसे बड़ी डिजिटल अर्थव्यवस्थाओं में से एक बनने की राह पर है, वर्तमान में साइबर अपराधियों के रडार पर है। वर्षों के दौरान भारत में इंटरनेट उपयोग और डिजिटल सेवाएँ व्यापक रूप से बढ़ी हैं। UPI, ई-कॉमर्स, सरकारी ई-गवर्नेंस (आधार, डिजिटल इंडिया) जैसे प्रयासों से डिजिटल पहुँच बढ़ी है, परंतु इसका परिणाम यह भी हुआ कि खतरा सतह बहुत बड़ा हो गया। जैसे-जैसे वित्तीय लेन-देन और व्यक्तिगत जानकारी ऑनलाइन होती गई, अपराधी भी नए-नए तरीकों से निशाना साधने लगे। अब साइबर अपराध सिर्फ कुछ विशेषज्ञों के हाथ का खेल नहीं रहा; आम नागरिक, छोटे व्यवसाय, बड़े अस्पताल, स्कूली बच्चे, सरकारी संस्थान सभी निशाने पर हैं।

इस परिवेश में भारत में साइबर अपराध की प्रवृत्ति की एक समग्र समझ बेहद जरूरी हो गई हैं।भारत में इंटरनेट का प्रसार न केवल शहरों तक सीमित रहा है, बल्कि ग्रामीण क्षेत्रों में भी स्मार्टफोन की पहुंच बढ़ी है। भुगतान प्रणालियों (UPI), सोशल मीडिया और ई-कॉमर्स ने हमारे जीवन को सुगम बनाया है। हालांकि, इस 'डिजिटल क्रांति' ने अपराधियों को एक नया और सुरक्षित मंच प्रदान किया है जहाँ वे भौतिक सीमाओं के बिना अपराध कर सकते हैं।साइबर अपराध अब केवल डेटा चोरी तक सीमित नहीं हैं; इसमें अब वित्तीय धोखाधड़ी, साइबर बुलिंग, डार्क वेब गतिविधियाँ और राष्ट्र-विरोधी साइबर हमले शामिल हो गए हैं। समस्या यह है कि तकनीक जितनी तेजी से बदल रही है, हमारी सुरक्षा प्रणालियाँ और कानूनी प्रक्रियाएं उतनी गति से अपडेट नहीं हो पा रही हैं।

शोध के उद्देश्य (Objectives of the Study)

1. भारत में साइबर अपराध के विभिन्न प्रकारों और उनके बदलते स्वरूप की पहचान करना।
2. पिछले पांच वर्षों में साइबर अपराध की सांख्यिकीय वृद्धि का विश्लेषण करना।
3. साइबर अपराध के पीछे के सामाजिक, आर्थिक और तकनीकी कारणों को समझना।
4. भारतीय सूचना प्रौद्योगिकी अधिनियम (IT Act) और नई न्याय संहिताओं की प्रभावशीलता का मूल्यांकन करना।
5. साइबर सुरक्षा को मजबूत करने के लिए सुझाव प्रस्तुत करना।

साहित्य समीक्षा

भारत में साइबर अपराध पर कई अध्ययन प्रकाशित हुए हैं। इनमें से अधिकांश ने वित्तीय धोखाधड़ी और पहचान की चोरी जैसे मामलों पर प्रकाश डाला है।अनुज वानखेड़े (2025) के अनुसार प्रमुख साइबर अपराधों में फिशिंग, रैनसमवेयर, डेटा उल्लंघन और पहचान चोरी शामिल हैं।बसुंधरा सोनी (2025) ने बताया कि साइबर अपराधों में निरंतर वृद्धि हो रही है, हालांकि रिपोर्टिंग गैप के कारण वास्तविक आंकड़े अधिक हो सकते हैं।साइबर अपराध पर दूसरे अध्ययनों से भी पता चलता है कि अपराधी लगातार तकनीकों में निपुण हो रहे हैं और नई तकनीक (एआई, डीपफेक) का दुरुपयोग बढ़ा है। Seqrite की एक रिपोर्ट के अनुसार अक्टूबर 2024-सितंबर 2025 में भारत के लगभग आधे साइबर हमले हेल्थकेयर, शिक्षा और विनिर्माण क्षेत्रों पर केंद्रित थे; अकेले हेल्थकेयर-फार्मा क्षेत्र में

