Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0054

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

भंडारा जिल्हयातील सायबर क्षेत्रातील वाढलेले गुन्हे : एक समस्या

संशोधनकर्ता
प्रा. सुनिल बी. उईके
सहा. प्राध्यापक,
आठवले समाजकार्य महाविद्यालय, भंडारा
Mol No. 8149365817
E-mail – 72suniluikey@gmail.com

सारांश:—

संगणकीय क्षेत्रात सायबर क्राईमचा झालेला शिरकाव हा अनेक अनर्थ व संकटांना आमंत्रण देणारा आहे. साधारणत: सर्वसामान्य नागरिकांचा असा समज आहे की, सायबर क्राईमशी आपला काही संबंध नाही. या समजामुळे नागरिक सायबर क्राईमबाबत अनभिज्ञ आहेत. पण जरा सूक्ष्म विचार करून पाहिलं तर आपल्याला रोजच या साबयर क्राईमचा सामना करावा लागतो. आपल्या ई—मेलवर स्पॅममेल येत असतात, मोबाईलवर अनावश्यक कॉल, मेसेजेस येतात, नेट बँकिंग अकाऊंट असेल तर त्याचा पासवर्ड, आय.डी. हॅक होतो. हे सर्व प्रकार सायबर गुन्हेगारीमध्ये मोडतात.

प्रस्तावना:

गुन्हेगारी क्षेत्रात समाजातील इतर क्षेत्राप्रमाणेच नवनविन बदल होत असतात. गुन्ह्यचे नवीन प्रवाह, नवीन प्रकार घडतांना आढळतात. जग जसे बदलत आहे तसेच गुन्हेगारीची तंत्रे, स्वरूपही बदलत असताना दिसत आहे.

गेल्या तीन दशकांमध्ये जगातील जवळपास सर्वच देशांमध्ये क्षेत्राचा शिरकाव व विकास झालेला दिसतो. झपाट्याने वाढणाऱ्या संगणकीकरणामुळे आणि संगणक क्रांतीने जगाला एका खेड्यत रूपांतरीत केले आहे. तंत्रज्ञानाचा उपयोग सर्वच क्षेत्रात मोठ्य प्रमाणावर होताना दिसतो आहे, याचे कारण त्याची गती आणि जगातील अंतर नष्ट करण्याची कुवत होय.

संगणक अथवा माहिती तंत्रज्ञानाचा वापर गैरप्रकारांसाठी, गुन्हेगारीसाठी केला जात आहे यासच 'सायबर गुन्हा' म्हटले जाते. इंटरनेटच्या सकारात्मक वापराबरोबरच दुष्प्रवृतींद्वारे केला जाणारा दुरूपयोग सर्व सामान्याचे जीवन, राष्ट्राची सुव्यव्यवस्था, अर्थव्यवस्था डळमळीत करू शकतो. इंटरनेटद्वारे केल्या जाणाऱ्या गैरवापरास सायबर क्राईम म्हटले जाते.

तार्किक विचार शक्ती, कल्पना शक्ती आणि स्मृती ही मानवाला लाभलेली अफाट आणि उद्भूत अशी देणगी म्हणावी लागेल. मानावाने आपल्या या शक्तीच्या जोरावर कल्पना व क्षमतांचा विस्तार करू शकणाऱ्या संगणकाचा शोध लावला. गेल्या सुमारे ५० वर्षाच्या अवधीत संगणकाने मानवी आयुष्य पार बदलले आहे. इंटरनेटच्या उदयामुळे तर जग अधिक जवळ झाले आहे. ई—मेल, व्हिडिओ कॉन्फरन्सिंग, मेसेजिंग, चाटींग, स्मार्ट फोन हे शब्द सर्वसामान्यांच्या अगदी परिचयाचे बनले आहेत. दैनंदिन जीवनात या गोष्टींने मोठ्या प्रमाणात आक्रमण केले आहे. असे म्हटले तर ते वावगे ठरणार नाही. इंटरनेटच्या सकारात्मक वापराबरोबरच दुष्प्रवृतींद्वारे केला जाणारा दुरूपयोग सर्व सामान्याचे जीवन, राष्ट्राची व्यवस्था, अर्थव्यवस्था डळमळीत करू शकतो. इंटरनेटद्वारे केल्या जाणाऱ्या गैरवापरास सायबर क्राईम म्हटले जाते.

