CYBERCRIME AND SENIOR CITIZENS IN INDIA - A COMPARATIVE STUDY OF LEGAL FRAMEWORKS WITHIN CYBERSPACE GLOBALLY

Written by ***Adv. Aditi Srivastava* & Dr. Ritu Gautam*****

** Research Scholar, School of Law, Sharda University, Noida, India*

*** Assistant Professor, School of Law, Sharda University, Noida, India*

DOI: doi.org/10.55662/CYLR.2023.2102

ABSTRACT

Cyber space regulation is that arena which is growing very rapidly, due to multidisciplinary approach in tackling innovation, technological updation, persistent cybercrimes emerging from interactions within cyberspace. This doctrinal paper is a critical study and analysis of challenges faced by stakeholders, jurisprudence of crimes committed within cyberspace, effect on vulnerable group 'senior citizens' as potential victims since emergence of Information Communication Technology. Aimed to study international treaties, national policies of QUAD members, statutes, community help programs, emerging new theories of cyberspace jurisprudence, adopted by netizens, challenges that are being faced by all the stakeholders to influence cyberspace, socio economic legal disabilities within a sections of society, principles or prepositions thus found, important facets of cybercrime comprehensively to contribute in the development of Cyber Security legislations and Regulatory Framework of India, for a secure safe cyberspace as severity of the issues, challenges in cyber victimization against senior's can permeate legal gaps as previous research efforts have largely revolved around women and children, while neglecting them. Victimization in cyberspace is pushing seniors further away from use of technology confidently so as to kick off original plans for equalitarianism as envisioned in our constitution.

Keywords*: Cyberspace, Senior citizens, Victimization, Cybercrimes, Silver Economy*

1. INTRODUCTION

Senior Citizens with their invested capitals is becoming sinecure for perpetrators, the amount involved in bank fraud cases is amounting to 41,000 crores (*Reserve Bank of India Report, 2021-22).*

As per statistics 2/3 of the world's senior adults are living in developing countries, estimated to increase by 80% in 2050 to 2 billion approximately (*United Nations Population Division report, 2010)*. In United States of America, every 1 in 10 senior adults felt victim to cybercrimes specifically online frauds, which is 38 % approximately 6, 45,000 victimized (*Watson, 2020*). Statistical study of USA states that by 2030, senior's population will be 70 million as 20% will reach the age of 65 or older due to increase in life expectancy and will be victimized by cyber frauds due to social change which is pushing them from books or television to using internet for communication, healthcare, social interaction, entertainment, buying or banking activities.

Cyber space is a Greek word meaning 'steersman/communications', which is control interaction between machines and animals used by Norbert Wiener in 1948 in fields of "cybernetics". Later by Gibson in 1984 in his novel 'Necromancer' giving popularity to this term 'cyberspace' for wider acceptance to activities within virtual space e.g. cybercrime, cyber surfing, cyber transactions etc. Main importance of cyberspace is to connect people globally, share information in regard to the current state of affairs and on negative side this information can be used by cyber deviants to convert traditional crimes into technical in order to commit fraudulent activities or graver crimes carving a need for cyber laws and its regulations giving new terminologies e.g. cybercrimes, netizens etc. Digital technology's function is to shape social life, experiences, feelings, interactions, objects of emotions, relationships to integrate media and its usages *(Givskov, 2017).* Social media or virtual platforms have deep influence upon its users' perceptions, issues revolving around rights, privacy, time spend online and barriers to exchange of information *(Joo and Teng, 2017).*

International Community's commitment to secure their individual digital spaces can be seen by various measures implemented in their domestic legal arenas to finally assent to Budapest Convention. This era is known as an artificial intelligence age, cyber world is much bigger than any other dimension of traditional communication, wide spread participation with infinite contribution to reach human goal of attaining status of techno acme. Both are inseparable units. Even though it is aiding human community, technology has become biggest threat for breaching privacy, safety of users (data theft leading to cybercrimes) as prevention of cybercrimes require technical know-how. *"Cybercrime is a major challenge to a developing society and digital economy, Europol's main priorities is to fight cybercrime"* European Union Serious Organized Crime Threat Assessment (SOCTA) Report.

Cybercrime *(Sussman and Heuston, 1995)* is multiply definite word based on modus operandi, illegal acts, target or tool. It is used interchangeably as electronic crime, cybernetic crime, e-crime, information age crime or digital crime, high-technology crime. A perpetrators motive is to have fun and stealing *(R. Sabillon et. Al, 2016)*. At international level, cybercrimes fall under 2 broad distributions either

1. Financial or/and
2. Content motivated.

2. NEED FOR PROTECTED CYBERSPACE

Approximately 306 cybercrime cases got registered for child victims in 2019 increased to 1,102 cases in 2020 (*National Crime Records Bureau Report)*. Any law is outcome of social conflict caused due to different opinions on any prevalent ideas. Various communications happens within digital space with limited control over boundaries, cyber laws restore order and infringement of rights of digital society by penalizes criminal activities effecting cyber community. Any Contemporary society in digital era, due to direct import of electronic information, e-commerce, virtual data and intellectual properties, virtual banking are primary target leading to cyber invasion and crimes committed against a secured country with an intent to bring economic crisis, encounters several cybercrimes on daily basis. Thus, every State is vulnerable to cybercrime of new age sand misuse of cyberspace new age.

Parliament of India legislated "Information and Technology Act, 2000" and amendments to important statutes, exclusively for addressing cybercrimes contraventions and forthcoming Data Privacy Bill, 2022 protects the right to privacy as directed by Honorable Supreme Court will qualities of being adaptable and internationally aligned yet, balancing interest of all the stakeholders.