14.24% हमलों (3.79 मिलियन डिटेक्शन) की सूचना मिली। साहित्य से यह भी स्पष्ट होता है कि भारत में साइबर अपराध की आधिक्यताएँ प्रायः वित्तीय फायदे पर आधारित हैं। सरकारी रिपोर्टें बताती हैं कि नागरिकों को ठगने के लिए कॉलर ID स्पूफिंग, सिम स्वैप, या नकली सरकारी/बैंकिंग अपील जैसे तरीकों का भारी उपयोग हो रहा है। साथ ही स्त्री एवं बाल शोषण या ऑनलाइन उत्पीड़न के मामलों में भी वृद्धि की प्रवृत्ति देखी गई है। अध्ययन यह भी रेखांकित करते हैं कि रिपोर्टिंग की बाधाएं (लोग शिकायत नहीं कर पाते, पुलिस विभागात्मक सीमाएं) के कारण वास्तविक आंकड़े कम दर्ज होते हैं।

साइबर अपराध के प्रमुख प्रकार (Types of Cybercrimes)

भारत में प्रचलित साइबर अपराधों को निम्नलिखित श्रेणियों में विभाजित किया जा सकता है:

वित्तीय अपराध (Financial Crimes)

- UPI और बैंकिंग धोखाधड़ी: फर्जी कॉल (Vishing), फिशिंग लिंक और स्क्रीन-शेयरिंग ऐप्स के जरिए पैसे निकालना।
- निवेश घोटाले: 'वर्क फ्रॉम होम' या क्रिप्टो-करेंसी में निवेश के नाम पर करोड़ों की ठगी।

सामाजिक और व्यक्तिगत अपराध

- साइबर स्टॉकिंग और बुलिंग: सोशल मीडिया पर महिलाओं और बच्चों को परेशान करना।
- पहचान की चोरी (Identity Theft): किसी दूसरे के नाम पर फर्जी प्रोफाइल बनाकर धोखाधड़ी करना।
- साइबर आतंकवाद और जासूसी
- सरकारी डेटाबेस (जैसे AIIMS या पावर ग्रिड) पर रैंसमवेयर (Ransomware) हमले।

सांख्यिकीय विश्लेषण (Statistical Analysis)

वर्ष	दर्ज साइबर अपराध (अनुमानित)	वृद्धि दर (%)	प्रमुख केंद्र
2022	65,893	24%	बेंगलुरु, हैदराबाद
2023	95,000+	44%	दिल्ली-NCR, जामताड़ा
2024-25	1,50,000+ (प्रत्याशित)	58%	अखिल भारतीय

नोट: डेटा दर्शाता है कि छोटे शहरों (जैसे जामताड़ा, मेवात) से संचालित होने वाले 'साइबर सिंडिकेट' में भारी वृद्धि हुई है।'

साइबर अपराध के कारण (Reasons for Growth)

1. डिजिटल साक्षरता की कमी: लोग तकनीक का उपयोग तो कर रहे हैं, लेकिन सुरक्षा सेटिंग्स (2FA, प्राइवेसी) के प्रति अनभिज्ञ हैं।
2. अपराधियों की गुमनामी: VPN और डार्क वेब के कारण अपराधियों को पकड़ना कठिन हो जाता है।
3. धीमी न्यायिक प्रक्रिया: साइबर मामलों में सजा की दर (Conviction Rate) भारत में काफी कम है।
4. सीमा पार से हमले: कई साइबर हमले पड़ोसी देशों या अंतरराष्ट्रीय सर्वरों से संचालित होते हैं, जिससे अधिकार क्षेत्र (Jurisdiction) की समस्या पैदा होती है।

कानूनी ढांचा और चुनौतियां (Legal Framework)

