
A CRITICAL ANALYSIS OF THE IMPACT OF DIGITAL MEDIA ON RIGHT TO PRIVACY IN INDIA

Manasvi Sunil, B.A.LLB., (Hons), Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai

ABSTRACT:

The right to privacy has been profoundly influenced by the digital revolution. Concerns about the interaction between digital media and the right to privacy are numerous and constantly changing. Digital media, which includes social networks, internet platforms, and communication technology, has revolutionised the creation, sharing, and accessibility of information. The right to privacy of persons is significantly impacted by this transformation. The objectives of the study are To analyse the right to privacy in the context of social media, To study the awareness of people on digital media and data protection in relation with a right to privacy, and To make people aware of the data protection laws. This is a descriptive study, that uses survey by questionnaire to collect data and the sample size is 210. The sample frame is Chennai, Tamil Nadu. The key findings of this study are people are unaware of data protection laws and how their data is being used even though a majority of the population uses digital media often, it is also found that legal literacy about data protection laws is low and sample respondents do not feel that their data is being adequately protected by digital media companies and the are not satisfied with governments initiative on data protection.

Keywords: Digital media, India, right to privacy, legal framework, data protection, social media, government surveillance, digital literacy,

INTRODUCTION:

Digital media has revolutionised the creation, distribution, and consumption of information, becoming an essential component of modern civilization. The right to privacy has been profoundly influenced by the digital revolution in India, as it has in many other countries. The historical background, existing legislative frameworks, influencing variables, current developments, and a comparison with other nations will all be covered in this critical analysis. The Indian Constitution is the source of the right to privacy, which is implied from the right to life and personal liberty under Article 21 but is not stated expressly. Historical cases such as *State of Uttar Pradesh v. Kharak Singh* (1964) and *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) have significantly influenced the privacy jurisprudence over time. With the passing of the Personal Data Protection Bill, 2019, privacy regulations in India have undergone substantial changes. If this measure is passed, it will provide a thorough framework for protecting personal data that includes requirements for individual consent and strict obligations for data processors.

But given the advent of cutting-edge technology like biometrics, artificial intelligence, and facial recognition, questions remain about how effective these regulations will be. The lack of a specific legislation pertaining to surveillance, in conjunction with the extensive jurisdiction of governmental bodies, prompts inquiries over the sufficiency of extant legal measures.

The impact of digital media on India's right to privacy is changing due to a number of causes. Personal data is always at risk in this environment due to the rapid improvements in technology, the growth of social media platforms, and the growing dependence on digital services. Vulnerabilities are further exacerbated by the population's low level of digital literacy.

Concerns over the possible erosion of privacy rights have been raised by government monitoring programmes, which are frequently justified on the basis of national security. This discourse is still heavily influenced by the delicate balance that must be struck between the rights of the individual and the common interest in security. A new era of surveillance capitalism, where user data is commodified for profit, has been brought about by the advent of the digital age. The increasing frequency of cyberattacks, data breaches, and the improper use of personal data highlight the critical need for effective privacy protection measures.

Furthermore, people are willingly disclosing a great deal of personal information on social media, erasing boundaries between the public and private domains. The preservation of private rights has particular difficulties as a result of this occurrence and the difficulties in enforcing

privacy settings. In contrast, different nations have taken differing stances when it comes to digital media and privacy. European countries have set strong requirements for data protection, with a focus on user consent, transparency, and severe consequences for noncompliance. This is especially true under the General Data Protection Regulation (GDPR).

On the other hand, certain nations—especially those with authoritarian regimes—have compromised people's right to privacy by using digital tools for widespread surveillance. These countries' experiences provide useful comparison points for assessing how well India is handling digital privacy. The impact of digital media on India's right to privacy is a complex and dynamic issue. The constantly evolving technology landscape requires constant adaptation, even in the face of legal measures to address the complexities of data protection. Maintaining a delicate balance between individual privacy and community interests calls for continued discussion, improved legislation, and a dedication to defending citizens' fundamental rights in the digital era.

OBJECTIVES:

- To analyse the right to privacy in context of social media
- To study the awareness of people on digital media and data protection in relation with right to privacy
- To make people aware of the data protection laws

REVIEW OF LITERATURE

Gry (2015) found that The way the right to privacy is framed does not appear to take into account the changes brought about by the Internet public realm. The findings of a qualitative study involving 68 high school students in Denmark provide insight into how individuals use social media to see, negotiate, and manage their private lives. There is a case to be made for incorporating these studies' findings into policy talks on online privacy.