3. IMPORTANCE OF DIGITAL INCLUSION FOR VULNERABLE GROUPS

Honorable Prime Minister of India has addressed the challenges of cyberspace and digital infrastructure with full commitment in formulating stringent cyber security framework, amendments to accommodate the philosophy of *'digital democracy'* to enjoy and improve technology eased living, exploited by all citizens with equality of access, empowering one's rights under Art 14, 19, 21 of Constitution and have State's sustainable development of cyber diplomacy (*Independence Day speech by PM Modi, 2020*). By 2050, global population in urban cities will increase by 8.9 billion faced with huge income disparities, economical imbalance leading to new avenues to generate income and social communication, United Nation's 65/230 resolution cautioned all member nations to frame their legal policies accordingly (*World Economic Forum Global Risks Report, 2012).*

Marginalization also called social exclusion refers to pushing of certain groups of society due to their distinct vulnerabilities such as lack of access to rights, opportunities poverty, lack of awareness, health issues and resources from main stream. A major cause of vulnerability is the exposure to a range of possible harms, victimization, in ability to deal with them adequately. Thus, staying tangled up in that vicious cycle of disability. The whole responsibility of cybercrime, guilt, shame lies on the shoulder of victim they are labeled to be *"ignorant, just greedy, idiots, unintelligent dope"*, shifting the whole focus from offender's illegal actions, psychological convincing, manipulating skills onto them addition to getting negative overreactions, with no support from family, friends, especially observed in online romance, financial frauds *(Cross, 2015).*The usual content that is received as part of cybercrime are emails, phone messages flashing common type of messages projected to availing discounts on medicines, healthcare services, financial benefits, equity and retirement, tax saving, short term

maturity schemes, marriage or dating sites all very specific yet generic to all seniors amounting to a loss of $34,200 *(McAfee's survey,2020)*.

But, as a progressive society legal frame work have addressed the issue of not having strong laws which need seriousness in investigation, reporting, maintain database for comparison and fast trials of such cybercrime cases. 'Digital Literary', communication and networking's aim is active participation or inclusion of all, irrespective to their age or needs in any given society *(Cross, 2015)*. Countries in Asia are amending their laws to get aligned with Budapest Convention.

4. FORM OF CYBERCRIME AGAINST SENIOR CITIZENS

Amid pandemic cybercrime rose against elderly victims as they migrated to accommodate this change and accepted shopping online, connect with others leading to easy venues for perpetrators to post false advertisements and defraud them. As based on types of cybercrimes seniors are victimized with main motive to gain monetary benefits rather than content based which has sexual abuse connotation as seen in cases of child or women victims. Therefore, with filed complaints it was observed that senior citizens are victims of phishing frauds, romance scams, financial scheme, tech support, tele caller frauds (posing as service representative to resolve compromised bank account/email or virus/license renewal advisor), lottery sweepstake scams, fake charity contributions, identity theft, Life insurance/savings with higher return prospects, Non-Payment/Non-Delivery, impersonation as government agent threatening arrest on alleged crime demanding in clearing the name or help in investigation. The total numbers of complaints were 105,301 amounting to a total loss of $1 billion, overall increase of approximately $300 million reported in 2020 as compared in 2019. Criminals used to groom the senior victim to gain his trust and use tactics of intimidation, threats or manipulation in order to take advantage and commit above crimes *(IC3, 2020).* Prevention, Control of Computer Related Crime states the difficulty to define or identify cybercrimes due to lack of comparative statistics, comparison to other types of tradition crimes due to ever changing nature.

2020 CRIME TYPES

Over 60 Victim Count

Crime Type	Victims	Crime Type	Victims
Extortion	23,100	Employment	1,867
Non-Payment/Non-Delivery	14,534	Terrorism/Threats of Violence	1,692
Tech Support	9,429	Investment	1,062
Identity Theft	7,581	IPR/Copyright and Counterfeit	552
Phishing/Vishing/Smishing/Pharming	7,353	Ransomware	365
Spoofing	7,279	Malware/Scareware/Virus	287
Confidence Fraud/Romance	6,817	Corporate Data Breach	285
Personal Data Breach	6,121	Health Care Related	243
Misrepresentation	4,735	Civil Matter	170
Government Impersonation	4,159	Re-shipping	114
Lottery/Sweepstakes/Inheritance	3,774	Charity	105
BEC/EAC *	3,530	Crimes Against Children	58
Other	3,259	Denial of Service/TDos	52
Credit Card Fraud	3,195	Gambling	16
Advanced Fee	3,008	Terrorism	7
Overpayment	2,196	Hacktivist	5
Real Estate/Rental	1,882		

Descriptors*

Social Media	4,533	These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.
Virtual Currency	9,447	

2020 Crime Types *Continued*

Over 60 Victim Loss

Crime Type	Loss	Crime Type	Loss
Confidence Fraud/Romance	$281,134,006	Overpayment	$11,212,323
BEC/EAC *	$168,793,903	Corporate Data Breach	$10,148,817
Tech Support	$116,415,126	Ransomware **	$5,332,312
Investment	$98,040,940	Health Care Related	$2,652,390
Real Estate/Rental	$50,098,565	Civil Matter	$1,866,788
Other	$49,689,594	Misrepresentation	$1,815,552
Government Impersonation	$45,909,970	Terrorism/Threats of Violence	$1,112,825
Spoofing	$40,886,040	Malware/Scareware/Virus	$671,667
Non-Payment/Non-Delivery	$40,377,167	Charity	$629,295
Identity Theft	$39,006,465	Re-shipping	$588,553
Lottery/Sweepstakes/Inheritance	$38,804,343	IPR/Copyright and Counterfeit	$479,375
Advanced Fee	$33,184,114	Crimes Against Children	$411,349
Personal Data Breach	$24,641,539	Denial of Service/TDos	$180,447
Credit Card Fraud	$20,780,800	Gambling	$17,450
Phishing/Vishing/Smishing/Pharming	$18,829,999	Terrorism	$0
Extortion	$18,503,168	Hacktivist	$0
Employment	$16,092,611		

Descriptors*

Social Media	$35,344,786	These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.
Virtual Currency	$55,056,901	

* Regarding BEC/EAC adjusted losses: This number also includes complaints in which an Over 60 person may be filing on behalf of a business who is the actual victim of a BEC scam.

** Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victims directly reporting to FBI field offices/agents.

Source FBI Report, 2020 Types of cybercrimes against Senior Citizens with number of victims and monetary loss

Above data show segregation of cybercrimes into types against senior citizens in year 2020 in USA with extortion as top cybercrime with maximum number of victims.

5. GLOBAL LEGAL FRAMEWORKS FOR CURBING CYBERCRIMES TO SECURE CYBERSPACE

In 2018, it was reported that 53% of the world's population had Internet access with 68% having smart mobile phones with direct connection between digital divide, different forms of social inequalities as main culprits such as lack of basic education, deficit access to technology or devices etc. to conclude that such divide is more socio legal rather than just lacking technological capacity. The data related to senior citizens using technologies/ internet in counties with Norway as highest 65%, Spain, Czech Republic to be 5% and Hong Kong, Macao (China), Slovakia, Singapore, and Korea to be 10%, Oman, El Salvador, Thailand, Colombia, Bangladesh, Iran, Ukraine, Bolivia, Belarus, Peru, and Palestine to be below 2% *(Guidelines of United Nations, UNESCO, NIS (Network and Information System)*.

In 21st century significant international and regional treaties to counter cybercrimes even racism, online grooming, computer offences etc. are formulated binding, non-binding and multilateral in nature:

(i) Europe Union's
(ii) League of Arab States
(iii) Shanghai Cooperation Organization,
(iv) African organizations,

a. In United States of America, every 1 in 10 senior adults felt victim to cybercrimes/frauds, 38% approximately 6,45,000 victimized by a peculiar cybercrime witnessed during Covid-19 pandemic, where fake websites were launch to sell online products e.g. medicines, oxygen cylinders, vaccines, air filters, blood test services, Covid testing home services, personal calls to stole personal information misrepresenting as government agencies, charities for pandemic donations, social security verification calls, provident fund or policy

relapse calls targeting elders (*IC3ElderFraud Report, 2020).*Offender used 'social engineering techniques' such as manipulation, psychological tactics to exploit the senior adult victims, who were influenced with the deceiving communication or promises that they ignored their own reasoning mind, discrimination nor taking advice from family and friends to prevent falling prey to cybercrimes *(Watson, 2020).*

Senior Citizens are 'disproportionately vulnerable' and 'Heterogonous group' *(America's Pew Research Center, 2016)* are both migrants and first generation users of current digital space, of information, communication technology, online banking system and personal smart phone and gadgets. Their digital engagement is based on '*uses and gratifications theory*' not uniform as influencing variables such as 'unequal access and incompetency' have direct and consequential influence for using digital media or similar technologies *(Ezeh and Mboso, 2019).*Typology of Schafer and Fattah's categories of cyber victims fall on a scale of non-participating, predisposed, provocative, precipitative, false victim, biologically weak, socially weak, self-victimizing and political victims *(Burgess et al., 2013).*Senior with their own set of disabilities like other vulnerable groups, need to be empowered to establish coping and digital skills under a sensitive legal support system at their own convenience and pace to be able to see red flags prevent, protect their own savings But, if defrauded than have a plan to activate police investigation, judicial proceedings for recovery along with legal, financial and psychological counseling to resolve feelings of trauma and carryon with judicial process to seek justice. It was observed that humor was used to reduce the seriousness as a coping mechanism cope with cybercrime victimization or aversive experiences of life *(Pogrebin and Poole, 1988).*Victims of cybercrime project pain as hilarious incident, trying to not look like fool, seeking solidarity to reduce the actual impact of mental trauma thus suffered (Cross, 2015).

Collective actions taken within legal framework and community help group such as '*Senior Tech Program*' teaching computer, mailing and how to use internet to senior adults, CWAG (*Coalition of Wisconsin Aging Groups)*, '*Elder Law'* to educate for seeing red flags of cyber frauds, scams and empower by cybercrime content such as Identity Theft Toolkit; Prevent and Protect; Elder Exploitation Basics and assist in legal aid, pushing agencies for investigation, funding and to make specific laws as and when needed. Police run '*Surf*

Days'; '*Operation Web Snare and E-Con'* covering domestic, international, economic cybercrimes as a coordinated efforts towards prevention by awareness, sharing data base information, active investigation, arresting, punishing. *BT Grandparent* teaches skills to operate, share data, personal information, detect cybercrime or fraud by younger citizens. Who educate seniors along with training to bank staff, police personnel on how to respond to complain by senior adults, gather evidence, stop data leaks etc. Collective participation of youth, community and family will create a secure environment for not getting victimized by cyber criminals. Los Angeles' *Elder Abuse Forensic Centre* have clinicians, who evaluate seniors' living environment, financial decision making, cognitive functioning via cognitive tests to conclude on 'consent' in case of financial exploitation done by family members or cybercrimes *(IC3 Federal Bureau of Investigation Report, 2020).*