संगणकाच्या माहिती तंत्रज्ञानाच्या माध्यमातून इंटरनेटद्वारे आपण प्रत्यक्ष एकेठिकाणी बसून जगातील कोणत्याही व्यक्तीपर्यंत पोहोचू शकतो. त्यासाठी प्रत्यक्ष जाण्याची गरज नाही. असे तंत्रज्ञान असणारा समाज ''सायबर समाज'' म्हणून ओळखला जातो व अशा समाजात अशा तंत्रज्ञानाचा वापर करून केलेला गुन्हा म्हणजे ''सायबर गुन्हा'' होय. या प्रकारची गुन्हेगारी म्हणजे 'सायबर गुन्हेगारी' होय.

याबाबत कॉम्प्यूटर सोसायटी ऑफ इंडियाच्या सॉफ्टवेअर विभागाचे अध्यक्ष दिपक शिकारपूर आपल्या ''सायबर कायदा आणि आपण'' या पुस्तकात म्हणतात. ''संगणकीय माहितीच्या गैरवापर करून वा अनाधिकृतरित्या दुसऱ्याच्या संगणकावर प्रवेश करून माहितीचे नुकसान करणे वा ती नष्ट करणे असे विकृत प्रकार गेली १० वर्षे सायबर विश्वास सर्रास चालू आहेत.

थोडक्यात चोर ज्याप्रमाणे घरात घुसून पैसे, सोनंनाणं, वस्तूंची चोरी करतो त्याचप्रकारे सायबर गुन्हेगार बेकायदेशिररित्या दुसऱ्या व्यक्ती वा संस्थेच्या संगणकाच्या प्रणालीत शिरकाव करून त्यातील माहिती, ज्ञान व अन्य सामग्री बिघडतात, नष्ट करतात किंवा चौर्यकर्माने फाईल्य, प्रोग्रॅम्स स्वत:साठी उपयोगात आणतात. मात्र हे करण्यासाठी संगणक बुध्दीमत्ता आणि ज्ञान अपरिहार्य आहे. त्याशिवाय हे शक्य नाही. सायबर गुन्हा संगणक अज्ञानी माणूस करूच शकत नाही.

सायबर गुन्ह्यत चोरीचा माल म्हणजे दुसऱ्याच्या संगणकातील फाईल्स, प्रोग्रॅम्स माहिती चोरून घेणे, बेकायदेशिररित्या चोर मार्गाने ''पासवर्ड'' मिळवून दुसऱ्याच्या संगणकात शिरून माहिती, ज्ञान लुटणे म्हणजे 'सायबर गुन्हा' होय.

सायबर क्राईमच्या माध्यमातून सर्वसामान्य नागरिक ते एखाद्या देशाची सर्व प्रकारची व्यवस्था ढासळू शकते इतकी त्याची व्याप्ती व आवाका गंभीर स्वरूपाचा आहे. साधारणत: सायबर क्राईमचे ५ प्रकार दिसून येतात. त्यापैकी पहिला 'डेटा थेप्ट' करणे. या प्रकारात सायबर, गुन्हेगार अथवा हॅकर एखाद्या संगणकातील माहिती पेनड्राईव्ह, साडीचा वापर करून चोरतो. या माहितीचा गैरवापर होऊ शकतो, अथवा हि माहिती विकली जाते. कार्पोरेट क्षेत्रात अशा स्वरूपाचे गुन्हे वारंवार घडतात. या गुन्ह्यंचे प्रमाण ३१ टक्के इतके असल्याचे दिसते.

