KIU LAW JOURNAL
Vol. 7 Issue 2, (2025)
Received: February 21st, 2025
Revised: September 13th, 2025
Accepted: November 1st, 2025
DOI: https://doi.org/10.59568/KIULJ-2025-7-2-01
ISSN: 2519-9501
Kampala International University Law Journal

An empirical study on Indian cybercrime laws for the protection of Senior Citizens of Indore City

Priyanacy Gupta[1]

[1] *Department of law, Sage University, Indore, India. E-mail: priyanacy6@gmail.com*

***Author Correspondence email**: *priyanacy6@gmail.com*

Abstract

The widespread use of computers has led to a rise in cybercrime. One of the most intricate problems in the cyber world is cybercrime. A computer can be considered an illegal tool or a target in cybercrime. The internet has advanced to enable the effortless exchange of data and information worldwide. The subject of this research is Indian cybercrime laws for the protection of Senior Citizens in Indore city. The research is explanatory in nature. The primary data is used in the paper. A self-structured questionnaire was circulated to the senior citizens of Indore city. The data collected was analysed through a purposive sampling technique in a Statistical Package for Social Sciences software package, and the statistical results were examined. 115 respondents were obtained from the survey. Correlation, ANOVA, regression and demographic analysis are utilised to analyse the collected data. The outcome of the study exposed that senior citizens of Indore have awareness of cyber laws, and they also faced some issues regarding cybercrime, and they also reported to the higher officials are some of the most significant issues identified. The paper concludes that the senior citizens have an awareness of cybercrime because Indore is a city which has a high literacy level, and they are ready to face the hurdles of cybercrime and report a complaint.

Keywords: Cybercrime, Senior Citizens, SPSS, Indore, Cyber Security

1. Introduction

The world has not always dealt with cybercrime. Any unlawful behaviour that happens on, over, or through the computers, internet, or other kind of technology recognised by the Information Technology Act is defined as cybercrime[1]. Several illegal behaviours are conducted by technically skilled offenders on the internet[2]. If we implement a comprehensive definition, we could say that cybercrime is defined as any illegal behaviour that uses the computer or the internet as a target, a tool, or both of them. Cybercrime is an irrepressible evil that has its origins in the misapplication of the community's reliance on computers. The utilisation of computers and other associated technology in day-to-day life is increasing rapidly and has become a requirement that enables the users' convenience[3]. It is an unquantifiable, limitless medium. Cyber terrorism, cyber stalking, email spoofing, cyber pornography, email bombing, cyber defamation, and so on are some current cybercrimes. If a conventional crime is done through the Internet or a computer, it might come under the classification of cybercrime[4]. Cybercrime comprises anything from electronic cracking to denial-of-service attacks, is a phrase utilised to comprehensively describe the criminal action done by computer networks or computers as a target, a tool, or a place of unlawful activity[5].

It can also refer to traditional crimes in which the illegal activities are made easily with the help of networks or computers[6]. Cybercrime can stop any railway wherever it may be, steer planes in the wrong direction while they are in flight, provide foreign countries admission to any sensitive military data, shut down electronic media, and can bring down any type of system in seconds[7]. The cybercrime prevalence is increasing, and the current technical methods to preventing it are unsuccessful at preventing this growth[8]. This displays the requirement for extra preventive approaches to lower cybercrime. "Cyber law" is referred as the legal concerns linked with the usage of communications technology, known as "cyberspace," the Internet. It aims to integrate the challenges imposed by online behaviour with the existing lawful framework that administers the real world[9]. These digital crimes often target the elderly and seniors[10]. They usually have much better credit than the younger

---

[1] O R Ehimen and A Bola, 'Cybercrime in Nigeria' (2010) 3 *Business Intelligence Journal* 93.

[2] Ibid

[3] O Goni, 'Cyber Crime and Its Classification' (2022) 10 *International Journal of Electrical and Electronics Engineering Applications* 1.

[4] K J Dashora, 'Cyber Crime in the Society: Problems and Preventions' (2011) 3 *Journal of Advances in the Social Sciences* 240.

[5] S Kharat, 'Cyber Crime–A Threat to Persons, Property, Government and Societies' (1 March 2017) *Property, Government and Societies*.

