Research Vidyapith International Multidisciplinary Journal

(International Open Access, Peer-reviewed & Refereed Journal)

(Multidisciplinary, Monthly, Multilanguage)

* Vol-2* *Issue-12* *December 2025*

www.researchvidyapith.com ISSN (Online): 3048-7331

Mapping the Dark Side of Digitalization: Nature, Forms, and Impact of Cybercrime Against Women

Surendra Kumar

Guest Faculty, Sociology and Social Work, Govt. J. Yoganandam Chhattisgarh College, Raipur, Chhattisgarh, India

Dr. Akhil Yadu

Guest Faculty, Sociology and Social Work, Govt. J. Yoganandam Chhattisgarh College, Raipur, Chhattisgarh, India

ABSTRACT

Digital world looks like two side edge of human development, progress and advantage as well as humiliation, disguise and oppression especially in associated with women it gets spikier and hornier. The advanced world is a PC created reenactment where everyone conceals their own character. There are a couple of bad behaviors known and a dark to standard person who is for the most part ladies' get taken advantage of. A couple of law breaker like software engineers, saltines, and stalkers have association techniques and measures to hamper with web accounts acquired induction to client's PC system may took the critical data of the client. If client is ladies', infringement like bullying through mail, computerized following, advanced sex, advanced analysis, photo changing, non-consensual sensual amusement, kid pornography, computerized irritating, computerized getting ready, disseminating foul material in electronic construction, etc.

Present article will highlight especially about the nature and class of advanced infringement which could occur against women while using web. The most huge is the kind of measures and procedure, capacities used by the criminals through which setback may easily trap. It moreover will analyze about methodology for answer for the women when they got under these mindful cybercrime and genuine plan and procedural point to get audit of this kind of situation. What kind key gauges actually must will be valuable for online security while using the web.

KEY WORDS- Technology, Crime, Harassment, Computer, Security

INTRODUCTION

The information in the public region is like toothpaste, when it is out of the chamber one can't get it back in and when the information is in the public space it will not at any point disappear. There are a couple of gathering behind web who endeavor to upset ladies' by sending email, following simply by using conversation channels, locales like facebook, twitter, instagram. Computerized bad behaviors against ladies' consolidate advanced following, computerized pornography, revolving around pictures, video fastens of ladies' partaken in confidential shows, changing, sending foul, harmful,

bothering messages, online savaging, torturing, constraining, risk or threatening, and email mocking and pantomime. This overview isn't particular it is thorough, because on electronic stage computerized hacking is getting a steadily expanding number of master and made, these people by and large find some extraordinary sharp expense for problem the individual being referred to and exploit them.

"Violence against ladies'" is described by the Board of Europe as 'an encroachment of normal opportunities and a sort of exploitation women and will mean all shows of direction based severity that result in, or are presumably going to achieve, physical, sexual, mental or money related naughtiness or persevering to women, including risks of such exhibits, pressure or sporadic difficulty of opportunity, whether occurring out in the open or in confidential life".

Bad behavior against ladies' in computerized world similarly treated as encroachment of balance and security of ladies. The most renowned meaning of "right to security" is- - "the choice to be not to mention". The European Affiliation Rule of 20165 has seen what has been named as "the choice to be dismissed". This doesn't suggest that all pieces of earlier presence are to be pulverize, as some could have a social repercussion. In the event that we some way or another ended up seeing a relative right, it would simply suggest that an individual, who is as of now not jealous of his own data to be dealt with or taken care of, should have the choice to kill it from the system where the singular data/information is as of now unreasonable, critical, or is off-base and serves no veritable interest. Such a right can't be polished where the information/data is key, for rehearsing the right of chance of explanation and information, for consistence with legal responsibilities, for the introduction of a task did out so everyone can see interest, on the grounds of public interest in the space of general prosperity, for documenting in the public interest, coherent or undeniable investigation purposes or quantifiable purposes, or for the establishment, exercise or gatekeeper of genuine cases. Such legitimizations would be genuine in all occurrences of break of safety, including breaks of data security."

MEANING AND DEFINITION OF CYBER-CRIME

A lot of composition on PC bad behavior revolves around PC related deception. "Distortion is the deliberate or cognizant debasement of truth to obtain a preposterous advantage". This is clearly a tremendous piece of PC bad behavior anyway is perhaps with everything taken into account excessively restricted for our inspirations. Various others, when they think about PC bad behavior, simply consider the people who break into laptops to take then again obliterate information.