दुसरा प्रकार आहे सायबर स्टॉकिंग ई–मेल अथवा फेसबुक, याहू मेसेन्जर सारख्या सोशल साईटद्वारा चॉटिंग वा सर्फिंगच्या माध्यमातून गुन्हेगार आपली संगणकीय ओळख (आय.डी.) पासवर्ड हॅक करतात. विशिष्ट व्हायरस आपल्या संगणकात डाऊनलोडसाठी पाठवून आपली संपूर्ण वैयक्तिक माहिती, संगणकावर केल्या जाणाऱ्या सर्व क्रिया, बँक अकाऊंट नंबर, पासवर्ड चोरून नागरिकांना मोठ्य प्रमाणात आर्थिक भुर्दंड सोसावा लागल्याची अनेक उदाहरणे आहेत.

तिसरा प्रकार आहे हॉकिंग कोणत्याही संगणक, संगणक प्रणालीमध्ये अनाधिकृत केलेला प्रवेश म्हणजे हॉकिंग आणि तो करणारा हॅकर. सायबर क्राईममध्ये हॉकिंग व हॅकर या दोन संकल्पना वारंवार पुढे येतांना दिसतील. ई–कॉमर्स साईटवर हॉकिंगचे प्रमाण अधिक आहे. हॉकिंगला 'डिनायल ऑफ सर्व्हिस' म्हटले जाते. एखाद्या ई–मेलद्वारे व्हायरसची एक्झ्युक्युटेबल फाईल पाठवून दुसऱ्या संगणकात डाऊनलोड करून हॉकिंगद्वारा अनाधिकृत प्रवेश केला जातो व विविध प्रकारे त्या यंत्रणेला नुकसान पोहचविले जाते. हॉकिंगच्या गुन्ह्यचे प्रमाण ३१ टक्के इतके आहे.

चौथा प्रकार आहे, व्हायरस ऍटॅक या वारसर ऍटॅकमध्ये एखाद्या संगणक प्रणालीत ई–मेल, चाटिंग याद्वारे व्हायरस पाठवून संगणक प्रणाली हॅकरच्या नियंत्रणाखाली आणली जाते. व्हायरसचे विविध प्रकार आहे. संगणक यंत्रणा बिघडणे, ठप्प करणे, नियंत्रण बाह्य करण्यासाठी हे व्हायरस कार्यरत असतात. ट्रोजन सारख्या व्हायरसद्वारे जगाच्या कोणतही कोपऱ्यात बसून जगभरातील कोणत्याही संगणकावर नियंत्रण ठेवणे शक्य आहे. याचे स्वरूप गंभीर आहे. प्रतिस्पर्धी राष्ट्रांतर्गत व्हायरस ऍटॅकचे प्रमाण वाढले आहे. व्हायरस ऍटॅकच्या गुन्ह्यचे प्रमाण ६ टक्के आहे.

पोर्नोग्राफी हा सायबर क्राईम मधील पाचवा प्रकार. अश्लिल चित्रफिती, छायाचित्रे, मजकूर, इंटरनेटद्वारे डाऊनलोड करणे, प्रसारित करणे, पहाणे असे प्रकार पोर्नोग्राफीमध्ये मोडतात. पोर्नोग्राफीवर आपल्या देशात देशात पूर्णत: बंदी असली तरी इंटरनेटच्या महाजालात आजूनतरी त्यावर बंधने नाहीत. टाईम मॅगेझिन ग्रुपने केलेल्या एका सर्वेक्षणानुसार विविध वेबसाईटनी पोर्नोग्राफीच्या लिंक अतिबाद बंद केल्या तर अनेक लोक नेट सर्फिंग किंवा इंटरनेटचा वापर बंद करतील..!