[6] A Di Nicola, 'Towards Digital Organized Crime and Digital Sociology of Organized Crime' (2022) *Trends in Organized Crime* 1

[7] O Goni, 'Cyber Crime and Its Classification' (2022) 10 *International Journal of Electrical and Electronics Engineering Applications* 1

[8] J M Drew, 'A Study of Cybercrime Victimisation and Prevention: Exploring the Use of Online Crime Prevention Behaviours and Strategies' (2020) 6 *Journal of Criminological Research, Policy and Practice* 17.

[9] V K Reddy, 'Cyber Crimes and Cyber Laws in India: An Overview'.

[10] B K Payne, 'Criminals Work from Home During Pandemics Too: A Public Health Approach to Respond to Fraud and Crimes Against Those 50 and Above' (2020) 45 *American Journal of Criminal Justice* 563.

generation, better wealth, and a propensity to be more trustworthy. Since they are not aware of the reporting processes for cybercrimes against them, elders are seen by criminals as easy targets. Seniors who fell for the fraud seldom face embarrassment and guilt[11]. They could fear that their family members won't believe they can still handle their own finances. Here are some typical online fraud schemes that target elderly people, and tips on how to avoid them[12]: Tech support scam: Fraudsters posing as tech support staff promise to repair fabricated computer issues. The gadgets of the victims and whatsoever sensitive information they have stored on the devices are available to offenders remotely. Government impersonation scam: Thieves assume the persona of government agents and threaten to arrest or punish victims unless they hand over money. Financial scam: Criminals use phone credentials from legitimate services, such as reverse mortgages or credit restoration, to target potential victims. Romance scam: Criminals act as romantically interested individuals on social media or dating services, primarily focusing on females and newly widowed individuals. Using the romance scam to find victims for other unlawful behaviour is a novel variation.

This can entail applying for benefits in someone else's identity or legalizing illegally acquired funds via the bank account of the victim. Institutions might start to have suspicions, particularly if these transactions are unfamiliar. The elderly person runs the risk of facing legal repercussions if they close the victim's account or possibly send the case for prosecution.

2. Method

Research Design

A semi-structured questionnaire was used in this survey-based study, and data were gathered from the senior citizens of Indore. The questionnaire was categorized according to the study variables, and the purposive sampling analysis was used to collect the data. The quantitative evaluation is used to interpret the research objectives and establish the hypothesis for the empirical study. Figure 1 provides a summary of the proposed research design. The demographics of the population being studied were also observed, and the responses to those observations were analysed.

[11] D Rebovich and L Corbo, 'The Distillation of National Crime Data into a Plan for Elderly Fraud Prevention: A Quantitative and Qualitative Analysis of US Postal Inspection Service Cases of Fraud Against the Elderly' in *The New Technology of Financial Crime* (Routledge 2022) 126.

[12] P Datta and others, 'A Technical Review Report on Cyber Crimes in India' in *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)* (IEEE 2020) 269.

