IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

21वीं सदी में महिलाओं के प्रति बढ़ते साइबर अपराध

डॉ. गीता मीणा

सहआचार्य (ग्रहविज्ञान)

राजकीय कन्या महाविद्यालय, टोंक

शोध सारांश –

साइबर अपराध एक ऐसी अपराधिक गतिविधि है जिसे फोन, कम्प्यूटर और इन्टरनेट के द्वारा किया जाता है। यह आधुनिक एवं इन्टरनेट इलेक्ट्रॉनिक अपराध के रूप में भी जाना जाता है। यह ऐसा अपराध है जिसमें उपकरण की आवश्यकता होती है और उपकरण द्वारा उपकरण पर आघात किया जाता है। वैज्ञानिक जेवियर जिसके अनुसार साइबर क्राइम कम्प्यूटर और इंटरनेट के माध्यम से होने वाला अपराध है। इसके अन्तर्गत जालसार्जा, चाइल्ड पोर्नोग्राफी और साइबर स्टॉकिंग शामिल है। साइबर क्राइम में किसी की निजी जानकारी चुराने के अलावा दस्तावेज या डाटा चोरी धोखाधड़ी अश्लीलता और नफरत आदि अपराध आते हैं। साइबर क्राइम करने वाले को साइबर अपराधी कहा जाता है।

बीजक शब्द –

साइबर, अपराध, इन्टरनेट, आधुनिक, अश्लीलता, सोशल मीडिया।

महिलाओं की साइबर अपराध में किस प्रकार प्रभाव पड़ता है इसमें कई अध्ययनों से पता चला है कि महिलाएँ साइबर अपराध का शिकार तो होती है परन्तु ये अपने आप को एवं समाज को साइबर सुरक्षा भी प्रदान करती है। समय के साथ–साथ महिलाओं में साइबर अपराधों में वृद्धि हो रही है जैसे साइबर उत्पीडन करना, पीछा करना, सोशल मीडिया में आपत्तिजनक फोटों अपलोड़ करना ऑन लाइन अरेस्ट करना, साइबर उत्पीड़न और बदमाशी, साइबर स्टॉकिंग, यौन उत्पीडन, धोखाधड़ी मॉफिंग महिलाओं में होने वाले साइबर अपराध है।

1. ***साइबर उत्पीडन और बदमाशी*** *– महिलाओं को ऑनलाइन चमकाना।*

2. ***यौन उत्पीडन*** *– महिलाओं को ऑनलाईन यौन उत्पीड़न जैसे कि साइबर, पोर्नोग्राफी और साइबर यौन उत्पीडन का सामना करना पड़ता है।*

3. धोखाधड़ी *– महिलाओं को ऑनलाइन धोखाधड़ी जैसे कि फिशिंग और स्कैमिंग का शिकार बनाया जाता है।*

4. मॉर्फिंग *– साइबर मॉर्फिंग में मॉर्फिंग टूल का प्रयोग करके महिलाओं की तस्वीरों को बिना उनकी सहमति के बदल दिया जाता है जिससे उन्हें भावनात्मक परेशानी हो सकती है। क्योंकि उनकी तस्वीरों के साथ छेड़छाड़ और उनका दुरुपयोग बिना उनकी सहमति के किया जाता है। इससे उनकी प्रतिष्ठा को नुकसान होता है मॉर्फिंग से 70 प्रतिशत महिलाएँ पीड़ित हैं। साइबर सिविल राइट्स इनिशिएटिव ने खुलासा किया है कि 93 प्रतिशत महिलाओं को पता ही नहीं होता है कि उनकी तस्वीर के साथ मॉर्फिंग हो रही है और पता चलता है तो तब वह इतनी चिंतित, उदास और शक्तिहीन हो जाती है और भावनात्मक प्रभाव में नेगेटिव असर देखने को मिलता है।*

5. साइबर मानहानि *– साइबर मानहानि कई महिलाओं के लिए एक गंभीर समस्या है जिन्हें अक्सर मानसिक स्वास्थ्य विशेषज्ञों की मदद की जरूरत होती है। ऐसा तब होता है जब इंटरनेट पर उनके बारे में झूठी और हानिकारक बाते कही जाती है। जिससे उनकी प्रतिष्ठा को नुकसान पहुँचता है और भावनात्मक क्षति पहुँचती है।*