सायबर क्राईमची काही उदाहरणे आज जगातील प्रत्येक क्षेत्र, व्यवसाय, इंटरनेटने प्रभावित झालेला दिसतो. इंटरनेटच्या या मायाजालाचा हॅकर अतिशय क्लुप्तीने गैरवापर करतात. मध्यंतरी रशियाने जॉर्जी वयावर हल्ला करून हा देश आपल्या ताब्यात घेतला होता. मात्र या हल्याआधी रशियन इंटेलिजन्यच्या हॅकर्सने जॉर्जीयाच्या संगणक प्रणाली, दूरसंचार यंत्रणा, प्रमुख सर्व्हर हॅक करून दळणवळण यंत्रणा या सायबर हल्ले करून आपल्या नियंत्रणाखाली आणल्यामुळे जॉर्जीयावर प्रत्यक्ष हल्ला करणे रशियाला अगदी सोपे झाले. इराणची न्यूक्लियर वेपनसिस्टीम (क्षेपणास्त्र यंत्रणा) मये स्टक्स नेट हा व्हायरस डाऊनलोड करण्याचा प्रयत्न झाला. अल–कायदाच्या हॅकर्सचा यात हात असल्याचा संशय आहे. तर अमेरिकेतील एका १२ वर्षे मुलाने नासा या अमेरिकेन अंतराळ संशोधन संस्थेतील न्यूक्लिअर वेपन्सची दिशा हॉकिंगद्वारे बदलली होती.

भारतातील मुख्य बँका जशा आरबीआय, एसबीआय, त्याचप्रमाणे मुंबई पोलीस यांच्या वेबसाईट सुध्दा हॅक करण्यात आल्या होत्या. रशियातील सिटी बँकेचे पासवर्ड, नेट बँकींग आयडी, हॅक करून रशियाच्या विविध सिटीबँकेच्या खात्यातील १० हजार लक्ष डॉलर्स विविध शाखांतून काढण्यात आले. एखाद्या देशाच्या अर्थ व्यवस्थेबरोबरच सुरक्षा व्यवस्थेलाही मोठा धोका सायबर क्राईमद्वारे होऊ शकतो. सायबर स्टॉकिंग या गुन्ह्यची अनेक उदाहरणे आहेत. ई–मेल, चॉटिंगच्या माध्यमातून विशेषत: महिलांचे बँक अकाऊंट क्रमांक, पावसर्ड, आयडी क्रमांक, वैयक्तिक माहिती, वेगकॅमेर्याने आक्षेपार्ह छायाचित्रे काढणे, या महिलांना ब्लॅकमेल करणे, धमकी देणे, पैसे उकळणे असे अनेक गुन्हे उघडकीस आले आहेत.

ई–मेल, एसएमएस, चॉटिंग याद्वारे फसवणूक :

हो ही वस्तूस्थिती आहे. स्पॅम मेलचा हा प्रकार आहे. अशा प्रकारचे मेल किंवा एसएमएस आपल्याला वारंवार येतात. हा नायजेरियन सायबर फ्रॉड समजला जातो. यामध्ये संबंधितास लॉटरी किंवा मोठे बक्षिस मिळाल्याचे कळवून त्यापोटी प्रोसेसिंग फी किंवा नवीन अकाऊंट उघडण्यासाठी २५ हजार ते १ लाखापर्यंतची रक्कम संबंधिताकडून उकळती जाते. एवढ्यवर न थांबता संबंधिताच्या नेट बँकींग खात्यातून रक्कम काढणे किंवा मोठ्याप्रमाणात खरेदीचे प्रकार घडले आहेत.

यावर प्रतिबंध :

इंटरनेट वापरतांना आपला आयडी क्रमांक, नेट बँकींग अकाऊंट क्रमांक, आपला आयडी क्रमांक, पासवर्ड, क्रेडीट किंवा डेबीट पासवर्ड क्रमांक अथवा आपली वैयक्तिक माहिती उघड करतांना सावधानता बाळगली. ऑन लाईन खरेदी करतांना सुरक्षिततेचे उपाय योजावेत. आपली संगणक सिस्टीम ऍन्टी व्हायरस, फायर वॉलने सुरक्षित ठेवावी. स्पॅम मेल, फसवे मेल यावर डबल क्लिक करून उघडण्याचा प्रयत्न करू नये. अशा मेल मधून व्हायरसची एक्झीक्युटेबल फाईल आपल्या नकळत डाऊनलोड होते. आपण जेव्हा संगणकावर काम करतो तेव्हा केलेल्या कामाची एक डुप्लीकेट फाईल तयार होऊन ती हार्ड डिक्सवर सेव्ह होते. जेव्हा आपण इंटरनेट चालू करतो तेव्हा अलगदपणे ही माहिती हॅकरला मेल द्वारे प्राप्त होते. त्यामुळे पुढील फसगत टाळण्यासाठी अशा प्रकारचे फसवे मेल डीलीट करणे हाच मोठा प्रतिबंधात्मक उपाय ठरतो.