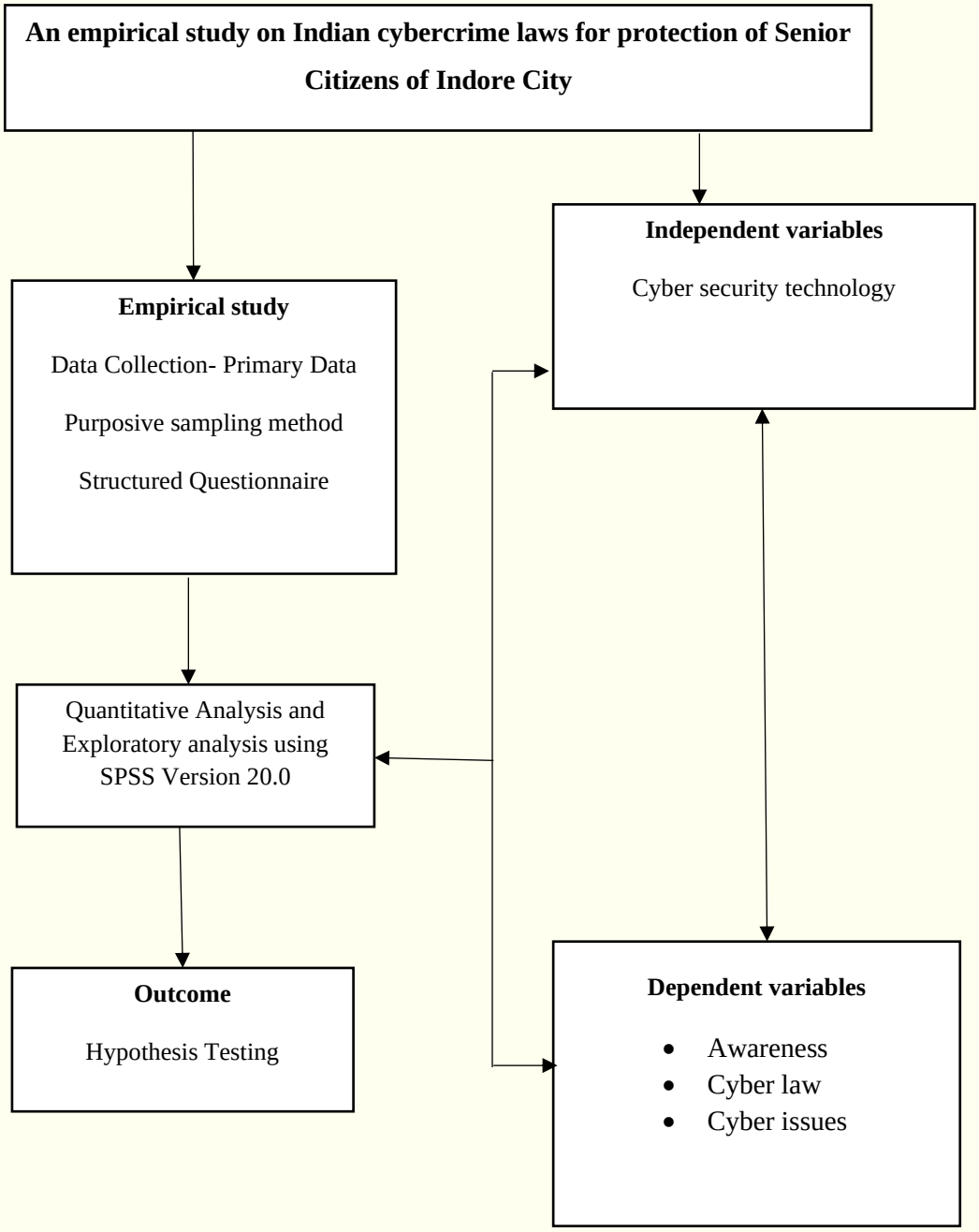

Figure 1. Research Design

Research hypothesis

H_10: There is no awareness of cybercrime law among the Senior Citizens.

H_11: There is awareness of cybercrime law among the Senior Citizens.

H_20: There are no cybercrime issues faced by the Senior Citizens

H_21: There are cybercrime issues faced by the Senior Citizens

H_30: There is no impact of cybercrime law on cybercrime issues faced by the Senior Citizens.

$H_3 1$: There is an impact of cybercrime law on cybercrime issues faced by the Senior Citizens.

Sampling method and Participants

The purposive sampling technique was chosen for the statistical quantitative analysis after the data were gathered. The survey's respondents were asked age, designation. The questionnaires were grouped according to the study variables after the necessary data for the analysis were gathered (Figure 1). The study population consisted of those who were senior citizens in Indore. The population of the study is 115. The focus of the study confirmed that the responses were strong enough to satisfy the objectives and support the hypotheses.

Research Instrument

The five-point Likert scale was used to adapt a standard research instrument for the primary data analysis. All the questions had the responses “Strongly Agree (SA),” "Agree (A)," "Neither agree nor disagree (N)," "Disagree (DA)" “Strongly Disagree (SDA)” in it. This rating scale is used to determine how the independent variables affect the dependent variables.

Quantitative analysis

Quantitative examination approach [13]can be expressed as peculiarity of information assortment and executing measurable, numerical and computational investigation. This strategy removes information from imminent and potential clients, consolidating examining procedures and display surveys, online exploration and overviews. The results came in the form of numbers. The numerals were used to evaluate the upcoming research and make the necessary adjustments after careful data interpretation. This approach [14]yields empirical evidence to support the efficacy of numerous potential solutions for achieving the research's goals.

