IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

साइबर अपराध से सुरक्षा एवं न्यायिक समाधान

दिलीप कुमार, (नेट)

भाोध छात्र

(भूगोल विभाग)

श्री बलदेव स्नातकोत्तर महाविद्यालय बड़ागॉव, वाराणसी

सारांश

साइबर अपराध वे अपराध हैं जो कंप्यूटर, इंटरनेट या डिजिटल डिवाइसों का उपयोग करके किए जाते हैं। आधुनिक युग में डेटा चोरी, पहचान को छिपाना, स्पैम ईमेल, सोशल नेटवर्किंग साइटों पर अफवाह फैलाना, हैकिंग, फिशिंग, साइबर स्टॉकिंग, वायरस फैलाना, फर्जी बैंक कॉल, और अन्य प्रकार के डिजिटल धोखाधड़ी शामिल हैं। साइबर अपराध में कम्प्यूटर प्रौद्योगिकी के ज्ञान का दुरुपयोग कानून विरोधी और अनैतिक कार्यो के लिए किया जाता है। इसमें कम्प्यूटर तकनीक से सम्बन्धित प्रतिभावान व्यक्ति कम्प्यूटर का दुरुपयोग करके विभिन्न ऑकड़ों और सामग्रियों को अवैध, अनैतिक और अनधिकृत रुप से संसाधित और सम्प्रेषित करने का काम करते हैं। जैसे साइबर अपराध पूरे वि"व के लोगों के सामने एक गम्भीर समस्या पैदा की है जिसने मानवीय जीवन को भयावह एवं अक्रान्त बना दिया है।

मुख्य शब्द – साइबर अपराध, डेटा चोरी, पहचान को छिपाना, स्पैम ईमेल, हैकिंग, फिशिंग, वायरस फैलाना, फर्जी बैंक कॉल, सोशल नेटवर्किंग साइटों पर अफवाह फैलाना,

प्रस्तावना

वर्तमान युग में वैज्ञानिक तथा प्रौद्योगिकी विकास ने जहाँ एक ओर पूरे वि"व को एक वै"वक गाँव के रुप में बदल दिया है वहीं दूसरी ओर साइबर अपराध के रुप में सम्पूर्ण वि"व के सामने अनेक नई चुनौतिया उत्पन्न की है।

साइबर अपराध एक शब्द है जिसका उपयोग मोटे तौर पर आपराधिक गतिविधि का वर्णन करने के लिए किया जाता है जिसमें कंप्यूटर या कंप्यूटर शामिल हैं नेटवर्क एक उपकरण, लक्ष्य या आपराधिक गतिविधि का स्थान है और इसमें इलेक्ट्रॉनिक से लेकर सब कुछ शामिल है जिसमें पारंपरिक अपराधों को भी शामिल करने के लिए इसका उपयोग किया जाता है अवैध गतिविधि को सक्षम करने के लिए कंप्यूटर या नेटवर्क का उपयोग किया जाता है। कंप्यूटर अपराध में कंप्यूटर सिस्टम में अनधिकृत पहुंच, डेटा परिवर्तन, डेटा विनाश, बौद्धिक चोरी मुख्य रूप से शामिल हैं। राष्ट्रीय सुरक्षा के संदर्भ में साइबर अपराध में सक्रियता, जासूसी, या सूचना युद्ध और संबंधित गतिविधियाँ, पारंपरिकता शामिल हो सकता है।

