साइबर अपराध और सोशल मीडिया की भूमिका

drishtiias.com/hindi/printpdf/cyber-crime-and-role-of-social-media

इस Editorial में The Hindu, The Indian Express, Business Line आदि में प्रकाशित लेखों का विश्लेषण किया गया है। इस लेख में साइबर अपराध और सोशल मीडिया की भूमिका से संबंधित विभिन्न पहलुओं पर चर्चा की गई है। आवश्यकतानुसार, यथास्थान टीम दृष्टि के इनपुट भी शामिल किये गए हैं।

संदर्भ

हम जितनी तेज़ी से डिजिटल दुनिया की ओर बढ़ रहे हैं, ठीक उतनी ही तेज़ी से साइबर अपराध की संख्या में भी वृद्धि हो रही है। जिस गति से तकनीक ने उन्नति की है, उसी गति से मनुष्य की इंटरनेट पर निर्भरता भी बढ़ी है। एक ही जगह पर बैठकर इंटरनेट के ज़रिये मनुष्य की पहुँच, विश्व के हर कोने तक आसान हुई है। आज के समय में हर वो चीज़ जिसके विषय में इंसान सोच सकता है, उस तक उसकी पहुँच इंटरनेट के माध्यम से हो सकती है, जैसे कि सोशल नेटवर्किंग, ऑनलाइन शॉपिंग, डेटा स्टोर करना, गेमिंग, ऑनलाइन स्टडी, ऑनलाइन जॉब इत्यादि। आज के समय में इंटरनेट का उपयोग लगभग हर क्षेत्र में किया जाता है। इंटरनेट के विकास और इसके संबंधित लाभों के साथ साइबर अपराधों की अवधारणा भी विकसित हुई है।

वर्तमान में भारत की बड़ी आबादी सोशल नेटवर्किंग साइट्स का उपयोग करती है। भारत में सोशल नेटवर्किंग साइट्स के उपयोग के प्रति लोगों में जानकारी का अभाव है। इसके साथ ही अधिकतर सोशल नेटवर्किंग साइट्स के सर्वर विदेश में हैं, जिससे भारत में साइबर अपराध घटित होने की स्थिति में इनकी जड़ तक पहुँच पाना कठिन होता है।

इस आलेख में साइबर अपराध, उसके प्रकार, बचाव के उपाय और सरकार के द्वारा किये गए प्रावधानों पर विमर्श किया जाएगा। इसके साथ ही साइबर अपराध में सोशल नेटवर्किंग साइट्स की भूमिका का भी मूल्यांकन किया जाएगा।

साइबर अपराध क्या है?

- साइबर अपराध विभिन्न रूपों में किये जाते हैं। कुछ साल पहले, इंटरनेट के माध्यम से होने वाले अपराधों के बारे में जागरूकता का अभाव था। साइबर अपराधों के मामलों में भारत भी उन देशों से पीछे नहीं है, जहाँ साइबर अपराधों की घटनाओं की दर भी दिन-प्रतिदिन बढ़ती जा रही है। साइबर अपराध के मामलों में एक साइबर अपराधी, किसी उपकरण का उपयोग, उपयोगकर्ता की व्यक्तिगत जानकारी, गोपनीय व्यावसायिक जानकारी, सरकारी जानकारी या किसी डिवाइस को अक्षम करने के लिये कर सकता है। उपरोक्त सूचनाओं को ऑनलाइन बेचना या खरीदना भी एक साइबर अपराध है।

- इसमें कोई संशय नहीं है कि यह एक आपराधिक गतिविधि है, जिसे कंप्यूटर और इंटरनेट के उपयोग द्वारा अंजाम दिया जाता है। साइबर अपराध, जिसे 'इलेक्ट्रॉनिक अपराध' के रूप में भी जाना जाता है, एक ऐसा अपराध है जिसमें किसी भी अपराध को करने के लिये कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क का उपयोग, एक वस्तु या उपकरण के रूप में किया जाता है। जहाँ इनके (कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क) ज़रिये ऐसे अपराधों को अंजाम दिया जाता है वहीँ इन्हें लक्ष्य बनाते हुए इनके विरुद्ध अपराध भी किया जाता है।
- ऐसे अपराध में साइबर जबरन वसूली, पहचान की चोरी, क्रेडिट कार्ड धोखाधड़ी, कंप्यूटर से व्यक्तिगत डेटा हैक करना, फ़िशिंग, अवैध डाउनलोडिंग, साइबर स्टॉकिंग, वायरस प्रसार, सहित कई प्रकार की गतिविधियाँ शामिल हैं। ग़ौरतलब है कि सॉफ्टवेयर चोरी भी साइबर अपराध का ही एक रूप है, जिसमें यह जरूरी नहीं है कि साइबर अपराधी, ऑनलाइन पोर्टल के माध्यम से ही अपराध करे।