This study uses a significant sample size to target the intended population. Proper examination strategies ought to be integrated while extracting the examples to support the reason for the review. Tables, graphs, and other non-numerical representations are typically used to identify quantitative data. This is a straightforward approach for evaluating the extracted data and confirming the research's acceptability. The results obtained from this method can be far-reaching for to target population to go to important lengths for upgrade. The essential components of the quantitative methodology are utilized in the examination to quantify things which can be counted and ensure adequate information is collected to perform the statistical examination. The distinction of the procedure is that subjective methodology explores and investigates the reactions and responses of the people. The following are some benefits of quantitative analysis[15].

---

[13] H Dzwigol, ‘Innovation in Marketing Research: Quantitative and Qualitative Analysis’ (2020).

[14] L K Fryer, J Larson-Hall and J Stewart, ‘Quantitative Methodology’ in *The Palgrave Handbook of Applied Linguistics Research Methodology* (Palgrave Macmillan 2018) 55.

[15] D Eyisi, ‘The Usefulness of Qualitative and Quantitative Approaches and Methods in Researching Problem-Solving Ability in Science Education Curriculum’ (2016) 7 *Journal of Education and Practice* 91.

Findings from studies: The statistics are used to calculate a significant amount of the retrieved data. This conquers the idea of predisposition. When a large number of researchers attempt to work with the collected data, they all produce the same result.

Persistent: The design of the examination is engaged before it is begun, and research is utilized to evaluate a hypothesis or an idea; it will be either upheld or dismissed.

Offers greater controllability: When the data goes beyond the scope of the study, the researcher will absolutely have more control over the collection of the data. Using this method can result in a broader perception.

Oversees enormous examples: The size of the samples that represent the intended audience will ultimately determine the outcomes. The majority of the time, a large sample size will assist in obtaining statistically valid results.

Inclination less: The specialist centres for inclination less results. The specialist will approach questions which will have outlined replies.

Sorted using simple analytical methods: The majority of the data that is retrieved is organized in the form of graphs, charts, and other numerical representations.

Adaptable: The examination can essentially be rehashed or repeated, which outcomes in high accuracy.

Ethical Considerations

Certain morals will be followed while directing the exploration investigation because the study is based on an investigation into Indian cybercrime laws for the protection of Senior Citizens of Indore City. The responses are highly confidential. Before the researcher's survey evaluation, according to the research's ethics, respondents are provided with information. The respondents are not constrained to use any means to give their reactions. Just willing respondents are chosen for the review examination. Respondents are only required to respond to the questionnaire; they are not compelled to disclose their private data or reports. The research study does not contain any false data because it only analyses original data. The organized and gathered data would be kept very secret. Based on this research study, these are the ethical considerations that the researcher used for the analysis of the survey. They are accurate in their knowledge.

3. Analysis or Discussion

3.1. Conceptual Discussion on the protection of Senior Citizens of Indore City from Cybercrime

The key aim of this study is to evaluate the kinds of cybercrime and how elders have faced that cybercrime. The study adopted a cross-sectional research design to evaluate this research. The outcome of the study reveals that the maximum participants know about cybercrime[16]. In the research of Mesko, the main purpose

[16] N Arfi and S Agarwal, 'Assessment of Knowledge of Cybercrime Among Elderly Across Residence' (2013) 2 *International Journal of Innovative Research and Studies* 643.

is to analyse the awareness and fear of people in cybercrime. The study adopted an online survey method to analyse the study. The outcome of the study reveals that the majority of people have an awareness of cybercrime, and they don't fear reporting or approaching a complaint[17]. In the Rao study, the key purpose of conducting this study is to evaluate the kinds of cybercrime and how elders face and they overcome cybercrime. The researcher utilized a cross-sectional design in this research. As an outcome majority of participants reported that they had not faced any phishing, credit card fraud, money laundering, cyber pornography, password sniffer, and also web jacking, either among elders who live in their own homes or elders who reside in old age homes[18].