आधुनिक युग में कम्प्यूटर से सम्बन्धित टेक्नोलॉजी के कारण हम कुछ ही क्षणों में दुनिया भर में कहीं भी सन्देशों का आदान प्रदान कर सकते सभी तरह की सूचनाएं प्राप्त कर सकते हैं। कुछ समय पहले तक जिन ऑकड़ों, सूचनाओं और तथ्यों को सुरक्षित रखने के लिए कार्यालयों में हजारों फाइलें रखी जाती थीं, वहीं आज कम्प्यूटर की सहायता से हम सभी ऑकड़े एक साफ्टवेयर में रखकर उसका कभी भी उपयोग कर सकते हैं। आज नेटवर्किंग के माध्यम से एक–दूसरे से हजारों किलोमीटर दूर स्थापित कम्प्यूटरों को एक–दूसरे से इस तरह जोड़कर रखा जा सकता है कि एक साइट से सम्बन्धित सामग्री का उपयोग दूसरे सभी कम्प्यूटरों द्वारा किया जा सकता है। यह आधुनिकता की दिशा में होने वाली एक ऐसी उपलब्धि है जिसने प्रौद्योगिकी, औद्योगीकरण, वैज्ञानिक विकास, आन्तरिक तथा बाह्य सुरक्षा एवं जीवन के सभी पक्षों को प्रभावित किया है। कम्प्यूटर से जुड़ी आधुनिक टेक्नोलाजी से जहाँ एक ओर व्यापक लाभ हुए है वहीं दूसरी ओर इससे अपराधों में भी वृद्धि हुई है। यह वे साइबर अपराध हैं जो मानवाधिकारों का हनन करने के अतिरिक्त मानवीय मूल्यों के लिए एक बड़ा खतरा बन गए हैं।

साइबर अपराध के उद्देश्य –

वर्तमान जीवन में साइबर अपराधों के क्षेत्र में लगातार वृद्धि होती जा रही है। इन अपराधों के उद्देश्यों का सम्बन्ध आर्थिक, सैनिक, सांस्कृतिक अथवा व्यक्तिगत किसी भी पक्ष से हो सकता है। इसके प्रमुख उद्देश्य हैं–

(1) किसी एक देश के द्वारा दूसरे देश की सैनिक जासूसी करना तथा रक्षा सम्वन्धी सूचनाओं की चोरी करके एक किसी देश को लाभ पहुचाना होता है।

(2) वै"वीकरण व उदारीकरण के दौर में विभिन्न देशों के बीच होने वाली आर्थिक प्रतिस्पर्धा में साइबर अपराध एक प्रभावशाली साधन बनता जा रहा है।

(3) साइबर अपराध का एक प्रमुख उद्देश्य किन्ही दो देशों के बीच के राजनीतिक और आर्थिक सम्बन्धों में टकराव पैदा करना है।

(4) इसका एक विशेष आर्थिक उद्देश्य बड़े–बड़े इलैक्ट्रॉनिक जुआघरों की व्यवस्था तथा संचालन करना है।

(5) साइबर अपराध का एक प्रमुख उद्देश्य प्रमुख राजनीतिक दलों की गुप्त सूचनाए, प्रमुख राजनीतिज्ञों की वार्ता और गतिविधियों की जानकारी दूसरे राजनीतिक दल को देकर उसके हितों को हानि पहुँचाना है।

(6) बड़े–बड़े उद्योगपति भी दूसरे उद्योगपतियों के फार्मूले, पेटेन्ट और बाजार सम्बन्धी सूचनाएँ चोरी करने के लिए कम्प्यूटर प्रौद्योगिकी के उच्च ज्ञान से सम्बन्धित लोगों की सेवाओं का उपयोग करते हैं।

साइबर अपराध के प्रकार –

(1) स्पैम ईमेल – ईमेल पर अनेक प्रकार के स्पैम ईमेल आते है जिससे ईमेल भी होते है जो सिर्फ कम्प्यूटर को नुकसान पहुचाते है। उन ईमेल से सारे कम्प्यूटर में खराबी आ जाती है।

(2) हैकिंग – किसी की भी निजी जानकारी को हैक कर जैसे की उपयोगकर्ता का नाम या पासवर्ड और उसके ऑकड़ों में फेर बदल करना हैकिंग कहलाता है।

(3) फिशिंग – किसी के पास स्पैम ईमेल भेजकर उसकी अपनी निजी जानकारी प्राप्त करना और उस जानकारी से उसको नुकसान पहुचाना।

