July-
September 26

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

Vol - 2
Issue - 3

भारत में साइबर अपराधों की रोकथाम एवं नियंत्रण की विधिक व्यवस्था : एक विश्लेषण

भारती निरंजन
सहायक प्राध्यापिका
विधि विभाग
आर्यावर्त यूनिवर्सिटी, सीहोर (म.प्र.)

सारांश

सूचना एवं संचार प्रौद्योगिकी के तीव्र विकास ने मानव जीवन को अत्यधिक सुविधाजनक बनाया है। इंटरनेटए स्मार्टफोन डिजिटल बैंकिंगए ऑनलाइन खरीदारी सोशल मीडिया तथा डिजिटल सेवाओं के विस्तार ने आर्थिक एवं सामाजिक गतिविधियों को नई गति प्रदान की है। इसके साथ ही साइबर अपराधों के स्वरूप और संख्या में भी वृद्धि हुई है। साइबर अपराध ऐसे अपराध हैं जिनमें कंप्यूटर, मोबाइल, इंटरनेट, नेटवर्क या अन्य डिजिटल तकनीकों का उपयोग अपराध करने के साधन के रूप में किया जाता है अथवा डिजिटल प्रणाली स्वयं अपराध का लक्ष्य बनती है।

भारत में साइबर अपराधों की रोकथाम एवं नियंत्रण के लिए विभिन्न विधिक प्रावधान विकसित किए गए हैं। सूचना प्रौद्योगिकी अधिनियमए 2000 इस क्षेत्र का प्रमुख कानून है। इसके अतिरिक्त भारतीय न्याय संहिता 2023 भारतीय नागरिक सुरक्षा संहिताए 2023 तथा भारतीय साक्ष्य अधिनियमए 2023 में भी साइबर अपराधों से संबंधित परिस्थितियों में महत्वपूर्ण प्रावधान लागू होते हैं। डिजिटल साक्ष्य इलेक्ट्रॉनिक अभिलेख साइबर धोखाधड़ी पहचान की चोरी ऑनलाइन उत्पीड़न तथा अन्य डिजिटल अपराधों के मामलों में विधिक व्यवस्था की भूमिका महत्वपूर्ण हो जाती है।

प्रस्तुत शोधपत्र में भारत में साइबर अपराध की अवधारणा, प्रकृति, प्रमुख प्रकार, साइबर अपराधों के कारण उनके सामाजिक एवं आर्थिक प्रभाव तथा रोकथाम एवं नियंत्रण के लिए उपलब्ध विधिक व्यवस्था का विश्लेषण किया गया है। अध्ययन में साइबर अपराधों की जाँचए डिजिटल साक्ष्य न्यायिक प्रक्रिया तथा वर्तमान विधिक चुनौतियों पर भी चर्चा की गई है। अध्ययन से यह निष्कर्ष निकलता है कि साइबर अपराधों की प्रभावी रोकथाम के लिए केवल

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

कठोर कानून पर्याप्त नहीं हैं कानून के प्रभावी क्रियान्वयन साइबर पुलिसिंग डिजिटल साक्षरता तकनीकी क्षमता तथा नागरिक जागरूकता का समान रूप से विकास आवश्यक है।

प्रमुख शब्द

साइबर अपराध, सूचना प्रौद्योगिकी अधिनियम, डिजिटल साक्ष्य, साइबर सुरक्षा, साइबर कानून, ऑनलाइन धोखाधड़ी, विधिक व्यवस्था।

1. प्रस्तावना

वर्तमान युग को सूचना एवं प्रौद्योगिकी का युग कहा जाता है। इंटरनेट एवं डिजिटल तकनीक ने संचारए शिक्षाए व्यापारए बैंकिंगए प्रशासन तथा मनोरंजन के क्षेत्र में व्यापक परिवर्तन किया है। आज व्यक्ति अपने मोबाइल फोन के माध्यम से बैंकिंगए खरीदारीए शिक्षा एवं अनेक सरकारी सेवाओं का उपयोग कर सकता है। डिजिटल तकनीक ने जहाँ जीवन को सरल बनाया हैए वहीं इसके दुरुपयोग से नए प्रकार के अपराध भी उत्पन्न हुए हैं। पारंपरिक अपराधों की तुलना में साइबर अपराधों की प्रकृति अलग है। इनमें अपराधी अक्सर दूर बैठे हुए डिजिटल माध्यम से किसी व्यक्तिए संस्था या सरकारी प्रणाली को नुकसान पहुँचा सकता है।