In the Arfi study, the key purpose of conducting this study is to evaluate awareness of cybercrime among elderly people for both genders in Lucknow. The researcher had utilised a cross-sectional research design with a survey method to analyse the study. The researcher had utilised a cross-sectional research design because it is broad and it is used to analyse a large sample size in a short period of time. The outcome of the study reveals that males have more awareness of cybercrime when compared to females it is because female elders don't have internet facilities[19]. The key goal of this research is to discover the thoughts regarding cybersecurity among Malaysian elders and its effect on their safety. The researcher utilized qualitative methodology in this study, so the researcher conducted face-to-face interviews to gather the data. As an outcome, the research reveals that most of the participants from the civil service have knowledge of cybersecurity, and they were unaware of the actual modus operandi of the cyber criminals[20].

This research[21] is conducted to recognise the hurdles faced by elders in cybersecurity and to suggest solutions for these hurdles. The researcher had utilised a systematic literature review that was done on Google Scholar, IEEE Xplore, Pubmed, ScienceDirect and Proquest databases by using suitable keywords. 29 review articles were significant with the title, and among 29 review articles, 14 were significant for the solution of the problem. As an outcome, physical and psychological challenges were identified, including mobility decline, increased online service usage, memory recall issues, and cognitive impairment. Data also encompasses the patterns of Internet usage, IT proficiency, and their perception of

---

[17] G Mesko and I Bernik, 'Cybercrime: Awareness and Fear: Slovenian Perspectives' in *2011 European Intelligence and Security Informatics Conference* (IEEE 2011) 28.

[18] Y S Rao, 'Cyber Crime Assessments' in Prof (Dr) Hima Bindu Maringanti (ed), *Cybercrime Assessments* 10.

[19] N Arfi and S Agarwal, 'Knowledge of Cyber-Crime among Elderly across Gender' (2014) 2 *International Journal for Advance Research in Engineering and Technology* 7.

[20] S L Tan and others, 'Cybersecurity and Privacy Impact on Older Persons amid COVID-19: A Socio-Legal Study in Malaysia' (2020) 2 *Asian Journal of Research in Education and Social Sciences* 72.

[21] S Sivagumaran, 'Challenges of Online Security for Senior Citizens' (2023).

potential risks in the digital. Lack of awareness about cybersecurity defence among Internet users is one of the reasons behind the rise of cyber-attack vectors. Based on the literature, this study proposes a framework for understanding cybersecurity for older adults that can be used as guiding principles to educate and prevent cybercrime. This study will also analyse and discuss the challenges faced by seniors in cybersecurity. As an outcome, this study reveals that there is an awareness of cybercrime among elders[22].

3.2. Legal Framework on Indian Cybercrime for the Protection of Senior Citizens

The Information Technology Act, 2000, amended in 2008 and 2021, is the bedrock of India's cyber law regime[23]. It prescribes punishment and penalty for cybercrimes like identity theft (Section 66C), cyber cheating by impersonation (Section 66D), and breach of privacy (Section 72). Senior citizens becoming victims of spoofed calls seeking OTPs or banking information are given protection under these sections. Section 67 covers the case of transmitting obscene content, which can be utilized in cases of online harassment of the elderly. Such provisions are significant in curbing crimes such as financial fraud and invasion of privacy, which often target the elderly[24].

Besides the IT Act, the Indian Penal Code (IPC), 1860, provisions are utilized in cybercrime cases. Offenses like 420 (cheating and dishonestly inducing delivery of property), 499 and 500 (defamation), and 354D (cyber stalking, among others) are regularly used in cases involving cyber fraud or online harassment. These are particularly applicable when elderly individuals are cheated using fake online websites or threatened and humiliated on social media. Though the IPC is pre-digital, its application to cybercrime has been upheld through interpretations of laws[25]. The Digital Personal Data Protection Act, 2023, is one of the new pieces of cyber legal legislation in India. It requires explicit consent for processing personal data, gives individuals the rights to access and correct their information, and imposes severe penalties for unauthorised disclosure of data. The act is especially meaningful for elderly citizens who post sensitive personal data online, including health or financial data, and pose as possible targets of exploitation or identity theft. The law gives them the power to decide what is done with their information, in line with contemporary international norms of data protection[26].

---

[22] N H N Zulkipli, 'Synthesizing Cybersecurity Issues and Challenges for the Elderly' (2021) 12 *Turkish Journal of Computer and Mathematics Education* 1775.

[23] K Jaiswal, 'Effectiveness of Cybercrime Laws and Regulations in India: A Critical Study' (2022).

[24] G Kaur, 'Internet Crimes against Minors and Legal Framework in India' (2022) 68 *Indian Journal of Public Administration* 705.

