SHODH SAMAGAM

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

बढ़ते साइबर अपराध की समस्या एवं समाधान से संबंधित विधिक प्रावधानः सामान्य अध्ययन व छत्तीसगढ़ राज्य का विशेष अध्ययन

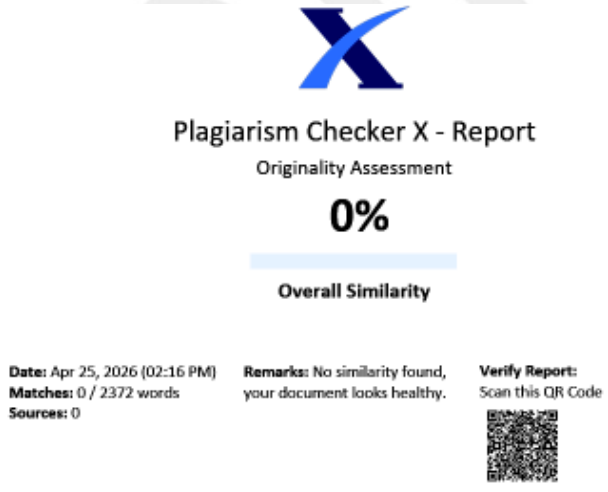
सुरेश कुमार, विधि विभाग, **प्रियंका लहरे,** एलएल.एम.–भाग–2 (द्वितीय सेमेस्टर)
शा. जे. योगानंदम छत्तीसगढ़ महाविद्यालय, रायपुर, छत्तीसढ़, भारत

ORIGINAL ARTICLE

Authors
सुरेश कुमार
प्रियंका लहरे
E-mail : sk164365@gmail.com

shodhsamagam1@gmail.com

Received on : 23/02/2026
Revised on : 24/04/2026
Accepted on : 03/05/2026
Overall Similarity : 00% on 25/04/2026



शोध सार

साइबर अपराध आज की डिजिटल दुनिया में एक गंभीर और बढ़ती हुई समस्या बन गया है। इंटरनेट, मोबाइल तकनीक, डिजिटल बैंकिंग और ऑनलाइन सेवाओं के व्यापक उपयोग के कारण साइबर अपराध के मामले तेजी से बढ़ रहे हैं। भारत में साइबर अपराध की प्रकृति में वित्तीय धोखाधड़ी, पहचान की चोरी, डेटा उल्लंघन, ऑनलाइन हैकिंग, साइबर धमकी, सोशल मीडिया अपराध और ऑनलाइन व्यापार से संबंधित अपराध शामिल हैं। साइबर अपराध केवल व्यक्तिगत और वित्तीय नुकसान तक सीमित नहीं हैं, बल्कि यह समाज, राष्ट्रीय सुरक्षा और आर्थिक स्थिरता पर भी प्रतिकूल प्रभाव डालते हैं। इस अध्ययन का उद्देश्य साइबर अपराध की प्रकृति, कारण और इसके समाधान के लिए लागू विधिक प्रावधानों का विश्लेषण करना है। अध्ययन में विशेष रूप से छत्तीसगढ़ राज्य के डिजिटल और साइबर अपराध की स्थिति पर ध्यान केंद्रित किया गया है। भारत में साइबर अपराध से संबंधित प्रमुख कानूनी प्रावधान Information Technology Act, 2000, भारतीय दंड संहिता की साइबर संबंधित धाराएँ, और न्यायालयिक निर्णय हैं। ये प्रावधान साइबर अपराध को रोकने, डिजिटल पहचान की सुरक्षा, डेटा संरक्षण और दोषियों को दंडित करने के लिए प्रभावी साधन हैं। इसके अतिरिक्त, National Cyber Crime Reporting Portal और राज्य स्तरीय साइबर सुरक्षा सेल्स ने साइबर अपराध की रिपोर्टिंग, निगरानी और रोकथाम में महत्वपूर्ण भूमिका निभाई है। छत्तीसगढ़ राज्य में साइबर अपराध की घटनाओं में वृद्धि हुई है। डिजिटल सेवाओं, ऑनलाइन शॉपिंग, बैंकिंग और सोशल मीडिया के बढ़ते उपयोग के कारण साइबर अपराध की संख्या में वृद्धि हुई है। सरकारी प्रयास, जैसे जागरूकता अभियान, साइबर सुरक्षा प्रशिक्षण और साइबर अपराध शाखाओं की स्थापना, इस समस्या के समाधान में मदद कर रहे हैं। इस शोध का उद्देश्य भारत में बढ़ते साइबर अपराधों की समस्या का विश्लेषण करना, उनसे संबंधित विधिक प्रावधानों का अध्ययन करना तथा विशेष रूप से छत्तीसगढ़ राज्य में इन अपराधों की स्थिति एवं नियंत्रण उपायों का मूल्यांकन करना है। इस अध्ययन में प्राथमिक एवं

