International Journal of Advance and Applied Research (IJAAR)
Peer Reviewed Bi-Monthly

ISSN – 2347-7075
Impact Factor – 7.328
Vol.9 No.4 Mar – Apr 2022

भारतातील सायबर गुन्हेगारी: एक अभ्यास

डॉ.अर्जुन जाधव

डी. के. ए. एस. सी. कॉलेज, इचलकरंजी.

प्रास्ताविक:

प्रत्येक समाजात प्रचलित असणारा कायदा आणि मूल्य यांच्या विरुद्धचे वर्तन म्हणजे गुन्हा होय सद्यस्थितीमध्ये संपूर्ण समाज व्यवस्थेसाठी इंटरनेटचावापर अनिवार्य झाला आहे. प्रत्येक व्यक्ती संगणक, लॅपटॉप, मोबाइल किंवा अन्य इलेक्ट्रॉनिक डिवाइस इत्यादींच्या माध्यमातून इंटरनेटचा वापर करून जगासोबत जोडलेला आहे. प्रत्येक इंटरनेट वापरकर्त्याला सायबर गुन्हा म्हणजे काय तसेच त्याचे प्रकार माहिती असणे अत्यंत आवश्यक आहे. इंटरनेटचा वापर करत असताना तो सुरक्षितरित्या केला गेल्यास त्यापासून कोणताही धोका होत नाही. परंतु या संदर्भातील नियम आणि अटी माहिती नसतील किंवा अनावधानाने काही माहिती प्रसारित झाल्यास गुन्ह्याची नोंद होऊ शकते. म्हणून प्रत्येक इंटरनेट वापरकर्त्यालासायबर गुन्हयांच्या बद्दल माहिती असणे, तसेच सायबर कायद्याबद्दल माहिती असणे अत्यंत आवश्यक आहे.सायबर गुन्हेगारीचा नकारात्मक परिणाम समाजावर होत आहे.

सायबर गुन्ह्यांमध्ये तंत्रज्ञानाचा वापर केला जातो यावेळी तंत्रज्ञान हे माध्यम म्हणून वापरले जाते तसेच सर्वात महत्वाचे म्हणजे, गुन्हा करणारी व्यक्ती, म्हणजेच गुन्हेगार तंत्रज्ञानाचा आधार घेऊन आपल्या प्रत्यक्ष उपस्थिती शिवाय गुन्हा घडवून आणत असते

माहिती तंत्रज्ञानाचे युग विकसित झाल्यानंतर संगणक इंटरनेट आणि सोशल मीडियाचा वापराशिवाय मानवाला जीवन जगणे शक्य नाही. ज्याप्रमाणे इंटरनेट सोशल मीडिया यांचा वापर वाढत गेला, त्याच प्रमाणे सायबर गुन्ह्यांचे प्रमाणही वाढण्याची भीती व्यक्त होत आहे गुन्हेगारी प्राचीन काळापासून जरी चालत आली असली तरी गुन्हे होऊ नयेत यासाठी विविध कायद्यांची निर्मिती करण्यात आली आहे सायबर गुन्हा करणाऱ्यांना सायबर गुन्हेगार म्हटले जाते.

सायबर क्राईम मध्ये संगणक आणि इंटरनेटचा वापर करून गुन्हा केला जातो थोडक्यात, संगणक किंवा इंटरनेटच्या माध्यमातून केलेल्या गुन्ह्याला सायबरक्राईम असे म्हणतात. उदा. हॅकिंग, डेटा चोरी, पायरेसी इत्यादी

> "ज्या प्रकारच्या गुन्ह्यांमध्ये प्रत्यक्ष उपस्थित न राहता गुन्हेगारांकडून संगणक मोबाईल, इंटरनेट इत्यादींचा माध्यम म्हणून वापर केला जातो आणि गुन्हा केला जातो, त्याला सायबर गुन्हा असे म्हणतात."

उद्दिष्टे:

1. भारतातील सायबर गुन्हेगारीची सद्यस्थिती अभ्यासणे.
2. सायबर गुन्ह्यांचेप्रकार स्पष्ट करणे

3. सायबर गुन्हावरील उपाय योजना स्पष्ट करणे.

संशोधनपद्धती:

प्रस्तुत संशोधन लेखासाठी दुय्यम साधनसामग्रीचा वापर करण्यात आलेला आहे सायबर गुन्हा संकल्पना, भारतातील सायबर गुन्हेगारीची सद्यस्थिती, सायबर गुन्ह्यांचे प्रकार व त्यावरील उपाय योजना अभ्यासण्यासाठी शासकीय वेबसाईट, संदर्भग्रंथसंशोधन पेपर इत्यादींचा आढावा घेण्यात आला आहे.