Department on Protective Services for Aging of Temple University formulated plan to bridge the gap between all the stakeholders to solve fragmentation approach of getting timely justice, conviction in cyber crimes involving senior citizens as "notion of offense seriousness" and "notion of accumulated legal capital" can greatly affect victims' behavior to report cybercrimes with level of motivation showed by authorized agency to acknowledge full cycle of offence as a "serious offence" even though not being physically violent like other traditional crimes or perceived *(Black, 2000).*Researches are being conducted in technological innovations for developing senior citizens friendly website to avoid falling prey *(Patsoule and Koutsabasis, 2014)* which use very innovative, simple methods to commit cyber crimes *(Governmental Accountability Office, USA, 2020)* studied by Adult Protective Services agency and American Association of Retired People (USA) agencies.

b. In Canadian movements such as '*Safe Pharmacy'* under Canadian Network for the Prevention of Elder Abuse's guidelines advising lifestyle, support groups, detecting red flags, not to transfer money to vague unknown sources etc. is being run. Taking cybercrimes against seniors very seriously, collective actions within legal framework are identity theft penalty, spyware (I-SPY) prevention, computer crimes acts and community run programs based on USA's '*Elders in Action*' giving legal guidance, latest information,

support, recovery of defrauded money, report suspicious messages to groups officers address issues of cybercrimes targeting senior's.

Source: Canadian Network for the Prevention of Elder Abuse's guidelines, accessed at 4.40 pm on April 26, 2022 Twitter

c. **In Europe/United Kingdom** have accepted specific punishments for specific cyber crimes, thereby enforcing a positive change for senior citizens to have a vision for formulating educational strategies, technology skills for holistic inclusion of elderly population. European Union Agency for Network and Information Security looks into cyber security certification framework for products and services, outlining best practices, steps against ransom ware, promoting cyber resilience, cooperation to member States in case of major cross-border cyber attacks and crises. European Union's Convention, 2020 advised all member states of United Nation to develop a State level 'Minimum access policy'; 'Unique user identification';'Clean desk policies','Biometric identification','Antivirus software/encryption algorithms', 'Scanners for malware/mobile network', 'Firewalls and password securities to achieve a safer cyberspace

(Simasathiansophon et al., 2021). Action Fraud (United Kingdom) is agency to take cognizance of Cybercrimes against Senior Citizens.

d. **In Japan** Penal Code was revised in 2009 for facing challenges of cybercrime, strengthening investigative powers by seizure of data (from computer servers), punishing creation, storage or acquiring of virus, sending pornography emails, request of internet service providers to retain communications logs by authorities e.g. list of names of email senders and recipients up to 60 days *(Kyodo, 2011).*

e. **In Australia** Cyber Security Centre (ACSC) improve cyber resilience, community support. It delivers understanding of cyber threats/crimes, gives advice and assistance to its citizens to manage digital risks. Department of Home Affairs, Australian Federal/Criminal Intelligence Commission, Security Intelligence Organization, Joint Cyber Security Centers (JCSC) in Brisbane, Perth, Melbourne, Adelaide and Sydney help all agencies to collaborate in cyber secure interaction. Reporting systems such as ACORN is used.

6. INDIAN'S EFFORT TO CURB CYBERCRIMES AND SECURE CYBERSPACE

"India is 4th among top 50 countries in terms of number of cyber crime complaints to Internet Crime Complaint Centre" (The Telegraph, 2015)

New dynamics of '*Digital India initiative, 2015*' shall affect State's and citizens legal, communication rights with increased online crimes/frauds. How larger goal of safe digital framework can be enjoyed by our society especially vulnerable, marginalized sections has been the foremost aim of every egalitarian society in areas concerning children, women and minority groups, with '*digital have and have not's*. It is been observed that due to their specific disabilities senior citizens are lacking behind, who are either first generation migrants or due to every second evolving cyberspace, lack updated awareness when compared to other vulnerable sections. Digital inclusion can make them contribute and form a productive segment in consumer market without fear of cyber abuse, harassment and online financial frauds as

observed by increased number of cases of cybercrimes since information technology penetration in pre, during and post Covid pandemic *(Duggal HT, 2021)*. Digital rights' infringement, existing vulnerabilities ranging from financial, physical, emotional and technical to counter cybercrimes perpetrated against them, causation with targeted solutions, current inclusion in 'Digital Initiative' undertaken by Government of India, under the flagship of Honorable Prime Minister *(5th Global Conference on Cyber Space, New Delhi 2017)*. Along, with ground level perception of information technology, changing social interactions amid Covid-19 pandemic, cyberspace knowledge at hand to address issues of privacy, preserving personal data, evidence, how to activate legal machinery to fully confront online frauds, cybercrimes and utilization of aligned initiatives to promote *'Silver Economy'* undertaken by Ministry of Social Justice and Empowerment and reminding us the importance of '*Free and Fair Digital Economy*, evolving consumer market segments to included senior citizens as users of digital products and increase their 'Legal capital and cyber skills/awareness' *(SAGE and SACRED initiatives,2022*). By understanding the trauma, victimhood suffered by senior citizens in cases of cybercrimes one can use this phenomenon and make suggestions for a stronger legal framework having effective reporting, acknowledgement of crime, to take stricter actions against the perpetrators *(Cross, 2015).*