साइबर अपराध की सबसे बड़ी विशेषता इसकी सीमा.विहीन प्रकृति है। अपराधी एक देश में रहते हुए दूसरे देश में स्थित व्यक्ति या संस्था को निशाना बना सकता है। इससे अपराध की जाँच और अपराधी की पहचान करना चुनौतीपूर्ण हो जाता है। भारत में डिजिटल लेन.देन तथा इंटरनेट उपयोगकर्ताओं की संख्या बढ़ने के साथ साइबर अपराधों की रोकथाम और नियंत्रण एक महत्वपूर्ण विधिक एवं सामाजिक विषय बन गया है। इसलिए प्रभावी कानून तथा उसके उचित क्रियान्वयन की आवश्यकता है।

2. साइबर अपराध का अर्थ एवं अवधारणा

साइबर अपराध से आशय ऐसे अपराध से है जिसमें कंप्यूटर मोबाइल इंटरनेटनेटवर्क या डिजिटल तकनीक का उपयोग अपराध करने के लिए किया जाता है।

सामान्य रूप से साइबर अपराध को दो प्रमुख रूपों में समझा जा सकता है -

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

- कंप्यूटर या डिजिटल प्रणाली को लक्ष्य बनाकर किया गया अपराध।
- कंप्यूटर या इंटरनेट को अपराध करने के साधन के रूप में उपयोग करने वाला अपराध।

उदाहरण के रूप में किसी कंप्यूटर नेटवर्क को है करना डिजिटल डेटा चोरी करना किसी व्यक्ति की ऑनलाइन पहचान का दुरुपयोग करना फिशिंग के माध्यम से बैंकिंग जानकारी प्राप्त करना या ऑनलाइन धोखाधड़ी करना साइबर अपराध की श्रेणी में आ सकते हैं।

3. साइबर अपराध की प्रमुख विशेषताएँ

साइबर अपराध की प्रमुख विशेषताएँ निम्नलिखित हैं

- साइबर अपराध में अपराधी और पीड़ित अलग.अलग देशों में हो सकते हैं।
- अपराधी अपनी वास्तविक पहचान छिपाने के लिए विभिन्न डिजिटल तकनीकों का प्रयोग कर सकता है।
- साइबर अपराधों की जाँच के लिए विशेष तकनीकी ज्ञान आवश्यक होता है।
- डिजिटल माध्यम से अपराध बहुत कम समय में किया जा सकता है।
- एक साइबर हमला हजारों या लाखों लोगों को प्रभावित कर सकता है।
- डिजिटल साक्ष्य पर निर्भरता
- ऐसे मामलों में डिजिटल रिकॉर्ड महत्वपूर्ण साक्ष्य बन सकते हैं।

aryavart
Journal of Multidisciplinary Research

4. भारत में साइबर अपराधों के प्रमुख प्रकार

भारत में विभिन्न प्रकार के साइबर अपराध सामने आते हैं।

4.1 हैकिंग

बिना अनुमति किसी कंप्यूटरए नेटवर्क या डिजिटल प्रणाली तक पहुँच प्राप्त करना हैकिंग कहलाता है।

4.2 फिशिंग

फर्जी ई.मेलए संदेश या वेबसाइट के माध्यम से व्यक्ति से गोपनीय जानकारी प्राप्त करने का प्रयास फिशिंग कहलाता है।

4.3 पहचान की चोरी

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

किसी व्यक्ति की व्यक्तिगत या डिजिटल पहचान संबंधी जानकारी का अनधिकृत उपयोग पहचान की चोरी के अंतर्गत आता है।

