eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

साइबर अपराध और चुनौतियाँः भारत के संदर्भ में एक विश्लेषण

डा0 अवनीश कुमार गौतम[1], डा0 अनूप कुमार[2]
[1]असिस्टेंट प्रोफेसर, राजनीति विज्ञान विभाग, राजकीय महाविद्यालय, कॉट, शाहजहॉपुर, उ0प्र0
[2]असिस्टेंट प्रोफेसर, वनस्पति विज्ञान विभाग, राजकीय महाविद्यालय, कॉट, शाहजहॉपुर, उ0प्र0

Received: 20 March 2026 Accepted & Reviewed: 25 March 2026, Published: 31 March 2026

Abstract

भूमंडलीकरण की शुरुआत 1980 के दशक से हुई। भूमंडलीकरण के द्वारा राष्ट्रों के मध्य तकनीकी का तेजी से विकास हुआ। तकनीकी का आदान–प्रदान होने से लगभग विश्व के सभी देशों को इसका फायदा पहुंचा कुछ देशों को अधिक तो कुछ को कम। वर्ल्ड वाइड वेब, कंप्यूटर एवं तीव्र गति से मोबाइल के इस्तेमाल ने मानव जीवन को सरल एवं सहज बनाया है। इस टेक्नोलॉजी के प्रयोग से ही आज पूरा विश्व लाभान्वित है। वहीं कुछ लोग इस टेक्नोलॉजी का दुरुपयोग भी कर रहे हैं खुद को फायदा और दूसरों को नुकसान पहुंचा रहे हैं विशेषकर 21वीं सदी के प्रारंभ से सूचना एवं तकनीकी का विस्तार कंप्यूटर एवं मोबाइल के प्रयोग की बढ़ोतरी के चलते साइबर क्राइम एक बड़ी चुनौती के रूप में उभरा है, जो व्यक्तियों, संगठनों और राष्ट्रों की सुरक्षा को खतरे में डाल रहा है। साइबर अपराध के चलते अनेक लोग बैंक ठगी के शिकार हो रहे हैं तथा अपनी जमा पूँजी खो रहे हैं। साइबर अपराध आज भारत सहित संपूर्ण विश्व के लिए एक चुनौती बना हुआ है। यह शोध पत्र भारत में साइबर अपराधों के उदय, उनके प्रकारों, उत्पन्न होने वाली चुनौतियों, साइबर अधिनियमों तथा संभावित समाधानों पर केंद्रित है। डिजिटल इंडिया जैसी पहलों के बावजूद, साइबर ठगी, हैकिंग, ब्लैकमेलिंग और डिजिटल अरेस्ट जैसे अपराधों में वृद्धि हो रही है। इस शोध पत्र में साइबर से जुड़े आकड़ों के आधार पर विश्लेषण प्रस्तुत किया गया है। एवं उसके आधार पर साइबर क्राइम से बचने के सुझाव भी दिए गए हैं। उसके साथ सूचना एवं तकनीकी अधिनियम सन 2000 की चर्चा की गई है प्रमुख निष्कर्षों में भारत में इंटरनेट का उपयोग करने वालों की संख्या 1 अरब पार कर चुकी है, इसके साथ ही साइबर अपराध से जुड़ी घटनाएं लगातार बढ़ रही हैं।, जो 2025 के अन्त तक और अधिक बढ़ने की आशंका है। समाधान के रूप में जागरूकता, कानूनी सुधार और तकनीकी की आवश्यकता पर जोर दिया गया है।

मूल शब्द– कंप्यूटर, साइबर क्राइम, बैंकिंग ठगी, डिजिटल अरेस्ट, जागरूकता, साइबर लॉज, चुनौती एवं समाधान।

Introduction

वर्तमान डिजिटल युग में इंटरनेट और सूचना प्रौद्योगिकी के उपयोग ने जीवन को सुगभ बना दिया है, परंतु इसके साथ ही साइबर अपराधों का खतरा भी बढ़ गया है। साइबर अपराध से तात्पर्य उन गैर कानूनी गतिविधियों से है जो कंप्यूटर, नेटवर्क या डिजिटल माध्यमों के माध्यम से की जाती हैं। भारत जैसे विकासशील देश में, जहां ट्राई के अनुसार इंटरनेट उपयोगकर्ताओं की संख्या 2025 में 100 करोड़ से अधिक हो चुकी है, साइबर अपराध की जड़ें तकनीकी प्रगति में हैं, लेकिन इसका प्रसार मानवीय कमजोरियों, जैसे जागरूकता की कमी और कमजोर सुरक्षा प्रणालियों से हुआ है। भारत में डिजिटल इंडिया, आधार

eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

और UPI जैसी पहलों ने अर्थव्यवस्था को मजबूत किया है, लेकिन सुरक्षा को लेकर जोखिमों में भी वृद्धि हुई है। उदाहरणस्वरूप, 2023 में 'रिसिक्योरिटी' रिपोर्ट ने 81.5 करोड़ भारतीयों के डेटा को डार्क वेब पर बिक्री के लिए उपलब्ध होने का खुलासा किया। इस प्रकार साइबर अपराध राष्ट्र की सुरक्षा के लिए चुनौती बन चुका है।

इस शोध पत्र का उद्देश्य साइबर अपराधों की प्रकृति, भारत में उनकी वर्तमान स्थिति, उत्पन्न चुनौतियों और समाधानों का मूल्यांकन करना है। इस शोध पत्र के अंतर्गत साहित्य समीक्षा, साइबर अपराधों के प्रकार, भारत में साइबर क्राइम की स्थिति, चुनौतियाँ, समाधान और निष्कर्ष के अंतर्गत व्याख्या की गई है। जिसमें यह प्रयास किया गया है कि भारत में साइबर क्राइम को समझा जा सके तथा इससे निपटने के सुझाव दिए जा सके।

साहित्य समीक्षा

वर्तमान समय में साइबर अपराध से संबंधित अनेक अखबारों में दिन प्रतिदिन सूचनाओं पढ़ने को मिलती हैं अनेक लोग साइबर क्राइम के नए–नए तरीके से शिकार हो रहे हैं इसके साथ ही अनेक पुस्तकें भी साइबर क्राइम पर लिखी जा चुकी हैं। इसी क्रम में सुदीप सरवान की पुस्तक ''साइबर अपराध'' (2020) साइबर क्राइम के विकास को कंप्यूटर के इतिहास से जोड़कर समझाया है। इसमें बताया गया है कि भूमंडलीकरण के साथ ही साइबर अपराधों का जन्म 1980 के दशक में वायरस और हैकिंग के रूप में हुआ, जो आज फिशिंग और रैनसमवेयर तक विस्तृत हो गया। इस पुस्तक में लेखक ने तर्क दिया है कि साइबर अपराध केवल तकनीकि ही नहीं बल्कि सामाजिक एवं मनोवैज्ञानिक कारणों के द्वारा भी तेजी से बढ़ा है।[1] इसी प्रकार नरेंद्र कुमार शर्मा की पुस्तक ''साइबर अपराधः चुनौतियाँ और प्रबंधन'' (2018) में भारत–केंद्रित दृष्टिकोण अपनाया गया है। इन्होंने साइबर अपराध को तीन श्रेणियों में विभाजित किया है जिसमें कंप्यूटर के विरुद्ध अपराध, कंप्यूटर का उपयोग करके अपराध, और कंप्यूटर से संबंधित अपराध शामिल हैं। चुनौतियों के रूप में कानूनी अस्पष्टता और जांच प्रक्रिया की जटिलता पर प्रकाश डाला गया है।

पुस्तक में सुझाव दिया गया है कि साइबर प्रबंधन के लिए बहु–स्तरीय सुरक्षा प्रणाली को अपनाना आवश्यक है।[2] इसी तरह से अरुण कुमार पाठक की पुस्तक ''साइबर क्राइम एंड साइबर लॉज '' (2020) कानूनी प्रावधानों पर प्रकाश डालती है, जहां आईटी एक्ट 2000 की धारा 66 को साइबर अपराधों के लिए आधारभूत माना गया है।[3] इसी तरह अंग्रेजी साहित्य में, कनक गुप्ता की पुस्तक ''बाइबल ऑफ साइबर क्राइम्स इन इंडिया'' (2024) में हैकर्स की तकनीकों और केस स्टडीज जैसे कोस्मोस बैंक लूट पर विस्तार से चर्चा करती है। इस पुस्तक में साइबर अपराधों के जन्म से लेकर अब तक की चर्चा की गई है। इसी प्रकार से मंजू मिश्रा की पुस्तक, ''साइबर सिक्योरिटी इन इंडियाः चैलेंजेस एंड ऑप्शंस'' (2023) में साइबर युद्ध और जासूसी जैसे राष्ट्रीय स्तर की चुनौतियों का विश्लेषण है।[5]