We can get a to some degree greater definition by seeing what is truly investigated by guideline approval workplaces. The FBI Public PC Bad behavior Team (NCCS) worries pretty much all bad behavior remembering laptops for no less than two states. It contemplates the going with to be critical PC bad behaviors:

1. Interruptions of the Public Traded Association (the telephone association)
2. Significant PC network interferences
3. Network dependability encroachment
4. Protection encroachment
5. Modern mystery exercises
6. Pilfered PC programming
7. Different bad behaviors where the PC is a primary thought in completing the criminal offense

CYBER-CRIMES AGAINST WOMEN IN INDIA

CYBER STALKING

Digital Following is sending email, texts or to go on in web, it may not sexual or genuine in nature still it could annoy, pursue, torture to the individual being referred to. It is interfere into a particular security. In this bad behavior transgressor endeavor to spread out a relationship (on the web or certifiable) without her consent. Sending email, texts which are terrible, disgustful in view of loss caught in a difficult situation or in fear. Posting affected, antagonistic comments, sharing comfortable photos or video of setback through cell or web. Follow discreetly and following a women's, on the web and detached activities and improvements of ladies. All information of ladies collect through web that furthermore without her knowledge like what is her benefit, likes detestations, friends and family, relationship, road number, contact detail, ordinary timetable, etc.

NON-CONSENSUAL PORNOGRAPHY

It suggests without consent of loss online scattering of sexual reasonable or revolting photographs or accounts. It could in like manner call as Exhibitions of voyeurism. The blameworthy party as a rule ex-associate of the loss who get photograph and sickening accounts of the individual being referred to and it could posted on electronic stage or online presented on porn alludes on. This is also being called as 'retaliation porn'. The justification for this bad behavior may be to humiliate or disgrace the individual being referred to unreservedly. In any case it isn't needed that liable party would from normal relationship or ex-accessory of the individual being referred to and reasoning may not be by and large retribution from the individual being referred to. Occasionally it could have business or business motivation to post private photographs or accounts of setback. There are a couple no. of locales open on web where clients can post pictures and accounts close by confidential information, for instance, loss address and individual contact number.

MORPHING

For this present circumstance defaulter could download the setback picture or accounts from social destinations or hacking from individual record of loss, changed the picture again reposted or moves on different locales by making fake profile account ensuing to modifying them. Generally an image of the women may be centered around, and woman face may associated with the uncovered or skimpily clad combination of porn star or one more through using picture changing programming.

As a rule whiz or support and model are the simple goal of these guilty party b t a portion of the time commonplace women moreover being assigned the justification for this may be to humiliate explicit woman or impoliteness in the overall population, stigmatize her character, etc.

SENDING OBSCENE, DEFAMATORY, INSULTING MESSAGES

This is offense associated with posting a woman photograph or flexible number or some other contact nuances on profane site, to show that she is remember for sex worker business. This is the encroachment of insurance of the woman as her own information posted on open. Sending disgusting and bothering messages through WhatsApp, electronic mail, Second Messenger and other such modes, are various kinds of computerized infringement against women.

ONLINE TROLLING, BULLYING

Bullying is the forceful conduct through utilization of unrivaled strength or predominant position; digital harassing alludes to a similar demonstration through the electronic medium.

It is the "willful and rehashed hurt inflicted through the utilization of PCs, phones or other electronic gadgets, by sending messages of a scary or compromising nature. Since the electronic medium loans the power and strength of obscurity and boundless contact across the world, even an individual who might be harassed, in actuality, turns into the harasser online regardless of the absence of unrivaled actual strength or predominant situation in the public eye"

EMAIL SPOOFING AND IMPERSONATION

Tricky email movement in which shipper address and different pieces of beginning of mail polluted so mail is by all accounts obscure objective. Programmer might change the properties of mail like its header, return way, and answer and so on so it will show up from somebody mail other than shipper address. While utilizing this procedure guilty party might include into wrongdoing like annoying the person in question, sending obscure and disgusting message, badgering messages or extortion the casualty for physical, efficient or physiological advantages.

Manish kathuria case in 2001, who bugged the person in question (Ritu kohli) on discussion board, dispersed her telephone number in broad daylight because of that she was getting calls from obscure numbers. However, delhi police captured him under IPC for insulted the unobtrusiveness of ladies, yet not arraigned under genuine wrongdoing due to need of appropriate lawful arrangement.

