Migration Letters

Volume: 20, No: S12 (2023), pp. 978-986

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Navigating The Digital Data Age: Legal Challenges And Opportunities For The India's Migrating Seniors Population

Ms. Aditi Srivastava[1], Dr. Ritu Gautam (Corresponding Author)[2]

Abstract

To achieve a 'Free and Fair Digital Economy' under 'Digital Initiative' undertaken by Government of India, which focuses to achieve a sensitive balance between right to privacy of citizens, individual, corporate, governmental information against data infringement, graver cybercrimes. Digital Personal Data Protection Act, 2023 is an important limb in overarching cyber security framework, along with informational technology act, 2008 and government's infrastructure for regulating cyber breaches. The historical analysis of the act will present a critical scrutiny of challenges faced by all the stakeholders, while managing, processing big and mega data sets. The model of India's previous bill in comparison to new modified Act, shall either anchor India's integrity at the centre of data governance at international level or opens it to greater risks, undermining its aim. The black letter doctrinal analysis shall identify potential implications of this "good law", highlighting United Nations organs, Europe's General Data Protection Regulation's international principles, cyber conventions, jurisprudence, theories and case laws used as founding stone in bringing forth this Acts. The introduction of Artificial Intelligence, digital tools such as data analytics, cognitive computering focuses to achieve a sensitive balance between bouquet of right within cyber space for seniors against infringement of data for cybercrimes aimed to harm the integrity of India. Considering emerging trends, societal shifts, technological advancements, potential policy decision undertaken by Government of India, that will steer the trajectory of Indian health care system to understand the import of cyber victimization, digital isolation and exclusion due to lack of skills, unsafe cyber activities and in an important juncture where global sharing of big data and governance of data via various countries, specifically accepting Europe's General Data Protection Regulation, founding stone in bringing forth Act of 2023, is at par with India's socio legal and highest court's consensus amid rising cases of cyber attacks be prevented. The academia shall benefit by this paper to understand the actual import of handling Senior's interest and big data, to fostering safe cyberspace practices, prevention of data theft, this paper endeavors to offer an in-depth assessment and suggestions regarding the influential factors that could potentially shape the landscape of cyber space with data regulation and uploading the rights of senior's in India in the near future.

Keywords: *Silver Digital Economy, Cyber Space Regulation, Information Technology Act, Big Data, Privacy.*

1. Introduction

"In view of the escalating pac[1]e and costs related to data cyber attacks in India, it's vital for businesses to allocate resources towards advanced security strategies and solutions" - Viswanath Ramaswamy, VP, Technology at IBM India and South Asia.

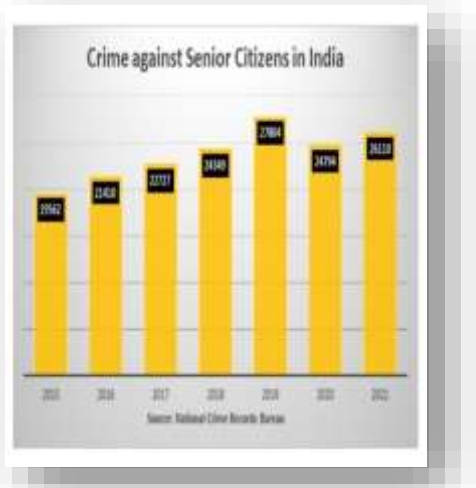
[1]Research Scholar, Sharda University (Orcid id: 0000-0003-2398-3866) C/o Mr. Suresh. Kr Srivastava, Lane no.5, Alaknanda Vihar, Nakronda, Dehradun (Uttarakhand) 248008 (Landmark: Mangalam Wedding Hall lane, near to BSNL Tower)

Interestingly, the report singled out social engineering as the most expensive factor causing breaches, with an average cost of ₹19.1 crore, while malicious insider threats followed closely at an approximate cost of ₹18.8 crore. The significant impact of implementing security adoption of Artificial Intelligence and automation had a marked effect on the pace of identifying and containing breaches. Indian companies extensively using these technologies, experienced a notable 153-day decrease in the data breach lifecycle compared to those that didn't employ them 225 days versus 378 days (IBM Data Breach Report, 2023). The response from Ms. Bhoumick, Minister of State for Ministry of Social Justice and Empowerment, against a query in Lok Sabha on 25th November 2023, underscored the government's dedication to the welfare of senior citizens by outlining various developmental initiatives and the implementation of government schemes aimed at providing financial security, healthcare, nutrition, shelter and overall welfare for the elderly population.