भारतातील सायबर गुन्हेगारीची सद्यस्थिती:

इंटरनेटच्या माध्यमातून सायबर स्पेस मध्ये केले जाणारे गुन्हे म्हणजे सायबर गुन्हे होय़ माहिती तंत्रज्ञानाचा चुकीचा वापर करून त्यामुळे समाजातील इतर व्यक्तींचे नुकसान केले जाते याला सायबर गुन्हे असे म्हणतात. भारतामध्ये माहिती तंत्रज्ञान कायदा 2000 हा कायदा आयटी ॲक्ट 2000 म्हणून ओळखला जातो. प्रामुख्याने हॅकिंग सारख्या सायबर गुन्ह्यांवर नियंत्रण मिळवण्यासाठी हा कायदा करण्यात आलेला दिसू येतो. त्यासोबतच बँकिंग क्षेत्रातील ऑनलाइन गुन्हेगारी टाळण्यासाठी व त्याला प्रतिबंध करण्यासाठी हा कायदा उपयुक्त आहे.

भारतातील सायबर गुन्हे (राज्यनिहाय) 2020			
राज्य	**संख्या (दर लाखामागे)**	**राज्य**	**संख्या (दर लाखामागे)**
आंध्र प्रदेश	1899	महाराष्ट्र	5496
आसाम	3530	मेघालय	142
बिहार	1512	ओरिसा	1931
छत्तीसगढ	297	पंजाब	378
गुजरात	1283	राज्यस्थान	1354
हरियाना	656	सिक्कीम	0
झारखंड	1204	तामिळनाडू	782
कर्नाटक	10741	तेलंगाना	5024
केरळ	426	उत्तर प्रदेश	11097
मध्य प्रदेश	699	उत्तराखंड	243

(Source: https://ncrb.gov.in/en/crime-in-india)

सायबर गुन्ह्याचे प्रकार:

सायबर गुन्ह्यामध्ये प्रामुख्याने हॅकिंग़सायबर स्टॉकिंग, आयडेंटिटी थीफ, डेटा हॅकिंग, वायरस, फिशिंग इत्यादी प्रकार दिसून येतात.

- **हॅकिंग:**

यामध्ये गुन्हेगार हा वापरकर्त्याच्या परवानगीशिवाय त्यांची वैयक्तिक आणि संवेदनशील माहिती चोरून त्याचा गैरवापर करतो ज्यामुळे वापरकर्त्याला धोका निर्माण होतो.

- **सायबर स्टॉकिंग:**

यामध्ये एखाद्या व्यक्तीला ऑनलाइन त्रास दिला जातो किंवा सोशल मीडियाच्या वेबसाईट वरून त्रास दिला जातो. ज्यामध्ये वाईट संदेश किंवा ईमेल एखाद्याला पाठविले जाऊ शकतात. प्रामुख्याने लहान मुले आणि स्त्रिया यांना यामध्ये विक्टिम बनवले जाते. त्यांची वैयक्तिक माहिती ,फोटो , पत्ता इत्यादींचा वापर करून त्यांना ब्लॅकमेल करण्याचा प्रयत्न केला जातो . सोशल मीडिया प्लॅटफॉर्मवरून अशा प्रकारच्या सायबर गुन्हेगारीचे प्रमाण मोठ्या प्रमाणात असल्याचे दिसून येते.

- **आयडेंटिटी थीफ :**

यामध्ये प्रामुख्याने बँकिंग सेवांमधील ऑनलाईन गुन्हेगारीचा समावेश होतो. डेटाची चोरी करणे, एखाद्याच्या बँकेचा खाते क्रमांक, क्रेडिट कार्ड, डेबिट कार्ड, इंटरनेट बँकिंग संदर्भातील सर्व तपशील वैयक्तिक माहिती किंवा इतर संवेदनशील माहिती चोरली जाते आणि त्या माहितीचा वापर करून विक्टिम चे आर्थिक नुकसान केले जाते.

- **डेटा हॅकिंग:**

यामध्ये एखाद्या व्यक्तीच्या परवानगीशिवाय संगणक इंटरनेट इत्यादीं वरून डेटा कॉपी करणे किंवा त्याचा प्रसार करणे इत्यादी गोष्टी डेटा चोरी या गुन्ह्यांमध्ये दिसून येतात किंवा पेन ड्राईव्ह, मेमरी कार्ड, हार्ड डिस्क इत्यादींच्या मदतीने डेटा चोरी केला जातो.

- **वायरस:**

एखाद्या संगणकामध्ये विशिष्ट प्रोग्रॅम द्वारे प्रवेश केला जातो आणि त्या संगणकामधील माहिती विस्कळीत केली जाते किंवा तिचा फॉर्मेट बदलला जातो, जेणेकरून वापरकर्त्याला नुकसान सहन करावे लागते.