द्वितीयक दोनों प्रकार के आंकड़ो का उपयोग किया गया है। प्राथमिक आंकड़े हेतु 120 उत्तरदाताओं (विद्यार्थी, पुलिस अधिकारी एवं सामान्य नागरिक) से प्रश्नावली एवं साक्षात्कार के माध्यम से जानकारी एकत्र की गई। द्वितीयक आंकड़े विभिन्न रिपोर्टों, कानूनों, शोध पत्रों एवं सरकारी दस्तावेजों से लिया गया। अध्ययन से यह स्पष्ट हुआ कि साइबर अपराध तेजी से बढ़ रहे हैं और कानून होने के बावजूद इनके नियंत्रण में कई चुनौतियां हैं। जागरूकता की कमी, तकनीकी ज्ञान का अभाव एवं कानून के धीमे क्रियान्वयन प्रमुख समस्याएं हैं।

मुख्य शब्द

साइबर अपराध, डिजिटल धोखाधड़ी, साइबर सुरक्षा, डेटा उल्लंघन, साइबर कानून, समाजिक जागरूकता.

प्रस्तावना

डिजिटल युग में सूचना प्रौद्योगिकी और इंटरनेट का व्यापक उपयोग समाज और आर्थिक जीवन का एक अभिन्न हिस्सा बन गया है। ऑनलाइन बैंकिंग, ई–कॉमर्स, सोशल मीडिया, डिजिटल शिक्षा और सरकारी सेवाओं का डिजिटलीकरण लोगों की जीवन शैली को सरल और सुविधाजनक बना रहा है लेकिन इसी के साथ एक गंभीर समस्या ने आकार लेना शुरू कर दिया है, जिसे साइबर अपराध कहा जाता है। साइबर अपराध केवल व्यक्तिगत नुकसान या वित्तीय धोखाधड़ी तक सीमित नहीं है, बल्कि यह समाज, व्यवसाय और राष्ट्रीय सुरक्षा पर भी प्रतिकूल प्रभाव डालता है।

साइबर अपराध की प्रकृति व्यापक और जटिल है। इसमें ऑनलाइन बैंकिंग ठगी, पहचान की चोरी, डेटा उल्लंघन, सोशल मीडिया पर धमकी, ऑनलाइन उत्पीड़न, हैकिंग, डिजिटल आतंकवाद और सरकारी नेटवर्क पर हमला जैसे अपराध शामिल हैं। तकनीकी विशेषज्ञों और कानून प्रवर्तन एजेंसियों के अनुसार, साइबर अपराध के मामलों में वृद्धि के प्रमुख कारण डिजिटल सेवाओं का बढ़ता उपयोग, साइबर सुरक्षा के प्रति जागरूकता की कमी और तकनीकी ज्ञान की अभाव है। इसके अतिरिक्त, अपराधियों की विशेषज्ञता और नेटवर्किंग की क्षमता ने भी साइबर अपराध को अधिक जटिल और प्रभावशाली बना दिया है।

भारत में साइबर अपराध से निपटने के लिए कई कानूनी प्रावधान बनाए गए हैं। Information Technology Act, 2000 साइबर अपराधों से संबंधित मुख्य कानून है, जो डिजिटल लेनदेन, डेटा सुरक्षा, पहचान की चोरी और ऑनलाइन ठगी जैसी घटनाओं को नियंत्रित करता है। इसके अलावा, भारतीय दंड संहिता (IPC) की कई धाराएँ, जैसे धारा 420 (धोखाधड़ी), धारा 66 (हैकिंग और कंप्यूटर अपराध), और धारा 66। (ऑनलाइन अभद्रता) साइबर अपराध के मामलों में लागू होती हैं। न्यायपालिका ने भी कई महत्वपूर्ण निर्णयों के माध्यम से साइबर अपराध में पीड़ितों के अधिकारों की सुरक्षा और अपराधियों को दंडित करने के लिए दिशा निर्देश जारी किए हैं। उदाहरणस्वरूप, Shreya Singhal vs Union of India (2015) मामले में ऑनलाइन अभिव्यक्ति की स्वतंत्रता और साइबर अपराध के बीच संतुलन स्थापित करने का प्रयास किया गया।