Anderi (2021) aimed to look into how social media and privacy are related. It was discovered that social media privacy is less about protecting property rights and more about having control over how one presents oneself. Privacy is made possible by social media, but authenticity and honesty suffer as a result. Additionally, there are exposure risks that may make it more difficult for people to decide what parts of themselves they choose to disclose to others.

Anderi (2020) Examined the relationship between privacy and social media is the study's main

goal. Data protection and the effect of social media on privacy as self-presentation will be highlighted. Research indicates that social media offers a great degree of privacy, but it also carries substantial risks of exposure that could compromise people's ability to decide what parts of themselves they choose to share with others.

R.D Wolf (2015) aimed to present an overview of privacy as it relates to social media, comprehends and investigates privacy through the lenses of different disciplines in the social sciences, and addresses the lack of a single definition of privacy relevant to all elements of social media. The primary conclusion of the paper is that privacy in the context of social media is intricate and multidimensional, necessitating the synthesis of viewpoints from several academic fields in order to provide a thorough framework that directs research on privacy and information disclosure.

E. Rodríguez,(2019) investigated how Digital Rights Management (DRM) concepts may be used to better enforce existing privacy laws and cater to social network users' privacy preferences. The paper's primary conclusions are that, although users are currently protected to some degree by online social networks' privacy regulations, individuals may eventually have more influence over their privacy preferences.

Beigi, G., & Liu, H. (2018). aimed to review and contrast the most recent algorithms for anonymization and privacy leakage attacks, as well as to talk about unresolved issues and potential future research topics for user privacy concerns on social media. The vulnerability of user-generated data to identity and attribute disclosure attacks, the need to sanitise user-generated data to preserve users' privacy, and the grouping of pertinent works into five categories pertaining to privacy threats in social media are the paper's primary conclusions.

Sabine(2020) Reviewing the concept "control" in privacy theory and developing an understanding of online privacy with communication serving as the primary mechanism for privacy regulation are the goals of this study. The paper's primary conclusions are that privacy on social media is a mutually understood concept and that control is not necessarily the best method to preserve it.

P. Campis(2009) Highlighting the primary privacy issues associated with social media use and offering technologically sound and procedurally sound alternatives to social multimedia networking are the goals of this study. The article discusses the primary privacy risks associated

with using social media networks, the trend in Web usage towards involvement and information sharing through these networks, and privacy-friendly ways to social multimedia networking.

Eileen L. Zurbriggen (2016) examined privacy concerns across a range of social media use contexts and comprehended the privacy paradox in these contexts. The paper's key conclusions are as follows: - Social media users disclose personal information broadly despite their concerns about privacy because of social media's affordances, which can improve relationships and social communication; - There are actual and substantial privacy hazards associated with using social media.

Ghazaleh Beigi, Huan Liu (2020) the study's objective is to present a thorough analysis of previous research on user privacy concerns and solutions in social media, with an emphasis on anonymization algorithms and privacy leakage attacks. The primary conclusions show that people's behaviour, social media sharing, and interpersonal interactions have all changed significantly as a result of the Web's tremendous rise.

Elie Raad, Richard Chbeir(2013) The study's goal is to draw attention to the value of social network data as well as the privacy hazards associated with network analysis and data mining methods. Because users find it difficult to completely secure their accounts and personal information from unauthorised access, privacy concerns are a major problem in online social networks. Social media platforms have total control over the information that users share, and they may purposefully or inadvertently give such information to unapproved parties or third parties.

Jeffry (2021) examines the advantages and disadvantages of social media, concentrating on safe information sharing, privacy issues, the effect of social media on job searches, and the significance of safeguarding private information and maintaining one's reputation. There is very little privacy on social media, and no laws or regulations safeguarding informal information exist. Social media is a valuable resource for job seekers, but unprofessional profiles and inappropriate content can damage one's reputation and reduce one's chances of landing a position

Nadine Barrett-Maitland, Jenice M. Lynch(2020) highlight the value of privacy in today's IT-configured society by examining the expanding usage of social media for personal security and privacy. The primary conclusions highlight the effects of social media use on individual privacy, the significance of monitoring privacy settings and upholding universal moral

principles, and the possibility of security and privacy breaches brought on by unethical social media use

Dr. Shambhu Singh Rathore(2023) The emergence of Web 2.0 has led to social profiling and increased awareness of online privacy issues. Web 2.0 is the framework that makes it easier for users to collaborate and share content in real-time on social networking sites like Facebook and MySpace. The late 2000s saw a surge in the popularity of these social networking services. Numerous people are disclosing their personal information online via these websites. All interactions that take place on these social networks' websites are recorded and archived for future use. Cyberstalking, location disclosure, social profiling, the publication of personal information about third parties, and the use of social media networks by the government for investigative purposes without a search warrant are among the problems.