State/UT-wise Number of Cyber Crimes against Women during 2022

Published on: 12/04/2024

Sl. No.	State/UT	Cyber Blackmailing/ Threatening (Sec.506, 503, 384 IPC r/w IT Act)	Cyber Pornography/ Hosting/ Publishing Obscene Sexual Materials (Sec.67A/67B(Girl Child) of IT act r/w other IPC/SLL)	Cyber Stalking/ Cyber Bullying of Women (Sec.354D IPC r/w IT Act)	Defamation/ Morphing (Sec.469 IPC r/w IPC and Indecent Rep. of Women (P) Act & IT Act)	Fake Profile (IT Act r/w IPC/SLL)	Other Crimes against Women	Total Cyber Crimes against Women
1	Andhra Pradesh	16	89	129	1	2	400	637
2	Arunachal Pradesh	0	1	0	0	0	4	5
3	Assam	10	101	3	0	41	455	610
4	Bihar	1	4	18	0	12	49	84
5	Chhattisgarh	3	200	7	0	0	69	279
6	Goa	1	4	1	0	0	26	32
7	Gujarat	3	43	48	0	7	251	352
8	Haryana	12	71	28	0	7	209	327
9	Himachal Pradesh	0	21	12	0	3	10	46
10	Jharkhand	0	10	2	1	0	93	106
11	Karnataka	1	234	0	0	0	3669	3904
12	Kerala	0	122	45	2	9	203	381
13	Madhya Pradesh	8	96	82	2	1	201	390
14	Maharashtra	11	75	578	3	27	1836	2530
15	Manipur	0	0	5	0	0	8	13
16	Meghalaya	0	5	0	0	4	18	27
17	Mizoram	0	0	0	0	0	0	0
18	Nagaland	0	1	0	0	0	0	1
19	Odisha	0	269	0	273	0	32	574
20	Punjab	3	33	26	0	6	126	194
21	Rajasthan	16	136	79	3	11	253	498
22	Sikkim	0	1	0	0	0	10	11
23	Tamil Nadu	3	82	31	24	22	239	401
24	Telangana	23	14	279	0	3	943	1262
25	Tripura	0	2	0	0	2	0	4
26	Uttar Pradesh	2	450	27	1	4	617	1101
27	Uttarakhand	10	21	17	75	8	30	161
28	West Bengal	0	9	11	0	3	119	142
Total State (S)	Total State (S)	123	2094	1428	385	172	9870	14072
29	Andaman and Nicobar Islands	0	3	1	0	0	8	12
30	Chandigarh	0	2	2	0	0	12	16
31	Dadra and Nagar Haveli and Daman and Diu	0	4	0	0	0	1	5
32	Delhi	2	118	24	0	5	101	250
33	Jammu and Kashmir	0	25	2	0	2	10	39
34	Ladakh	0	0	0	0	0	0	0

Source: https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf

STRATEGIES TO PREVENT CYBER CRIME AGAINST WOMEN

1. A coactive approach involving the initiatives and steps taken by the Government and other legislative bodies to
2. address such crimes would be the best way to tackle these cybercrimes to avoid cyber stalking it is advisable not to disclose any personal information online.
3. Sending personal pictures online to friends and
4. strangers during chat has been seen a major cause for crimes against women. Refraining from such acts is essential
5. It is cautious to keep the credit and debit card details confidential at any cost. Reliable sources should be checked in case of genuine transaction
6. Empower and educate women and children with adequate knowledge and awareness about the occurrence of such gross crimes in the society to keep them protected and safe
7. Firewalls serve as a great first line of defence when it comes to checking such trespasses. Ensure the safe use of security checks. Always enable the firewall that comes with your router
8. Exercise caution and Presence of mind in dealing with such threats. Do not fall prey to fancies
9. Become aware of the legal framework and proceedings that are connected to such crimes, in order to take action immediately when trapped
10. Be well informed about the advancements in the technology and internet to stay unharmed.

Information Technology Act 2000

This act is known as the cyber law of India. It is India's mother legislation, regulating the use of computers, computer system, computer networks, communication devices as also data and information in electronic format. This legislation has touched various aspect of crime like cybercrimes and liability of network providers. The said act was amended in the year 2008Due to amendment all kinds of cell phones, phones, tablets and personal digital have been brought within the ambit of cyber law.

Salient Features of the Act related to cybercrime against women-

Information Technology Act 2001 is a key weapon to prevent cybercrime. The act basically deals with online transaction but some its provisions deals with the offence against human body. The major provisions of the Act are as follows-

Electronic obscene content-

Section 67 of IT Act prevents publishing and transmitting of obscene contents on the internet which disturbs public order and morality. It is based on sec 292 of IPC. But the amount of punishment is higher in IT Act2000. It is a bailable offence.

Sending of offensive messages

Section 66 A provides for the offence of sending offensive messages through communication devices or computer resources. Section 66A makes it a offence when it is send by means of a computer resource-

Spam Messages

It is important that 66A©tries to cover slightly the phenomenon of spam. But this provision is not very effective.