[25] L Gaur, 'Evolution of Cyber Laws in India' (2022) 3 *Jus Corpus Law Journal* 670.

[26] D Chakraborty, 'Copyright Challenges in the Digital Age: Balancing Intellectual Property Rights and Data Privacy in India's Online Ecosystem' (2023) SSRN 4647960.

The Indian Constitution also serves to safeguard senior citizens' rights in cyberspace. Article 21, which protects the right to life and liberty, has been interpreted by the Supreme Court to encompass the right to privacy[27]. This right, as enshrined in the constitution, safeguards people against unwarranted surveillance, misuse of data, and exploitation in the virtual world. Article 14 ensures that citizens are treated equally before the law, so that senior citizens get equitable legal protection and are not discriminated against online[28]. Further, the Directive Principles of State Policy, particularly Article 41, specifically highlight the responsibility of the state to make public assistance available in old age as well as during disability.

3.3. Results

The Result of the study is presented as follows: after a detailed distribution of questions to respondents and based on their responses, the result was formulated.

Demographic analysis

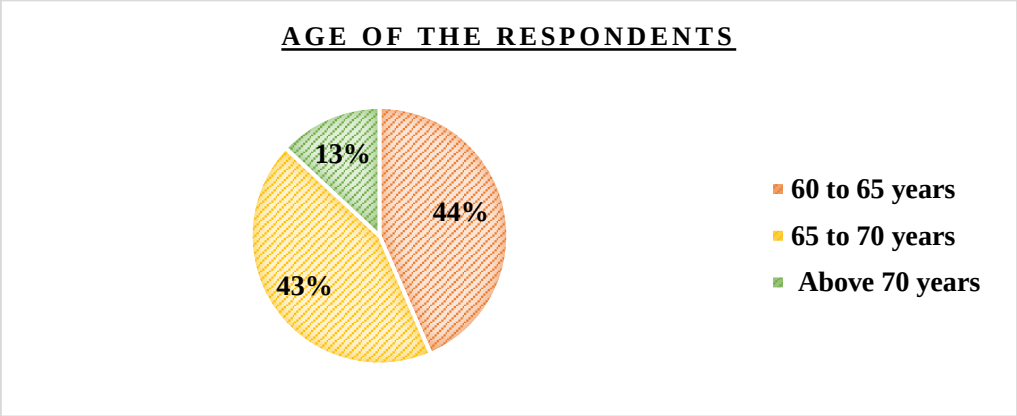

Figure 2. Respondent's age group

Figure 2 illustrates the age group of the respondents from the questionnaire. The figure clearly delivers that most of the respondents' ages belong to the age group of 60-65 years, which is 44% of the total respondents' age, and 43% of the respondents group belongs to the age group of 65 to 70 years. 13% of the respondents belong to the age group of above 70 years.

[27] M S Bhasker and M K Singh, 'Right to Privacy is an Intrinsic Part of Right to Life and Personal Liberty' *Journal of Legal Studies* 84.
[28] M Matić Bošković, 'Addressing Access to Justice for Elderly People' (2023).

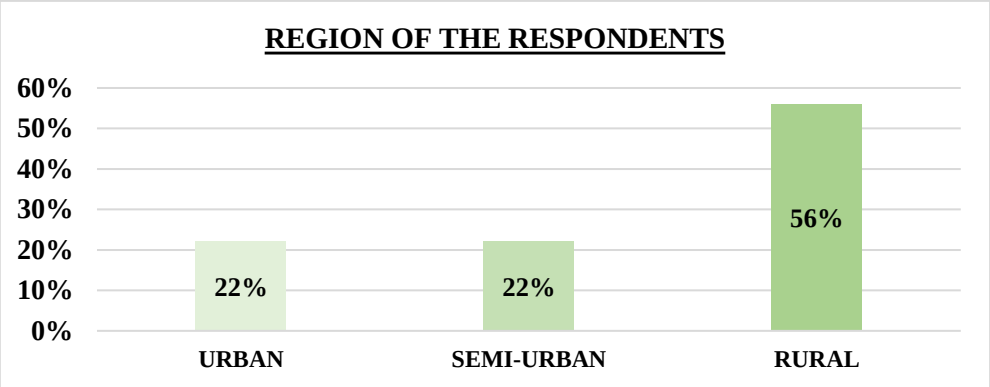

Figure 3. Respondent's Region

Figure 3 illustrates the region of the respondents from the questionnaire. The figure clearly delivers that most of the respondents' age belongs to the rural region, which is 56% of the total respondents' region, and 22% of respondents belong to the semi-urban region, and 22% of the respondents belong to the urban region.