सेंट्रर फॉर इनोवेटिव पब्लिक हेल्थ रिसर्च द्वारा किये गए एक सर्वेक्षण में पाया गया है कि 18 से 24 वर्ष की आयु की 26 प्रतिशत युवा महिलाओं को किसी न किसी रूप में ऑनलाइन बदनामी का सामना करना पड़ता है। जिसमें इंटरनेट पर उनके बारे में फैलाई गई झूठी अफवाहें या गपशप भी शामिल है।

डिजिटल सिटीजन्स एलायेस ने बताया कि ऑनलाइन बदनामी अभियानों का लक्ष्य बनने की पुरुषों की तुलना में महिलाओं की संभावना अधिक है। तथा 61 प्रतिशत महिलाएँ पीड़ित है।

6. साइबर स्टॉकिंग *– साइबर स्टॉकिंग में लोगों के सोशल मीड़िया अकाउंट और उनकी गतिविधियों पर नजर रखना शामिल है। इसमें व्यक्ति के मान–सम्मान व आपसी रिश्तों में नुकसान पहुँचाया जाता है।*

कभी–कभी ये पीछा करना हैकिंग में परिवर्तित हो जाता है जिससे खातों में हेराफेरी करने उनके पासवर्ड जानने के बाद उन तक पहुँच प्राप्त कर सकते हैं।

राष्ट्रीय अतरंग साथी और यौन हिंसा सर्वेक्षण (एन आई एसबीएस) ने बताया कि 16.2 प्रतिशत महिलाओं ने अपने जीवनकाल में पीछा किए जाने का अनुभव किया है जो इस साइबर खतरे की व्यापकता पर जोर देता है।

अमेरिकन जर्नल ऑफ पब्लिक हेल्थ ने अपने निष्कर्ष प्रकाशित किए है जिनसे पता चलता है कि साइबर सटॉकिंग की शिकार महिलाओं असमनजस, चिंता और नींद सही से न आने की शिकायत की संभावना उन महिलाओं में अधिक देखी जाती है जिसमें साइबर स्टॉकिंग की पीड़ा को सहा है।

7. डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विस अटैक – *इसका प्रयोग किसी ऑनलाइन सेवा को अनुपलब्ध बनाने और विभिन्न स्त्रोतों से वेबसाइट पर अत्यधिक ट्रैफिक के माध्यम से नेटवर्क को बाधित करने के लिए किया जाता है।*

8. बॉटनेट – *यह कम्प्यूटर का ऐसा नेटवर्क है जिसे दूर बैठे हैकर्स द्वारा बाह्य रूप से नियंत्रित कर लिया जाता है। रिमोर्ट हैकर्स या तो स्पैम भेजते है या इन बॉटनेट के माध्यम से कम्प्यूटरों पर हमला करते हैं।*

9. फिशिंग – *यह एक प्रकार का सोशल इंजीनियरिंग हमला है जिसका उपयोग अक्सर उपयोग कर्ता का डेटा चुराने के लिए किया जाता है। इसके अन्तर्गत क्रेडिट कार्ड के नम्बर आदि आते हैं।*

भारत में साइबर सुरक्षा से संबंधित चुनौतियाँ –

- *लाभ–उन्मुख अवसंरचना की मानसिकता इसके अन्तर्गत लाभ पर अधिक ध्यान रहता है जिससे चर्चित व लाभ वाले अक्सर ही लेते हैं।*
- *पृथक प्रक्रियात्मक संहिता का अभाव*
- *साइबर हमलों की अंतर्राष्ट्रीय (ट्रांस–नेशनल) प्रकृति*
- *डिजिटल परितंत्र का विस्तार*
- *सीमित विशेषज्ञता और प्राधिकार*

राजस्थान सरकार एवं पुलिस विभाग द्वारा साइबर सुरक्षा के लिए अभियान जारी किया जा रहा है जिसके अन्तर्गत राजस्थान पुलिस के प्रवर्तन जागरूकता और पुरानी रणनीति को विकास के साथ रखकर एक नई नीति तैयार की है इस नई रणनीति में विशेष सावधानियों को ध्यान में रखा है साइबर ईकाईयों की स्थापना से लेकर डिजिटल सुरक्षा के बारे में लोगों को जागरूक करने का भी उद्देश्य रखा है।