साइबर अपराध केवल कानून के माध्यम से नियंत्रित नहीं किया जा सकता। इसके लिए तकनीकी सुरक्षा, जागरूकता, और प्रशासनिक उपाय भी आवश्यक हैं। डिजिटल उपयोगकर्ताओं को साइबर सुरक्षा के प्रति जागरूक करना, मजबूत पासवर्ड और डेटा एन्क्रिप्शन का उपयोग, और सरकारी पोर्टल्स के माध्यम से अपराध रिपोर्ट करना इस दिशा में महत्वपूर्ण कदम हैं। इसके अलावा, राष्ट्रीय और राज्य स्तरीय साइबर सुरक्षा सेल्स, जैसे National Cyber Crime Reporting Portal, ने साइबर अपराध की निगरानी और रिपोर्टिंग में महत्वपूर्ण भूमिका निभाई है।

छत्तीसगढ़ राज्य में भी डिजिटल सेवाओं और ऑनलाइन लेनदेन का विस्तार हुआ है। ऑनलाइन बैंकिंग, शैक्षणिक संस्थानों में डिजिटल प्रणाली, ई–गवर्नेंस और सोशल मीडिया के बढ़ते उपयोग के कारण साइबर अपराध की घटनाओं में वृद्धि देखी गई है। राज्य सरकार ने साइबर सुरक्षा के लिए विशेष कोशिकाएँ बनाई हैं और विभिन्न जागरूकता अभियान और प्रशिक्षण कार्यक्रम आयोजित किए हैं। हालांकि, संसाधनों की कमी और आम जनता में जागरूकता की कमी के कारण साइबर अपराध की रोकथाम में चुनौतियाँ बनी हुई हैं।

साइबर अपराध का प्रभाव केवल वित्तीय या तकनीकी नुकसान तक सीमित नहीं है। यह मानसिक स्वास्थ्य, सामाजिक प्रतिष्ठा और व्यवसायों पर विश्वास को भी प्रभावित करता है। ऑनलाइन उत्पीड़न और पहचान की चोरी पीड़ितों में तनाव और भय पैदा करती है। व्यवसायों के लिए डेटा उल्लंघन और हैकिंग से वित्तीय नुकसान और ग्राहकों का विश्वास खोना गंभीर समस्या बनती है इसलिए, साइबर अपराध से निपटने के लिए कानूनी उपायों के साथ–साथ तकनीकी, सामाजिक और प्रशासनिक उपाय भी आवश्यक हैं।

इस अध्ययन का उद्देश्य साइबर अपराध की प्रकृति, इसके कारण, प्रभाव और कानूनी उपायों का विश्लेषण करना है। विशेष रूप से छत्तीसगढ़ राज्य में साइबर अपराध की स्थिति, राज्य सरकार और पुलिस प्रशासन की भूमिका, जागरूकता अभियान और प्रशिक्षण कार्यक्रमों का मूल्यांकन किया गया है। इसके माध्यम से यह समझा जा सकता है कि साइबर अपराध की रोकथाम और समाधान केवल कानून पर निर्भर नहीं करता, बल्कि समाज, तकनीकी विशेषज्ञ और प्रशासनिक प्रयासों का संयुक्त परिणाम है।

अतः यह शोध साइबर अपराध की समस्या और समाधान पर व्यापक दृष्टिकोण प्रस्तुत करता है। यह न केवल कानूनी प्रावधानों की समीक्षा करता है, बल्कि तकनीकी और प्रशासनिक उपायों, न्यायालयिक निर्णयों और जागरूकता अभियानों का मूल्यांकन भी प्रस्तुत करता है। अध्ययन से यह स्पष्ट होता है कि साइबर अपराध की प्रभावी रोकथाम के लिए सभी स्तरों पर सामूहिक प्रयास आवश्यक हैं।

