SHODH SAMAGAM

ISSN : 2581-6918 (Online), 2582-1792 (PRINT)

भारत में साइबर अपराधः आधुनिक परिपेक्ष्य में अलोचनात्मक मूल्यांकन

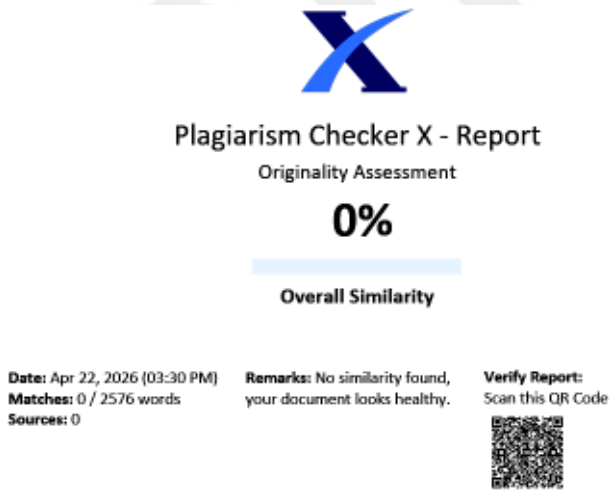
भूपेंद्र करवन्दे, पीएच–डी, विधि विभाग, **नेहा साहू,** एलएल.एम.–भाग–2 (द्वितीय सेमेस्टर)
शा. जे. योगानंदम छत्तीसगढ़ महाविद्यालय, रायपुर, छत्तीसढ़, भारत

ORIGINAL ARTICLE

Authors
भूपेंद्र करवन्दे
नेहा साहू
E-mail : 1983abk@gmail.com

shodhsamagam1@gmail.com

Received on : 20/02/2026
Revised on : 21/04/2026
Accepted on : 30/04/2026
Overall Similarity : 00% on 22/04/2026



शोध सार

साइबर क्राइम का मतलब है ऐसे क्रिमिनल जुर्म जो इंटरनेट या किसी दूसरे कंप्यूटर नेटवर्क का इस्तेमाल करके किए जाते हैं। साइबर क्राइम इंटरनेट और कंप्यूटर का इस्तेमाल करके किसी व्यक्ति की पहचान चुराने या गैर–कानूनी तरीके से प्रोग्राम इंपोर्ट करने या खराब प्रोग्राम को इंपोर्ट करने के लिए किए जाते हैं। आधुनिक समय मे साइबर क्राइम काफी हद तक बढ़ता जा रहा है, साइबर क्राइम हर व्यक्ति के लिए बहुत नुकसानदायक है, क्योंकि इसमें सीधे तौर पर उसके पर्सनल डेटा की चोरी शामिल होती है जिससे समाज में उसकी इज्ज़त को नुकसान पहुँच सकता है, साइबर क्राइम का हमारे समाज और इकॉनमी और बिज़नेस पर बहुत बुरा असर पड़ता है। यह पूरे विश्व में एक बहुत बड़ी समस्या है जो बहुत तेजी से बढ़ रही है। साइबर अपराध के विभिन्न रूप हमारे समाज को प्रभावित कर रहे हैं जिसका उदाहरण साइबर पोर्नोग्राफी, साइबर आतंकवाद, साइबर बदमाशी, बच्चों का शोषण और बच्चों की तस्करी, साइबर उत्पीड़न, वित्तीय अपराध, ऑनलाइन जुआ, जालसाजी, साइबर मानहानि, साइबर स्टॉकिंग, ईमेल स्पूफिंग, ईमेल आदि हैं। ये अपराध न केवल किसी व्यक्ति को आर्थिक रूप से प्रभावित करते हैं बल्कि यह उस व्यक्ति को मानसिक रूप से भी प्रभावित करते हैं, जैसे महिलाओं की तस्वीरों को इंटरनेट पर साझा करके महिलाओं की गरिमा को ठेस पहुंचाना और यह आजकल किसी भी किशोर के मानसिक स्वास्थ्य के लिए बहुत हानिकारक है। यह विकास में बाधा डालता है, क्योंकि कई किशोर इस साइबर जाल में फंस जाते हैं और आत्महत्या या अन्य अवैध प्रकार के कृत्य करके अपना जीवन समाप्त कर रहे हैं।

मुख्य शब्द

साइबर, अपराध, हैकिंग, साइबर मानहानि, साइबर कानून, आई टी अधिनियम 2000.