Statistical analysis of the data

Table 1: Linear Regression Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Significance
		B	Standard Error	Beta		
1	(Constant)	.387	.114		3.399	.001
	Did you disclose any of your financial information to strangers	.431	.119	.343	3.607	.000
	Did someone misuse your ATM and Credit card	.418	.119	.336	3.543	.000

Table 1 illustrates the strength of the relationship among the variables. Did you disclose any of your financial information to strangers? Did someone misuse your ATM and Credit card? These variables are considered to analyse the threat rate of cybercrime among senior citizens. This analysis supports in performing the hypothesis for the research. The significance value is below the tolerable level of 0.05 for a 95% confidence interval. As the significance value is below 0.05, the null hypothesis is rejected, H1: cybercrime issues faced by the Senior Citizens. These further reveals that there is awareness of cybercrime among senior citizens because most of the Citizens in Indore are educated.

Table 2: ANOVA

	Sum of Squares	df	Mean[2]	F	Significance
Male	62.890	50	.293		
Female	100.7in29	65	50.364	172.178	.000
Total	163.619	115			

ANOVA analysis is executed to find the association between dependent and independent variables, and it is represented in Table 2. This research is generally executed to define the statistical variance among independent variables. The significant value attained for the measured concept is 0.00, and hence, there exists a significant relationship among independent groups. The two variables considered for defining the statistical variance are reporting the cybercrime issue to the local police station, with an independent variable gender of the respondents. This denotes that the factor represents that they report the cybercrime issue to the local police station. Hence, the null hypothesis that there is no cybercrime issues are not faced by the Senior Citizens can be rejected.

Table 3: Bi-variant Correlations

		Did the government authority actively work on solving the cybercrime issue	**Are you satisfied with the current cybercrime law in India**
Did the government authority actively work on solving the cybercrime issue	**Pearson Correlation**	1	-.625**
	Significance (2-tailed)		.000
	N	115	115
Are you satisfied with the current cybercrime law in India	**Pearson Correlation**	-.625**	1
	Significance (2-tailed)	.000	
	N	115	115

Analysing in Table 3, correlation in data exploration is a statistical method used to calculate the power of the correlation or relationship among the measured factors and calculate their association through the significant coefficient value of Pearson. When the Pearson correlation coefficient values of the variables are observed to be the same, they are negatively correlated. The Pearson coefficient value of -0.625 indicates that there is a negative relationship between the two considered variables. The government authority actively worked on solving the cybercrime issue has a negative relationship with you are not satisfied with the current cybercrime law in India. Hence, there is an association between the considered variables as the significant value is 0.00, which shows that the two considered variables impact each other, and the null hypothesis the no impact of cybercrime law on cybercrime issues faced by the Senior Citizens can be rejected.

Table 4: Bi-variant Correlations

		Have you faced cybercrime issues even after complaining to the cyber cell	**Do you know the procedure to file a case in the cyber cell**
Do you faced cybercrime issues even after complaining to cyber cell	**Pearson Correlation**	1	.348**
	(2-tailed) significance		.000
	N	115	115
	Pearson Correlation	.348**	1

Do you know the procedure to file case in cyber cell	**(2-tailed) Significance**	.000	
	N	115	115

Table 4 provides the outcome of bi-variant correlation among the variables: have you faced cybercrime issues even after complaining to the cyber cell, and do you have knowledge of the procedure to file a case in the cyber cell? The Pearson coefficient value is positive and which states that the variables are correlated with each other, and the Pearson coefficient value is 0.348. Further, there is a significant relation among the variables as the significance value is 0.05. The table clearly illustrates that senior citizens have faced cybercrime issues even after complaining to the cyber cell, and they have knowledge of the procedure to file a case in the cyber cell.