Althaf Marsoof(2011) The global dissemination of information has been accelerated by the development of information technology. Specifically, personally identifiable information has been leaked on the Internet as a result of recent "Social Networking" trends. This essay's goal is to show how far current legislation can be stretched to combat online privacy violations, particularly when it comes to social networking. The best way to safeguard online privacy, it is suggested, is through privacy-specific legislation.

Senthil Kumar (2015) Social networks allow people to share a wide range of information, including news, education, business, and entertainment, and have become indispensable to human life. To guarantee that users' confidential information is kept secret and unavailable to third parties, they also need stringent security and privacy safeguards.

Ivana Stepanović (2014) The essay explores how technology has altered privacy perceptions, making it challenging to differentiate between public and private spaces. It suggests a need for a new definition of privacy to better protect this fundamental human right, a key tenet of democratic society, and protect individuals from oppressive authorities.

NEŞ PESCHKE Lutz PESCHKE (2013) Social media significantly impacts personal rights, including data protection and image rights. It has accelerated media communication changes, leading to a shift in media culture and privacy. This paper provides an overview of the current legislative framework for privacy protection in Germany and Turkey.

Lilian (2016) discusses the shift from traditional police surveillance to profiling and pre-crime methods, focusing on the rise of open source and social media intelligence. It examines privacy

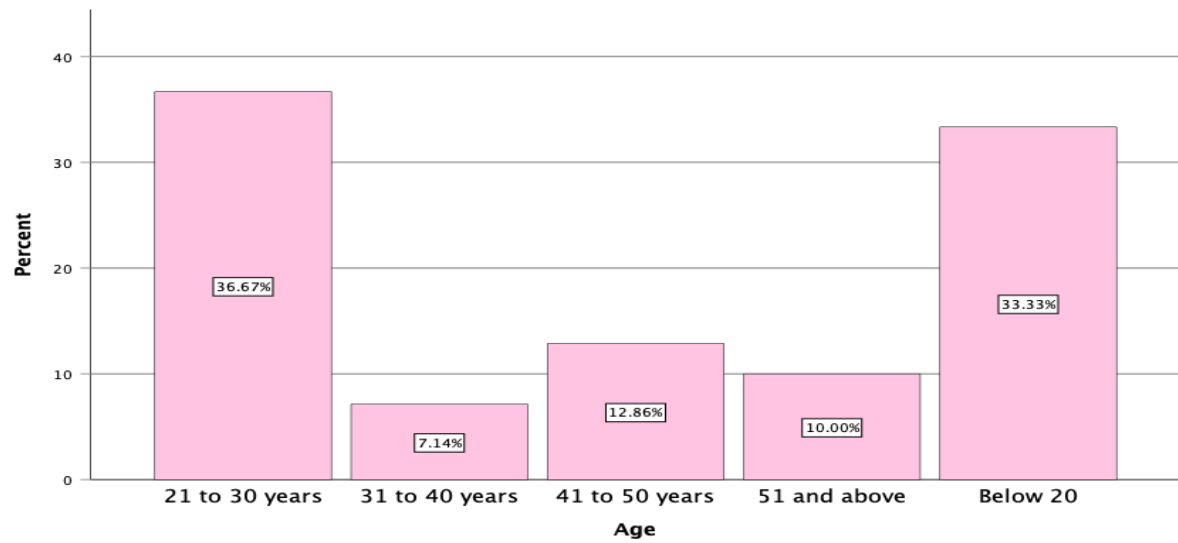
protection in UK law for SOCMINT and suggests that reasonable expectations of privacy may be supported by users' perception of the environment and the impact of search engines on traditional state surveillance. The paper concludes that existing law lacks adequate protection for open SOCMINT.

Emily (2017) initially examines the form and narrative of online shaming, classifying it into broad categories such as bullying, vigilantism, bigotry, and gossiping. These categories are then used throughout the essay to assess various viewpoints on the privacy issues brought up. Secondly, this study investigates shaming through the lens of three major privacy debates: the social dimension of privacy, the relationship between privacy and dignity, and the right to privacy in public spaces. This study revealed some themes. Public humiliation is a prevalent element of online shaming, too.