समाचार पत्रों में, इंडियन एक्सप्रेस के 17 दिसंबर 2024 के लेख ''2024: व्हेन साइबरक्राइम्स केम क्लोजर होम'' में 2024 की जटिल धोखाधड़ी स्कीम्स का उल्लेख है, जो निवेश घोटालों और डर–आधारित फ्रॉड पर केंद्रित हैं।[6] जनसत्ता के हालिया लेख ''भारत में बढ़ता साइबर अपराध और डिजिटल गिरफ्तारी घोटाला'' में 2022 से 2023 तक मामलों में 31 प्रतिशत वृद्धि का आंकड़ा दिया गया है।[7] उपरोक्त स्रोतों में

eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

साइबर अपराधों की बहुआयामी प्रकृति को रेखांकित किया गया है, लेकिन इन पुस्तकों में एवं खबरों में साइबर क्राइम से सुरक्षा एवं बचाव को लेकर कम ध्यान दिया गया है।

साइबर अपराधों के प्रकार

साइबर अपराधों को वर्गीकृत करना आवश्यक है ताकि उनकी प्रकृति को समझा जा सके। इसके प्रमुख प्रकार निम्न हैं:–

1. ***फिशिंग और घोटाला:–*** फिशिंग एक प्रकार का सामाजिक इंजीनियरिंग हमला है जिसमें डिजिटल उपयोग करता को लक्ष्य बनाया जाता है तथा उपयोगकर्ता के बारे में संवेदनशील जानकारी प्राप्त करने के लिए फर्जी संदेश और ईमेल भेजकर उन्हें धोखा देने का प्रयास किया जाता है या हानिकारक सॉफ्टवेयर डाउनलोड करने और लक्ष्य सिस्टम पर उसका शोषण करने का प्रयास करता है। अमित दुबे की पुस्तक ''अदृश्य जाल: साइबर क्राइम की सच्ची कहानियां'' (2022) में जमतारा फिशिंग गिरोह की कहानी वर्णित है, जहां हजारों लोग बैंक विवरण खो चुके।[8]

2. ***रैनसमवेयर:–*** रैनसमवेयर डिजिटल क्राइम करने का सामान्य माध्यम है जिसके अंतर्गत उपयोग कर्ता के मोबाइल अथवा कंप्यूटर को हैक कर उसके एक्सेस को हैकर द्वारा चुरा लिया जाता है। इसके पश्चात् हैकर द्वारा व्यक्ति की सूचनाओं एवं निजी जानकारी को लेकर फिरौती की धमकी दी जाती है। तथा कई बार इसमें सफल भी हो जाते हैं।

3. ***डिजिटल गिरफ्तारी और ब्लैकमेलिंग:–*** हाल ही के सालों में डिजिटल अरेस्ट का ट्रेंड तेजी से बढ़ा है डिजिटल अरेस्ट में ज्यादातर महिलाओं, बुजुर्गों एवं जिनके पास अधिक धन है उन्हें शिकार बनाया जाता है। तथा उन्हें ईडी, सीबीआई एवं पुलिस का भय दिखाकर उनसे पैसों की ठगी की जाती है। इसके अंतर्गत ठग वीडियो कॉल पर गिरफ्तारी या किसी अन्य चीज का डर दिखाते हैं बीबीसी हिंदी के 17 अक्टूबर 2025 के लेख में डिजिटल अरेस्ट को प्रमुख खतरे के रूप में चित्रित किया गया है।

4. ***पहचान की चोरी:–*** पहचान की चोरी तब होती है जब कोई साइबर अपराधी किसी अन्य व्यक्ति के व्यक्तिगत डेटा जैसे क्रेडिट कार्ड नंबर, आधार नंबर, पासपोर्ट, वोटर आईडी कार्ड को हासिल कर उसमें फेरबदल करता है और उसका उपयोग वह गैर कानूनी धंधों में करता है साथ ही इनमें व्यक्तिगत तस्वीरों का उपयोग धोखाधड़ी या अपराध करने के लिए उसकी अनुमति के बिना करता है।