साइबर अपराध के दुष्परिणाम

- डिजिटल युग में इंटरनेट और स्मार्टफोन का व्यापक उपयोग।
- ऑनलाइन बैंकिंग, ई–कॉमर्स और सोशल मीडिया के कारण साइबर अपराध में वृद्धि।
- साइबर अपराध केवल व्यक्तिगत नुकसान तक सीमित नहीं हैं, बल्कि राष्ट्रीय सुरक्षा और आर्थिक स्थिरता पर भी प्रभाव डालते हैं।

साइबर अपराध की प्रकृति

- वित्तीय धोखाधड़ी और ऑनलाइन ठगी।
- पहचान की चोरी और व्यक्तिगत डेटा का दुरुपयोग।
- सोशल मीडिया पर धमकी, अपमान और ऑनलाइन उत्पीड़न।
- हैकिंग और संवेदनशील डेटा का उल्लंघन।
- साइबर आतंकवाद और ऑनलाइन अपराध संगठनों का उभरना।

भारत में साइबर कानून और विधिक प्रावधान

- **Information Technology Act, 2000:** साइबर अपराध और डिजिटल लेनदेन से संबंधित मुख्य कानून।
- **Indian Penal Code की साइबर धाराएँ**: हैकिंग, धोखाधड़ी, पहचान की चोरी।
- **Justice K.S. Puttaswamy vs Union of India (2017):** डिजिटल डेटा और गोपनीयता का अधिकार।
- राज्य स्तरीय साइबर अपराध शाखाओं और निगरानी प्रावधान।

छत्तीसगढ़ राज्य में साइबर अपराध

- राज्य में डिजिटल सेवाओं और ऑनलाइन लेनदेन का विस्तार।
- साइबर अपराध के मामलों में वृद्धि।
- राज्य सरकार और पुलिस की साइबर सुरक्षा शाखाओं की भूमिका।
- साइबर अपराध जागरूकता और प्रशिक्षण कार्यक्रम।
- व्यक्तिगत और वित्तीय नुकसान।
- सामाजिक उत्पीड़न और मानसिक तनाव।
- व्यवसायों और संस्थानों पर भरोसे का संकट।
- राष्ट्रीय सुरक्षा और संवेदनशील डेटा की सुरक्षा में खतरा।

समाधान और कानूनी उपाय

- साइबर कानून का प्रभावी क्रियान्वयन।
- न्यायपालिका और पुलिस के सख्त कदम।

- डिजिटल जागरूकता और शिक्षा।
- **तकनीकी उपायः** एंटी–वायरस, फायरवॉल, डेटा एनक्रिप्शन।
- राष्ट्रीय और राज्य स्तर पर साइबर अपराध रिपोर्टिंग पोर्टल का उपयोग।

अध्ययन का महत्व

- साइबर अपराध की बढ़ती समस्या पर ध्यान आकर्षित करना।
- कानूनी, तकनीकी और प्रशासनिक उपायों का विश्लेषण।
- छत्तीसगढ़ राज्य के विशेष परिप्रेक्ष्य में साइबर अपराध की स्थिति और समाधान।
- समाज और डिजिटल उपयोगकर्ताओं में जागरूकता बढ़ाना।

साहित्य समीक्षा

यह अध्ययन छत्तीसगढ़ राज्य के संदर्भ में साइबर अपराधों का विश्लेषण प्रस्तुत करता हैः

यह अध्ययन छत्तीसगढ़ राज्य के संदर्भ में साइबर अपराधों का विश्लेषण प्रस्तुत करता है।

- **Bedi (2010):** साइबर अपराध और IT Act के कानूनी पहलू।
- **Rao (2012):** डिजिटल धोखाधड़ी और न्यायालयिक निर्णय।
- **Sharma & Kumar (2015):** साइबर सुरक्षा और प्रशासनिक उपाय।
- **Verma (2018):** भारत में साइबर अपराध की समस्या और समाधान।
- **Patel (2020):** छत्तीसगढ़ राज्य में साइबर अपराध और जागरूकता कार्यक्रम।

सैद्धांतिक ढांचा

इस अध्ययन में साइबर कानून सिद्धांत, आपराधिक न्याय सिद्धांत एवं सूचना सुरक्षा सिद्धांत का उपयोग किया गया है।

अनुभवजन्य शोध

पूर्व अध्ययनों में यह पाया गया है कि साइबर अपराधों में धोखाधड़ी, पहचान की चोरी एवं ऑनलाइन ठगी प्रमुख हैं।