3.4. Discussion

Various studies have found that there is an awareness of cybercrime among elders[29]. They did not face any phishing, cyber pornography, money laundering, password sniffer, credit card fraud or even web jacking, either among elders who reside in their own homes or among elders who reside in old age homes[30]. Males have more awareness of cybercrime when compared to females it is because female elders don't have internet facilities[31]. The outcome of the study reveals that the maximum participants know about cybercrime[32]. The majority of people have an awareness of cybercrime, and they don't have a fear of reporting or approaching a complaint[33].

The rejection of all null hypotheses in this study highlights a clear pattern that senior citizens of Indore are not only aware of cybercrime laws but are also encountering cyber threats, and India's legal framework has been effective in addressing these challenges. The IT Act, 2000, especially Sections 66C (identity theft), 66D (cyber impersonation), and 72 (privacy protection), equips elderly citizens with legal tools to recognize and report cybercrimes[34]. The recent Digital Personal Data Protection Act, 2023, strengthens their rights by ensuring transparency and accountability regarding the use of personal data, thereby fostering greater trust among seniors in

[29] N H N Zulkipli, 'Synthesizing Cyber security Issues and Challenges for the Elderly' (2021) 12 *Turkish Journal of Computer and Mathematics Education* 1775.
[30] Y S Rao, 'Cyber Crime Assessments' in Prof (Dr) Hima Bindu Maringanti (ed), *Cybercrime Assessments* 10.
[31] N Arfi and S Agarwal, 'Knowledge of Cyber-Crime among Elderly across Gender' (2014) 2 *International Journal for Advance Research in Engineering and Technology* 7.
[32] N Arfi and S Agarwal, 'Assessment of Knowledge of Cybercrime among Elderly across Residence' (2013) 2 *International Journal of Innovative Research and Studies* 643.
[33] G Mesko and I Bernik, 'Cybercrime: Awareness and Fear: Slovenian Perspectives' in *2011 European Intelligence and Security Informatics Conference* (IEEE 2011) 28.
[34] S Katkuri, 'Indian Cyber Law' (2018) 3 *International Journal of Advanced Research and Development* 640.

digital transactions such as online banking and e-services[35]. Beyond statutory laws, constitutional protections under Article 21 (right to privacy) and Article 14 (equality before the law) provide a robust legal safety net for senior citizens in cyberspace[36]. The positive correlation between legal awareness and cybercrime reporting also indicates growing confidence in the justice system and government initiatives like CERT-In and MeitY's awareness campaigns. Overall, the findings reflect a constructive and supportive legal environment where statutory provisions, constitutional rights, and institutional support collectively empower senior citizens to navigate the digital world with enhanced security, confidence, and dignity.

To determine the significant association between the research variables, an empirical investigation was done. The study objectives were used to construct the hypotheses, which were then evaluated using statistical analysis. The correlation test was used to evaluate the relevance of the component that contributes to government authority actively working on solving the cybercrime issue, compared to be you are satisfied with the current cybercrime law in India. The one-way ANOVA test demonstrates the significance of the dependent variables of the cybercrime issue to the local police station, with an independent variable called gender of the respondents and the statistical analysis result with a significance level less than 0.05. The study's main goal was to show that Indian cybercrime laws are for the protection of Senior Citizens. The aims and hypotheses of the study have been validated by the research design and technique that have been suggested. This shows that the investigation of the variables has been showed that how senior citizens in Indore have faced those cybercrimes and how they overcome them. The study, however, solely concentrated on Indore. Therefore, the results of this study are merely a sample and can be used for the projects.

4. Conclusion

Cybercrime comprises anything from electronic cracking to denial-of-service attacks, and is a phrase utilised to comprehensively describe the criminal action done by computer networks or computers as a target, a tool, or a place of unlawful activity. It can also refer to conventional crimes where the illegal action is made possible by computers or networks. Cybercrime can stop any railway wherever it is, steer planes in the wrong direction while they are in flight, provide foreign nations access to any sensitive military information, shut down e-media, and bring down any system in a matter of seconds The paper concludes that the senior citizens have an awareness on cybercrime because Indore is a city which has high literacy level and they are ready to face the hurdles of cybercrime and report a complaint.

[35] S Bhatnagar, 'Digital Trust Certification: Building Resilient, Ethical, and Citizen-Centric Digital System' (2025).
[36] N Das, 'Right to Privacy in Cyberspace: A Constitutional Analysis' (2024).