(4) वायरस फैलाना – साइबर अपराधी कुछ ऐसे सॉफ्टवेयर आपके कम्प्यूटर पर भेजते हैं जिसमें वायरस छिपे हो सकते हैं, इनमें वायरस वर्म, टार्जन हार्स, लाजिक हार्स आदि वायरस शामिल हैं। यह आपके कम्प्यूटर को काफी हानि पहुँचा सकता हैं।

(5) सॉफ्टवेयर पाइरेसी – सॉफ्टवेयर की नकल तैयार कर सस्ते दामों में बेचना भी साइबर क्राइम के अन्तर्गत आता है। इससे साफ्टवेयर कम्पनियों को भारी नुकसान उठाना पड़ता है साथ ही साथ आपके कीमती उपकरण भी ठीक से काम नहीं करते हैं।

(6) फर्जी बैंक कॉल – आपको जाली ईमेल, मैसेज या फोन कॉल प्राप्त हो जो आपकी बैंक डिटेल पूछा जाये कि आपके एटीम नंबर और पासवर्ड का आवश्यकता है और यदि आपके द्वारा यह जानकारी न दी गयी तो आपका खाता बन्द कर दिया जाएगा या लिंक पर सूचना दें। हालांकि किसी भी बैंक द्वारा ऐसी जानकारी कभी भी नहीं मांगी जाती है और भूलकर भी अपनी किसी भी इस प्रकार की जानकारी को इन्टरनेट या फोन काल ये माध्यम से साझा न करें।

(7) सोशल नेटवर्किंग साइटों पर अफवाह फैलाना– बहुत से लोग सोशल नेटवर्किंग साइटों पर पारिवारिक, सामाजिक, सांस्कृतिक, धार्मिक, राजनीतिक अफवाह फैलाने का काम करते हैं, लेकिन यूजर्स उनके इरादें समझ नही पाते हैं और जाने–अनजाने में ऐंसे लिक को शेयर करते रहते हैं, लेकिन यह भी साइबर अपराध और साइबर आतंकवाद की श्रेणी में आते हैं।

(8) साइबर बुलिंग – फेसबुक जैसी सोशल नेटवर्किंग साइटों पर अशोभनीय कमेंट करना, इंटरनेट पर धमकियां देना किसी का इस स्तर तक मजाक बनाना कि तंग हो जाये, इंटरनेट पर दूसरों के सामने शर्मिंदा करना, इसे साइबर बुलिंग कहते हैं । अक्सर बच्चे इसका शिकार होते है। इससे इनके सेहत पर भी असर पड़ता है।

सारणी–1 साइबर अपराध (2019, 2020,व 2021)

क्र0 सं0	राज्य / केंद्र शासित प्रदेश	2019	2020	2021	मध्य वर्ष अनुमानित जनसंख्या (लाख में)	कुल साइबर अपराध की दर (2021)
1	2	3	4	5	6	7
राज्य						
1	आंध्रप्रदेश	1886	1899	1875	528.5	3.5
2	अरुणाचल प्रदेश	8	30	47	15.4	3.1
3	असम	2231	3530	4846	351.6	13.8
4	बिहार	1050	1512	1413	1237.0	1.1
5	छत्तीसगढ़	175	297	352	296.1	1.2
6	गोवा	15	40	36	15.6	2.3
7	गुजरात	784	1283	1536	700.8	2.2
8	हरियाणा	564	656	622	296.0	2.1
9	हिमाचल प्रदेश	76	98	70	74.1	0.9
10	झारखंड	1095	1204	953	386.4	2.5
11	कर्नाटक	12020	10741	8136	669.9	12.1
12	केरल	307	426	626	355.4	1.8
13	मध्यप्रदेश	602	699	589	848.6	0.7
14	महाराष्ट्र	4967	5496	5562	1247.6	4.5
15	मणिपुर	4	79	67	31.7	2.1
16	मेघालय	89	142	107	33.0	3.2
17	मिजोरम	8	13	30	12.2	2.5
18	नागालैंड	2	8	8	22.0	0.4
19	ओड़ीशा	1485	1931	2037	457.9	4.4
20	पंजाब	243	378	551	304.0	1.8
21	राजस्थान	1762	1354	1504	795.7	1.9
22	सिक्किम	2	0	0	6.8	0.0
23	तमिलनाडु	385	782	1076	764.8	1.4
24	तेलंगाना	2691	5024	10303	377.7	27.3
25	त्रिपुरा	20	34	24	40.8	0.6
26	उत्तराखंड	11416	11097	8829	2317.0	3.8
27	उत्तर प्रदेश	100	243	718	114.4	6.3
28	पश्चिम बंगाल	524	712	513	982.9	0.5
	कुल राज्य	44511	49708	52430	13283.6	3.9
केंद्र शासित प्रदेश						
29	अंडमान एवं निकोबार द्वीप समूह	2	5	8	4.0	2.0
30	चण्डीगढ	23	17	15	12.1	1.2
31	दादरा तथा नगर हवेली और दमन एवं दीव	3	3	5	11.1	0.5
32	जम्मू एवं कश्मीर	115	168	356	207.0	1.7
33	लद्दाख	73	120	154	134.4	1.1
34	लक्षद्वीप	–	1	5	3.0	1.7
35	राष्ट्रीय राजधानी क्षेत्र दिल्ली	4	3	1	0.7	1.5
36	पुडुचेरी	4	10	0	15.8	0.0