4.4 ऑनलाइन वित्तीय धोखाधड़ी

फर्जी लिंक बैंकिंग संदेश या अन्य डिजिटल माध्यमों से धन की धोखाधड़ी करना एक गंभीर साइबर अपराध है।

4.5 साइबर स्टॉकिंग

इंटरनेट एवं डिजिटल माध्यमों से किसी व्यक्ति का लगातार पीछा करनाए निगरानी करना या परेशान करना साइबर स्टॉकिंग से संबंधित हो सकता है।

4.6 साइबर बुलिंग

सोशल मीडिया या डिजिटल माध्यमों से किसी व्यक्ति को धमकाना अपमानित करना या परेशान करना साइबर बुलिंग कहलाता है। ऐसे साइबर हमले जिनमें डिजिटल डेटा या सिस्टम को बाधित करके धन की मांग की जाती हैए रैनसमवेयर हमलों के रूप में जाने जाते हैं।

4.8 साइबर मानहानि

डिजिटल माध्यमों से किसी व्यक्ति की प्रतिष्ठा को नुकसान पहुँचाने वाली सामग्री का प्रसार भी कानूनी विवाद का कारण बन सकता है।

5. साइबर अपराध के प्रमुख कारण

साइबर अपराधों के बढ़ने के कई कारण हैं

- इंटरनेट का तेजी से विस्तार।
- डिजिटल भुगतान का बढ़ता उपयोग।
- साइबर सुरक्षा के प्रति कम जागरूकता।
- तकनीकी ज्ञान का दुरुपयोग।
- कमजोर पासवर्ड एवं सुरक्षा व्यवस्था।
- सोशल मीडिया का असावधानीपूर्वक उपयोग।
- व्यक्तिगत जानकारी का अनियंत्रित डिजिटल साझा करना।
- बेरोजगारी एवं आर्थिक लाभ की लालसा।

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

- अंतरराष्ट्रीय साइबर अपराध नेटवर्क।
- कानून प्रवर्तन एजेंसियों के सामने तकनीकी चुनौतियाँ।

6. साइबर अपराध का सामाजिक प्रभाव

साइबर अपराध का प्रभाव केवल आर्थिक नुकसान तक सीमित नहीं है। इसके कारण व्यक्ति की निजताए प्रतिष्ठा और मानसिक शांति प्रभावित हो सकती है।साइबर बुलिंग और ऑनलाइन उत्पीड़न विशेष रूप से युवाओं को प्रभावित कर सकते हैं। निजी तस्वीरों या जानकारी का दुरुपयोग व्यक्ति के सामाजिक जीवन पर गंभीर प्रभाव डाल सकता है। इसलिए साइबर अपराध को केवल तकनीकी समस्या नहीं बल्कि सामाजिक एवं विधिक समस्या के रूप में भी देखना आवश्यक है।

7. साइबर अपराध का आर्थिक प्रभाव

साइबर अपराधों से व्यक्तियोंए बैंकोंए कंपनियों तथा सरकारी संस्थाओं को आर्थिक नुकसान हो सकता है। ऑनलाइन बैंकिंग एवं डिजिटल भुगतान के बढ़ते उपयोग के कारण वित्तीय धोखाधड़ी का खतरा भी बढ़ा है। व्यवसायों के लिए साइबर हमले के कारण डेटा हानिए सेवा बाधित होने तथा प्रतिष्ठा को नुकसान जैसी समस्याएँ उत्पन्न हो सकती हैं। इसलिए साइबर सुरक्षा अब व्यवसाय एवं वित्तीय व्यवस्था का महत्वपूर्ण हिस्सा बन चुकी है।

8. भारत में साइबर अपराध संबंधी विधिक व्यवस्था

भारत में साइबर अपराधों के नियंत्रण के लिए प्रमुख कानूनों एवं विधिक प्रावधानों का विकास किया गया है।