सायबर क्राईमचे गुन्हे उघडकीस आणणे शक्य आहे. सर्वसाधारण लहान मोठ्य गुन्ह्यतील गुन्हेगारांना शोधण्यापेक्षा सायबर गुन्हे व गुन्हेगार शोधणे सोपं आहे. मात्र सायबर क्राईमध्ये फसले गेलेले लोक पुढे येऊन तक्रार देण्याचे प्रमाण दुर्देवाने कमी आहे. फ्रॉड मेल, धमकी देणारे मेल, किडनॉपिंग, फिशिंग, पोर्नोग्राफी आदींचे गुन्हे उघड करणे अतिशय सोपे आहे. यासाठी वापरात आलेल्या संगणक किंवा मेलवरून गुन्हेगाराचा आयपी ऍड्रेस (इंटरनेट प्रोटोकॉल ऍड्रेस) शोधला जातो. असा मेल कोणत्या सर्व्हरवरून आला हे शोधले जाते. आयपी ऍड्रेसवरून वापरण्यात आलेले संगणक, त्याचा प्रकार, इंटरनेट स्पीड, सर्व्हरचे लोकेशन व सदरचा मेल कोठून आला हे उघड करून गुन्हेगाराला शोधता येते.

मात्र आता सायबर क्राईम करणारे गुन्हेगार देखील अद्यावत यंत्रणेचा वापर करू लागले आहेत. आपला आपयी ऍड्रेस सापडू नये यासाठी प्रॉक्सी सर्व्हरचा वापर केला जाऊ लागला आहे. एखाद्याची आयडेंटी हॅक करून तिचा वापर सायबर क्राईमसाठी केला जातो. तथापि कोणताही सायबर ऍटॅक आयपी ऍड्रेसद्वारे शोधणे शक्रू आहे. सुरक्षितता, सावधगिरी बाळगून इंटरनेटचा वापर करणे ही काळाची गरज आहे. इथे एक गोष्ट प्रामुख्याने सांगितली पाहिजे, देशातील आर्थिक विषयमतेची दरी या सिलीकॉन व्हॅलीमुळे भरून निघत आहे. मात्र या ताकदवान माध्यमाचा सकारात्मक वापर होणे गरजेचे आहे. याबाबत व्यक्तीसापेक्षा जागरूकता बाळगली पाहिजे. फेसबुक या प्रचंड लोकप्रिय वेबसाईटचा निर्माता मार्क झुकरबग याचे वेब पेज सुध्दा हॅक करण्यात आले होते..!

भारतीय कायद्यानुसार सायबर गुन्हा (माहिती तंत्रज्ञान कायदा २०००)

कलम ६५: संगणकीय दस्ताऐवजीतील फेरफार :

संगणक, संगणक यंत्रणा किंवा संगणक नेटवर्क यासाठी वापरावयाचे आणि कायद्यानुसार जतन करावयाचे संगणकीय संकेत, जो कोणी जाणूनबुजून किंवा हेतुपूर्वक लपवेल/नष्ट करेल किंवा त्यात फेरफार करेल किंवा हेतुपूर्वक, जाणीवपूर्वक दुसऱ्यास असे संकेत लपविण्यास/नष्ट करण्यास/फेरफार करण्यास कारणीभूत ठरेल त्यास तीन वर्षापर्यंतची कैदेची किंवा दोन लाख रूपयापर्यंतच्या दंडाची किंवा दोन्हीही शिक्षा देता येतील.