"Senior citizens are estimated to be 10.38 crore (8.6 %) of the total nation's population"- Census Report, 2011

According to projections from the Technical Group on Population Projections (2011-2036) for India and States, as outlined in the report from the National Commission on Population of the Government of India published in July 2020, it was suggested that the senior citizen's demography is expected to increase to 22.7 crore by 2036, making up approximately 15 percent of the country's total population. Thus, highlighted key initiatives including the Integrated Programme for Senior Citizens (IPSrC) which provides grant-in-aid to Implementing Agencies for the operation and upkeep of Senior Citizens Homes. These homes offer basic necessities such as shelter, food, medical attention and entertainment to the elderly destitute individuals. The Rashtriya Vayoshri Yojana (RVY) aims to support senior citizens from economically disadvantaged families or those with age-related disabilities by providing free assisted living gadgets through camp settings. The Elder/National Helpline for senior citizens (NHSC) offers free advice, emotional support and intervention in cases of abuse or neglect. An essential legislative step towards protecting senior citizens was the introduction of the Maintenance and Welfare of Parents and Senior Citizens Act by expanding the definition of "children" to include stepchildren, adopted children and children-in-law, making them obligated to care for elderly parents. The cap on parent maintenance payments and established regulations for private nursing facilities and organizations providing aged care is also removed. Yet, concerns are now raised by alarming cyber abuse, which could adversely affect the social fabric. The key areas such as hospices, home care services, standards for old-age facilities and awareness-raising initiatives for the protection of elderly lives and property must also included safe cyber space inclusion. In light of the rising crimes against senior citizens, including cybercrimes the government should prioritized providing legal initiatives, cyber skills aimed at protecting the elderly population. Rather than solely focusing on institutional care services, the emphasis must also be placed on generating awareness to safeguard the lives and property of senior citizens in cyber world. This approach acknowledges the importance of addressing the root causes of elderly vulnerability and ensuring their safety and security in society. Moreover, the both the figures illustrates the trends in crimes committed against senior citizens in India from 2015 to 2021, emphasizing the need for concerted efforts to address this concerning issue.

[2]Assistant Professor, School of Law (Orcid id: 0000-0001-8207-9565) Sharda University, 3rd Floor, Block 7, Plot No. 32 - 34, Knowledge Park III, Greater Noida, Uttar Pradesh – 201310.