परिचय

प्रकृति ने मनुष्य को अन्य प्राणियों की तुलना में बेहतर सोचने और समझने की क्षमता और बुद्धि प्रदान की है, जो उसे

अन्य प्राणियों से अलग करती है और ब्रह्मांड में अन्य प्राणियों से श्रेष्ठ बनाती है। मानव सभ्यता की प्रगति ने जीवन रक्षा की आवश्यकता से लेकर आधुनिक जीवन की विलासिता तक, विभिन्न विचारों, खोजों और आविष्कारों को जन्म दिया है साइबर अपराध से तात्पर्य कंप्यूटर, नेटवर्क या डिजिटल तकनीकों का उपयोग करके की जाने वाली आपराधिक गतिविधियों से है। इन अपराधों में कई प्रकार की अवैध गतिविधियाँ शामिल हैं, जैसे हैकिंग, पहचान की चोरी, फ़िशिंग, मैलवेयर का प्रसार, ऑनलाइन धोखाधड़ी, साइबरबुलिंग आदि। डिजिटल तकनीकों पर बढ़ती निर्भरता के साथ, साइबर अपराध दुनिया भर में व्यक्तियों, व्यवसायों और सरकारों के लिए गंभीर खतरा पैदा करता है, जिसके परिणामस्वरूप अक्सर वित्तीय नुकसान, डेटा लीक और प्रतिष्ठा को क्षति पहुँचती है। साइबर अपराध से निपटने के प्रयासों में साइबर सुरक्षा उपाय, कानून, कानून प्रवर्तन और अंतर्राष्ट्रीय सहयोग शामिल हैं। साइबर अपराध एक सामान्य शब्द है जो कंप्यूटर, नेटवर्क या किसी अन्य डिजिटल उपकरण का उपयोग करके की जाने वाली असंख्य आपराधिक गतिविधियों का वर्णन करता है। साइबर अपराध साइबर अपराधियों द्वारा किया गया एक अवैध हिंसक अपराध है। इनमें हैकिंग, फ़िशिंग, पहचान की चोरी, रैंसमवेयर और मैलवेयर हमले आदि शामिल हैं। इस अपराध का ढांचा पूरी दुनिया में फैला हुआ है। साइबर अपराध व्यक्तियों, व्यवसायों और सरकारी संस्थाओं के लिए एक गंभीर खतरा है और इसके परिणामस्वरूप भारी वित्तीय नुकसान, प्रतिष्ठा को क्षति और रिकॉर्ड का उल्लंघन हो सकता है। इंटरनेट के आगमन के साथ ही अपराधों की एक नई पीढ़ी सामने आई है, जिनमें सॉफ्टवेयर पायरेसी, इंटरनेट पर बाल यौन शोषण, औद्योगिक जासूसी, पासवर्ड क्रैकिंग, स्पूफिंग, दूरसंचार धोखाधड़ी, ईमेल बॉम्बिंग, स्पैमिंग, अश्लील सामग्री और अवैध या बिना लाइसेंस वाले उत्पाद और सेवाएं शामिल हैं। सॉफ्टवेयर पायरेसी तेजी से बढ़ता हुआ व्यवसाय बन गया है, जिससे कई प्रकार के बेहद खतरनाक अपराध जन्म ले रहे हैं, इंटरनेट पर महिलाओं की तस्वीरें अपलोड करना आजकल किशोरों के मानसिक स्वास्थ्य के लिए बेहद हानिकारक है। यह उनके विकास में बाधा डालता है, क्योंकि कई किशोर इस साइबर जाल में फंसकर आत्महत्या या किसी अन्य अवैध कृत्य के जरिए अपनी जान गंवा रहे हैं। अवैध रूप से पैसा कमाने के लिए साइबर अपराध दुनिया भर में तेजी से बढ़ रहे हैं। सर्वेक्षणों के आंकड़ों से पता चलता है कि साइबर अपराध दुनिया भर में खतरनाक दर से बढ़ रहा है। साइबर अपराध किसी भी सीमा या भौगोलिक बाधा का सम्मान नहीं करते। साइबर जगत को सुरक्षित बनाना सभी हितधारकों के लिए एक प्रमुख चिंता का विषय है। इस संबंध में, प्रत्येक देश अपने देश में साइबर अपराधों को नियंत्रित करने के लिए अपना साइबर कानून या इंटरनेट कानून बनाएगा। भारत सरकार ने सूचना प्रौद्योगिकी अधिनियम, 2000 नामक एक कानून भी बनाया, जिसका उद्देश्य इलेक्ट्रॉनिक माध्यमों से किए गए लेन–देन को कानूनी मान्यता देना है।