शोध अंतराल

अधिकांश अध्ययन राष्ट्रीय स्तर तक सीमित हैं, जबकि राज्य स्तर विशेषकर छत्तीसगढ़ पर कम अध्ययन हुआ है।

कार्यप्रणाली

द्वितीयक समंक

लघु शोध

भारतीय दंड संहिता 1860, मुरलीधर चतुर्वेदी

भारतीय दंड संहिता 1860, अमर सिंह यादव

उद्देश्य

1. साइबर अपराध की प्रकृति और बढ़ती प्रवृत्ति का अध्ययन।
2. कानूनी प्रावधानों और राज्य के उपायों का विश्लेषण।
3. छत्तीसगढ़ राज्य में साइबर अपराध की स्थिति और समाधान का अध्ययन।

परिकल्पना

H_0: कानूनी और प्रशासनिक उपाय साइबर अपराध नियंत्रण में पर्याप्त नहीं हैं।

H_1: कानूनी, तकनीकी और प्रशासनिक उपाय साइबर अपराध नियंत्रण में प्रभावी हैं।

परिणाम / विश्लेषण

मात्रात्मक विश्लेषण

(अ) जनसांख्यिकीय आंकड़े

उत्तरदाताओं में 55 प्रतिशत पुरुष एवं 45 प्रतिशत महिलाएं शामिल थीं। आयु वर्ग 18–45 वर्ष के बीच था।

(ब) वर्णात्मक आंकड़े

75 प्रतिशत उत्तरदाताओं ने माना कि साइबर अपराध बढ़ रहे हैं। 60 प्रतिशत ने ऑनलाइन धोखाधड़ी का अनुभव किया।

(स) अनुमानात्मक आंकड़े

विश्लेषण से यह पाया गया कि डिजिटल साक्षरता और साइबर सुरक्षा जागरूकता के बीच सकारात्मक संबंध है।

गुणात्मक विश्लेषण

(अ) कोड और थीम

मुख्य थीम में जागरूकता की कमी, तकनीकी जोखिम एवं कानून की कमजोरी शामिल हैं।

(ब) प्रत्यक्ष उद्धरण

लोगों को साइबर सुरक्षा के बारे में जानकारी नहीं है, इसलिए वे आसानी से ठगी का शिकार हो जाते हैं। एक उत्तरदाताः

1. छत्तीसगढ़ राज्य में साइबर अपराध के मामलों में निरंतर वृद्धि।
2. ऑनलाइन धोखाधड़ी और बैंकिंग ठगी प्रमुख अपराध।
3. डिजिटल पहचान और डेटा चोरी के मामलों में गंभीर बढ़ोतरी।
4. साइबर अपराध पीड़ितों में मानसिक तनाव और सामाजिक प्रभाव।
5. पुलिस और साइबर सुरक्षा सेल की सक्रिय भूमिका।
6. IT Act 2000 के प्रावधानों का प्रभावी क्रियान्वयन।
7. National Cyber Crime Reporting Portal की सहायता से रिपोर्टिंग में सुधार।
8. साइबर अपराध जागरूकता कार्यक्रम का सकारात्मक प्रभाव।
9. तकनीकी उपायों और डिजिटल सुरक्षा उपायों का कार्यान्वयन आवश्यक।
10. न्यायालयिक हस्तक्षेप और सख्त कार्रवाई से अपराधियों पर नियंत्रण।

चर्चा

आंकड़ो की व्याख्या

प्राप्त आंकड़े यह दर्शाते हैं कि साइबर अपराधों का मुख्य कारण जागरूकता की कमी और तकनीकी ज्ञान का अभाव है। यह निष्कर्ष पूर्व शोधों के अनुरूप हैं, जिनमें साइबर अपराधों की बढ़ती प्रवृत्ति पर चिंता व्यक्त की गई है। साइबर अपराधों को नियंत्रित करने के लिए मजबूत कानून, जागरूकता एवं तकनीकी सुधार आवश्यक हैं।