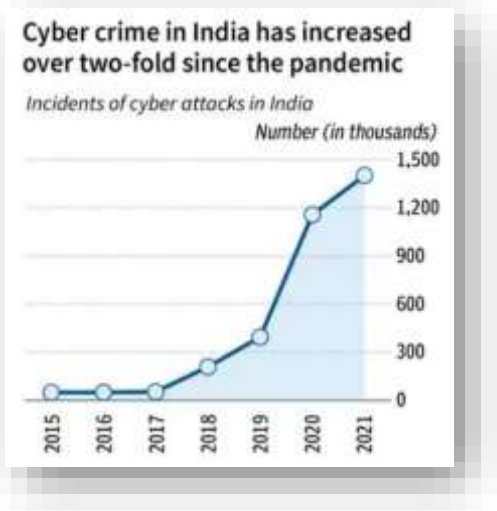


Figure 1: Data on Crime against Senior Citizens in India 2015 – 2021

Figure 2: Data on Cybercrime in India 2015 – 2021

1.1 Legal Challenges of Migrating Seniors into Digital Space

The report on cybercrime released today highlights a concerning trend in India, with the cybercrime rate rising from 3.9 cases per hundred thousand people in 2021 to 4.8 in 2022. This indicates a notable increase in criminal activities involving the use of computers or the internet to perpetrate crimes or target victims. Among the states, Telangana stands out with the highest cybercrime rate of 40.4, followed by Karnataka with 18.6 and Maharashtra with 6.6. On the other hand, Himachal Pradesh and Madhya Pradesh have the lowest cybercrime rates, with Bihar following suit, particularly when excluding north-eastern states. These statistics underscore the importance of robust cyber security measures and increased awareness among individuals and organizations to mitigate the risks associated with cybercrimes such as frauds, ransomware attacks, and impersonation. The recent revelation regarding cybercrime trends in India highlights a significant escalation in illicit online activities, attributed largely to the widespread adoption of internet and mobile technologies. Over the past decade, instances of cybercrime have surged dramatically, skyrocketing from 3,693 cases in 2012 to a staggering 65,893 cases in 2022. This surge correlates closely with the exponential growth in mobile internet users, which has risen

from approximately 12.5% to a striking 76.6% of the population, as per data provided by the telecom ministry to Parliament.

Despite the surge in reported cybercrimes, there exists a notable discrepancy between the number of complaints lodged and the cases formally registered by law enforcement agencies. Data sourced from the National Cyber Crime Reporting Portal reveals that out of the 1.6 million complaints received between January 2020 and December 2022, only a mere 32,000 resulted in police investigations and subsequent legal proceedings. The distribution of cybercrime cases across different states within India paints a diverse and complex picture. While Delhi, for instance, accounted for a relatively minor 1.2% of the total complaints received, states like Telangana and Karnataka registered significantly higher percentages, suggesting regional disparities in cybercrime prevalence and reporting practices, which also effects dismally upon elderly population. In response to the escalating threat posed by cybercrimes, states with more advanced infrastructure and resources, such as Karnataka, have implemented specialized anti-cybercrime units and employed cutting-edge technologies to combat these offenses effectively but, not individually to cater to the needs of seniors (Murthy, 2022).

However, the investigation and prosecution of cybercrimes present formidable challenges, primarily due to the often elusive nature of digital evidence. A significant number of cases are closed due to the lack of concrete evidence, undermining efforts to hold perpetrators accountable and deliver justice to victims. The notorious cyber fraud hotspots Jharkhand and Haryana, paradoxically report lower numbers of officially registered cybercrimes despite their notoriety. This discrepancy underscores the complex interplay of socioeconomic factors, law enforcement capabilities and reporting mechanisms in shaping the cybercrime landscape at the regional level. The motives driving cybercriminal activities are multifaceted, with fraud emerging as the most prevalent, followed by extortion and sexual exploitation. States like Karnataka, Telangana, and Maharashtra predominantly witness cyber frauds, while others like Uttar Pradesh and Assam report significant instances of extortion and sexual exploitation. Furthermore, specific categories of cybercrimes exhibit notable variations across states, reflecting the diverse socio-political contexts within which these offenses occur. Certain states record higher incidences of cybercrimes aimed at tarnishing the reputation of public servants or perpetuating politically motivated cyber offenses. To effectively address the escalating threat posed by cybercrimes, law enforcement agencies must intensifying their efforts through a multifaceted approach that encompasses technological innovation, legislative reforms such as Digital Personal Data Protection Act,2023 and a proactive community engagement for seniors. Advanced training programs for cybercrime officials, coupled with increased public awareness campaigns aim to empower individuals, seniors and organizations to recognize and mitigate cyber security risks proactively. The challenges posed by cybercrimes extend beyond traditional law enforcement paradigms, requiring holistic strategies that leverage technological advancements and foster collaboration between government agencies, private sector stakeholders and civil society organizations. Only through such concerted efforts can India hope to mitigate the risks posed by cybercrimes and safeguard its digital ecosystem for future generations (Murthy, 2022)

There has being a rise of 5.3 percent in 2021 of traditional crimes against senior. Under the Indira Gandhi National Old Age Pension Scheme (IGNOAPS) a fully funded centrally sponsored program by the Department of Rural Development, seniors in the age group of 60-79 years belonging to Below Poverty Line (BPL) households receive a monthly pension of Rs. 200. This amount is increased to Rs. 500 per month upon reaching the age of 80 years. While the government implements various measures to empower senior citizens, the effectiveness of mere financial assistance is very limited and it hardly encompasses cyber crimes (National Crime Records Bureau, 2024).