8.1 सूचना प्रौद्योगिकी अधिनियमए 2000

भारत में साइबर कानून की आधारभूत व्यवस्था सूचना प्रौद्योगिकी अधिनियमए 2000 से संबंधित है। इस कानून का उद्देश्य इलेक्ट्रॉनिक रिकॉर्ड एवं इलेक्ट्रॉनिक संचार को कानूनी

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

मान्यता देना तथा कंप्यूटर संसाधनों से संबंधित विभिन्न अपराधों के लिए विधिक व्यवस्था प्रदान करना है।

इस अधिनियम में कंप्यूटर संसाधनों के अनधिकृत उपयोगए पहचान की चोरीए कंप्यूटर संबंधी धोखाधड़ी तथा अन्य साइबर गतिविधियों से संबंधित प्रावधान मौजूद हैं।

9. सूचना प्रौद्योगिकी अधिनियम की महत्वपूर्ण धाराएँ

साइबर अपराध के अध्ययन में अधिनियम की विभिन्न धाराएँ महत्वपूर्ण हैं।

धारा 43

कंप्यूटर या कंप्यूटर प्रणाली को बिना अनुमति नुकसान पहुँचाने या अनधिकृत रूप से संबंधित गतिविधियों के लिए क्षतिपूर्ति संबंधी प्रावधान से संबंधित है।

धारा 65

कंप्यूटर स्रोत दस्तावेज से संबंधित छेड़छाड़ को अपराध के रूप में संबोधित करती है।

धारा 66

कंप्यूटर संबंधी अपराधों से संबंधित प्रावधान प्रदान करती है।

धारा 66

पहचान की चोरी से संबंधित अपराधों को संबोधित करती है।

धारा 66

कंप्यूटर संसाधन या संचार उपकरण का उपयोग करके प्रतिरूपण द्वारा धोखाधड़ी से संबंधित है।

धारा 66

निजता के उल्लंघन से संबंधित अपराध को संबोधित करती है।

धारा 67

इलेक्ट्रॉनिक रूप में अश्लील सामग्री के प्रकाशन या प्रसारण से संबंधित अपराधों के संबंध में प्रावधान करती है।

महत्वपूर्ण सूचना प्रौद्योगिकी अधिनियम की धारा 66। को सर्वोच्च न्यायालय ने 2015 में निरस्त कर दिया थाए इसलिए इसे वर्तमान लागू प्रावधान के रूप में नहीं माना जाना चाहिए।

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

10. भारतीय न्याय संहिताए 2023 एवं साइबर अपराध

भारतीय न्याय संहिताए 2023 ने भारतीय दंड संहिताए 1860 का स्थान लिया है। साइबर अपराधों के अनेक मामलों मेंए अपराध की प्रकृति के अनुसार सामान्य आपराधिक प्रावधान भी लागू हो सकते हैं। उदाहरण के लिए धोखाधड़ीए जालसाजीए धमकीए मानहानि तथा अन्य अपराध यदि डिजिटल माध्यम से किए जाते हैं तो मामले की परिस्थितियों के आधार पर संबंधित दंडात्मक प्रावधान लागू हो सकते हैं। इस प्रकार साइबर अपराधों के नियंत्रण के लिए केवल सूचना प्रौद्योगिकी अधिनियम पर निर्भर रहना पर्याप्त नहीं हैय अपराध की प्रकृति के अनुसार अन्य आपराधिक कानून भी महत्वपूर्ण हैं।

11. भारतीय नागरिक सुरक्षा संहिता 2023 की भूमिका

भारतीय नागरिक सुरक्षा संहिताए 2023 ने आपराधिक प्रक्रिया से संबंधित विधिक ढाँचे को पुनर्गठित किया है। साइबर अपराधों की जाँच में -

- शिकायत दर्ज करना
- जाँच
- तलाशी
- जब्ती
- डिजिटल उपकरणों की जाँचए
- अभियोजन

जैसी प्रक्रियाएँ महत्वपूर्ण होती हैं। साइबर अपराधों में डिजिटल साक्ष्यों को सुरक्षित रखना एवं उनकी विश्वसनीयता बनाए रखना न्यायिक प्रक्रिया के लिए अत्यंत आवश्यक है।