5. ***सॉफ्टवेयर चोरी:–*** सॉफ्टवेयर चोरी, कॉपीराइट या लाइसेंस प्रतिबंधों का उल्लंघन करते हुए भुगतान किए गए सॉफ्टवेयर का अवैध उपयोग या प्रतिलिपि बनाना है। सॉफ्टवेयर पाइरेसी का एक उदाहरण तब होता है जब आप विंडोज की एक नई, बिना एक्टिवेटेड कॉपी डाउनलोड करते हैं और विंडोज एक्टिवेशन के लिए वैध लाइसेंस प्राप्त करने के लिए ''क्रैक्स'' नामक तकनीक का इस्तेमाल करते हैं। इसे सॉफ्टवेयर पाइरेसी माना जाता है। सॉफ्टवेयर पायरेसी के अंतर्गत न केवल सॉफ्टवेयर बल्कि संगीत, फिल्में या चित्र भी पायरेटेड हो सकते हैं।

6. ***साइबर स्टॉकिंग एवं बुलिंग:–*** इसके अंतर्गत किसी को बार–बार ऑनलाइन परेशान करना, गाली देना, धमकी देना या डराना साइबर स्टॉकिंग एवं बुलिंग कहलाता है। वर्तमान में विशेष रूप से सोशल मीडिया और मैसेजिंग प्लेटफॉर्म के माध्यम से यह समस्या तेजी से बढ़ रही है।

eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

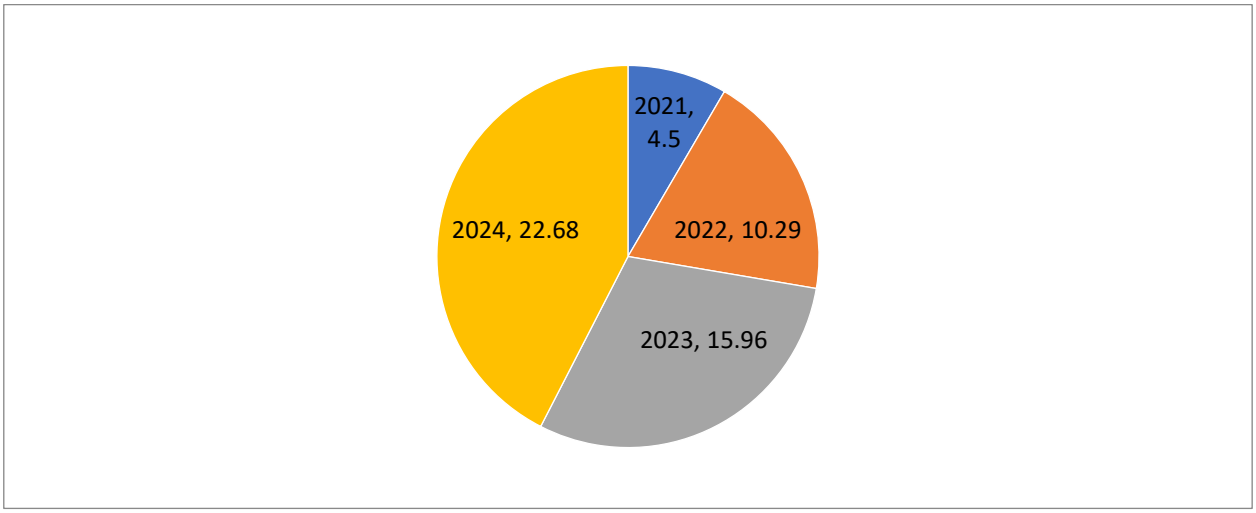
7. ***अश्लील सामग्री का प्रसारः—*** इंटरनेट पर अश्लील सामग्री, चाइल्ड पोर्नोग्राफी या आपत्तिजनक कंटेंट फैलाना भी साइबर अपराध के अंतर्गत आता है। अश्लील सामग्री का प्रसार बहुत तेजी से हो जाता है। इस पर और अधिक सख्त कानून बनाकर लगाम लगाने की जरूरत है।

8. ***ऑनलाइन भर्ती धोखाधड़ीः—*** वर्तमान समय में नौकरी के नाम पर ठगी का बहुत तेजी से प्रचलन हुआ है। बहुत से लोगों को मैसेज, ईमेल या फोन पर कालिंग के माध्यम से नौकरी का प्रलोभन दिया जाता है तथा नौकरी के नाम पर उनसे पैसे वसूल कर लिए जाते हैं एवं पीड़ित व्यक्ति को पता तब चलता है जब उसे नौकरी के नाम पर मोटी रकम वसूल कर ली जाती है परंतु उसे कोई भी नौकरी प्राप्त नहीं होती है। ठगों द्वारा फर्जी कंपनी/संस्था से अपने आप को जुड़े होने का हवाला दिया जाता है तथा उसे कंपनी या संस्था में नौकरी देने की गारंटी दी जाती हैं। तथा जैसे ही ठग अपने मकसद में कामयाब हो जाते हैं वह फोन बंद कर लेते हैं।