a. Vulnerable cyberspace and current status of cybercrimes

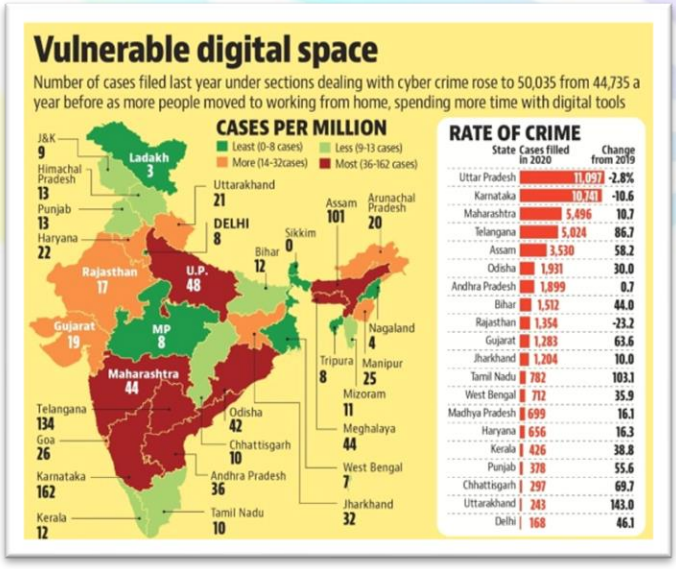
Total rate of cybercrimes per 1, 00,000 people have increased from 3.3 to 3.7 in 2020 with registered cases rising from 50,035 to 44,735 from 2019 to 2022 (Reuters).

NCRB on cybercrimes has very limited picture to present as reality is way graver due to pandemic turning this crime into cottage industry as reported where online financial frauds targeted smaller cities and vulnerable section of society. Online Survey of 1,200 adults gave an overview post pandemic that 90% felt they would take data privacy seriously, if it was treated like a currency as they still were unsure about cyber risks, personal information theft and safety of financial data. Nor they felt confident in their ability to prevent a cyber attack or hacking of private details like address, date of birth, banking details (invading their right to privacy, forgotten) even though they purchased security software to counter exposure to online

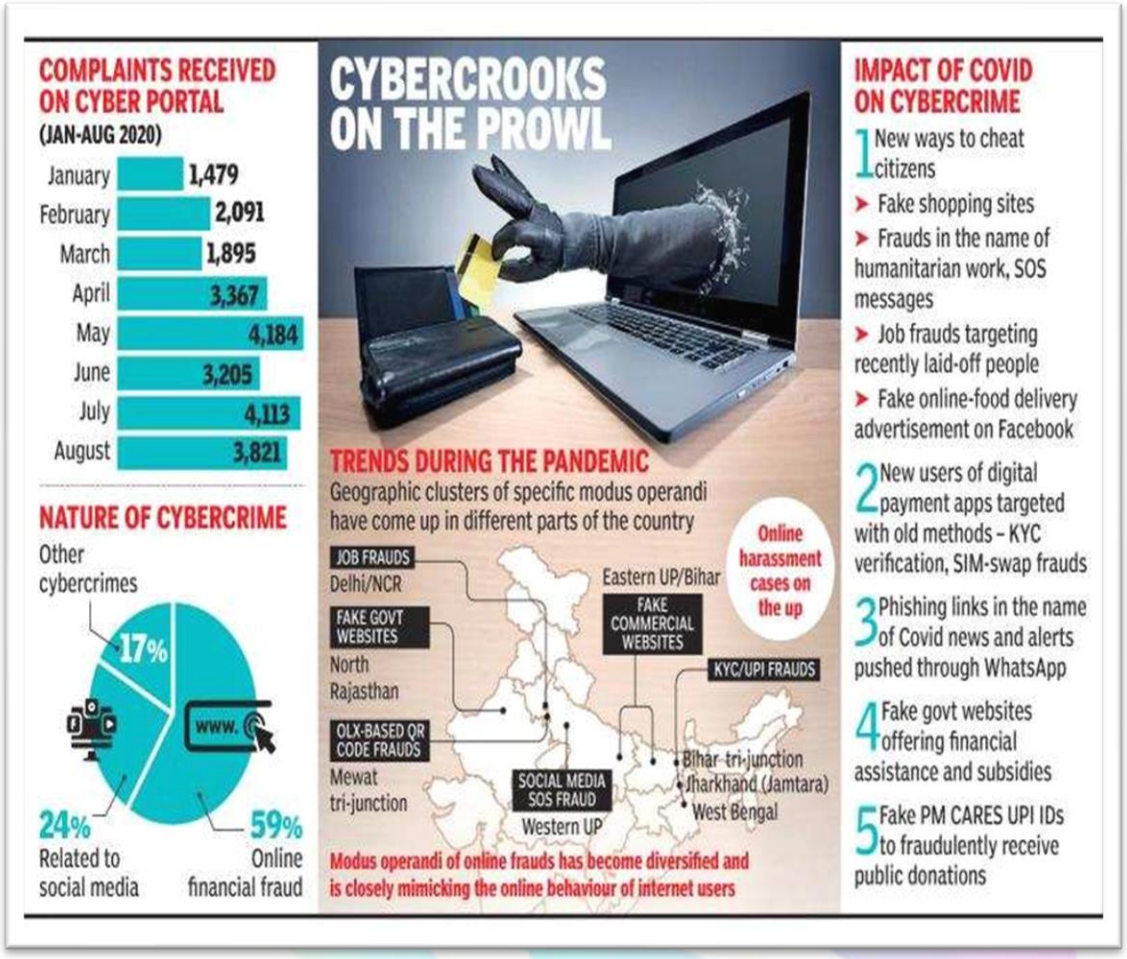
activities which ranged from ordering food with maximum comfort level to least being online dating. *(Duggal HT, 2021).*

There has been an urgent need to fill up the gap created with digital inclusion for more robust elder care ecosystem in India, as witnessed amid Covid phase, as elderly population is increasing from 7.5% in 2001 to 19.5% in 2050. The promotion of '*Silver Economy'* as a sector and expanded business opportunities will emerge from technological enterprises, roping in big brands for retraining the seniors' in legal, financial, insurance, medico-legal, food, health, infrastructure etc. services e.g. such as senior care centers, housing, improved living facilities only possible with active data enabled researches and ideas called from all (*SAGE, The Ministry of social justice and empowerment*, 2022).