	कुल केंद्र शासित प्रदेश	224	327	544	388.1	1.4
	भारत में कुल	44735	50035	52974	13671.8	3.9

स्रोत– राष्ट्रीय अपराध रिकॉर्ड ब्यूरो सन् 2021

भारतीय दण्ड संहिता (IPC) में साइबर अपराधों से है संबंधित प्रावधान –

(1) ईमेल के माध्यम से धमकी भरे संदेश भेजना– IPC article 503

(2) ईमेल के माध्यम से ऐसे संदेश भेजना जिससे मानहानि होती हो– IPC article 499

(3) फर्जी इलेक्ट्रानिक रिकार्डस का इस्तेमाल–IPC article 463

(4) फर्जी – वेबसाइट या साइबर फ्रॉड का इस्तेमाल–IPC article 420

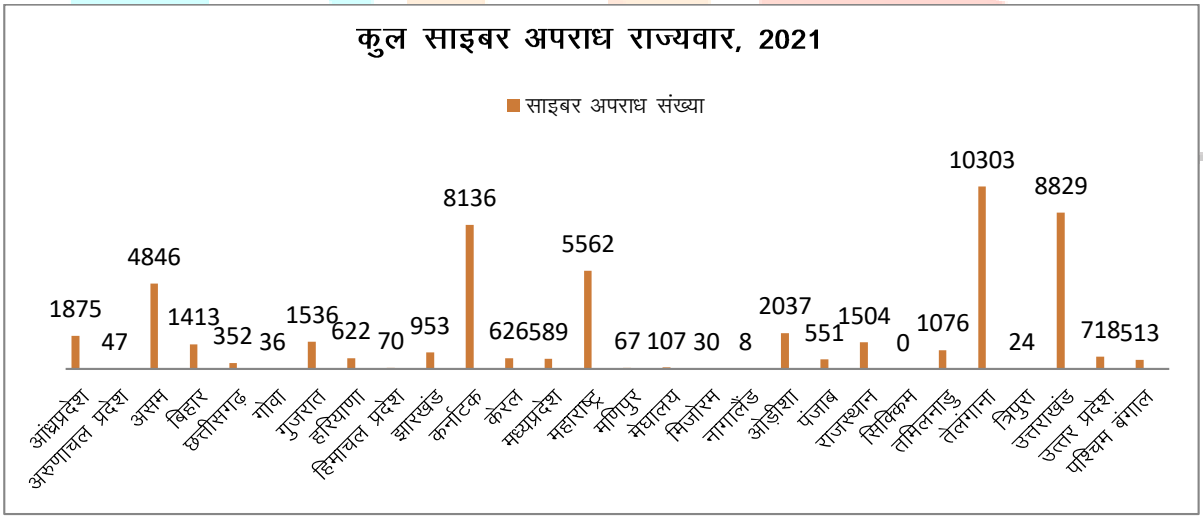
(5) चोरी–छुपे किसी के ईमेल पर नजर रखना– IPC article 463