भारत में साइबर अपराध का इतिहास

1. **प्रारंभिक दौर (1990)**: भारत में इंटरनेट की शुरुआत 1995 में हुई (VSNL द्वारा)। इसी समय से ईमेल धोखाधड़ी, हैकिंग जैसे शुरुआती साइबर अपराध सामने आने लगे।
2. **सूचना प्रौद्योगिकी अधिनियम, 2000**: साइबर अपराधों को नियंत्रित करने के लिए भारत सरकार ने IT Act, 2000 लागू किया। यह भारत का पहला प्रमुख साइबर कानून था, जिसमें हैकिंग, डेटा चोरी आदि को अपराध घोषित किया गया।
3. **संशोधन (2008)**: तकनीकी विकास और नए अपराधों को देखते हुए IT Act में 2008 में संशोधन किया गया। इसमें साइबर आतंकवाद, पहचान की चोरी (Identity Theft), और ऑनलाइन धोखाधड़ी जैसे अपराधों को शामिल किया गया।
4. **वर्तमान स्थिति**: आज सोशल मीडिया, ऑनलाइन बैंकिंग और ई–कॉमर्स के बढ़ने से साइबर अपराध (जैसे फिशिंग, साइबर ठगी, मानहानि) तेजी से बढ़ रहे हैं। सरकार और न्यायालय समय–समय पर नए नियम और दिशानिर्देश जारी करते हैं (जैसे IT Rules 2021)।

भारत में साइबर अपराध का इतिहास इंटरनेट के विकास के साथ जुड़ा हुआ है, और इसे नियंत्रित करने के लिए कानून लगातार विकसित होते रहे हैं।

साइबर अपराध के उद्देश्य

साइबर अपराध के उद्देश्य व्यापक रूप से भिन्न हो सकते हैं, लेकिन इनमें अक्सर वित्तीय लाभ, जासूसी, तोड़फोड़, सेवाओं में बाधा, संवेदनशील जानकारी की चोरी, पहचान की चोरी, मैलवेयर या वायरस फैलाना और कभी–कभी वैचारिक कारणों से अराजकता या नुकसान पहुंचाना शामिल होता है। साइबर अपराध के उद्देश्य व्यापक रूप से भिन्न हो सकते हैं, लेकिन कुछ सामान्य लक्ष्यों में वित्तीय लाभ, डेटा चोरी, तोड़फोड़, जासूसी, सेवाओं में बाधा और यहां तक कि राजनीतिक या वैचारिक

मकसद भी शामिल हैं। साइबर अपराध इंटरनेट उपयोगकर्ताओं को नुकसान पहुंचाने के उद्देश्य से किए जाते हैं।