गहन प्रवर्तन – *इसके अंतर्गत लम्बे समय से जिनका वारंट हो। साइबर संबंधित मामलों में अपराधी घोषित है उन्हें गिरफ्तार करना होता है।*

अपराध के प्रमुख स्थानों को चिन्हित करना – *साइबर अपराध–गतिविधियों वाले क्षेत्र को पहचान कर उसमें निगरानी रखने का कार्य करते हैं और उसे अंजाम देते है जैसे कि ''ऑपरेशन एंटी–वायरस'' है जो मेवात क्षेत्र में साइबर धोखाधड़ी नेटवर्क पर कार्रवाई के लिए शुरु किया गया था।*

अवैध–नेटवर्क को अवरूद्ध करना – *इसके अन्तर्गत धोखाधडत्री गतिविधियों से जुड़े संदिग्ध–सिमकार्ड और प्डम्प नंबरों की पहचान करने और उन्हें बंद करने का कार्य किया जाता है।*

आपराधिक डेटा बेस बनाना – *पुलिस विभाग साइबर अपराध में शामिल व्यक्तियों का रिकॉर्ड तैयार कर डेटा बनाती है।*

विशिष्ट साइबर इकाइयाँ तैयार करना –

(क) साइबर पुलिस स्टेशन – *इसमें राजस्थान सरकार ने 1000 से अधिक पुलिस स्टेशन में साइबर सेल बनाने का कार्य कर रही है जो कि केवल जटिल साइबर अपराधों को ही निपटाने का कार्य करेगी।*

(ख) साइबर हेल्प डेस्क – *इसके अन्तर्गत एक विशेष टीम कार्यरत रहती है ये टीम नागरिकों की शिकायत दर्ज करने, धोखाधड़ी में खोई धनराशि, मीडिया अकाउंट हटाने जैसे समस्याओं से निवारण करवाती है।*

(ग) साइबर सहायता केन्द्र – *यह जयपुर में शुरू किया गया है। डिजिटल उत्पीडन, वित्तीय धोखाधड़ी औन ऑनलाइन बदमाशी के पीडितों की सहायता के लिए बना है इसके अन्तर्गत विशेष–विशेषज्ञों और परापर्शदाताओं को रखा जाता है।*

(घ) साइबर सुरक्षा केन्द्र – *सरदार पटेल अंतर्राष्ट्रीय हवाई अड्डे पर जोधपुर पुलिस विश्वविद्यालय में यह सिति है यहाँ से सूचना ऑडित होती है फिर विभागों तक दी जाती है।*

तकनीकी उन्नत रिपोटिंग और जांच उपकरण –

(क) राष्ट्रीय सहयोग पोर्टल – *इसके अन्तर्गत राजस्थान से धोखाधड़ी से जुड़े मामलों को अन्य राज्यों से विचाराधीन कर एजेन्सियों के साथ मिलकर कार्य करती है।*

(ख) डिजिटल हेल्पलाइन – *इसके लिए (1930) नम्बर दिये है। साथ ही व्हाट्सप्प हेल्पलाइन शुरू कर शिकायत को दूर किया जाता है।*

(ग) मोबाइल डिवाइस रिकवरी – *चोरी या खोए हुए मोबाइल को वापस मालिक तक पहुँचाना और साइबर हेल्प डेस्क पीडितों को ब्म्प्ट पोर्टल का उपयोग करके चोरी या खोए फोन को ब्लोक करने का तरीका बताते हैं।*

जन–जागरूकता एवं सलाह –

(क) व्यापक जागरूकता अभियान – *पुलिस विभाग द्वारा फिशिंग ऑनलाइन घोटाले और डिजिटल गिरफ्तार जैसे सामान्य साइबर खतरों के बारे में जनता विशेष रूप से छात्रों और कमजोर समूहों को शिक्षित करने के लिए नियमित रूप से जागरूकता कार्यक्रम अभियान में चलाये जा रहे हैं।*

(ख) ***साइबर जागरूकता दिवस*** *– यह 15 नवम्बर को ''साइबर जागरूकता दिवस के रूप में मनाया जाता है।*

(ग) ***उभरते खतरों पर सलाह*** *– समय–समय पर आमजन को साइबर अपराधों के बारे में बताना व उनसे कैसे बचा जाए इसकी जानकारी देने का कार्य भी करती है।*