- **फिशिंग:**

हा सायबर गुन्ह्याचा एक प्रकार आहे यामध्ये पीडित व्यक्तीला ई-मेल पाठवून गोपनीय माहिती मिळविण्याचा प्रयत्न केला जातो आणि त्या व्यक्तीची फसवणूक केली जाते.

- **स्पॅमिंग:**

यामध्ये प्रामुख्याने वापरकर्त्याला एकदा ई-मेल पाठविला जातो आणि त्या ईमेलच्या माध्यमातून एखादी लिंक किंवा प्रोग्रॅम पाठविला जातो, ज्याचा परिणाम म्हणून संगणकावरती वायरसचा हल्ला होऊ शकतो आणि सिस्टम मधील विविध फाइल्स किंवा माहिती चोरी होते.

- **पायरेसी:**

पायरेसी हासुद्धा एक सायबर गुन्हा आहे एखाद्या सॉफ्टवेअरची कॉपी केली जाते आणि ती कॉफी कमी दरामध्ये विकली जाते यामुळे सॉफ्टवेअर तयार करणाऱ्या कंपन्यांचे मोठ्या प्रमाणात नुकसान होते

- **फ्रॉड बँक कॉल:**

या प्रकारच्या सायबर गुन्ह्यांमध्ये गुन्हेगारहा आपण बँकेतील कर्मचारी किंवा महत्त्वाची व्यक्ती आहे असे भासवतो आणि कॉल वरून समोरील व्यक्तीची क्रेडिट कार्ड डेबिट कार्ड किंवा इंटरनेट बँकिंग संदर्भातील सर्व माहिती विचारून घेतो आणि त्या माध्यमातून ग्राहकाच्या बँक खात्यातून पैसे चोरले जातात यामध्ये ग्राहकांवरती दबावतंत्राचा वापर केला जातो. उदारणार्थ अशा प्रकारची माहिती ग्राहकांनी जर दिली नाही तर त्यांना आर्थिक स्वरूपातील दंड किंवा त्यांचे खाते बंद केले जाईल

- **अफवा पसरविणे:**

काही वेळा सोशल मीडियाचा वापर करून सोशल नेटवर्किंग साईट्स वरून सामाजिक धार्मिक राजकीय अफवा पसरविल्या जातात आणि त्यामुळे समाजामध्ये तेढ निर्माण होते.

- **सायबर बुलींग:**

या प्रकारच्या सायबर गुन्ह्यांमध्ये सोशल साईट्सवर ती एखाद्याचा छळ केला जातो किंवा त्याला त्रासदायक किंवा वाईट वाटेल अशी विधाने पसरविली जातात विशेषतः मुले आणि इंटरनेटचा वापर करणारे नवीन लोक अशा प्रकारच्या गुन्ह्याला बळी पडत असते दिसून येतात

सायबर गुन्ह्यावरील उपाय:

राष्ट्रीय सायबर क्राईम रिपोर्टिंग पोर्टल:

भारतामध्ये राष्ट्रीय सायबर क्राईम रिपोर्टिंग पोर्टल वरती सायबर गुन्हयांची तक्रार करता येते. यासाठी भारत सरकारने तक्रार नोंद करण्याची सुविधा उपलब्ध करून दिली आहे. यासोबतच इंटरनेटचा वापर करत असताना लहान मुलांनी कोणती काळजी घेणे आवश्यक आहे,याबाबतची माहिती प्रसारित करण्यात आली आहे. प्रसार माध्यमांचा सोशल मीडियाचा सुरक्षित वापर कसा करावा, याबाबतच्या सूचना या पोर्टल वरती देण्यात आलेले आहेत.

- नेहमी विश्वसनीय स्त्रोताद्वारे किंवा आपलिकेशन द्वारे सॉफ्टवेअर डाऊनलोड करावे.
- आपल्या संगणकावर ती अँटीव्हायरस इन्स्टॉल करावा.
- महत्वपूर्ण डेटा किंवा फाईल या बॅकअप मध्ये सुरक्षित ठेवाव्यात
- कंप्यूटर मधील फायरवॉल नेहमी ऑन ठेवावी.
- आपण वापरत असलेली ऑपरेटिंग सिस्टिम नेहमी अपडेट करावे.
- आपल्या संगणकाचा किंवा कोणत्याही ऑनलाइन खात्याचा पासवर्ड सहज ट्रेक करता येईल असा नसावा.
- प्रत्येक अकाऊंटचा पासवर्ड वेगळा असावा.
- काही नियमित वेळेनंतर पासवर्ड बदलावा.