2. Challenges posed to Traditional System

"In 2011, India had 104 million elderly individuals, aged 60 and above, with 53 million females and 51 million males, anticipated to surge to 173 million by 2026" - Projections from the United Nations Population Fund and Help Age India Report 2022

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" 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 It is been observed that due to specific factors senior citizens are lacking behind, who are first generation migrants due evolving cyberspace, lack of updated awareness, they are excluded to contribute and form a productive segment due to 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 (Indian Express, 2021).

"In 2022, cybercrimes surged by 24%, while economic offenses increased by 11%, crimes against senior citizens by 9%, and crimes against women by 4%" (National Crime Records Bureau, 2024)

Senior's digital rights' infringement is directly connected to existing factors ranging to counter cybercrimes perpetrated against them with targeted solutions, current inclusion in 'Digital Initiative' undertaken by Government of India is rewriting the digital narrative, it is crucial to consider the specific challenges faced by senior citizens, ranging from health to technical to have best outcomes in the ongoing efforts to prevent cybercrimes targeting mitigating demographic specifically seniors and have active inclusion in digital advancements (Digital Personal Data Protection Act, 2023).

2.1 Invasion of Privacy of Senior Citizens

Landmark case **Justice K.S. Puttaswamy and Anr. v. Union of India and Ors**. serves as a catalyst in recognizing the 'right to privacy' inherent in Article 21 as an essential aspect of the fundamental right to life in India. By highlighting the importance of 'informational privacy', the ruling established the foundational framework for protecting this right within the country's legal system. While acknowledging this significance, the court abstained from outlining specific criteria for safeguarding informational privacy. Government's subsequent withdrawals of Data Bill reflect a responsive approach, to address potential shortcomings found in earlier versions, keeping strict adherence to Indian Constitution Article 19, which bestows freedom to individuals as a right to determine their preferences in alignment, Article 21, which grants liberty, the freedom to choose across life's facets—food, attire, faith and privately one's thoughts and Article 25 provides freedom of religion inherently includes the right to choose and express faith. Privacy is a cornerstone for freedom, crucial in exercising individual liberties, involving provisions enabling the government to request "data fiduciaries or processors" to provide "anonymized personal data" or "other non-personal data"(Digital Personal Data Protection Act, 2023.

Privacy stands as an indispensable cornerstone of fundamental human rights, enshrined in various international and regional agreements. It encapsulates the right to be shielded from unwarranted intrusion into one's personal life, family, home and also communication. The Asia-Pacific Economic Cooperation (APEC) Privacy Framework of 2004 and the Economic Community of West African States Supplementary Act on data protection from 2010 exemplify regional efforts to bolster data privacy. In an increasingly digitized world where personal data is a valuable commodity, the right to privacy assumes heightened

significance. It serves as a bulwark against abuses of power and fosters democratic principles by preserving individual autonomy and fostering trust in institutions. Without privacy protections, individuals may refrain from exercising these rights due to concerns about surveillance and potential repercussions. Thus, privacy acts as a catalyst for the flourishing of democratic societies, enabling individuals to engage in civic activities and contribute to public discourse without fear of reprisal. By ensuring the confidentiality of sensitive information, privacy encourages individuals and organizations to engage in research and development activities without the fear of intellectual property theft or unauthorized access. This, in turn, fosters a conduct environment for creativity and entrepreneurship, driving technological advancements and economic prosperity. In the realm of healthcare, privacy plays a pivotal role in maintaining the confidentiality of medical records and preserving patient trust. Patients must feel secure in disclosing sensitive information to healthcare providers without the fear of their data being exploited or disclosed without consent. Privacy protections in healthcare settings not only uphold ethical standards but also promote better health outcomes by encouraging individuals to seek timely medical care without reservation. In context of education, privacy safeguards are essential for protecting senior's records (Official Journal of the European Union, 2018).