भारत में साइबर अपराध की स्थिति

भारत में साइबर अपराध तेजी से बढ़ रहे हैं। एनडीटीवी के 2 अगस्त 2025 के लेख के अनुसार, 2024 में 23,000 करोड़ रुपये चोरी हुए।[9] इंडिया टुडे (1 अगस्त 2025) में बताया गया कि मामलों में चार गुना वृद्धि हुई, महाराष्ट्र, उत्तर प्रदेश एवं कर्नाटक सबसे प्रभावित राज्य हैं साथ ही बताया गया है कि 2021 में भारत में साइबर क्राइम के कुल 4.5 लाख मामले थे जो 2024 में बढ़कर 22 लाख हो गये जिसमें 401 प्रतिशत की वृद्धि हुई जोकि एक चिंता का विषय है।[10]

एनसीआरबी द्वारा जारी साइबर क्राइम के आकड़े 2021–24 तक (लाख में)



एनसीआरबी के द्वारा साइबर क्राइम पर जारी किए गए आंकड़ों से स्पष्ट है कि 2021 में भारत में साइबर क्राइम की संख्या 4.5 लाख, 2022 में 10.29 लाख, 2023 में 15.96 लाख एवं 2024 में 22.68 लाख दर्ज की गई तथा अनुमानित आंकड़ों के अनुसार 2025 में साइबर अपराधों की संख्या 24 लाख तक हो सकती है इस प्रकार भारत में प्रतिवर्ष साइबर अपराध की संख्या में बढ़ोतरी एक गंभीर चिंता का विषय है जो कि

eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

शासन और प्रशासन के लिए बड़ी चुनौती है यह आंकड़े दर्शा रहे हैं कि आने वाले समय में साइबर अपराधों की संख्या में और अधिक बढ़ोतरी हो सकती है।[11] यह स्थिति डिजिटल इंडिया को चुनौती दे रही है।

भारत में साइबर क्राइम से निपटने हेतु सरकार द्वारा उठाए गये कदमः

साइबर अपराध तेजी से बढ़ते खतरे के रूप में उभर रहे हैं, जो व्यक्तियों, संगठनों और राष्ट्रीय सुरक्षा को प्रभावित कर रहे हैं। भारत सरकार ने इस चुनौती से निपटने के लिए कानूनी, तकनीकी, जागरूकता और समन्वयित प्रयासों के माध्यम से कई महत्वपूर्ण कदम उठाए हैं। ये कदम सूचना प्रौद्योगिकी मंत्रालय, गृह मंत्रालय और अन्य एजेंसियों द्वारा संचालित हैं। नीचे प्रमुख पहलों का संक्षिप्त विवरण दिया गया हैः–