Prompt measures though still in process taken by Reserve Bank of India to make opening of bank account more stringent, issuance of sim cards using KYC done by physical verification and by providing guidelines 'Safe Digital Banking Practices', Department of Telecom launched portal called TAFCOP (Telecom Analytics for Fraud management and Consumer Protection) for checking duplicate sim cards being used against 1Adhaar card are some of current updates in securing cyberspace.



Picture 1 - Source by NCRB 2020, Sep 16, 2021 04:51 pm Hindustan Times



Picture 2 - Source by NCRB 2020, Feb 4, 2022 05.02 pm Times of India

It can be seen from the above statistics that rates of serious crimes fell of per state but, cases of cybercrime rose with 11.8% parallel with increased digital penetration. This itself gives a fair idea that cyberspace requires immediate attention with more stringent legal regulations. Cybercrime arrests were registered as 841 out of 4,212 for 2014 to 2018 and solved bank fraud were 1,532 (only 11%) with only 5% total stolen money recovered *(Narayan, 2019)*. Internet access is achieved in class 'A' cities of India such as Mumbai, opportunity exploited by educated senior adults, such as using latest mobile phones to stay connected with friends and families, banking services or just entertainment, exposing them to cyber crimes due to lack of knowledge, trusting nature, exposure to abuse from care givers, health and dependency on others also added to victimization. Major concerns were how to approach the legal system for

proper active steps, to resolve cyber crimes, inadequate access to published data by government authorities, which in turn are helping perpetrator to criminally defraud senior adults in Mumbai city together with rising cases in pan India, where cyber crimes are under reported due to shame, cumbersome process, lack of trust in police and banks as data is breached from such entities, establishing attributes of an organized crime, having interstate operations adding to the woes *(Tripathi et.al, 2019).*

Level of awareness about cybercrime phenomena, in both settings where senior adults stay in old age homes and at home with family was studied in Lucknow City, resulting in disparity of digital literacy (medium level of knowledge) to those residing at old age homes (minimum level of knowledge). An active social life, financial health and being part of digital inclusion, presents an opportunities to cybercriminals to commit cyber crimes against seniors adults, even though they feel pressurized to use smart phones as part of digital initiative still they were unsure to handle online banking or prevent cybercrime, leading to feeling depressed, as ways to counter these criminals is unknown to them. Memory loss, ageing are few of the major disabilities barring them to search, preserve evidences from their smart phones. With investigating agencies putting the onus on them to learn, protect their leaked data, while banking sector faces neutral response from police as a generalized statement 'its everyday's common incident and very hard to respond to each and every complaint'. Nascent Laws for securing cyberspace as compared to developed nations in customer's data privacy and security add woes in smooth functioning of online transfers. Banking laws need to be modified to take on liabilities for fraud compensation, accountability for data theft, lacking security or employee's dishonest action facilitating such crimes *(Agarwal and Nabat, 2014).*

Picture 3 - Source Cyber Dost App accessed at 4.39 pm April 26, 2022 Twitter

PLAINS TOP IN FRAUD, HILLS IN RECOVERY

DISTRICT	Cases of cyber financial fraud reported	Cases in which the money was recovered	Recovery rate (%)
Almora	149	44	29.5
Bageshwar	93	32	34.4
Chamoli	140	36	25.7
Champawat	106	51	48.1
Dehradun	2059	544	26.4
Haridwar	756	201	26.6
Nainital	464	140	30.2
Pauri	229	130	56.8
Pithoragarh	190	66	34.7
Rudraprayag	86	22	25.6
Tehri	184	68	36
US Nagar	574	146	25.4
Uttarkashi	115	32	27.8
TOTAL	**5,145**	**1512**	**29.4**

Source: Data on cyber fraud from June, 2021, to February, 2022, as provided by Uttarakhand Police

It can be clearly understood from the above data that cybercrime in Uttarakhand's plain districts with most digital penetration is rising, mostly cyber frauds with less recovery rate and very

surprisingly with more recovery rate with less digital penetration in hilly districts. *(Das.K, Times Of India,2022)* ranking as top in all Himalayan hilly state with most numbers of cyber online financial fraud victims total of 775 in 2018- 2022 cybercrimes followed by Himachal, Tripura, Arunachal Pradesh, Meghalaya, Nagaland, Sikkim, Manipur and Mizoram amounting losses up to 1.68 Crore still expanding(*(SSP STF, Singh. A, Indian Express, 2022).* Financial gain is the constant motive for committing cybercrimes apart from revenge, extortion, political causes *(Goel, 2016).* India's own Database System, Quantam Tec's role (not foreign cloud or domains cyberspace) solve storage issues and secure data infringement or theft which the perpetrator used as means to commit cybercrimes *(Sanjeev, 2021).*

Surat City Police's '*No Tolerance against Cybercrime'* campaign and seminar at Vanita Vridashram campus (150 club's senior members of city participated) to create awareness about cybercrimes with help of retired professionals, as an experiments to educate senior citizens about 35 modus operandi of cyber frauds, who shall further educate their families /neighbors, literature about online risks, prevention mechanism was also shared. As it was observed seniors are not comfortable with technology, smart phones (video calling, checking messages) thus, becoming susceptible victims of loan, insurance policy, provident fund frauds or sharing personal information *(ACP, Y.A Gohil, Times Of India,2021).*

b. Judicial Intervention for Senior Citizens.