Senior's population prediction by 2050, accompanied by a simultaneous decline in the number of young individuals will transform the social fabric, introduce unique challenges and opportunities, particularly in the realm of cyber security, healthcare and finance, it is imperative to address the potential adverse effects of digitalization on the elderly, both financially and societal. India's 'Silver Economy' refers to the economic potential associated with the growing elderly population. As seniors become a larger consumer demographic, there is a vast opportunity to explore and develop markets and services tailored to their unique needs. But, the optimism surrounding the Silver Economy is tempered by a notable increase in cyber threats targeting the elderly. Recent times have witnessed a surge in incidents of cyber victimization among seniors, posing significant financial risks. It is crucial to acknowledge this dark side of digital inclusion to address the detrimental consequences of online exploitation. The Challenge needs heightened awareness, protective measures and targeted interventions (Chou, 2003).

2.2 Enactment of Digital Personal Data Protection Act, 2023

This Act marks a significant step forward in safeguarding digital personal data, aiming to find a delicate balance between protecting individual rights and enabling lawful data processing. At its core, the Act emphasizes the responsibilities of those managing data called "Data Fiduciaries" and the rights of individuals known as "Data Principals" and the consequences for breaches through financial penalties. This legislation aims to introduce a robust data protection law with minimal disruption while nurturing an environment that promotes both the ease of living and ease of doing business. These principles serve as the structure for responsible data management placing a priority on individual privacy while demanding responsible behavior from entities handling personal data. Also, to safeguard the privacy and confidentiality of individuals whose data had been anonymized. By outlawing such actions, it aimed to discourage attempts to identify individuals from datasets devoid of personal identifiers, preserving privacy rights and ensuring the integrity of anonymized data by categorizing and stipulating varying levels of safeguards for distinct categories of personal data. (Bengaluru Bureau, 2030). In 2017, Honorable Supreme Court ruled in **Justice K.S. Puttaswamy and Anr. v. Union of India and Ors.** solidified and acted as a catalyst to bring forth 'right to privacy' contained within as an innate component of the fundamental right to life in India. Emphasizing the critical role of 'informational privacy', the judgment laid the foundational groundwork for safeguarding such right within the nation's legal structure, despite acknowledging, the court refrained from prescribing specific parameters for protecting informational privacy. This spurred discussions to explicitly address data protection concerns, gap between rights to privacy and a concrete

infrastructure. In 2018, a bill proposed by Justice B.N. Sri Krishna committee under Ministry of Electronics & Information Technology and Honorable Prime Minister Shri Narendra Modi, established data protection standards, heavily relying on globally accepted European Union's General Data Protection Regulation (GDPR).

The predecessor bill "Personal Data Protection Bill of 2019" delayed due to pandemic, was retracted by the government and replaced with revised new draft "Digital Personal Data Protection Bill of 2022", which amalgamates elements of revised draft and evolving perspectives, pivotal to present data security issues. The Act notably addresses the safeguarding of children's personal data, stating that processing such information necessitates explicit parental consent and put stringent penalties for non-compliance or failing to implement reasonable security measures to prevent data breaches can reach up to Rs. 2.5 billion (approximately USD $30 million) irrespective to absence is a provision for compensating affected data subjects, raising concerns regarding redressal.

As per National Crime Records Bureau (NCRB) crime against senior citizens dropped to 22 in 2021 before spiking to 74 in 2022, marking a remarkable 236% increase. This surge in crime rates against the elderly far exceeds the national average, which stands at just 27 such crimes per year. Among the 74 senior citizens targeted in 2022, a significant portion, 55 individuals, fell victim to forgery, cheating, and cybercrimes. The remaining victims were subjected to various other crimes, including theft, robbery, criminal trespass, and even attempted murder. The rise in cybercrimes targeting senior citizens is the increasing prevalence of forgery and cheating schemes perpetrated online. As more elderly individuals embrace digital technologies for banking, shopping, and communication, they become susceptible to various forms of online fraud. The most significant data breach occurred in 2020, attributed to Cam4, involving over 10.8 billion compromised data records. Following closely, in 2017, Yahoo experienced the second-largest data breach, with more than 3 billion compromised data records (The Hindu, 2023).