- साइबर क्राइम से निपटने के लिए संयुक्त राष्ट्र संकल्प के बाद भारत ने मई 2000 में सूचना प्रौद्योगिकी अधिनियम–2000 को पारित कर दिया और 17 अक्टूबर 2000 को अधिसूचना जारी कर इसे लागू कर दिया। सूचना प्रौद्योगिकी अधिनियम–2000, 13 अध्यायों में विभक्त है जिसमें कुल 94 धाराएं हैं। 27 अक्टूबर 2008 को इस कानून को एक घोषणा द्वारा संशोधित किया गया। इसे 5 फरवरी 2009 को फिर से संशोधित किया गया, जिसके तहत अध्याय 2 की धारा 3 में इलेक्ट्रॉनिक हस्ताक्षर की जगह डिजिटल हस्ताक्षर को जगह दी गई। इसके लिए धारा 2 में उपखंड (एच) के साथ उपखंड (एचए) को जोड़ा गया, जो सूचना के माध्यम की व्याख्या करता है। इसके अनुसार, सूचना के माध्यम से तात्पर्य मोबाइल फोन, किसी भी तरह का व्यक्तिगत डिजिटल माध्यम या फिर दोनों हो सकते हैं, जिनके माध्यम से किसी भी तरह की लिखित सामग्री, वीडियो, ऑडियो या तस्वीरों को प्रचारित, प्रसारित या एक से दूसरे स्थान तक भेजा जा सकता है।[12]
- इसी प्रकार से राष्ट्रीय साइबर सुरक्षा नीति को 2013 में ऑनलाइन खतरों पर नजर रखने, सुरक्षा प्रदान करने और उनसे बचाव के उपायों को मजबूत करने के लिए बनाया गया था। इस नीति का उद्देश्य लोगों, व्यवसायों और सरकार के लिए एक विश्वसनीय और सुरक्षित इंटरनेट प्रदान करना है। 2 जुलाई 2013 को, मांग के जवाब में, सरकार ने राष्ट्रीय साइबर सुरक्षा नीति जारी की। संस्थागत संरचनाओं, प्रक्रियाओं, प्रौद्योगिकी और सहयोग के उपयोग के माध्यम से, यह नीति साइबरस्पेस में सूचना बुनियादी ढांचे की सुरक्षा, कमजोरियों को कम करने, साइबर खतरों को रोकने और उनका जवाब देने की क्षमता बनाने और साइबर घटना से होने वाले नुकसान को कम करने का प्रयास करती है।[13]
- डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट, 2023 (DPDP Act): व्यक्तिगत डेटा की सुरक्षा के लिए लागू, जो डेटा उल्लंघनों पर कड़े दंड लगाता है। इससे साइबर अपराधों की रोकथाम में मजबूती आई है।
- **कानूनी प्रावधान**: भारत में साइबर अपराधों से निपटने के लिए कई कानूनी प्रावधान हैं, जो निम्नलिखित हैं:–

1. IT Act, 2000 की धारा 66 हैकिंग और अनधिकृत एक्सेस को दंडनीय अपराध मानती है।
2. धारा 66C और 66D पहचान की चोरी और ऑनलाइन धोखाधड़ी पर लागू होती है।

eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

3. धारा 67 अश्लील सामग्री के प्रसार पर रोक लगाती है।
4. IPC की धारा 420, 468, 469 भी धोखाधड़ी और जालसाजी पर लागू होती हैं।

- **अन्य प्रयासः** सरकार ने साइबर सुरक्षा को मजबूत करने के लिए कई कदम उठाए हैंः

1. सीसीपीडब्ल्यूसी योजनाः 33 राज्यों में साइबर फॉरेंसिक लैब, 24,600 कर्मियों का प्रशिक्षण (रू0 132.93 करोड़ बजट)।
2. ट्रेनिंगः साइट्रेन पोर्टल पर 1.05 लाख पुलिसकर्मी पंजीकृत, 82,704 प्रमाणपत्र जारी।
3. बजट 2025–26ः साइबर सुरक्षा पर रू0 782 करोड़।
4. हेल्पलाइनः 1930 नंबर और रिपोर्टिंग पोर्टल।
5. कानूनी कदमः ऑनलाइन गेमिंग बिल 2025 पारित, 3,962 स्काइप आईडी और 83,668 व्हाट्सएप अकाउंट ब्लॉक।