(6) वेब जैकिंग– IPC article 463

(7) ईमेल का गलत के इस्तेमाल– IPC article 383

(8) दवाओं को ऑनलाइन का बेचना–NDPS act

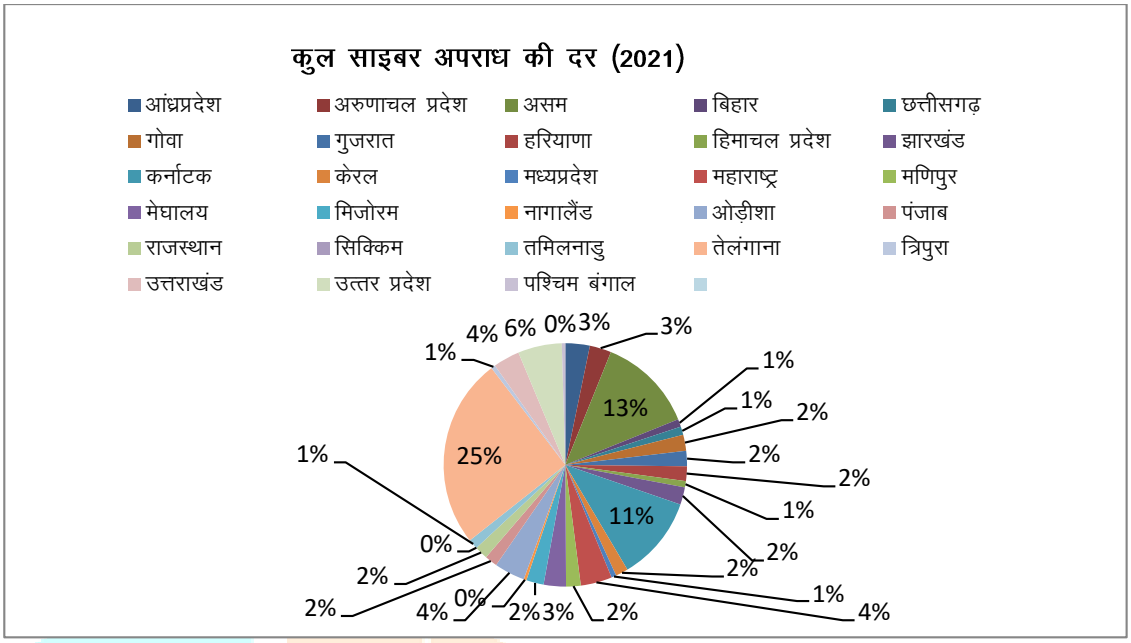
(9) हथियारों की ऑनलाइन खरीद–बिक्री arms act.



स्रोत– राष्ट्रीय अपराध रिकॉर्ड ब्यूरो सन् 2021

चित्र–1

कुल साइबर अपराध की दर राज्यवार, 2021



स्रोत– राष्ट्रीय अपराध रिकॉर्ड ब्यूरो सन् 2021

चित्र–2

सारणी–1 के आंकड़ों का विश्लेषण साइबर अपराध के पैटर्न और प्रवृत्तियों को समझने में सहायक हो सकता है। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो 2021 के अनुसार, भारत में कुल साइबर अपराध 52974 (3.9 प्रति"ात,) हुआ है। के विभिन्न राज्यों से प्राप्त ऑकड़ों में तेलंगाना साइबर अपराध में प्रथम स्थान रखता है, चित्र 1, 2 व सारणी 1 के अनुसार तेलंगाना में 10303 (27.3 प्रति"ात) जो उच्चतम साइबर अपराध को प्रदर्"ात करता है। द्वितीय स्थान पर असम 4846 (13.8 प्रति"ात) व तृतीय स्थान पर कर्नाटक 8136 (12.1 प्रति"ात) जो उच्च साइबर अपराध को प्रदर्"ात करता है। नागालैण्ड 8 (0.4 प्रति"ात), पं0 बंगाल 513 (0.5 प्रति"ात) व त्रिपुरा 24 (0.6 प्रति"ात) जो न्यूनतम साइबर अपराध को प्रदर्"ात करता है। 2021 में सिक्किम में एक भी साइबर अपराध नही हुआ।