By enhancing the accessibility and usability of digital technologies such as simplified user interfaces, offering personalized assistance along with support and training can enable seniors to engage safely and confidently in the digital world. Beyond cybersecurity measures, addressing the underlying socio-economic factors contributing to crime against senior citizens is crucial for fostering a safer and more inclusive society. Initiatives aimed at promoting social integration, financial literacy, and elder-friendly urban infrastructure can help mitigate the factors faced by elderly individuals and reduce their susceptibility to exploitation and victimization in digital space (Sareen, 2023).

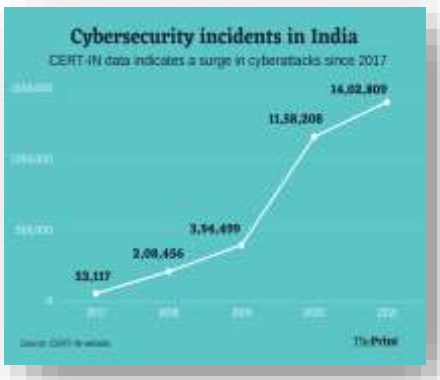


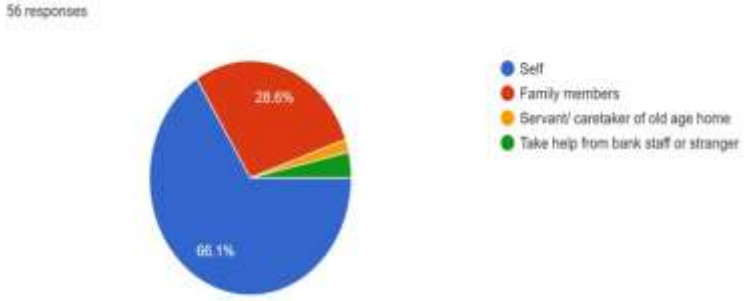
Figure 3. Cyber security Incidents in India by Print 2017 -2022

3. Findings and Discussion

The chosen strategy for data collection and analysis was using Goggle form as a questionnaire,circulated for feedback from selected sample of senior citizens from Greater

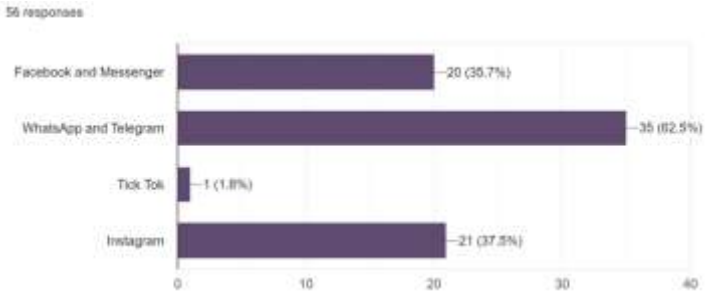
Noida and National Capital Region**.** The research questions in this study try to explore the challenges faced by senior citizens with digital migration and online participation and the infringement of their privacy or falling prey to cybercrimes.

Graph 1: Digital Transaction by Senior Citizens



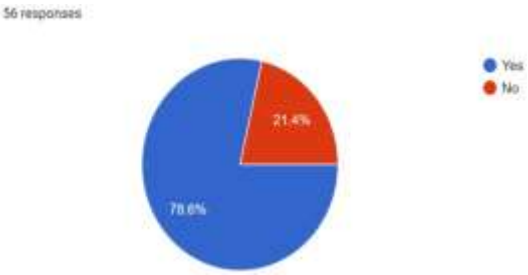
The data from the survey form with respondents as Seniors in Graph 1 represents that at least 66.1 % seniors are participating in digital transaction and 26.6% are dependent on family members, servants and some take help from bank staff or strangers on basis of good faith.