आईटी अधिनियम, 2000 (IT Act, 2000)

यह भारत का प्राथमिक कानून है। इसकी धारा 66 (कंप्यूटर संबंधी अपराध) और 67 (अश्लील सामग्री) महत्वपूर्ण हैं। हालांकि, क्लाउड कंप्यूटिंग और AI के इस दौर में यह कानून पुराना पड़ता जा रहा है।

नई न्याय संहिता (BNS 2023)

भारतीय न्याय संहिता में साइबर अपराधों को अधिक स्पष्टता से परिभाषित करने और कड़ी सजा के प्रावधान जोड़े गए हैं।

रोकथाम और नीतिगत सिफारिशें

भारत में साइबर अपराध की समस्या का सामना करने के लिए सुरक्षा, प्रशिक्षण और जागरूकता पर विशेष ध्यान देना होगा। निम्नलिखित नीतिगत उपाय सुझाए जाते हैं:

• साइबर जागरूकता अभियानों का विस्तार: स्कूलों, महाविद्यालयों और गांव-शहरों में नियमित शिक्षा कार्यक्रम हो। उदाहरणस्वरूप, बैंक खाते सुरक्षा, पासवर्ड

प्रबंधन, संदिग्ध लिंक से सावधानी इत्यादि विषय पढ़ाए जाएँ। मीडिया (रेडियो, टीवी, सोशल मीडिया) के माध्यम से 'डिजिटल जागरूकता' अभियान नियमित रूप से चलाया जाए।

• प्राथमिकी से एफआईआर तक प्रक्रिया की सरलता: वर्तमान में केवल ~2–3% शिकायतें FIR में परिवर्तित हो रही हैं। पुलिस को निर्देश दिए जाएँ कि साइबर सेल में शिकायत आने पर त्वरित जाँच शुरू की जाए। डिजिटल शिकायतें प्राप्त होते ही स्वत: नोटिस/रिपोर्ट बोर्ड की स्थापना हो, ताकि कम्प्यूटर/मोबाइल फोरेंसिक के लिए टीम सक्रिय हो सके। SOP (जैसा कि जनवरी 2026 में जारी की गई) का कड़ाई से पालन सुनिश्चित किया जाए।

• क़ानूनी दंड की सख्ती एवं संसाधन: अपराधी को शीघ्र सज़ा मिलनी चाहिए। नागरिकों के मनोबल को बढ़ाने के लिए विशेष न्यायालय या समयसीमा-bound ट्रायल की व्यवस्था की जाए। साइबर सेल को संसाधन (तकनीकी उपकरण, प्रशिक्षित कर्मचारी) मुहैया करवाए जाएँ, ताकि इलेक्ट्रॉनिक साक्ष्य जल्दी संगृहीत हो सकें। पीड़ितों को कम्प्यूटरीकृत सहायता (जैसे साइबर हेल्पलाइन 1930) उपलब्ध कराई जाए।

• निजी क्षेत्र सहयोग: बैंक, इंटरनेट सर्विस प्रोवाइडर, सोशल प्लेटफ़ॉर्म आदि कंपनियों को साइबर सुरक्षा मानकों का कड़ाई से पालन करना अनिवार्य किया जाए। उन्हें धोखाधड़ी की सूचना तुरंत CERT-In/पुलिस को भेजनी चाहिए। डिजिटल भुगतान सिस्टम (UPI, BHIM आदि) में हील्टगे की तरह अतिरिक्त द्वि-कारक प्रमाणीकरण प्रणाली लागू होनी चाहिए।

• बजटीय आवंटन: राष्ट्रीय सुरक्षा के लिए साइबर सुरक्षा ख़ास है। सालाना बजट में रक्षा के समान साइबर सुरक्षा हेतु पर्याप्त वित्त आरक्षित किया जाना चाहिए (जैसा कि बजट 2025-26 में ₹782 करोड़ आवंटित हुए)। यह धन मुख्यतः जनता जागरूकता, पुलिस प्रशिक्षण, साइबर लैब उन्नयन, और राष्ट्रीय CERT-In गतिविधियों पर खर्च किया जाना चाहिए।