कलम ६६ — संगणक हँक करणे :

१) कोणा व्यक्तीचे नुकसान होण्यास जो जाणीवपूर्वक कारणीभूत होतो किंवा अशी हानी लोकांना पोहोचविण्यास आपण कारणीभूत होऊ शकू याची जाणीव असूनही जो संगणकातील माहिती नष्ट करतो, बदलतो किंवा त्यातील काही माहिती गाळून टाकतो, त्या संगणकाची उपयुक्तता नष्ट करतो तो ''संगणक हँकर'' ठरतो.

२) जो कोणी संगणक हँक करतो त्याला तीन वर्षापर्यंतची कैदेची किंवा दोन लाख रूपयापर्यंतच्या दंडाची किंवा दोन्हीही शिक्षा दिल्या जातील.

कलम — ६७ इलेक्ट्रॉनिक स्वरूपात अश्लील माहितीचे प्रकाशन :

लोकांची लैंगिक विषयक उत्सुकता वाढविणारे किंवा त्यांना कुमार्गाला नेणारे किंवा त्यांना भ्रष्ट करणारे असे कोणतेही इलेक्ट्रॉनिक स्वरूपातील साहित्य वाचविण्यासाठी, पाहण्यासाठी किंवा ऐकण्यासाठी प्रकाशित करणारा किंवा प्रसारित करणारा किंवा अशा साहित्याच्या प्रकाशनाला कारणीभूत ठरणाऱ्या व्यक्तीस शिक्षा दिली जाईल. गुन्हा

दुसऱ्यांदा केलेला असेल किंवा पहिल्याच्या पाठोपाठच केलेला असेल तर जास्तीत जास्त १० वर्षापर्यंतची कैदेची आणि दोन लाख रूपया पर्यंतच्या दंडाची शिक्षा दिली जाईल.

कलम ६८ —

मध्ये शासनास वा नियंत्रण अधिकार असलेल्या अधिकाऱ्यांना संगणक प्रणालीबाबत योग्य तो आदेश देण्याचा किंवा कामकाज थांबविण्याचा अधिकार बहाल केला आहे. याचा भंग करणाऱ्यास जास्तीत जास्त तीन वर्षे शिक्षा अगर दोन लाखांचा दंड होऊ शकतो.

कलम ६९ — माहिती पुरविण्याबाबत शासन/नियंत्रकाचे बंधन :

देशाच्या एकतेसाठी, देशाच्या सार्वभौमत्वासाठी, देशाच्या सुरक्षिततेसाठी परदेशाशी असलेल्या मैत्रीपूर्ण संबंधासाठी किंवा सार्वजनिक हितासाठी तसेच दखलपात्र गुन्ह्यला मिळणारे प्रोत्साहन रोखण्यासाठी कोणत्याही संगणकाद्वारे देण्यात येणारी माहिती अडवून मिळण्याचा शासन संस्थेला वा नियंत्रकाला अधिकार आहे. संगणकधारकाने तांत्रिक माहिती व सहाय्य देणे बंधनकारक आहे. या कलमानुसार नियंत्रकास वा शासनास देशहितासाठी माहिती न देणाऱ्या व्यक्तीस जास्तीत जास्त सात वर्षाची शिक्षा देण्याची तरतूद आहे. देशहित व समाजहित विरोधी या तंत्रज्ञानाचा उपयोग होऊ नये यासठी ही तरतूद आहे.

कलम ७० — संरक्षित किंवा सुरक्षित यंत्रणा :

१) योग्य ते सरकार, अधिकृत गॅझेटमधील प्रकटनाद्वारे कोणताही संगणक, संगणक यंत्रणा किंवा संगणक नेटवर्क सुरक्षित यंत्रणा म्हणून घोषित करू शकतो.

