JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

बैंकिंग धोखाधड़ी और साइबर सुरक्षा कानून

साक्षी हिवसे

एल.एल.एम. (प्रथम सेमेस्टर) इनरॉलमेंट नंबर 25LAW4LLM0023

के मार्गदर्शन में

डॉ. मुकेश कुमार कोरी

(सहायक प्रोफेसर विधी संकाय)

सारांश:-

डिजिटल बैंकिंग के बढ़ते उपयोग के कारण, इंटरनेट बैंकिंग, मोबाइल बैंकिंग, UPI और अन्य डिजिटल माध्यम से लोगों का जीवन आसान बन गया है, लेकिन इसके साथ ही बैंकिंग धोखाधड़ी और साइबर अपराध भी बढ़े हैं। भारतीय रिजर्व बैंक की रिपोर्ट के अनुसार हाल के वर्षों में बैंकिंग धोखाधड़ी के मामले में भी उल्लेखनीय वृद्धि हुई है। इस धोखाधड़ी से बचने के लिए, साइबर कानूनी सुरक्षा में, सूचना प्रौद्योगिकी अधिनियम 2000 और भारतीय न्याय संहिता 2023 जैसे कानून शामिल हैं, जिससे धोखाधड़ी से बचा जा सकता है। यह शोध पत्र बैंकिंग धोखाधड़ी की अवधारणा, उसके प्रकार, साइबर सुरक्षा कानूनों की भूमिका तथा भारत में मौजूद कानूनी ढांचे का सरल और सामान्य भाषा में अध्ययन करना है।

मुख्य शब्द:-

बैंकिंग धोखाधड़ी, साइबर सुरक्षा, कानूनी ढांचा, डिजिटल बैंकिंग।

01. परिचय:-

डिजिटल क्रांति और ऑनलाइन बैंकिंग के बढ़ते उपयोग ने वित्तीय सेवाओं को सुलभ बनाया है। इंटरनेट बैंकिंग, मोबाइल बैंकिंग, ATM, डेबिट, क्रेडिट कार्ड तथा UPI जैसी सेवाओं ने बैंकिंग को सरल, सुविधाजनक एवं तेज बना दिया है, लेकिन इसी सुविधा का फायदा उठाकर अपराधी धोखाधड़ी कर रहे हैं, जिससे बैंकिंग क्षेत्र के लिए एक बड़ी चुनौती खड़ी हो गई है। फिशिंग, मैलवेयर, पहचान की चोरी और खाता अधिग्रहण जैसे अपराधों में भी तेजी से वृद्धि हुई है, जिससे ग्राहकों और वित्तीय संस्थानों दोनों को भारी नुकसान हो रहा है। तकनीकी प्रगति के साथ साइबर अपराधी भी अपने तरीके को बदल रहे हैं जिससे मौजूदा साइबर सुरक्षा

उपाय और कानूनी ढांचा अपर्याप्त साबित हो रहे हैं। इसलिए साइबर सुरक्षा कानूनों की आवश्यकता बढ़ गयी है।

02. उद्देश्य:-

इस शोध पत्र का प्रमुख उद्देश्य भारत में बैंकिंग धोखाधड़ी के प्रमुख प्रकारों और उनके बढ़ते रुझानों का अध्ययन करना, डिजिटल धोखाधड़ी से निपटने में मौजूदा साइबर सुरक्षा कानूनों (जैसे सूचना प्रौद्योगिकी अधिनियम 2000) की भूमिका और सीमाओं का विश्लेषण करना है। यह अध्ययन मूल्यांकन करने का प्रयास करता है कि, वर्तमान साइबर कानून, बैंकिंग धोखाधड़ी को किस हद तक रोकने के लिए सक्षम है और भविष्य में किस प्रकार के कानूनी एवं नितीगत सुधार आवश्यक हैं।