सूचना तकनीक कानून, 2000 के अन्तर्गत साइबरस्पेस में क्षत्राधिकार संबंधी प्रावधान –

सूचना तकनीक कानून के अन्तर्गत उल्लिखित आरोपों की सूची निम्न है–

(1) कम्प्यूटर संसाधनों से छेड़छाड़ की कोशिश – धारा 65

(2) कम्प्यूटर में संग्रहित डाटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश– धारा 66

(3) संवाद सेवाओं के माध्यम से प्रतिबंधित सूचनाएं भेजने के लिए दंड का प्रावधान– धारा 66 (ए)

(4) कम्प्यूटर या अन्य किसी इलेक्ट्रानिक गैजेट से चोरी की गई सूचनाओं का गलत तरीके से हासिल करने के लिए दंड प्रावधान–धारा 66 (बी)

(5) किसी की निजता को भंग करने के लिए दंड का प्रावधान–धारा (इ)

(6) आपत्तिजनक सुचनाओं क प्रकाशन स जुड़े प्रावधान–धारा 67

(7) इलेक्ट्रानिक या अश्लील सूचनाओं को प्रकाशित या प्रसारित करने का प्रावधान –धारा 67 (ए)

(8) फर्जी डिजिटल हस्ताक्षर का प्रका"ान प्रावधान –धारा 73।

भारतीय दण्ड संहिता (आईपीसी) में साइबर अपराधों से संबंधित प्रावधान

(1) ईमेल के माध्यम से धमकी भरे संदेश भेजना–आईपीसी की धारा 503

(2) ईमेल के माध्यम से ऐसे संदेश भेजना, जिससे मानहानि होती हो–आईपीसी की धारा 499

(3) फर्जी इलेक्ट्रॉनिक रिकॉर्ड्स का इस्तेमाल–आईपीसी की धारा 463

(4) फर्जी वेबसाइट्स या साइबर फ्रॉड–आईपीसी की धारा 420

(5) चोरी–छुपे किसी के ईमेल पर नजर रखना–आईपीसी की धारा 463

(6) वेब जैकिंग–आईपीसी की धारा 383

(7) ईमेल का गलत इस्तेमाल–आईपीसी की धारा 500

(8) दवाओं को ऑनलाइन बेचना–एनडीपीएस एक्ट

(9) हथियारों की ऑनलाइन खरीद–बिक्री–आर्म्स एक्ट

साइबर अपराध से सुरक्षा –

साइबर अपराध पर नियन्त्रण रखने के लिए कुछ विशेष उपाय करना अत्यन्त आवश्यक है जो निम्न हैं–

(1) सुरक्षित पासवर्ड मजबूत और जटिल पासवर्ड का उपयोग करें, जिसमें अक्षर, अंक, और विशेष वर्ण शामिल हों।

(2 नियमित रूप से अपने ऑपरेटिंग सिस्टम और सॉफ्टवेयर को अपडेट रखें। अपने सिस्टम को सुरक्षित रखने के लिए प्रभावी एंटीवायरस और एंटी–मालवेयर सॉफ्टवेयर का उपयोग करें।

(3) संदिग्ध ईमेल या लिंक पर क्लिक करने से बचें और अनजान स्रोतों से फाइलों को डाउनलोड न करें। नेटवर्क और कंप्यूटर को सुरक्षित रखने के लिए फायरवॉल का उपयोग करें।