साइबर अपराध का वर्गीकरण

साइबर विशेषज्ञों के अनुसार, अपराध की श्रेणी को दो वर्गों में विभाजित किया जा सकता है-

- वे अपराध जिनमें कंप्यूटर पर हमला किया जाता है। इस तरह के अपराधों के उदाहरण हैकिंग, वायरस हमले आदि हैं।
- वे अपराध जिनमे कंप्यूटर को एक हथियार/उपकरण/ के रूप में उपयोग किया जाता है। इस प्रकार के अपराधों में साइबर आतंकवाद, आईपीआर उल्लंघन, क्रेडिट कार्ड धोखाधड़ी, पोर्नोग्राफी आदि।

साइबर अपराध की श्रेणियाँ

- साइबर अपराध के अंतर्गत 3 प्रमुख श्रेणियाँ आती हैं जिसमें व्यक्ति विशेष, संपत्ति और सरकार के विरुद्ध अपराध शामिल हैं।
    - **व्यक्ति विशेष के विरुद्ध साइबर अपराध-** ऐसे अपराध, यद्यपि ऑनलाइन होते हैं, परंतु वे वास्तविक लोगों के जीवन को प्रभावित करते हैं। इनमें से कुछ अपराधों में साइबर उत्पीड़न और साइबर स्टॉकिंग, चाइल्ड पोर्नोग्राफी का वितरण, विभिन्न प्रकार के स्पूफिंग, क्रेडिट कार्ड धोखाधड़ी, मानव तस्करी, पहचान की चोरी और ऑनलाइन बदनाम किया जाना शामिल हैं। साइबर अपराध की इस श्रेणी में किसी व्यक्ति या समूह के खिलाफ दुर्भावनापूर्ण या अवैध जानकारी को ऑनलाइन लीक कर दिया जाता है।
    - **संपत्ति विशेष के विरुद्ध साइबर अपराध- कुछ ऑनलाइन अपराध संपत्ति के खिलाफ होते हैं, जैसे कि कंप्यूटर या सर्वर के खिलाफ या उसे ज़रिया बनाकर किये जाते हैं । इन अपराधों में हैकिंग, वायरस ट्रांसमिशन, साइबर और टाइपो स्क्वाटिंग, कॉपीराइट उल्लंघन, आईपीआर उल्लंघन आदि शामिल हैं । उदाहरण- कोई आपको एक वेब-लिंक भेजे, जिस पर क्लिक करने के पश्चात एक वेब पेज खुले जहाँ आपसे आपके बैंक खाते/गोपनीय दस्तावेज़ संबंधित सारी जानकारी मांगी जाए और ऐसा कहा जाए कि यह जानकारी रिज़र्व बैंक ऑफ़ इंडिया या सरकार की ओर से मांगी जा रही है, आप वहाँ सारी जानकारी दे दें और फिर उस जानकारी के इस्तेमाल से आपके दस्तावेज़ एवं बैंक खाते के साथ छेड़छाड़ की जाए, तो यह संपत्ति के विरूद्ध साइबर हमला कहा जायेगा ।**
    - **सरकार विशेष के विरुद्ध साइबर अपराध:** यह सबसे गंभीर साइबर अपराध माना जाता है। सरकार के खिलाफ किये गए ऐसे अपराध को साइबर आतंकवाद के रूप में भी जाना जाता है। सरकारी साइबर अपराध में सरकारी वेबसाइट या सैन्य वेबसाइट को हैक किया जाना शामिल हैं। ग़ौरतलब है कि जब सरकार के खिलाफ एक साइबर अपराध किया जाता है, तो इसे उस राष्ट्र की संप्रभुता पर हमला और युद्ध की कार्रवाई माना जाता है। ये अपराधी आमतौर पर आतंकवादी या अन्य शत्रु देशों की सरकारें होती हैं। इस प्रकार के साइबर अपराधों पर नियंत्रण के लिये प्रत्येक देश की सरकार द्वारा कठोर साइबर कानून बनाए गए हैं।