२) योग्य ते सरकार उपकलम (१) खाली जाहीर झालेल्या संरक्षित यंत्रणा हाताळण्याचा अधिकार असलेल्या व्यक्तींना, लेखी आदेशाद्वारे संबंधित यंत्रणा हाताळण्याचा अधिकार देऊ शकतो.

३) या कलमातील तरतूदींचा भंग करीत जी व्यक्ती संरक्षित यंत्रणेपर्यंत प्रवेश मिळवेल किंवा प्रवेश मिळविण्याचा प्रयत्न करले ती व्यक्ती जास्तीत जास्त १० वर्षे मुदतीपर्यंतची कैदेची शिक्षा आणि दंडाच्या शिक्षेला पात्र राहील.

कलम ७१ — गैरसादरीकरणा बद्दल दंड :

कोणताही परवाना किंवा डिजीटल स्वाक्षरी दाखला मिळविण्यासाठी नियंत्रकाकडे जो कोणी गैर माहिती सादर करेल किंवा जो कोणी महत्वाची माहिती दडवून ठेवेले त्याला जास्तीत जास्त दोन वर्षापर्यंतची कैदेची किंवा एक लाख रूपयापर्यंतच्या दंडाची किंवा दोन्ही शिक्षा देयात येतील.

कलम ७२ — खासगीपणा व गुप्तता तत्वचा भंग :

या कलमानुसार इलेक्ट्रॉनीक नोंदी/पुस्तके/रजिस्टर/पत्रव्यहार/ माहिती / दस्तऐवज किंवा इतर स्वरूपातील ाहित्य ज्या व्यक्तीचे आहे त्याचा परवानबीशिवाय त्याच्या इलेक्ट्रॉनीक साहित्यापर्यंत प्रवेश मिळविणे वा संमतीशिवाय अन्य व्यक्तीस उघड करून दाखविणे यासाठी जास्तीत जास्त दोन वर्ष मुदतीपर्यंतची कैद किंवा एक लाख रूपयापर्यंतचा दंड किंवा दोन्हीही शिक्षा देता येतील.

कलम ७३ — खोटा तपशील प्रकाशन :

माहिती तंत्रज्ञान कायदा (सायबर कायदा) नुसार डिजिटल स्वाक्षरी दाखल्यातील काही तपशील खोटा प्रकाशित केल्याबद्दल दोन वर्षापर्यंतची कैद किंवा १ लक्ष रूपयांपर्यंत दंडाची तरतूद आहे.

कलम ७४ — फसवणूकीच्या हेतूंसाठी प्रकाशन :

काही फसवणूकीया हेतूंनी किंवा बेकायदेशिर गोष्टींसाठी जो कोणी जाणूनबुजून डिजिटल स्वाक्षरी दाखला प्रकाशित करेल किंवा दुसऱ्यासाठी इतर मार्गांनी उपलब्ध ठेवेल त्याला जास्तीत जास्त २ वर्षापर्यंतची मुदतीची कैद किंवा एक लाख रूपयांपर्यंतचा दंड किंवा दोन्हीही शिक्षा देता येतील.

कलम ७५ :

नुसार याबाबत भारताबाहेर घडणाऱ्या सायबर गुन्ह्यंना किंवा कायदेभंगांनाही हा कायदा लागू केलेला आहे. तर कलम ७६, ७७ नुसार कोणताही संगणक, संगणक यंत्रणा, फ्लॉपीज, कॉम्पॅक्ट डिस्क, टेपड्राइव्ह किंवा संगणक संबंधित साधनसुविधा या कायद्याचा भंग झाल्यास जप्त करण्यात येतील. सायबर कायदा निर्माण करणारा भारत हा जगातील तेरावा देश आहे.

सायबर सुरक्षेचे मार्ग : सायबर पोलीस :

सायबर गुन्हेगार हे संगणकतज्ज्ञ असल्याने, त्यांना पकडण्यासाठी 'सायबर पोलिस' हे संगणक तज्ज्ञ असणे गरजेचे सते. ई—मेल बाबत गैरप्रकार होऊ नयेत म्हणून मेसेज सांकेतिकीकरणाने कोणासही सहजासहजी कळणार नाही अशा रूपात पाठविला जातो. हा ई—मेल कसा वाचायचा याची 'की', ई—मेल ज्याला पाठविला जातो त्यास दिली जाते. त्यामुळे ज्याच्याकडे 'की' आहे तोच ई—मेल वाचू शकतो.