03. बैंकिंग धोखाधड़ी:-

बैंकिंग धोखाधड़ी में चुनौतियां

- साइबर सुरक्षा और तकनीकी प्रगती:- हैकर्स सोशल इंजीनियरिंग और डेटा उल्लंघन से चोरी किए गए क्रेडेंशियल का उपयोग करके धोखाधड़ी करते हैं जिससे बैंकों के लिए डिजिटल प्लेटफार्म बचाना मुश्किल हो जाता है।
- नियामक और कानूनी बाधाएं:- भारतीय दंड संहिता (IPC) (BNS) में बैंकिंग धोखाधड़ी के लिए कोई अलग व्यापक कानून नहीं है। इसे धारा 420, 406, 409 जैसी विभिन्न धाराओं के तहत निपटाया जाता है, जिससे कानूनी प्रक्रिया लम्बी हो जाती है।
- KYC और AML की कमजोरी:- ग्राहक की सही पहचान (BNS) और मनी लाउंड्रिंग विरोधी (AML) मानदंडों का पालन न करना धोखाधड़ी को बढ़ावा देता है।

04. रिपोर्टिंग में देरी:-

बैंक अक्सर धोखाधड़ी का पता चलने के बहुत समय के बाद RBI को सूचित करते हैं, जिससे अपराधियों को भागने का मौका मिल जाता है।

05. साइबर कानूनी सुरक्षा:-

भारत में बैंकिंग धोखाधड़ी से बचाव के लिए कई साइबर कानून बनाए गए हैं। यह साइबर कानून तथा सुरक्षा उपाय महत्वपूर्ण भूमिका निभाते है।

सूचना प्रौद्योगिकी अधिनियम **2000**:-

भारत में इलेक्ट्रॉनिक वाणिज्य, डिजिटल हस्ताक्षर और साइबर अपराधों सहित साइबर गतिविधियों को नियंत्रित करने वाला प्राथमिक कानून है, जो इलेक्ट्रॉनिक रिकॉर्ड और डिजिटल हस्ताक्षरों को वैध बनाता है।

भारतीय दंड संहिता (IPC):-

भारतीय दंड संहिता सूचना प्रौद्योगिकी के साथ मिलकर कार्य करती है। साइबर अपराध पारंपरिक आपराधिक अपराधों के समान हैं जिसमें धारा 420, 468, 471, 500 धाराएं शामिल हैं।

RBI के दिशा निर्देश:- इसका मुख्य उद्देश्य वित्तीय संस्थानों, बैंकों को साइबर हमले से बचाना, ग्राहक डेटा की सुरक्षा करना, नेटवर्क और एप्लीकेशन सुरक्षा करना है।

06. साइबर सुरक्षा उपाय:-

साइबर सुरक्षा उपाय में बैंकों द्वारा मजबूत एप्लीकेशन सिस्टम, OTP और बायोमेट्रिक सुरक्षा, संदिग्ध ट्रांजेक्शन की निगरानी करना है, तथा राष्ट्रीय हेल्पलाइन नंबर 1930 पर तुरंत शिकायत व्यवस्था की गयी है।

उदाहरण:-

- पंजाब नेशनल बैंक बनाम नीरव मोदी मामला (2018):-

यह भारत का सबसे बड़ा बैंकिंग धोखाधड़ी का मामला माना जाता है।

- स्टेट बैंक ऑफ इंडिया बनाम श्यामा देवी (1978 ।प्त् 1263):-

ग्राहक के पैसे कर्मचारी ने धोखाधड़ी से ले लिए।

07. संदर्भ :-

साइबर धोखाधड़ी:- भारतीय बैंकिंग क्षेत्र के लिए एक बढ़ता खतरा और निवारक रणनीतियां (2023)

बैंकिंग धोखाधड़ी में नई चुनौतियाँ:- भारत में एक सामाजिक-कानूनी विश्लेषण (2025)

भारत के बैंकिंग क्षेत्र में धोखाधड़ी का रुझान विश्लेषण (हंसराज कॉलेज 2025)

08. निष्कर्ष :-

इस शोध अध्ययन से यह स्पष्ट होता है कि बैंकिंग धोखाधड़ी आज के डिजिटल युग में गंभीर और बदलती हुई समस्या है। बैंकिंग धोखाधड़ी को रोकने में बैंकों, सरकार और ग्राहकों तीनों की समान जिम्मेदारी है। बैंकों को मजबूत सुरक्षा प्रणाली अपनानी चाहिए, सरकार को सख्त कानून और जागरूकता कार्यक्रम चलाने चाहिए। अतः कहा जा सकता है कि, प्रभावी साइबर सुरक्षा कानून, तकनीकी उपायों और जन जागरूकता के माध्यम से बैंकिंग धोखाधड़ी पर काफी हद तक नियंत्रण पाया जा सकता है।