- **सोशल मीडिया की भूमिका**
    - बड़े पैमाने पर सोशल नेटवर्किंग साइट्स का उपयोग करने वाली जनसंख्या साइबर अपराध के खतरों से अनजान है। विभिन्न सोशल नेटवर्किंग साइट्स के सर्वर अन्य देशों में केंद्रित हैं, जिससे यह डर रहता है कि कहीं ये देश लोगों की व्यक्तिगत जानकारी का दुरुपयोग न करें।
    - विभिन्न सोशल नेटवर्किंग साइट्स पर लोग अपनी व्यक्तिगत जानकारियाँ साझा करते हैं, जिससे हैकर्स इन सोशल नेटवर्किंग एकाउंट्स को आसानी से हैक कर लेते हैं और फिर प्राप्त सूचना का दुरुपयोग करते हैं।
    - लोगों को सोशल नेटवर्किंग साइट्स पर हैकर्स ऑनलाइन ठगी का शिकार बनाते हैं।
    - सुरक्षा एजेंसियों द्वारा यह भी पता लगाया गया है कि ऑनलाइन मुद्रा स्थानांतरित करने वाले विभिन्न एप के माध्यम से आतंकवादियों और देशविरोधी तत्वों को फंडिंग की जाती है।
    - साइबर अपराधी विभिन्न ऑनलाइन गेम्स के माध्यम से बच्चों को अपराध करने के लिये प्रोत्साहित करते हैं।

साइबर अपराधों से निपटने की दिशा में सरकार के प्रयास

- भारत में 'सूचना प्रौद्योगिकी अधिनियम, 2000' पारित किया गया जिसके प्रावधानों के साथ-साथ भारतीय दंड संहिता के प्रावधान सम्मिलित रूप से साइबर अपराधों से निपटने के लिये पर्याप्त हैं।
- सूचना प्रौद्योगिकी अधिनियम 2000 की धाराएँ 43, 43ए, 66, 66बी, 66सी, 66डी, 66ई, 66एफ, 67, 67ए, 67बी, 70, 72, 72ए और 74 हैकिंग और साइबर अपराधों से संबंधित हैं।
- सरकार द्वारा 'राष्ट्रीय साइबर सुरक्षा नीति, 2013' जारी की गई जिसके तहत सरकार ने अति-संवेदनशील सूचनाओं के संरक्षण के लिये 'राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure protection centre-NCIIPC) का गठन किया।
- इसके अंतर्गत 2 वर्ष से लेकर उम्रकैद तथा दंड अथवा जुर्माने का भी प्रावधान है।
- विभिन्न स्तरों पर सूचना सुरक्षा के क्षेत्र में मानव संसाधन विकसित करने के उद्देश्य से सरकार ने 'सूचना सुरक्षा शिक्षा और जागरूकता' (Information Security Education and Awareness: ISEA) परियोजना प्रारंभ की है।
- सरकार द्वारा 'कंप्यूटर इमरजेंसी रिस्पॉन्स टीम (CERT-In)' की स्थापना की गई जो कंप्यूटर सुरक्षा के लिये राष्ट्रीय स्तर की मॉडल एजेंसी है।
- देश में साइबर अपराधों से समन्वित और प्रभावी तरीके से निपटने के लिए 'साइबर स्वच्छता केंद्र' भी स्थापित किया गया है। यह इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय (Ministry of Electronics and Information Technology-MeitY) के तहत भारत सरकार की डिजिटल इंडिया मुहिम का एक हिस्सा है।
- भारत सूचना साझा करने और साइबर सुरक्षा के संदर्भ में सर्वोत्तम कार्य प्रणाली अपनाने के लिये अमेरिका, ब्रिटेन और चीन जैसे देशों के साथ समन्वय कर रहा है।
- अंतर-एजेंसी समन्वय के लिये 'भारतीय साइबर अपराध समन्वय केंद्र' (Indian Cyber Crime Co-ordination Centre-I4C) की स्थापना की गई है।