चुनौतियाँः

साइबर अपराधों से जुड़ी प्रमुख चुनौतियाँ निम्नलिखित हैंः–

1. ***कानूनी और प्रक्रियागत कमियांः–***भारत का सूचना और प्रौद्योगिकी एक्ट सन 2000 में बना तथा कई बार इसमें संशोधन हुए इन सब के बावजूद अभी भी इसमें कमियॉ हैं। इसमें और अधिक संशोधन करने की आवश्यकता है या साइबर क्राइम से संबंधित किसी नए एक्ट को बनाकर लागू करने की जरूरत है। क्योंकि आईटी एक्ट होने के बावजूद भारत में साइबर क्राइम की घटनाएं प्रत्येक वर्ष पिछले वर्ष की तुलना में बढ़ रही है। जो की एक चिंता का विषय है आज प्रतिदिन के अखबारों में साइबर अपराध से जुड़ी हुई अनेक खबरें पढ़ने को मिलती हैं।
2. ***जागरूकता की कमीः–*** बीबीसी (7 सितंबर 2025) में ''डिजिटल अरेस्ट से लाखों डॉलर नुकसान'' के अर्न्तगत बताया गया है कि जागरूकता की कमी के चलते आज बड़े स्तर पर विशेष कर बुजुर्ग एवं ग्रामीण क्षेत्र से जुड़े हुए लोग साइबर क्राइम का अधिक शिकार हो रहे हैं। उसके साथ ही बड़े पैमाने महिलाएं भी साइबर ठगी का शिकार हो रही हैं।[14] तथा समय की आवश्यकता है कि साइबर क्राइम से निपटने के लिए सरकार द्वारा बड़े स्तर पर जन जागरूकता कार्यक्रम चलाए जाये, समाचार पत्रों एवं टीवी चैनलों पर साइबर क्राइम की चेतावनी से संबंधित विज्ञापनों को बढ़ावा दिया जाए।
3. ***तकनीकी ज्ञान एवं मानव संसाधन की कमीः–*** वर्तमान समय की जरूरत है कि साइबर क्राइम को नियंत्रित करने वाली संस्थाओं से संबंधित लोगों को बड़े स्तर पर तकनीकी एवं प्रशिक्षण दिया जाना चाहिए। विशेषकर इसके लिए पुलिस को ट्रेनिंग चाहिए ताकि वह बदलते परिवेश में साइबर क्राइम को समझ सके तथा साइबर क्राइम के शिकार लोगों को न्याय दिला सके।
4. ***अंतर्राष्ट्रीय घटकः–*** आज अनेक अंतर्राष्ट्रीय घटक हैं जिसमें विशेषकर विदेशी ठग जो साइबर क्राइम को बढ़ावा दे रहे हैं इन ठगों का जाल कई देशों में फैला हुआ है तथा इन्हें पकड़ पाना बहुत मुश्किल है

eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

क्योंकि यह विदेशों से अपने नेटवर्क को चला रहे होते हैं। जो कि एक बड़ी चुनौती है। ये चुनौतियाँ बहुआयामी हैं, जो तत्काल हस्तक्षेप मांगती हैं।

साइबर अपराध से बचने हेतु सुझावः

साइबर अपराध से बचने हेतु सुझाव निम्नलिखित हैः–

1. साइबर अपराध से बचने के लिए हमें यह सुनिश्चित करना चाहिए कि हम जिस डिवाइस का प्रयोग कर रहे हैं वह एंटीवायरस एवं फायर बाल जैसे अद्यतन सुरक्षा सॉफ्टवेयर से उपयुक्त हो। जिससे किसी भी वायरस अथवा हैकिंग से बचा जा सके।
2. अपने डिवाइस में सर्वोत्तम सुरक्षा सेटिंग का उपयोग करना चाहिए जो कि डिवाइस के पर्यावरणीय अनुकूल हो। तथा उक्त सेटिंग से छेड़छाड़ करने से बचना चाहिए कई बार कुछ समय के लिए डिवाइस की सेटिंग से की गई छेड़छाड़ ठगी को अंजाम दे देती है।
3. अविश्वसनीय वेबसाइट पर कुछ भी सर्च करने से बचना चाहिए। तथा ऐसी वेबसाइटों से अज्ञात फाइलों को डाउनलोड नहीं करना चाहिए क्योंकि कई बार यही अज्ञात फाइलें डिवाइस में आकर डिवाइस को हैकर्स हैक कर लेते हैं या डिवाइस की सूचनाओं को हैकर को इन फाइलों के माध्यम से पता चल जाता है। व्हाट्सएप या ईमेल अटैचमेंट देखते समय भी सावधान रहें। संदिग्ध लिंक पर क्लिक करने से बचना चाहिए।
4. मोबाइल फोन अथवा कंप्यूटर को लॉक–अनलॉक करने के लिए मजबूत पासवर्ड का प्रयोग करना चाहिए जन्मदिन, नाम या बच्चे का नाम आदि से पासवर्ड नहीं बनना चाहिए। साथ ही ईमेल एवं यूपीआई या अन्य बैंकिंग एप के पासवर्ड को जटिल बनाना चाहिए। तथा सुरक्षा के दृष्टि से उन्हें समय–समय पर बदलते रहना चाहिए एवं पासवर्ड को किसी को शेयर नहीं करना चाहिए।
5. ऑनलाइन या अपने सोशल मीडिया अकाउंट पर संवेदनशील जानकारी को साझा न करें। किसी के साथ बगैर जाने समझे किसी को फोन पर आए ओटीपी को शेयर नहीं करना चाहिए।
6. अपने बच्चों को मोबाइल फोन के सीमित उपयोग पर ध्यान देना चाहिए तथा उन्हें साइबर अपराध के बारे में भी जागरूक करना चाहिए। बच्चों को फोन पर नए–नए गेम को डाउनलोड करने से मना करना चाहिए। क्योंकि कई बार गेम डाउनलोड करने के चक्कर में हैकर्स फोन को हैक कर लेते हैं और जिससे एक बड़ा साइबर अपराध होने का खतरा हो सकता है।
7. साइबर अपराध का शिकार होने पर तत्काल पुलिस को सूचित कर प्राथमिकी दर्ज करानी चाहिए ताकि समय से पुलिस उस पर एक्शन ले सके, एवं पीड़ित को न्याय मिल सके।