• अंतरराष्ट्रीय सहयोग: चूंकि साइबर अपराध अंतरराष्ट्रीय नेटवर्क से जुड़े हैं, भारत को अंडरवर्ल्ड की मुलुकों से संगठनों के लिए अंतरराष्ट्रीय समझौते और आईपी interpol नेटवर्क का उपयोग बढ़ाना चाहिए। सीमापार मानव तस्करों और फर्जी कॉल सेन्टर ऑपरेटरों के विरुद्ध कनाडा, यूएस, ऑस्ट्रेलिया आदि देशों से सहयोग बढ़ाएँ।

• नए कानून: पास हुए डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट (2023) से व्यक्ति को डेटा पर अधिकार मिले, पर क़ानूनी लचक बढ़ाने के लिए साइबर अपराध विशेषज्ञ अदायगी अधिनियम पर पुनर्विचार हो सकता है। ऑनलाइन सुरक्षा विधेयक जैसी पहलें भी व्याध अनुपालन सुनिश्चित करें।

• प्रवर्तन एजेंसी और प्रशिक्षण: गृह मंत्रालय के अंतर्गत I4C, NCIIPC, NCSC तथा CERT-In जैसे संस्थानों के समन्वय में साइबर फ़ोरेंसिक प्रयोगशालाओं की संख्या बढ़ाई जाए, और राज्य/केंद्र साइबर पुलिस को निरंतर प्रशिक्षण मिले।

लागू करने की रूपरेखा

1. स्थानीय स्तर पर क्रियान्वयन: जिलेवार साइबर जागरूकता शिविर, पुलिस थानों में साइबर सेल मजबूती।
2. मध्यवर्ती स्तर: राज्यों में साइबर यूनिटों का सृजन एवं I4C के दिशानिर्देशों के तहत नियमित समीक्षा।
3. राष्ट्रीय स्तर: वर्ष 2026–27 तक सभी राज्य-केंद्र साइबर लैब को CERT-In से जोड़ना। वित्त वर्ष 2025–26 से हर साल 20% अधिक साइबर बजट आवंटित करना। संयुक्त परिचालन अभ्यास (जैसे NCCC अभियान) हर माह करना।
4. मूल्यांकन और निगरानी: केंद्रीय सरकार को प्रत्येक त्रैमासिक में प्रगति रिपोर्ट प्रकाशित करनी चाहिए, जिसमें मामलों का ट्रैक, मुकदमेबाज़ी की दर, सजाए गए अपराधियों की संख्या आदि सार्वजनिक हों। इन कार्यनीतियों से उम्मीद है कि साइबर अपराध की रोकथाम तथा प्रतिक्रिया व्यवस्था में मजबूती आएगी, जिससे नागरिकों का विश्वास बढ़ेगा और डिजिटल विकास की गति सुरक्षित रहेगी।

निष्कर्ष (Conclusion)

भारत में साइबर अपराध की बढ़ती प्रवृत्ति एक गंभीर राष्ट्रीय सुरक्षा चिंता है। केवल कानून बना देने से इस पर लगाम नहीं लगाई जा सकती। इसके लिए एक त्रि-आयामी दृष्टिकोण की आवश्यकता है:

1. अत्याधुनिक तकनीकी सुरक्षा।
2. जन-जागरूकता अभियान।
3. कुशल और त्वरित न्याय प्रणाली।

भविष्य में, आर्टिफिशियल इंटेलिजेंस (AI) और मशीन लर्निंग का उपयोग करके साइबर हमलों को रोकने के लिए 'प्रो-एक्टिव' सुरक्षा तंत्र विकसित करना होगा।

संदर्भ (References)

1. NCRB (2024), "Crime in India Report".
2. Ministry of Home Affairs (MHA), "Cyber Dost" Initiatives.
3. Singh, P. (2025), "Digital Security in Modern India", Academic Press.
4. Information Technology Act, 2000 (Amended 2008).
5. CERT-In (Indian Computer Emergency Response Team) Annual Reports.