12. भारतीय साक्ष्य अधिनियम 2023 एवं इलेक्ट्रॉनिक साक्ष्य

साइबर अपराध मामलों में इलेक्ट्रॉनिक एवं डिजिटल साक्ष्य का विशेष महत्व है। ई.मेल चैटडिजिटल दस्तावेजए कंप्यूटर रिकॉर्ड मोबाइल डेटा रिकॉर्डिंग एवं अन्य इलेक्ट्रॉनिक सामग्री किसी मामले में महत्वपूर्ण साक्ष्य बन सकती है। भारतीय साक्ष्य अधिनियमए 2023 ने साक्ष्य संबंधी विधिक व्यवस्था को नए कानून के रूप में व्यवस्थित किया है। डिजिटल एवं इलेक्ट्रॉनिक

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

रिकॉर्ड की स्वीकार्यता और प्रमाणिकता के संबंध में निर्धारित विधिक आवश्यकताओं का पालन करना महत्वपूर्ण है।

13. साइबर अपराध की जाँच में डिजिटल साक्ष्य

साइबर अपराध की जाँच में डिजिटल साक्ष्य महत्वपूर्ण भूमिका निभाते हैं।

डिजिटल साक्ष्य में शामिल हो सकते हैं

- मोबाइल फोन का डेटा
- कंप्यूटर रिकॉर्ड
- ई.मेल
- चैट रिकॉर्ड
- सर्वर लॉग
- फुटेज
- डिजिटल भुगतान रिकॉर्ड
- इलेक्ट्रॉनिक दस्तावेज

डिजिटल साक्ष्य के साथ छेड़छाड़ न होए इसके लिए उचित संरक्षण एवं दस्तावेजीकरण आवश्यक है।

14. साइबर अपराधों की रोकथाम में संस्थागत व्यवस्था

भारत में साइबर अपराधों की रोकथाम के लिए विभिन्न सरकारी एवं संस्थागत प्रयास किए जा रहे हैं। साइबर अपराध की शिकायतोंए साइबर सुरक्षा तथा डिजिटल जागरूकता के लिए विभिन्न संस्थागत व्यवस्थाएँ विकसित की गई हैं। साइबर अपराध के मामलों में पुलिसए साइबर सेलए डिजिटल फॉरेंसिक विशेषज्ञए बैंकिंग संस्थाएँ तथा अन्य संबंधित एजेंसियाँ अपनी.अपनी भूमिका निभाती हैं। प्रभावी साइबर अपराध नियंत्रण के लिए इन सभी संस्थाओं के बीच समन्वय आवश्यक है।

15. साइबर अपराधों की रोकथाम में नागरिकों की भूमिका

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

कानून के साथ नागरिक जागरूकता भी साइबर अपराध नियंत्रण का महत्वपूर्ण माध्यम है।

- किसी के साथ साझा नहीं करना चाहिए।
- संदिग्ध लिंक पर क्लिक नहीं करना चाहिए।
- मजबूत पासवर्ड का उपयोग करना चाहिए।
- बैंकिंग जानकारी सुरक्षित रखनी चाहिए।
- सोशल मीडिया पर निजी जानकारी सीमित रखनी चाहिए।
- संदिग्ध गतिविधि की तुरंत शिकायत करनी चाहिए।
- डिजिटल उपकरणों को नियमित रूप से अपडेट करना चाहिए।
- दोस्तरीय प्रमाणीकरण जैसी सुरक्षा सुविधाओं का उपयोग करना चाहिए।