भारत में साइबर कानून का दायरा

पहचान की चोरी, धोखाधड़ी और फ़िशिंग साइबर अपराध के ऐसे उदाहरण हैं जिनमें हाल के वर्षों में नाटकीय रूप से वृद्धि हुई है फिर भी, वर्तमान कानूनों के तहत इनका दायरा न तो पर्याप्त है और न ही व्यापक। इसके अलावा, भारत में साइबर अपराध की पैठ और भी अधिक बढ़ने की आशंका है। यह साइबर अपराध के खिलाफ सख्त नियम बनाने के साथ–साथ अधिक प्रभावी और निवारक कानूनी ढांचे के निर्माण के महत्व को उजागर करता है। साइबर अपराध का दायरा बहुत व्यापक है, जो व्यक्ति से लेकर पूरे समाज और राष्ट्र की सुरक्षा तक को प्रभावित करता है।

भारत में साइबर अपराध के प्रकार

साइबर अपराध वे अपराध हैं जो कंप्यूटर, इंटरनेट या डिजिटल माध्यम से किए जाते हैं। इनके प्रमुख प्रकार निम्नलिखित हैं:

1. **हैकिंग:** अनधिकृत रूप से किसी कंप्यूटर सिस्टम या नेटवर्क में प्रवेश कर डेटा चुराना या नुकसान पहुँचाना।
2. **पहचान की चोरी:** किसी व्यक्ति की निजी जानकारी (जैसे आधार, बैंक डिटेल) का दुरुपयोग कर धोखाधड़ी करना।
3. **साइबर ठगी:** फर्जी ईमेल, वेबसाइट या मैसेज के माध्यम से लोगों से पैसे या संवेदनशील जानकारी प्राप्त करना।
4. **साइबर मानहानि:** इंटरनेट पर किसी व्यक्ति की झूठी या अपमानजनक जानकारी फैलाकर उसकी प्रतिष्ठा को नुकसान पहुँचाना।
5. **साइबर स्टॉकिंग:** ऑनलाइन माध्यम से किसी व्यक्ति का लगातार पीछा करना, धमकाना या परेशान करना
6. **साइबर आतंकवाद:** सरकारी या महत्वपूर्ण सिस्टम (जैसे बैंक, रक्षा) पर हमला कर देश की सुरक्षा को खतरा पहुँचाना।
7. **अश्लील/आपत्तिजनक सामग्री का प्रसार:** इंटरनेट पर अश्लील सामग्री, बाल पोर्नोग्राफी या अवैध कंटेंट का प्रकाशन/वितरण।

साइबर अपराध के प्रकार बहुत विविध हैं और तकनीकी विकास के साथ लगातार बढ़ रहे हैं, इसलिए इनके नियंत्रण के लिए सख्त कानून और जागरूकता आवश्यक है।

साइबर अपराध का वर्गीकरण

- साइबर अपराध जिनमें कंप्यूटर को लक्ष्य के रूप में इस्तेमाल किया जाता है।
- साइबर अपराध जिनमें कंप्यूटर अपराध को अंजाम देने का साधन होता है।
- साइबर अपराध जिनमें कंप्यूटर अन्य अपराधों के लिए एक आकस्मिक भूमिका निभाता है।

साइबर अपराध का सामान्य वर्गीकरण

साइबर अपराध का सामान्य वर्गीकरण आमतौर पर अपराधों को तीन मुख्य श्रेणियों में विभाजित करता है:

- **व्यक्तियों के विरुद्ध साइबर अपराध:** पहचान की गई चोरी, ऑनलाइन उत्पीड़न, साइबर–धमकी, सेक्सटॉर्शन, व्यक्तियों को निशाना बनाने वाले वित्तीय घोटाले, धोखाधड़ीपूर्ण ऑनलाइन लेनदेन।
- **संपत्ति के विरुद्ध साइबर अपराध:** हैकिंग, मैलवेयर हमले, रैंसमवेयर, फ़िशिंग, बौद्धिक संपदा की चोरी (नकली सामान बनाना, जालसाजी), डेटा उल्लंघन, व्यवसायों और संगठनों को निशाना बनाने वाली ऑनलाइन धोखाधड़ी।
- **सरकार या समाज के विरुद्ध साइबर अपराध:** साइबर जासूसी, साइबर आतंकवाद, महत्वपूर्ण बुनियादी ढांचे पर हमले, दुष्प्रचार अभियान, राज्य–प्रायोजित हैकिंग, ऑनलाइन कट्टरपंथ।

साइबर स्पेस पर अधिकार क्षेत्र

साइबरस्पेस परस्पर जुड़े कंप्यूटर नेटवर्क द्वारा निर्मित आभासी वातावरण को संदर्भित करता है। इसमें इलेक्ट्रॉनिक रूप से मौजूद हर चीज़, सोशल मीडिया प्लेटफॉर्म (वेबसाइटें), ऑनलाइन डेटाबेस और डिजिटल संचार चौनल शामिल हैं। साइबरस्पेस भौगोलिक स्थिति की परवाह किए बिना उपयोगकर्ताओं के बीच सूचना आदान–प्रदान, डिजिटल लेनदेन और अंतःक्रिया को सुगम बनाता है।