Identity Threat-

Section 66 C has provided for the offence of identity theft. The said offence is bailable offence where the accused even if arrested be entitled to bail as a matter of right.[22]

REASONS FOR THE GROWTH OF CYBER-CRIME AGAINST WOMEN

The transcendental jurisdiction of Internet causes the major threat to the society in the form of cybercrime. The main victim of this transgression can be considered women and children. Studies shows that we have 52 million active internet users in India which reached at 71 million in the year 2009. Among them working women net users are 8% and 7% nonworking women in the year 2009 and 37% usage of all users accessing internet through cyber cafeì10. It is very common occurrence that the essential data of the internet surfer is being released effortlessly by the owners of cyber cafeì and then it is used for illegitimate dedications. Though acquaintance with technology is constructive facet that can be considered vital for the progress of any country but at the same time it is becoming the foundation to upsurge the offense rate with technology against the weaker sector of the society. Statistics also show that cyber awareness amongst people in India in really low.[3]

The objective of the IT Act is crystal clear from its preamble which confirms that it was formed largely for improving e-commerce hence it covers commercial or economic crimes i.e. hacking, fraud, and breach of confidentiality etc. but the drafters were unacquainted with the protection of net users. As we deliberated above that majority of cybercrimes are being prosecuted under Section 66 (Hacking), 67(publishing or transmitting obscene material in electronic form), 72(breach of confidentiality). The most of the cybercrimes other than e- commerce related crime are being dealt with these three sections. Cyber defamation, cyber defamation, email spoofing, cybersex, hacking and trespassing into ones privacy is domain is very common now days but IT Act is not expressly mentioning them under specific Sections or provisions11. Whereas IPC, Criminal Procedure Code and Indian Constitution give special protection to women and children for instance modesty of women is protected under Section 509 and rape, forceful marriage, kidnapping and abortion against the will of the woman are offences and prosecuted under IPC. Indian constitution guarantees equal right to live, education, health, food and work to women, however until recently there were no specific penal provisions protecting women specifically against internet crimes. Ever since the 2012 Delhi Gang Rape case (Nirbhaya Case) there has been a huge outcry over bringing out new reforms and penal provisions so as to protect women against the criminally minded. The 2013 Criminal Law Amendment Ordinance contains several additions to the Indian Penal Code, such as to sections 354, 354 A, 354 B, 354 C & 354 D, with the assistance of these sections now the issues of MMS scandals, pornography, morphing, defamation can be dealt in proper manner.

Most of the cybercrimes remain unreported due to the hesitancy and shyness of the victim and her fear of defamation of family's name. Many times, she considers that she herself is accountable for the crime done to her. The women are more vulnerable to the danger of cybercrime as the perpetrator's identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. Women fear that reporting the crime might make their family life difficult for them, they also question whether or not they will get the support of their family and friends and what the impression of society will be on knowing about them. Due to these fears women often fail to report the crimes, causing the spirits of culprits to get even higher.

CONCLUSION

Under the Indian Law enforcement framework, a solid correctional activity is

endorsed against the blamed for such egregious wrongdoing yet there is no system accessible as for the right of the casualty to get the shocking photos erased from the internet-based stage. No arrangement IPC and IT represent ground real factors of ladies' encounters. Procedural obstacles likewise are impeding equity to ladies. On the off chance that any photos posted on Global pornography site, there is no component accessible in India to erase that photos or video. The lady mindful going to how to utilize the web-based stages yet they don't know about what to do after trapped in tough spot and digital violations. Ladies will take alert prior to posting own or adore ones photos or video, essentially, they will give secret phrase for online material which will distribute in on the web. Change secret key opportunity to time.

Author's Declaration:

I/We, the author(s)/co-author(s), declare that the entire content, views, analysis, and conclusions of this article are solely my/our own. I/We take full responsibility, individually and collectively, for any errors, omissions, ethical misconduct, copyright violations, plagiarism, defamation, misrepresentation, or any legal consequences arising now or in the future. The publisher, editors, and reviewers shall not be held responsible or liable in any way for any legal, ethical, financial, or reputational claims related to this article. All responsibility rests solely with the author(s)/co-author(s), jointly and severally. I/We further affirm that there is no conflict of interest financial, personal, academic, or professional regarding the subject, findings, or publication of this article.

References-

1. https://www.researchgate.net/publication/346623839_Strategies_to_Prevent_and_Control_of_Cybercrime_against_Women _and_Girls/link/5fc9d5e1299 bf188d4f159bf/download
2. https://www.ijrar.org/papers/IJRAR1944342.pdf
3. SSRN-id2486125.pdf

Cite this Article

'Surendra Kumar; Dr. Akhil Yadu" Mapping the Dark Side of Digitalization: Nature, Forms, and Impact of Cybercrime Against Women", Research Vidyapith International Multidisciplinary Journal, ISSN: 3048-7331 (Online), Volume:2, Issue:12, December 2025.

Journal URL- https://www.researchvidyapith.com/

DOI- 10.70650/rvimj.2025v2i12004

Published Date- 03 December 2025