"It is the duty of court to see early disposal of cases on priority bases whether civil, criminal, services or any type of litigation to enable them to enjoy fruits of litigation during their lifetime. Delay is unreasonable and contrary to procedure contemplated by law. It is not sufficient to respect or honor senior citizens by giving concession in rails, buses, airfare or lower births in trains, comfortable seats in buses. Real respect is to get speedy justice for which they have legitimate expectation. Also, central government is fully committed to it under Article 21 of Constitution" - Honorable High Court of Andhra Pradesh

Maintenance and Welfare of Parents and Senior Citizens Act, 2007, **Section 2(h)** of defines "Senior Citizen to any person who has attained sixty years of age"

Cybercrimes have direct import on economy as they put financial strain, disturbing the fine balance between administration of justice within a democracy and it has been observed by various honorable High Courts in India, that speedy justice is imperative for both the government and individual litigants, who have invested emotionally, financially this productive years to seek remedy to the infringement of his rights and justice for crime committed against their dignity *(Directives for Senior Citizens Welfare, Ho'ble Uttarakhand High Court (PIL no. 52 of 2013), 2018).*

c. National Cyber Security Legal framework

Apart from *Information Technology Act* as umbrella legislation directly regulating data in the form of e-files, computer networks, liabilities of network providers, authentication and digital signature, and cybercrimes was outcome of United Nation's Palermo Convention resolutions 51/162 in order to adopt 'Model Law on Electronic Commerce' under International Trade Law resolution 55/25 which recommended all states to enact new cyber laws, so that uniformity may be observed in all cyber-nations, pertaining to World Trade Organization (WTO) obligations. Preamble of the Act, compiled as 12 chapters, amendments in 2008 added extraterritorial jurisdiction, gender neutral and aligned with Budapest Convention with strict extending to 10 years of maximum imprisonment with fine up to 1 crore. Along with *The Information Security Practices and Procedures for Protected System Rules, 2018*, *Constitution of India* - Article 14, 19 and 21 ensuring citizens enjoy right to freedom equality, speech, life and dignity, *Indian Penal Code* – Amendment Act, 2013 inserted online or offline stalking in section 354D, voyeurism against women in section 354C, distribution of disgusting pictures in section 292 etc., *Indian Evidence Act* - documentary evidence to include digital forms also, *Bankers Act* - accounting books to be digital too, *Reserve Bank of India Act, 1934*,guidelines for all scheduled commercial banks to adhere to strict cyber security and data protection guidelines. Recent *Data Protection Bills, 2022* based on *European Union's General Data Protection Regulation* upholds Right to privacy as fundamental right, Right to consent as obtaining data, imposing penalties as high as 500 crores, Cross border data transfer, Data Protection Board to be appointed by central government along with *IT (Intermediaries Guidelines and Digital Media Ethics Code), Rule 2021*- Due diligence in respect to content on

their platforms. Indian's upcoming *Cyber security Regulation Framework* under 'Cyber Surakshit Bharat' shall be based upon comparative study of *Germany's Cyber security Framework* for all shareholders. Infrastructure under direct control of Central Government (Prime Minister Office) such as *Telecom Regulatory Authority of India (TRAI), Data Security Council of India (DSCI), Regulations Appellate Tribunal (CRAT)* - section 48(1) of IT Act, *Indian Computer Emergency Response Team (CERT-In)* - Section 70B, *National Intelligence Grid (Nat grid) project of India* and *National Nodal Agency or National Critical Information Infrastructure Protection Centre* under Sec 70A are important organs of National cyber security framework.

7. CONCLUSION AND SUGGESTIONS

" "Legal order should be stable, dynamic and be overhauled, refitted continuously as per change in social life which it govern" - Roscoe Pound

Ubi jus ibi remidium (there is remedy, where there is a right). While looking at cyber laws, Indian or global its evident that every government is taking cyberspace as a new avenue to express, exploit opportunities as economic legal growth, taking stringent steps to eradicate new age crimes as this generation witnessed diverse social changes, techno-hypes, drastic lifestyle with new way to interact. Despite the enactments, regulation of cyber laws government's awareness drives among netizens prevention is always preferred in cybercrimes cases due to complexities involved, evolving concepts in cyberspace and lack of preparedness due to current stringent Cyber Security Framework. The subject matter of law is individuals, who's rights get infringed and as per legal jurisprudence such fundamental rights are greatly influenced by discovery of new rights under Art 21 e.g. Right to be erasure, right to know, nature of cybercrimes, one has to consider victim's emotional and mental injury along with physical disabilities leading to be victimized by perpetrator of cybercrime.

There is a need for amendments in IT Act and movement from 'one act syndrome' as deficiency in the law is unforgivable/law's purpose is to give just remedies. If Law is fair and right but, there is lack of institutions that implement it, result will not be achieved. As modus crimes

changes in cyberspace, according to time, than necessary changes in laws, institutions must accommodate that too which can be seen in Indian scenario such as cyber-cell has been created by police in every state, which deals with the investigation. But, special cyber court dedicated not been formed in India to hear only cyber-crime related cases (Tribunals under IT Act and Sessions Court take up matters) like adjudicating traditional, criminal, consumer, family cyber court appointed with expertise judges on the subject and experts to provide necessary updated information on cyber case with trained advocates and issues of digital evidence which is a difficult to obtain, preserve along with transnational and extraterritorial nature of crime, create hurdles leading to arrest of suspect or accused. Special cyber cell has been made to investigate which need more trained manpower together with social legal awareness."