Graph 2: Social Media Platform used by Senior Citizens



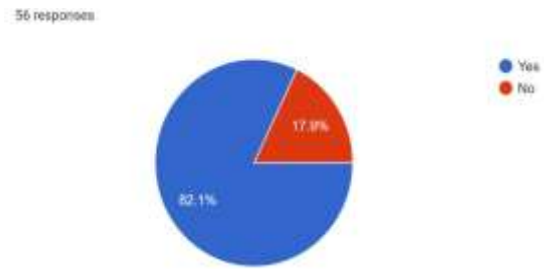
The data from the survey of respondents in Graph 2 represents that at least 62.5 % seniors use whatsapp and telegram; 35.7% use face book and messenger to communicate and 37.5% also share their personal data on Instagram application.

Graph 3: Fraudulent Calls and Invasion of Privacy of Senior Citizens



The data from the survey form with respondents as Seniors in Graph 3 represents that at least 78.6 % have received calls misrepresenting Government, bank employees to commit some fraud, cybercrime e.g. Grandparent's scam.

Graph 4: Digital Awareness among Senior Citizens



The data from the survey form with respondents as Seniors in Graph 4 represents that at least 82.1 % are not aware of Right to Privacy, legislations, Cyber security such as whom to approach if they fall victims to cyber crimes and 17.9 % were aware.

The study set to investigate the challenges faced by senior citizens within digital space, leading to their victimization in the area of Greater Noida and National Capital Region. The findings let to the understanding of the effects on their social participation, legal rights in a digitalised society is that they are not aware of the current steps undertaken by the government such as policies under Ministry of Social Justice and Empowerment nor legislations such as Information Technology Act, 2008, Digital Personal Data Protection Act,2023. Even though they are using social media applications, conducting online transactions, getting exposed to fraudulent calls, popup on sites and were victims of cybercrimes The study focused suggested that these challenges can also be converted to opportunities concerning the upliftment and exploiting the increasing population of seniors as asset of a productive segment and part of society but also because of their importance and variability in this study

4. Conclusion

Law enforcement has been proactive in addressing this concerning trend, particularly in combating cybercrimes targeting the elderly population. Cyber cell highlighted the importance of awareness campaigns in educating senior citizens about online scams and safe usage of digital payment applications. To this end, initiatives such as deploying cyber awareness vans in populated areas, broadcasting radio jingles, and conducting regular visits to senior citizens' homes have been undertaken to disseminate crucial information about cyber security but, still lot has to be achieved and amendments such as the concept of "legitimate interests", "unconditional" for data collection in the Act does not align with the GDPR's interpretation and provisions like “specified purpose" is without guidance on legitimate processing, exemptions to government, certain bodies from Act’s applicability may necessitate judicial intervention to set reasonable criteria. The Act's limited application to foreign personal data processed in India could hinder India's efforts to obtain adequacy rulings from entities like the European Union and impacting cross-border data flow assurances. Evolving landscape of data privacy and technology shall impact Right to Information Act, shifting greater protection of personal data over public interest, altering the balance in favour of data protection at the expense of transparency. To mitigate the risks associated with cybercrimes against senior citizens, it is essential to prioritize awareness and education initiatives tailored to their specific needs. Providing comprehensive guidance on recognizing and avoiding common online scams, safeguarding personal information, and securely navigating digital platforms can empower elderly individuals to protect themselves from cyber threats effectively.

5. References

Armstrong, R., et al. (2011) “Title of the scoping review article”. Journal Name,Volume(Issue), Page range. Arksey, H., & O'Malley, L. (2005) “Title of the methodological article” Journal Name, Volume (Issue), Page range.

Abrams, L. (2015, February 27). New TeslaCrypt Ransomware sets its scope on video gamers. BleepingComputer.