16. साइबर अपराधों के नियंत्रण में प्रमुख चुनौतियाँ

साइबर अपराधों के प्रभावी नियंत्रण में कई चुनौतियाँ हैं -

16.1 तकनीकी जटिलता

अपराधी नई तकनीकों का प्रयोग करते रहते हैं।

16.2 अंतरराष्ट्रीय सीमा

अपराधी और पीड़ित अलग अलग देशों में हो सकते हैं।

16.3 डिजिटल साक्ष्य की सुरक्षा

डिजिटल साक्ष्य आसानी से बदले या नष्ट किए जा सकते हैं।

16.4 विशेषज्ञों की आवश्यकता

साइबर अपराध की जाँच के लिए प्रशिक्षित तकनीकी विशेष आवश्यक हैं।

16.5 तेजी से बदलती तकनीक

कानून एवं जाँच व्यवस्था को तकनीकी परिवर्तन के साथ अद्यतन करना आवश्यक है।

17. न्यायिक दृष्टिकोण

भारतीय न्यायपालिका ने डिजिटल युग में निजताए अभिव्यक्ति की स्वतंत्रता और इंटरनेट से जुड़े अधिकारों पर महत्वपूर्ण निर्णय दिए हैं। साइबर अपराध संबंधी मामलों में न्यायालयों के

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

सामने डिजिटल साक्ष्य की विश्वसनीयताए निजताए स्वतंत्रता तथा कानून के उचित प्रयोग जैसे प्रश्न महत्वपूर्ण बने हुए हैं।

18. साइबर अपराध और निजता का अधिकार

डिजिटल युग में व्यक्ति की निजी जानकारी अत्यंत मूल्यवान हो गई है। मोबाइल नंबरए बैंकिंग जानकारीए पहचान संबंधी जानकारीए फोटोए लोकेशन एवं अन्य व्यक्तिगत डेटा का दुरुपयोग व्यक्ति की निजता को प्रभावित कर सकता है। भारत के संवैधानिक कानून में निजता के अधिकार को महत्वपूर्ण स्थान प्राप्त है। इसलिए साइबर अपराधों की रोकथाम करते समय अपराध नियंत्रण के साथ नागरिकों के मौलिक अधिकारों की रक्षा भी आवश्यक है।

19. साइबर अपराध नियंत्रण के लिए सुझाव

अध्ययन के आधार पर निम्नलिखित सुझाव दिए जा सकते हैं

- साइबर कानूनों के प्रभावी क्रियान्वयन को मजबूत किया जाना चाहिए।
- साइबर पुलिस एवं जाँच अधिकारियों को नियमित प्रशिक्षण दिया जाना चाहिए।
- डिजिटल फॉरेंसिक सुविधाओं का विस्तार किया जाना चाहिए।
- नागरिकों के लिए साइबर जागरूकता कार्यक्रम बढ़ाए जाने चाहिए।
- स्कूल एवं महाविद्यालय स्तर पर साइबर सुरक्षा शिक्षा को बढ़ावा दिया जाना चाहिए।
- बैंकिंग संस्थाओं को सुरक्षित डिजिटल लेन.देन के लिए जागरूकता बढ़ानी चाहिए।
- साइबर अपराधों की शिकायत दर्ज करने की प्रक्रिया सरल बनाई जानी चाहिए।
- अंतरराष्ट्रीय साइबर अपराधों के मामलों में अंतरराष्ट्रीय सहयोग मजबूत किया जाना चाहिए।
- डिजिटल साक्ष्य के संरक्षण की वैज्ञानिक व्यवस्था विकसित की जानी चाहिए।
- कानून एवं तकनीकी व्यवस्था को समय.समय पर अद्यतन किया जाना चाहिए।