निष्कर्षः–

भूमंडलीकरण के प्रारंभ से भारत में तकनीकि का तेजी से विकास हुआ है अब तक साइबर क्राइम को लेकर अपराध हर वर्ष पिछले वर्ष की तुलना में बढ़ते जा रहे हैं जो कि एक गंभीर चिंता का विषय है ट्राई के अनुसार सितंबर 2025 में भारत में इंटरनेट का उपयोग करने वालों की संख्या 100 करोड़ को पार कर गयी थी। भारत सरकार को चाहिए कि साइबर अपराध को रोकने के लिए कड़े कदम उठाए जाएं, कानून

eISSN 3049-2610
Research Stream
A Bi-Annual, Open Access Pear Reviewed International Journal
Volume 03, Issue 01, March 2026

में यथा संभव संशोधन किया जाए, बड़े साइबर अपराधों के लिए कड़ी सजा का प्रावधान होना चाहिए। साइबर अपराधों की घटनाओं को कम करने के लिए सरकार को अखबारों एवं टीवी चैनलों के माध्यम से रोकने हेतु प्रचार–प्रसार करना चाहिए एवं इससे बचने के उपाय सुझाने चाहिए। विशेष कर युवा पीढ़ी को साइबर क्राइम के प्रति अधिक सतर्क रहने की जरूरत है क्योंकि अधिकांश युवा पीढ़ी अपना ज्यादातर समय मोबाइल या सोशल मीडिया पर व्यतीत कर रही है जिसके चलते उन्हें मानसिक अवसाद तक का सामना करना पड़ रहा है साथ ही कई बार वह गलत लिंक पर जाकर सर्च करने से साइबर क्राइम के शिकार हो जाते हैं। साथ ही बच्चों को उनके माता–पिता द्वारा पपजी जैसे गेमों से दूर रखना चाहिए तथा उन्हें गेम या मोबाइल की लत न लगे दें। साइबर अपराध भारत की डिजिटल प्रगति को बाधित कर रहे हैं, लेकिन मजबूत इच्छाशक्ति से इन्हें नियंत्रित किया जा सकता है। 2025 में जागरूकता और निवेश से नुकसान कम हो सकता है। भविष्य के शोध में तकनीकी विश्लेषण पर फोकस हो।

संदर्भ सूचीः–

1. सरवन, सुदीप, ''साइबर अपराध''(2020)
2. शर्मा, नरेंद्र कुमार, ''साइबर अपराधः चुनौतियाँ और प्रबंधन'' (2018)
3. पाठक, अरुण कुमार, साइबर क्राइम एंड साइबर लॉज (हिंदी)(2020), पुस्तक सदन प्रकाशन.
4. Gupta, Kanak, (2024), "Bible of Cyber Crimes in India".
5. Mishra, Manju, (2023) Cyber Security in India Callenges and Options.
6. Indian Express, (17 dec 2024) , "When Cyber Crimes Came to Closer Home".
7. जनसत्ता. (5 नवंबर 2025). ''भारत में बढ़ता साइबर अपराध और डिजिटल गिरफ्तारी घोटाला''.
8. दुबे, अमित, ''अदृश्य जालः साइबर क्राइम की सच्ची कहानिया'' (2022), रेख्ता बुक्स.
9. NDTV, (2 August 2025), "Digital froud, cybercriminals Stole Rs 23000 core from Indians in 2024".
10. India Today,(1 August 2025), "Cyber crimes in India Jump up Four Times".
11. NCRB Data, July 2025.
12. सूचना प्रौद्योगिकी अधिनियम, 2000.
13. National Cyber security Act ,2013
14. बीबीसी (7 सितंबर 2025) में ''डिजिटल अरेस्ट से लाखों डॉलर नुकसान''