Anupriya Chaterjee, “India’s had its worst year of cyberattacks, but 2023 will see govt & firms ramp up defences” Hindustan Times, 30 December, 2022 10:07 am IST

BBC News. (2015, March 13). Gamers targeted by ransomware virus. Retrieved March 14, 2015.
BENGALURU BUREAU, "Average cost of data breach in India reaches ₹17.9 crore in 2023: IBM Security's Cost of a Data Breach Report" Updated - July 25, 2023 at 07:40 PM.
Ben-Rafael, E. (2001). Title of the article on economic and educational gaps. Journal Name, Volume(Issue), Page range.
Big Data in the Digital Economy: Prospects for Application and Legal Regulations
Blit-Cohen, E., et al.(2004). Elder participation in cyberspace: A qualitative analysis of Israeli retirees. Journal of Aging Studies, 18(4), 385-398.
Carpenter, B. D., et al. (2007) "Computer use among older adults in a naturally occurring retirement community" Computers in Human Behavior, 23(6), 3012-3024.
Chou, C (2003) "Incidences and correlates of Internet anxiety among high school teachers in Taiwan". Computers in Human Behavior, 19(6), 711-726.
'Concept of journalistic activities', Article 9 for Data Protection
Gubaydullina E.K. Samara State University of Economics, Samara, Russian Federation DOI 10.1007/978-3-030-83175-2_6
Gubaydullina E.K., Churakov A.N. "Legal regulation of big data in industrial systems: Problems and development prospects", Lecture Notes in Networks and Systems, 139, pp. 489-494, 2021
Gupte, Y. (Year). Data shows rise in crime against senior citizens in India: A look at steps taken by the government to protect the elders. https://www.indiatracker.in/story/data-shows-rise-in-crime-against-senior-citizens-in-india-a-look-at-steps-taken-by-the-government-to-protect-the-elderlies
Mathias Risse , "The Fourth Generation of Human Rights: Epistemic Rights in Digital Lifeworlds", Carr Center for Human Rights Policy Harvard Kennedy School, Harvard University September 17, 2021
Manral and Sinha (2024) Indian Express, "24% rise in cybercrime in 2022, 11% surge in economic offences"
Murthy, R. N. (2022, December 06), "Cyber crimes on rise with growing digitisation". Retrieved from [https://www.thehindubusinessline.com/data-stories/visually/cyber-crimes-on-rise-with-growing- digitisation/article66231903 .ece]
National Crime Records Bureau, 2024, February 11, "Cybercrimes see highest spike among cognisable offences in 2022". The Times of India.
https://timesofindia.indiatimes.com/city/delhi/cybercrimes-see-highest-spike-among-cognisable-offences-in-2022-says-ncrb/articleshow/88413850.cms
Rosemary Jay, Angus Hamilton, "Data Protection Law and Practise", 445, 1995
Sareen Kumar, A. (2023, December 14). Cheating, forgery top crimes against elderly in UT: NCRB report. Hindustan Times. Retrieved from [https://www.hindustantimes.com/cities/chandigarh-news/cheating-forgery-top-crimes-against-elderly-in-ut-ncrb-report-101702494187240.html]
Shayan Ghosh "The disturbing facts about India's know your customer data leaks", 28 March 2022, 10.19 pm
Singh, A. (2023, November 10). "Cybercrime cases targeting senior citizens on rise in Delhi." Times of India. Retrieved from [https://timesofindia.indiatimes.com/city/delhi/crimes-against-seniors-in-delhi-up-35-from-2022/articleshow/105107129.cms]
Will Thomas DeVries, "Protecting Privacy in the Digital Age, 18 Berkeley Technology law Journal", 283, 311 (2003)
WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR
INDIAhttps://Www.Meity.Gov.In/Writereaddata/Files/White_Paper_On_Data_Protection_In_India_171127 _Final_V2.Pdf
Freese, J., et al. (2006). Cognitive ability and Internet use among older adults. Poetics, 34(4-5), 236-259.
Levac, D., et al. (2010). Title of the methodological article. Journal Name, Volume(Issue), Page range.
Lissitsa, S., & Chachashvili-Bolotin, S. (2015). Digital skills and extrinsic rewards in late career. Technology in Society, Volume(Issue), Page range.
Peres, Y., & Ben-Rafael, E. (2006). Title of the article on economic and educational gaps. Journal Name, Volume(Issue), Page range.
F-Secure Labs. (n.d.). Trojan.TeslaCrypt Description. Retrieved from www.f-secure.com
Trend Micro USA. (n.d.). RANSOM_CRYPTESLA - Threat Encyclopedia. Retrieved from www.trendmicro.com