याशिवाय संगणकाच्या संरक्षणासाठी अनेक प्रकारचे सुरक्षा उपाय केले जात आहेत. त्यामध्ये संगणक सुरक्षेसाठी ही संरक्षक ढाल तयार केली जाते. बाहेरून आलेले संदेश फायर बॉलद्वारे तपासून घेऊनच संगणकामध्ये प्रवेश करू शकतात. बऱ्याचदा 'अज्ञान रिमेलर' वापरून गैरप्रकार, खोटे फसवे संदेश दिले जातात. त्याबाबत जागरूकता पाळावी लागते.

विषय निवडण्याचे कारण:—

आज जगामध्ये देशामध्ये व समाजात ''सायबर गुन्हयाचे'' गुन्हे आपल्याला पाहायला मिळतात. तेव्हा हया गुन्हयांमुळे समाजात दहशतीचे चित्र दिसून येते. या गुन्हयांबाबत दहशतीबाबत भंडारा शहरातील पोलीसांचे मत जाणून घेण्याचा निर्णय घेण्यात आला.

विषयासंबंधीत व्याख्या :

१) गुन्हा :—

''बेकायदेशिर व समाजविरोधी वर्तन करणे म्हणजे गुन्हा करणे होय''.

२) संगणक हँकर :—

''कोणा व्यक्तीचे नुकसान होण्यास जो जाणीवपूर्वक कारणीभूत होतो किंवा अशी हानी लोकांना पोहचविण्यास आपण कारणीभूत होऊ शकू यांची जाणीव असूनही जो संगणकातील माहिती नष्ट करतो, बदलतो किंवा त्यातील काही माहिती गाळून टाकतो त्या संगणकाची उपयुक्तता नष्ट करतो तो संगणक हँकर ठरतो''

निष्कर्ष:—

१) सायबर गुन्हा करणाऱ्यांमध्ये समाजातील शिक्षित वर्ग पुढे आहे.

२) संगणक जाळयाचा अति वापर समाजातील युवकांना सायबर गुन्हयास प्रवृत्त करतो.

३) गुन्हेगाराकडे समाजाचा पाहण्याचा दृष्टिकोण वाईट असतो.

४) सायबर गुन्हा करणाऱ्यास आर्थिक लाभ अधिक प्रमाणात मिळतो.

५) सायबर गुन्हयात वाढ होण्यासाठी आधुनिक वातावरण जबाबदार असते.

६) सायबर गुन्हाची माहिती समाजात तणाव निर्माण झाल्यावर मिळत आहे.

७) सायबर गुन्हेगार आपली ओळख लपवितात.

संदर्भ ग्रंथ सूची :—

१) डॉ. आगलावे प्रदिप, 'गुन्हेगारी शास्त्र', विद्या प्रकाशन नागपूर

२) डॉ. भांडारकर पु.ल., 'सामाजिक संशोधन पध्दती', विलास आधारे तिसरी आवृत्ती १९८७

३) जोशी वि.एस., 'भारतीय दंड संहीता'

४) मेश्राम सुरेश, 'प्रात्यक्षिक सामाजिक संशोधन', यश प्रकाशन, नागपूर: प्रथम आवृत्ती सप्टें.२०००

५) काळदाते सुधा, गोटे शुभांगी, 'गुन्हेगारांचे समाजशास्त्र' श्री विद्या प्रकाशन, शनिवार पेठ, पुणे

६) माणिक मणे, 'गुन्हेगारी शास्त्र', फडके प्रकाशन, नागपूर

७) दिपक शिकारपूर, 'सायबर कायदा आणि आपण'

८) इंटरनेट