20. प्रमुख निष्कर्ष

अध्ययन से निम्नलिखित प्रमुख निष्कर्ष प्राप्त होते हैं -

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

- साइबर अपराध आधुनिक तकनीकी समाज की गंभीर चुनौती है।
- भारत में डिजिटल तकनीक के विस्तार के साथ साइबर सुरक्षा का महत्व बढ़ा है।
- सूचना प्रौद्योगिकी अधिनियम 2000 साइबर कानून की प्रमुख आधारभूत व्यवस्था है।
- साइबर अपराधों के अनेक मामलों में सामान्य आपराधिक कानून भी लागू हो सकते हैं।
- डिजिटल साक्ष्य साइबर अपराधों की जाँच एवं न्यायिक प्रक्रिया में महत्वपूर्ण हैं।
- साइबर अपराधों की सीमाविहीन प्रकृति जाँच एजेंसियों के सामने चुनौती उत्पन्न करती है।
- साइबर पुलिस एवं डिजिटल फॉरेंसिक क्षमता को और मजबूत करने की आवश्यकता है।
- नागरिक जागरूकता साइबर अपराध रोकथाम का महत्वपूर्ण साधन है।
- साइबर अपराध नियंत्रण में कानूनए तकनीक और प्रशासन के बीच समन्वय आवश्यक है।
- साइबर अपराधों से निपटने के लिए विधिक व्यवस्था को तकनीकी परिवर्तन के साथ लगातार विकसित करना आवश्यक है।

21. निष्कर्ष

भारत में साइबर अपराधों का स्वरूप लगातार बदल रहा है। डिजिटल तकनीक ने आर्थिक एवं सामाजिक विकास को गति प्रदान की हैए लेकिन इसके साथ साइबर अपराधों की नई चुनौतियाँ भी सामने आई हैं। भारत में सूचना प्रौद्योगिकी अधिनियम 2000 साइबर अपराधों के नियंत्रण का महत्वपूर्ण आधार है। इसके साथ भारतीय न्याय संहिता 2023ए भारतीय नागरिक सुरक्षा संहिताए 2023 तथा भारतीय साक्ष्य अधिनियम 2023 जैसी विधिक व्यवस्थाएँ भी साइबर अपराध से जुड़े मामलों में महत्वपूर्ण भूमिका निभाती हैं।

हालाँकि केवल कानून बना देना पर्याप्त नहीं है। कानून का प्रभावी क्रियान्वयन प्रशिक्षित साइबर पुलिसए आधुनिक डिजिटल फॉरेंसिक सुविधाएँ न्यायिक क्षमताए संस्थागत समन्वय तथा नागरिक जागरूकता समान रूप से आवश्यक हैं। साइबर अपराधों की सीमा विहीन प्रकृति को देखते हुए अंतरराष्ट्रीय सहयोग भी आवश्यक है। भविष्य में कृत्रिम बुद्धिमत्ता एवं अन्य उन्नत

तकनीकों के बढ़ते उपयोग के साथ साइबर अपराध के नए रूप सामने आ सकते हैं। इसलिए भारत को अपनी विधिक एवं तकनीकी व्यवस्था को निरंतर अद्यतन करते रहना होगा।

अंततः यह कहा जा सकता है कि साइबर अपराधों की प्रभावी रोकथाम एवं नियंत्रण के लिए मजबूत कानूनए सक्षम प्रवर्तन तंत्रए आधुनिक तकनीक और जागरूक नागरिक इन चारों का समन्वित प्रयास आवश्यक है।

संदर्भ सूची

1. सूचना प्रौद्योगिकी अधिनियम 2000
2. भारतीय न्याय संहिता 2023
3. भारतीय नागरिक सुरक्षा संहिता 2023
4. भारतीय साक्ष्य अधिनियम 2023
5. साइबर कानून एवं साइबर अपराध से संबंधित मानक विधिक पुस्तकें।
6. साइबर अपराध एवं डिजिटल साक्ष्य से संबंधित शोध.पत्र।
7. सूचना प्रौद्योगिकी एवं साइबर सुरक्षा से संबंधित अकादमिक जर्नल।
8. भारत में साइबर सुरक्षा एवं डिजिटल अपराध से संबंधित सरकारी रिपोर्ट।
9. साइबर अपराध की रोकथाम एवं डिजिटल जागरूकता से संबंधित प्रकाशित सामग्री।
10. साइबर कानून एवं सूचना प्रौद्योगिकी से संबंधित न्यायिक निर्णय।
11. विधि एवं अपराधशास्त्र से संबंधित शोध साहित्य।
12. डिजिटल साक्ष्य एवं साइबर फॉरेंसिक से संबंधित अकादमिक अध्ययन।
13. साइबर सुरक्षा एवं डिजिटल शासन से संबंधित प्रकाशित शोध सामग्री।