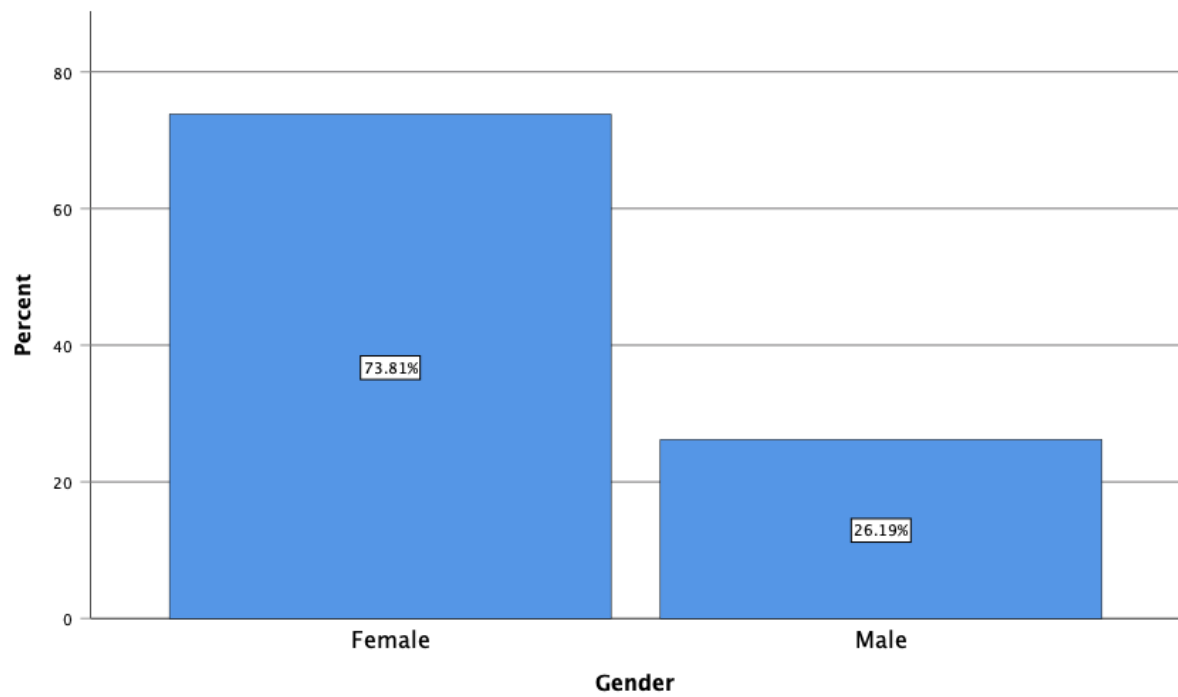
METHODOLOGY:

The type of research here is descriptive research. A total of 210 samples have been collected. The samples have been connected to the convenience sampling method. The sample names taken here are online in and around Chennai. The independent variables are age, gender, place of residence, and education qualification. The dependent variables most used platform in digital media the frequency of usage of digital media, experienced a breach of your digital privacy, agreeability that personal information is adequately protected by digital media companies in India, steps taken to enhance digital privacy, Awareness about data protection and privacy laws, Rate the Indian government's action for protecting data. The researcher used graphs to analyse the data collected.

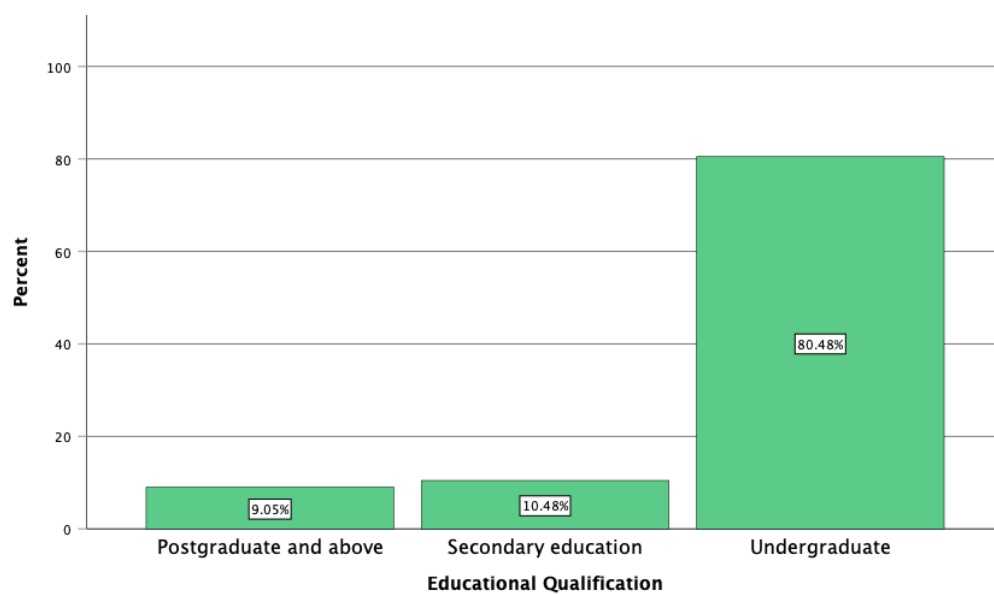
ANALYSIS:



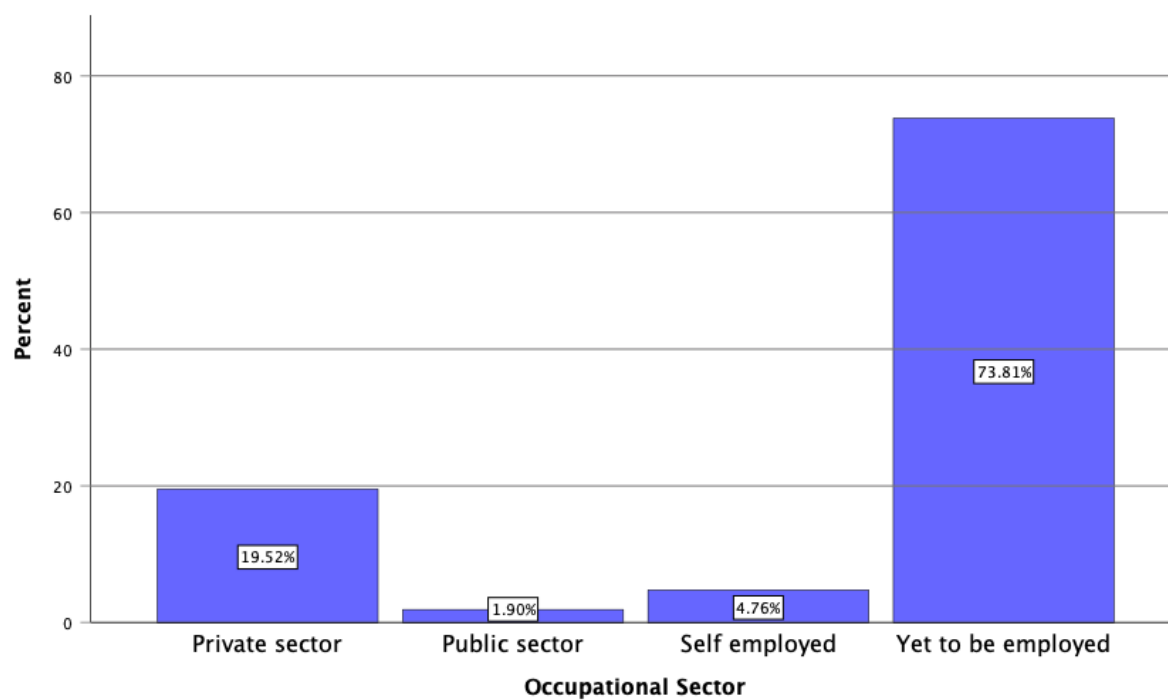
LEGEND: Figure 1 showing the age of sample respondents