पुलिस विभाग द्वारा समय–समय पर विश्वविद्यालयों, स्कूलों व जन रेलियों में नागरिकों को अपराधों के बारे में बताने का कार्य करती है। साथ ही उनसे बचने के उपाय भी बताती है। एवं पुलिस की मदद एक सामान्य व्यक्ति किस तरह से ले सकता है ये भी साझा करती है।

साइबर क्राइम से महिलाओं की सुरक्षा के लिए निम्न सुझाव –

- *महिलाओं को अपनी व परिवार की फोटो सोशल मीडिया पर अपलोड नहीं करनी चाहिए।*
- *सोशल मीडिया जैसे फेसबुक पर डाल रहे तो उनकी प्राइवेसी रखनी चाहिए।*
- *अपने सोशल मीडिया अकाउन्ट की सेटिग्स ऐसे रखे कि आपकी फोटो आपके दोस्त या आपसे जुड़े हुए व्यक्ति ही देख सके।*
- *अपने नाम के बारे में गूगल पर हमेशा सर्च करते रहे ताकि पता चलता रहे कि आपका नाम कहाँ पर और किस तरह की मीडिया पर आ रहा है।*
- *बिना अनुमति के यदि किसी जगह मीडिया में आपका नाम आता है तो उसे हटाने के लिए कहना चाहिए।*
- *अनजान लोगों को फेसबुक पर एवं ग्रुप में नहीं जोड़ना चाहिए।*
- *प्रोफेशन लोगों से केवल लिंग पर जुड़ना चाहिए। फेसबुक व इंस्टाग्राम पर नहीं जुड़ना चाहिए।*
- *ट्विटर के ऊपर बिल्कुल भी निजी तस्वीरे नहीं डालनी चाहिए क्योंकि यह एक सोशल नेटवर्किंग साइट नहीं है यह एक ट्विटिंग प्लेटफॉर्म है।*
- *ट्विटर पर सेटिंग इस तरह से हो कि बिना अनुमति के दूसरा व्यक्ति फॉलों न कर सके।*
- *स्वयं के द्वारा यदि किसी व्यक्ति का अकाउंट बंद कर दिया है तो उससे सर्तक रहना चाहिए क्योंकि वह अन्य किसी अकाउंट से नुकसान पहुँचाने के लिए ब्लॉक किये व्यक्ति के अकाउंट तक पहुँचना चाहेगा।*
- *अन्जान प्रोफाइल लिंग, फ्रेन्ड रिक्वेस्ट को स्वीकार नहीं करना चाहिए।*

- *उपरोक्त सुझावों को ध्यान में रखने के बाद भी यदि किसी समस्या में फंस जाते है तो परिवार के सदस्यों को एवं पुलिस को तुरन्त सुचना करनी चाहिए।*

निष्कर्ष –

साइबर अपराध एक ऐसा अपराध है जो कि मोबाइल या कम्प्यूटर अपराध का माध्यम होता है या अपराध करने के लिये एक उपकरण के रूप में प्रयोग किया जाता है। भारतीय संविधान की सातवीं अनुसूची के अनुसार साइबर अपराध राज्य सूची के अन्तर्गत आता है। इसके अवैध या अनधिकृत गतिविधियाँ शामिल है जो विभिन्न प्रकार के अपराध करने के लिए प्रौद्योगिकी का लाभ उठाती है। साथ ही साइबर अपराध में अपराधों की एक विस्तृत श्रृंखला शामिल है। यह महिला, पुरुष, बच्चों, संगठनों के साथ–साथ सरकारों को भी प्रभावित करते है। जिससे सभी पर शारीरिक, मानसिक, आर्थिक रूप से नकारात्मक प्रभाव पड़ता है, जो कि विकास को अवरूद्ध करता है। इसे रोकने के लिए विभिन्न कानून एवं नियम बनाये गये है। जन जागरूकता अभियान भी चलाऐं जा रहे हैं।

सन्दर्भ सूची –

1. *The art of deception controlling the human element of security by kevin Mitnik*
2. *People like her by elery lloyed*
3. *Police department reporting 2023-24*
4. *in/exnational/journal of novel research and development (IJNRD) https://www.ijnrd.org : papers, IJNRD 22/01/17*
5. *Cyber crimes against women a Glaomy outlook of technological advan*
6. *https://xiotz.com>top-cyber-crime-against-women*
7. *https://www.bbc.com.*