भारतीय साइबर अपराध समन्वय केंद्र

- जनवरी 2020 में गृह मंत्रालय द्वारा साइबर क्राइम से निपटने के लिये 'भारतीय साइबर अपराध समन्वय केंद्र' (Indian Cyber Crime Coordination Centre-I4C) का उद्घाटन किया गया है।

- इस योजना को संपूर्ण भारत में लागू किया गया है। साइबर क्राइम से बेहतर तरीके से निपटने के लिये तथा I4C को समन्वित और प्रभावी तरीके से लागू करने हेतु इस योजना के निम्नलिखित सात प्रमुख घटक है-
    - नेशनल साइबरक्राइम थ्रेट एनालिटिक्स यूनिट (National Cybercrime Threat Analytics Unit)
    - नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल (National Cyber Crime Reporting Portal)
    - संयुक्त साइबर अपराध जाँच दल के लिये मंच (Platform for Joint Cyber Crime Investigation Team)
    - राष्ट्रीय साइबर अपराध फोरेंसिक प्रयोगशाला पारिस्थितिकी तंत्र (National Cyber Crime Forensic Laboratory Ecosystem)
    - राष्ट्रीय साइबर क्राइम प्रशिक्षण केंद्र (National Cyber Crime Training Centre)
    - साइबर क्राइम इकोसिस्टम मैनेजमेंट यूनिट (Cyber Crime Ecosystem Management Unit)
    - राष्ट्रीय साइबर अनुसंधान और नवाचार केंद्र (National Cyber Research and Innovation Centre)

बुडापेस्ट कन्वेंशन क्या है?

- साइबर अपराध के संबंध में बुडापेस्ट कन्वेंशन (Budapest Convention on cyber crime) पर हस्ताक्षर करने के लिये गृह मंत्रालय द्वारा साइबर अपराध और डेटा सुरक्षा को बढ़ावा देने के लिये अंतर्राष्ट्रीय सहयोग की आवश्यकता पर बल दिया जा रहा है।
- **बुडापेस्ट कन्वेंशन साइबर क्राइम पर एक कन्वेंशन है, जिसे साइबर अपराध पर बुडापेस्ट कन्वेंशन के नाम से जाना जाता है ।**
- यह अपनी तरह की पहली ऐसी अंतर्राष्ट्रीय संधि है जिसके अंतर्गत राष्ट्रीय कानूनों को सुव्यवस्थित करके, जाँच-पड़ताल की तकनीकों में सुधार करके तथा इस संबंध में विश्व के अन्य देशों के बीच सहयोग को बढ़ाने हेतु इंटरनेट और कंप्यूटर अपराधों पर रोक लगाने संबंधी मांग की गई है।
- कन्वेंशन का अनुच्छेद 32B डेटा तक पहुँच की अनुमति देता है और इस प्रकार यह राष्ट्रीय संप्रभुता का उल्लंघन करता है, इसलिये भारत ने अभी तक इस पर हस्ताक्षर नहीं किये हैं।

निष्कर्ष- भारत इंटरनेट का तीसरा सबसे बड़ा उपयोगकर्ता है और हाल के वर्षों में साइबर अपराध कई गुना बढ़ गए हैं। साइबर सुरक्षा उपलब्ध कराने के लिये सरकार की ओर से कई कदम उठाए गए हैं। कैशलेस अर्थव्यवस्था को अपनाने की दिशा में बढ़ने के कारण भारत में साइबर सुरक्षा सुनिश्चित करना आवश्यक है। डिजिटल भारत कार्यक्रम की सफलता काफी हद तक साइबर सुरक्षा पर निर्भर करेगी अतः भारत को इस क्षेत्र में तीव्र गति से कार्य करना होगा। वहीँ दूसरी ओर सोशल मीडिया ने अभिव्यक्ति की स्वतंत्रता के अधिकार को नया आयाम दिया है, आज प्रत्येक व्यक्ति बिना किसी डर के सोशल मीडिया के माध्यम से अपने विचार रख सकता है और उसे हज़ारों लोगों तक पहुँचा सकता है, परंतु सोशल मीडिया का सावधानीपूर्वक उपयोग ही हमें ऑनलाइन ठगी तथा साइबर अपराध के गंभीर खतरों से बचा सकता है।

प्रश्न- साइबर अपराध से आप क्या समझते हैं? साइबर अपराध को रोकने में सरकार के द्वारा किये जा रहे प्रयासों का विश्लेषण कीजिये।