- स्पॅमिंग,फिशिंग मेल ओळखा.
- अनोळखी ईमेलमधील लिंकवर कधीही क्लिक करू नये.
- कोणत्याही वेबसाइटवर आपली वैयक्तिक,गोपनीय माहिती अपलोड करू नका.
- ऑनलाइन खरेदीकरताना विश्वसनीय साइटवरून खरेदी करने.
- मोफत वायफाय वापरणे टाळावे.

राष्ट्रीय सायबर क्राईम प्रशिक्षण केंद्र

सायबर गुन्ह्यांचा शोध घेणे तसेच त्यांना प्रतिबंध करण्यासाठी राष्ट्रीय सायबर गुन्हा प्रशिक्षण केंद्र महत्त्वपूर्ण कामगिरी बजावत आहे.याची मुख्य उद्दिष्टे पुढीलप्रमाणे

- सायबर गुन्ह्यांचा शोध घेणे
- सायबर गुन्हा संदर्भातील तक्रारींची नोंद करणे
- सायबर गुन्ह्यांच्या संदर्भात आलेल्या तक्रारींचे निवारण करणे
- समाजामध्ये सायबर गुन्ह्यांच्या बाबतीत जाणीव जागृती निर्माण करणे.
- सायबर स्पेस ची सुरक्षितता वाढविण्यासाठी प्रयत्न करणे.

या पोर्टल वरती सायबर गुन्हा विरोधात कार्य करण्यासाठीच्या विविध प्रशिक्षण कोर्सेसची यादी देण्यात आलेली आहे

माहिती तंत्रज्ञान अधिनियम 2000:

माहिती तंत्रज्ञान अधिनियम 2000 मध्ये प्रामुख्याने काही गोष्टींचा अंतर्भाव करण्यात आलेला आहे

- कलम 66 अ नुसार एखाद्या व्यक्तीबद्दल त्रासदायक संदेश पाठविणे किंवा खोटी माहिती पसरविणे, ज्यामुळे मानसिक त्रास, मानहानी, शत्रुत्व निर्माण होण्याची शक्यता असते किंवा त्या संदेशाचे मूळ स्त्रोत लपविण्याचा प्रयत्न करणे, अशा कृती केल्यास त्या व्यक्तीला तीन वर्षांचा कारावास आणि दंडाची तरतूद या कायद्यामध्ये आहे.
- कलम 66 क नुसार एखाद्याचा पासवर्ड चोरी करून त्याच्या परवानगीशिवाय त्या पासवर्डचा वापर करणे किंवा फिंगर प्रिंट चा वापर करणे ,यासाठी सुद्धा तीन वर्ष कारावास आणि आर्थिक दंडाची तरतूद करण्यात आली आहे.
- कलम 66 ड नुसार एखाद्या व्यक्तीचा डुप्लिकेट मेल आयडी किंवा प्रोफाइल तयार करून त्या व्यक्तीचे नावे ई-मेल पाठविणे एसएमएस पाठविणे, या मध्ये 3 वर्ष कारावास आणि आर्थिक दंडाची तरतूद करण्यात आली आहे.

सद्यस्थितीमध्ये सायबर गुन्ह्यांची संख्या वाढत असलेली दिसून येते त्यामुळे सायबर कायद्याचे महत्त्व वाढलेले दिसून येते. प्रत्येक व्यक्तीला न्यायालयामध्ये बाजू मांडण्यासाठी कायदेशीर असलेल्यांसाठी सायबर लॉयर सुद्धा महत्त्वाचा असलेला दिसून येतो. यादृष्टीने बौद्धिक संपदा कायदा, सॉफ्टवेअर पेटंट यासारख्या गोष्टी महत्त्वपूर्ण भूमिका बजावत असलेल्या दिसून येतात.

भारतामध्ये सायबर गुन्ह्याबद्दल तक्रार करण्यासाठी भारत सरकारच्या सायबर क्राइम पोर्टलवर वेबसाइटवर ऑनलाइन तक्रार नोंद करता येते. तसेच भारतातील महत्वपूर्ण शहरांमध्ये सायबर सेलची निर्मिती करण्यात आली . तसेच हेल्पलाईन सुरु केली आहे

संदर्भसूची:

1. Ahuja Ram (2001) “Research Methods”, Rawat Publications,Jaipur
2. Kothari C.R.(1989), Research Methodology: Methods and Techniques, willey Eastem, Bangalore.
3. A Handbook for Adolescents/ Students on Cyber Safety, Ministry of Home Affairs Government of India..2018.
4. https://mediavartanews.com/2020/10/18/what-is-cyber-crime-and-types-of-cybercrime/ retrieved on 05/05/2022
5. https://sandeepwaghmore.in/what-is-cyber-crime. retrieved on 07/05/2022
6. https://ncrb.gov.in/en/crime-in-india. retrieved on 07/05/2022