निष्कर्ष

ऑनलाइन प्लेटफॉर्म के माध्यम से इंटरनेट का उपयोग करने वाले लोगों की संख्या दिन–प्रतिदिन बढ़ती जा रही है। दूसरी ओर, अपराध भी तेजी से बढ़ रहे हैं, जिनमें साइबर अपराध भी शामिल हैं, जो इंटरनेट के माध्यम से किए जाते हैं। इन अपराधों से प्रभावी ढंग से निपटने के लिए, साइबर सुरक्षा बुनियादी ढांचे को मजबूत करना, लोगों में जागरूकता बढ़ाना, प्रभावी साइबर सुरक्षा उपायों को लागू करना और सार्वजनिक एवं निजी क्षेत्रों के बीच सहयोग को बढ़ावा देना आवश्यक हो गया है। इसके अतिरिक्त, ऑनलाइन जोखिमों के बारे में जागरूकता बढ़ाना और जनता को शिक्षित करना व्यक्तियों को अपनी और अपने डेटा की बेहतर सुरक्षा करने में मदद कर सकता है। आरटीआई को व्यवहार में लाकर और सक्रिय एवं सहयोगात्मक दृष्टिकोण अपनाकर एक सुरक्षित डिजिटल वातावरण बनाया जा सकता है और ऑनलाइन अपराधों, या साइबर अपराधों को काफी हद तक कम किया जा सकता है। साइबर अपराधों से लोगों, कंपनियों और समग्र रूप से भारतीय अर्थव्यवस्था को भारी वित्तीय नुकसान हुआ है। पहचान की चोरी, वित्तीय धोखाधड़ी और इंटरनेट घोटाले बढ़ रहे हैं, जिससे लोगों और व्यवसायों को भारी आर्थिक नुकसान हो रहा है और वे अपनी मेहनत की कमाई खो रहे हैं। जैसे–जैसे प्रौद्योगिकी आगे बढ़ रही है और अधिक लोग दैनिक कार्यों के लिए डिजिटल उपकरणों और नेटवर्क पर निर्भर हो रहे हैं, साइबर अपराध का खतरा लगातार बढ़ रहा है, जिससे इससे बचाव के लिए कदम उठाना पहले से कहीं अधिक महत्वपूर्ण हो गया है। साइबर अपराध के संबंध में निष्कर्ष यह है कि यह एक निरंतर और विकसित होता खतरा है जिसके लिए व्यक्तियों, व्यवसायों और सरकारों से लगातार सतर्कता और अनुकूलन की आवश्यकता है। साइबर अपराध से निपटने और समाज पर इसके प्रभाव को कम करने के लिए प्रभावी साइबर सुरक्षा उपाय, कानून प्रवर्तन प्रयास और अंतर्राष्ट्रीय सहयोग आवश्यक हैं। साइबर अपराधों और साइबर अपराध संबंधी कमजोरियों का एक बड़ा हिस्सा डेटा के उपयोग से अंजाम दिया जाता है। डेटा अपने उपयोगकर्ताओं (व्यक्तियों, व्यवसायों, संगठनों और सरकारों) को अनगिनत अवसर प्रदान करता है, लेकिन कुछ लोगों ने इन लाभों का दुरुपयोग अवैध गतिविधियों के लिए किया है, विशेष रूप से, डेटा का संग्रह, भंडारण, विश्लेषण और साझाकरण साइबर अपराधों को बढ़ावा देता है, साथ ही उपयोगकर्ताओं की सूचित सहमति और पसंद के बिना और आवश्यक कानूनी और सुरक्षा उपायों के बिना बड़े पैमाने पर डेटा का संग्रह, भंडारण, उपयोग और प्रसार भी साइबर अपराधों का कारण बनता है। इसके अलावा, डेटा संग्रह, विश्लेषण और स्थानांतरण इतने बड़े पैमाने पर होता है कि सरकारें और संगठन इसके लिए तैयार नहीं होते हैं, इसलिए साइबर सुरक्षा के कई खतरे मौजूद हैं। सिस्टम, नेटवर्क और डेटा सुरक्षा, गोपनीयता और डेटा संरक्षण सभी आपस में जुड़े हुए हैं। इसे देखते हुए, साइबर अपराध से बचाव के लिए ऐसे सुरक्षा उपायों की आवश्यकता है जो डेटा और उपयोगकर्ता की गोपनीयता की रक्षा के लिए डिज़ाइन किए गए हो, साइबर अपराध को किसी व्यक्ति की भौतिक या निजता का खतरनाक उल्लंघन कहा जा सकता है। कुछ बुनियादी तार्किक बातों का पालन करके और अपनी सामान्य बुद्धि का प्रयोग करके हम साइबर अपराध से बच सकते हैं। सबसे महत्वपूर्ण बात यह है कि साइबर अपराध न केवल मानवाधिकारों का उल्लंघन है, बल्कि कानून का भी उल्लंघन है, जैसा कि किसी ने सही कहा है कि "अपराध की दुनिया में गोलियों की जगह बाइट्स ले रही हैं।" पूरी दुनिया की तरह भारत में भी साइबर अपराध बढ़ रहे हैं और आज इसकी सीमा और जटिलता को कम करना बेहद ज़रूरी है। साइबर अपराधियों को साइबरस्पेस में निर्दोष लोगों को नुकसान पहुंचाने या भोले–भाले नागरिकों का फायदा उठाकर जल्दी पैसा कमाने के भरपूर अवसर मिलते हैं।

सुझाव

साइबर अपराध से निपटने के लिए कुछ सुझाव इस प्रकार हैं:

1. **उन्नत साइबर सुरक्षा उपाय:** ऑनलाइन हमलों से बचाव के लिए, एक मजबूत साइबर सुरक्षा बुनियादी ढांचे में महत्वपूर्ण निवेश करें, जिसमें घुसपैठ का पता लगाने वाली प्रणाली, फ़ायरवॉल और एन्क्रिप्शन शामिल होना चाहिए।
2. **नियमित अपडेट और पैचिंग:** साइबर अपराधियों द्वारा उपयोग की जाने वाली कमजोरियों को दूर करने के लिए सॉफ्टवेयर, ऑपरेटिंग सिस्टम और सुरक्षा अनुप्रयोगों को नवीनतम अपडेट और पैच के साथ अप–टू–डेट रखें।
3. **उपयोगकर्ता शिक्षा और जागरूकता:** उपयोगकर्ताओं को साइबर सुरक्षा के सर्वोत्तम तरीकों के बारे में जागरूक किया जाना चाहिए, जिसमें सुरक्षित पासवर्ड बनाना, फ़िशिंग प्रयासों को पहचानना और संदिग्ध दस्तावेज़ों और लिंक से दूर रहना शामिल है।
4. **अधिक सशक्त कानून और प्रवर्तन:** साइबर अपराधियों को प्रभावी ढंग से दंडित करने वाले कानूनों को लागू करना और उनका पालन करवाना, साथ ही कानून प्रवर्तन संगठनों को साइबर अपराधों की जांच करने और उन्हें दंडित करने