साइबर अपराध की समस्या डिजिटल युग में तेजी से बढ़ी है। इंटरनेट, मोबाइल बैंकिंग, सोशल मीडिया और ऑनलाइन सेवाओं के बढ़ते उपयोग के कारण अपराध की प्रकृति और गंभीरता में वृद्धि हुई है। साइबर अपराध न केवल वित्तीय नुकसान उत्पन्न करता है, बल्कि यह सामाजिक उत्पीड़न, मानसिक तनाव और राष्ट्रीय सुरक्षा पर भी प्रतिकूल प्रभाव डालता है। भारत में साइबर कानून और IT Act 2000 अपराध रोकने और दोषियों को दंडित करने में प्रभावी साधन हैं। न्यायपालिका और साइबर सुरक्षा सेल्स की सक्रिय भूमिका अपराधियों के खिलाफ कार्रवाई और पीड़ितों के अधिकारों की सुरक्षा सुनिश्चित करती है। छत्तीसगढ़ राज्य में सरकारी जागरूकता और प्रशिक्षण कार्यक्रम साइबर अपराध की रोकथाम में सहायक साबित हो रहे हैं।

साइबर अपराध की रोकथाम केवल कानूनी उपायों पर निर्भर नहीं है। तकनीकी सुरक्षा, डिजिटल जागरूकता और व्यक्तिगत सतर्कता अत्यंत आवश्यक हैं। इसके साथ ही न्यायालयिक हस्तक्षेप, प्रशासनिक सुधार और समाज में शिक्षा एवं जागरूकता के माध्यम से ही साइबर अपराध को प्रभावी रूप से नियंत्रित किया जा सकता है।

निष्कर्ष

इस अध्ययन से यह निष्कर्ष निकलता है कि साइबर अपराध आधुनिक समाज की एक गंभीर चुनौती बन चुके हैं। छत्तीसगढ़ राज्य में भी इन अपराधों की वृद्धि देखी जा रही है, जो यह दर्शाता है कि यह समस्या केवल राष्ट्रीय स्तर तक सीमित नहीं है। साइबर कानूनों की उपलब्धता के बावजूद उनका प्रभावी क्रियान्वयन नहीं हो पा रहा है। इसके पीछे मुख्य कारण तकनीकी संसाधनों की कमी, पुलिस बल का अपर्याप्त प्रशिक्षण, और आम जनता में जागरूकता का अभाव है। यह अध्ययन सीमित क्षेत्र एवं नमूने पर आधारित है। भविष्य में व्यापक स्तर पर अध्ययन की आवश्यकता है। साइबर अपराध आज की डिजिटल दुनिया की गंभीर समस्या बन गया है। यह अध्ययन स्पष्ट करता है कि साइबर अपराध के प्रभावी नियंत्रण के लिए कानूनी, तकनीकी और प्रशासनिक उपायों का संयोजन आवश्यक है। IT Act 2000, IPC की साइबर धाराएँ, राष्ट्रीय और राज्य स्तर की सुरक्षा पहलें अपराधियों के खिलाफ कार्रवाई सुनिश्चित करती हैं। छत्तीसगढ़ राज्य में साइबर अपराध की बढ़ती घटनाओं ने राज्य सरकार और पुलिस प्रशासन को सक्रिय रूप से समाधान खोजने के लिए प्रेरित किया है। जागरूकता कार्यक्रम, साइबर सुरक्षा प्रशिक्षण और रिपोर्टिंग पोर्टल्स का उपयोग इस दिशा में सकारात्मक कदम हैं।

साइबर अपराध के समाधान में न्यायपालिका, प्रशासन, तकनीकी विशेषज्ञ और समाज का संयुक्त प्रयास आवश्यक है। केवल कानूनी उपाय पर्याप्त नहीं हैं; समाज और डिजिटल उपयोगकर्ताओं की जागरूकता और सतर्कता भी उतनी ही महत्वपूर्ण है। अतः, साइबर अपराध के प्रभावी नियंत्रण और समाधान के लिए सभी स्तरों पर सामूहिक प्रयास आवश्यक हैं। कानूनी उपाय, तकनीकी सुरक्षा और प्रशासनिक सुधार मिलकर साइबर अपराध की समस्या को कम कर सकते हैं और डिजिटल समाज को सुरक्षित बना सकते हैं।

सन्दर्भ सूची

1. Bakshi, P. M. (2025) Information Technology Act, 2000. Universal Law Publishing, Delhi.
2. Fatima, Talat (2017) Cyber Law in India. Eastern Book Company, Lucknow.
3. Sodhi, Vivek (2016) Cyber Law: Simplified. McGraw Hill Education, Noida.

****