(4) साइबर अपराध को रोकने के लिए कम्प्यूटर प्रौद्योगिकी का उच्च ज्ञान रखने वाली एक प्रशिक्षित टीम को संगठित करना आवश्यक है। किसी भी प्रकार के साइबर अपराध की सूचना मिलने पर इसके द्वारा अपराध के स्रोत की जानकारी प्राप्त करके अपराधी को दण्डित किया जा सकता है।

(5) सरकार द्वारा ''सूचना प्रौद्योगिकी अधिनियम" पारित करने से यह आशा की गई थी कि इसकी सहायता से साइबर अपराध को कम करने में इसकी उपयोगी भूमिका हो सकेगी। इसके बाद भी यह अधिनियम इस कारण प्रभावपूर्ण नहीं बन सका कि इससे सम्बन्धित अधिकांश प्रावधान अधिक व्यावहारिक नहीं है। वर्तमान में इस अधिनियम को अधिक व्यावहारिक बनाने की जरुरत है ताकि साइबर अपराधियों को अति शीघ्र दण्डित किया जा सके।

(6) कम्प्यूटर द्वारा गबन व जालसाजी जैसे अपराधो को तभी कम किया जा सकता है जब विभिन्न लेखा परीक्षकों के लिए कम्प्यूटर का उच्च स्तरीय ज्ञान आवश्यक हो। बड़ी–बड़ी कम्पनियों और बैंको के सभी आकड़े अब कम्प्यूटर में ही सुरक्षित रहते हैं।

न्यायिक समाधान

साइबर अपराध रिपोर्टिंग– साइबर अपराध का सामना करने पर, इसे तुरंत स्थानीय पुलिस (1093) या साइबर क्राइम सेल में रिपोर्ट करें।

न्यायिक प्रक्रिया– न्यायिक प्रक्रिया के तहत अपराधियों के खिलाफ कानूनी कार्रवाई की जाती है, जिसमें सबूत एकत्र करना और केस की सुनवाई शामिल होती है।

साइबर लॉ– विभिन्न देशों में साइबर अपराध के खिलाफ कानूनी ढांचे को समझना और अपनाना महत्वपूर्ण है। जैसे भारत में, सूचना प्रौद्योगिकी अधिनियम (IT Act) साइबर अपराधों के लिए कानूनी ढांचा प्रदान करता है।

मुआवजा– पीड़ितों को न्याय दिलाने के लिए मुआवजे की प्रक्रिया भी होती है, जिसमें नुकसान की भरपाई की जाती है।

निष्कर्ष –

आधुनिक युग में सूचना एवं संचार प्रौद्योगिकी ने एक वैश्विक समस्या प्रस्तुत की है जिसका समाधान अति आवश्यक है। हांलाकि साइबर अपराध की प्रकृति इतनी एकाकी और अज्ञात होती है कि इनसे सम्बन्धित वास्तविक अपराधी को खोज पाना एक कठिन समस्या है। साइबर अपराध के विरुद्ध यदि प्रारम्भिक स्तर पर ही पर्याप्त कार्यवाही नहीं की जाती है तो मानवाधिकारों और मानवीय मूल्यों का हनन होने लगेगा। साइबर अपराध के विभिन्न उद्देश्य होते हैं और ये अपराधी के लक्ष्यों और प्रवृत्तियों पर निर्भर करते हैं। इन अपराधों से सुरक्षा के लिए त्वरित और प्रभावी उपाय अपनाना आवश्यक है, साथ ही कानूनी और न्यायिक कार्रवाई भी महत्वपूर्ण होती है।

सन्दर्भ सूची

1. Jain, Rohit Arvind (2018) “Cyber Crime & Law", Evincepub Publishing. ISBN&109789387905726

2. Chander, Harish, “Cyber Laws and IT Protection

3. भारतीय दण्ड संहिता (आईपीसी) में साइबर अपराधों

4. Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations-.Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

5. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing

6. www.ncrb.org.in (2021)

7. www.wikipedia.in

8. www. google.com

9.https://bh.wikipedia.org/wiki