के लिए आवश्यक उपकरण और निर्देश प्रदान करना।

5. **अंतर्राष्ट्रीय सहयोगः** सीमाओं से परे साइबर खतरों से निपटने के लिए देशों के बीच सहयोग और सूचना साझाकरण को बढ़ावा देना, जिसमें साइबर आपराधिक नेटवर्क को नष्ट करने और अपराधियों को प्रत्यर्पित करने के लिए समन्वित प्रयास शामिल हैं।
6. **सार्वजनिक–निजी भागीदारीः** साइबर अपराध से निपटने में खतरे की जानकारी, संसाधनों और विशेषज्ञता को साझा करने के लिए निजी क्षेत्र के संगठनों, सरकारी एजेंसियों और अकादमिक संस्थानों के बीच साझेदारी को बढ़ावा देना।
7. **अनुसंधान एवं विकास में निवेशः** उभरते साइबर खतरों से आगे रहने के लिए, अत्याधुनिक साइबर सुरक्षा प्रौद्योगिकी और रणनीतियों पर केंद्रित अनुसंधान एवं विकास परियोजनाओं का समर्थन करें।
8. **साइबर स्वच्छता प्रथाएंः** व्यक्तियों और संगठनों को अच्छी साइबर स्वच्छता का अभ्यास करने के लिए प्रोत्साहित करें, जैसे कि नियमित रूप से डेटा का बैकअप लेना, बहु–कारक प्रमाणीकरण लागू करना और सुरक्षा ऑडिट करना।
9. **घटना प्रतिक्रिया योजनाः** साइबर हमलों से प्रभावी ढंग से निपटने और उनसे उबरने के लिए घटना प्रतिक्रिया योजनाओं को विकसित करें और नियमित रूप से उनका परीक्षण करें, जिससे संचालन पर प्रभाव और डेटा हानि को कम किया जा सके।
10. **निरंतर निगरानी और विश्लेषणः** संदिग्ध गतिविधियों और संभावित सुरक्षा उल्लंघनों का वास्तविक समय में पता लगाने और उन पर प्रतिक्रिया देने के लिए नेटवर्क ट्रैफ़िक और सिस्टम लॉग की सक्रिय निगरानी और विश्लेषण लागू करें।

संदर्भ सूची

1. सूचना प्रौद्योगिकी (संशोधन) विधेयक, 2006।
2. https//intellipaat.com/blog/what-is-cybercrime/#no10, Accessed on 11/02/2026.
3. दुग्गल, पवन (2003) *साइबर क्राइम,* साक्षर लॉ पब्लिकेशंस, नई दिल्ली।
4. शर्मा, वकुल (2025) *साइबर जगत और साइबर कानून का परिचय,* यूनिवर्सल लॉ पब्लिशिंग, नई दिल्ली।
5. नागपाल, रोहास (2005) *एशियन स्कूल ऑफ साइबर लॉज़ः साइबर कानून के मूल सिद्धांत.* एशियन स्कूल ऑफ साइबर लॉज़, पुणे।
6. https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.htm, Accessed on 13/02/2026.
7. https://www.drishtijudiciary.com/hin/editorial/Cyber-Crime-in-India, Accessed on 14/02/2026.
8. सूचना प्रौद्योगिकी अधिनियम, 2000।

****