REFERENCES

1. Amaral Ines (2020) "Senior Citizens and the Internet", Chapter Title of Encyclopedia of Mass Media and Society, SAGE International, Access Date: December 13, 2019 doi:http://dx.doi.org/ 10.4135/ 97814833 75519.n597
2. Brown C (2018), "An Empirical Assessment of Senior Citizens: Cybersecurity Awareness,
3. Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude and Motivation to Acquire Cyber security Skills" doi: 10.1080/07418820100094931
4. Carlson.E.L (2006), "Phishing for elderly victims: as the elderly migrate to the Internet fraudulent schemes targeting them follow" published in Elder LJ.14:423.
5. Chudasama. D, Shah. A (2021), 'Investigating Various Approaches and Ways to Detect Cyber crime', Journal of Network Security DOI: 10.37591/JoNS
6. Copes H and Kent R (2001), 'Reporting Behavior of Fraud Victims and Black's Theory of Law: An Empirical Assessment. https://www.researchgate.net/publication/262970916 available from doi: 10.1080/07418820100094931[accessed on 8th November 2021]
7. Gautam, R., Kulshrestha, P. and Goswami, M.A.K., 2021. Mediation And Family Dispute Resolution Mechanism: A Case Study On Clinical Legal Education. *Elementary Education Online*, *20*(3), pp.2490-2490.
8. Deka C., (2018), "Global Conference on Cyber Space"

9. Rajan, M.S. and Gautam, R., 2022. Initiatives To Combat Cyber Crimes. In *About the conference* (p. 170). Singh, V. and Gautam, R., 2022. Cyber Crime, Security And Regulation In India. In *About the conference* (p. 148).
10. Gautam, R., "Proliferation of Cyber Crime and Indian legal system with special reference to Gwalior Division" Available at: https://shodhganga.inflibnet.ac.in/handle/10603/250817 Retrieved on: 22/07/2022
11. Cross C. (2015) 'No laughing matter: Blaming the victim of online fraud', International Review of Victimology, 21(2), pp. 187–204. Doi: 10.1177/0269758015571471
12. Gautam, Ritu (2023 January 10), Mediation Approaches in Family Dispute Resolution matters: Cases and commentaries, Retrieved from https://www.researchgate.net/publication/366928489_Mediation_Approaches_in_Family_Dispute_Resolution_Matters_Cases_and_Commentaries
13. Koutsabasis P., (2014), "Redesigning websites for older adults: A case study Behavior and Information Technology" published in
14. Gautam, Ritu., October 2022, Smart Technology, Digitalized Education Model and Young Vulnerable Brains in India: A Current Situational Analysis, The Review of Contemporary Scientific and Academic Studies, Issue-2,Vol.-10 DOI:10.55454/rcsas.2.10.2022.008
15. http://14.139.60.114:8080/jspui/bitstream/123456789/740/9/Preventive%20Detention%20Laws.pdf
16. Cross C. (2015) 'No laughing matter: Blaming the victim of online fraud', International Review of Victimology, 21(2), pp. 187–204. Doi: 10.1177/0269758015571471
17. Das. K(2022) 'U'khand saw 5k cyber frauds cases in last 8 months', The Times of India, June
18. Ezeh N.C., and Mboso A.G., Digital Migration and Social Inclusion of Senior Citizens Department of Mass Communication, Novena University, Nigeria
19. Hart T.A, Chaparro BS, Halcomb CG (2008) 'Evaluating websites for older adults: adherence to 'senior-friendly' guidelines and end-user performance. Journal of Behaviour and Information Technology. 27(3)191-9
20. IC3 Elders Fraud Report by FBI Internet Crime Complaints Centre.(2020) Independence Day speech of PM Modi, "India will soon introduce a new cyber security policy" (2020), The Indian Express, 15 August.

21. Joo T.M., & Teng C. E., (2017). "Impacts of social media (Facebook) on human communication and relationships: A view on behavioral change and social unity". International Journal of Knowledge Content Development & Technology .7(4), 27-50
22. Kate Conger and Erin Griffith., (2020) As Life Moves Online, an Older Generation Faces a Digital Divide, Published in New York Times, March 27, 2020, updated March 28, – Ph 2
23. Lennon B., Y.C. Chang, Roderick G.B., (2017), 'Cybercrime in Asia: Trends and Challenges', Asian Handbook of Criminology published in SSRN Electronic Journal, DOI: 10.2139/ssrn.2118322
24. Mazerolle L., Ryan K., Heemeng H., (2022), "Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review"
25. Munanga, A., (2019), 'Cybercrime: A New and Growing Problem for Older Adults', Journal of Gerontological Nursing; Thorofare Vol. 45, 2, 3-5. DOI: 10.3928/00989134-20190111-01
26. Rabiner D. J., O'Keeffe J., & Brown D., (2006) 'Financial exploitation of older persons: challenges and opportunities to identify, prevent, and address it in the United States', Journal of aging and social policy, 18(2), 47-68 by– Ph 1
27. Relia, S. (2021) "Cyber Security Risk Mitigation Road Map for CISO and CIO as Business Drivers", Analytics Insight digital magazine
28. R. Sabillon et. Al (2016) "International Journal of Computer Networks and Communications Security ", 4 (6)
29. "Senior Citizens and the Internet", Chapter Title of Encyclopaedia of Mass Media and Society, Pub. Date: 2020, Access Date: December 13, 2019 by The SAGE International.
30. SimasathiansophonN., Chaisongkram,P., Kaewsaiha P., Boonarchatong K., (2021) "Enhancing Digital Literacy of Senior Citizens", Eurasean: journal on global socio-economic dynamics", Volume 5 (30)
31. Tech Desk (2019), 'Indians would take data privacy more seriously if it was traded like a currency: McAfee survey' [Accessed on 22nd November, 2022, 11:19:03 am]
32. Tripathi.K., (2019), "A brief report on older people's experience of cybercrime victimization in Mumbai, India", Cooper Aam Brief Report.