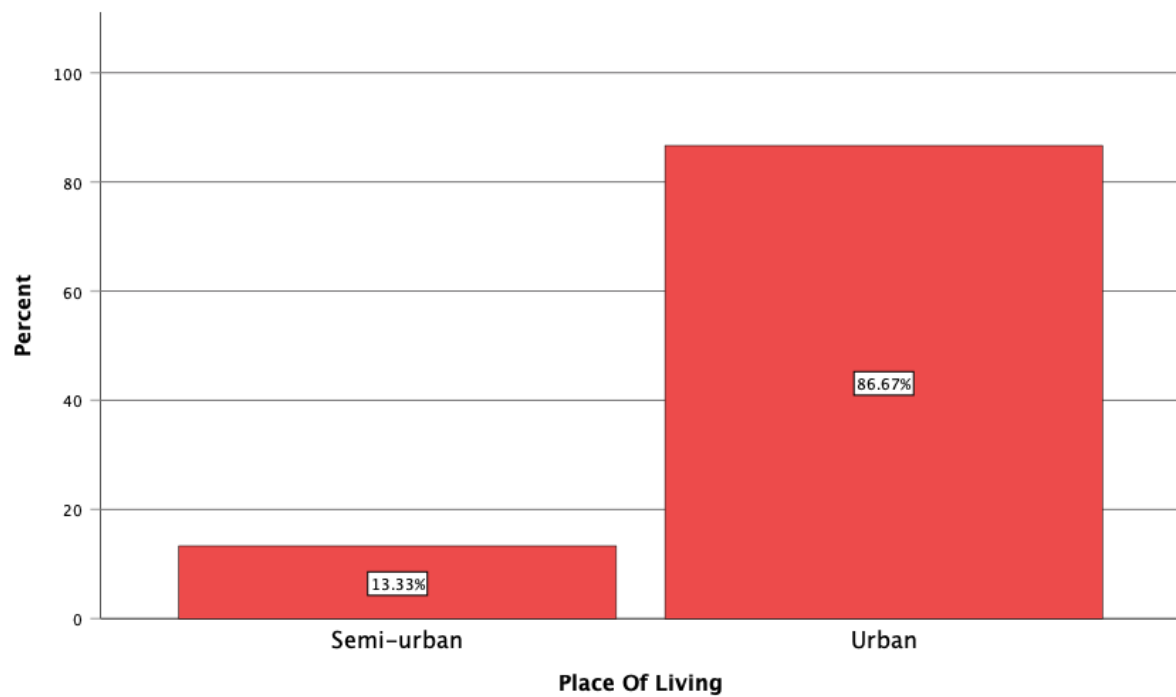
LEGEND: Figure 2 showing the gender of sample respondents



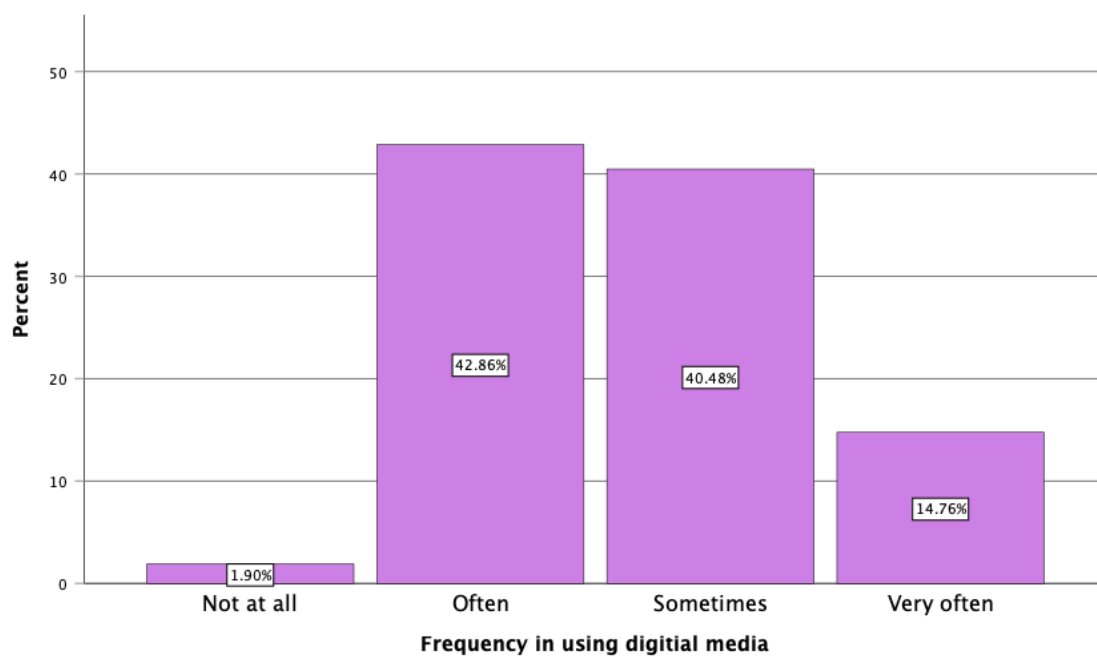
LEGEND: Figure 3 shows the educational qualification of sample respondents



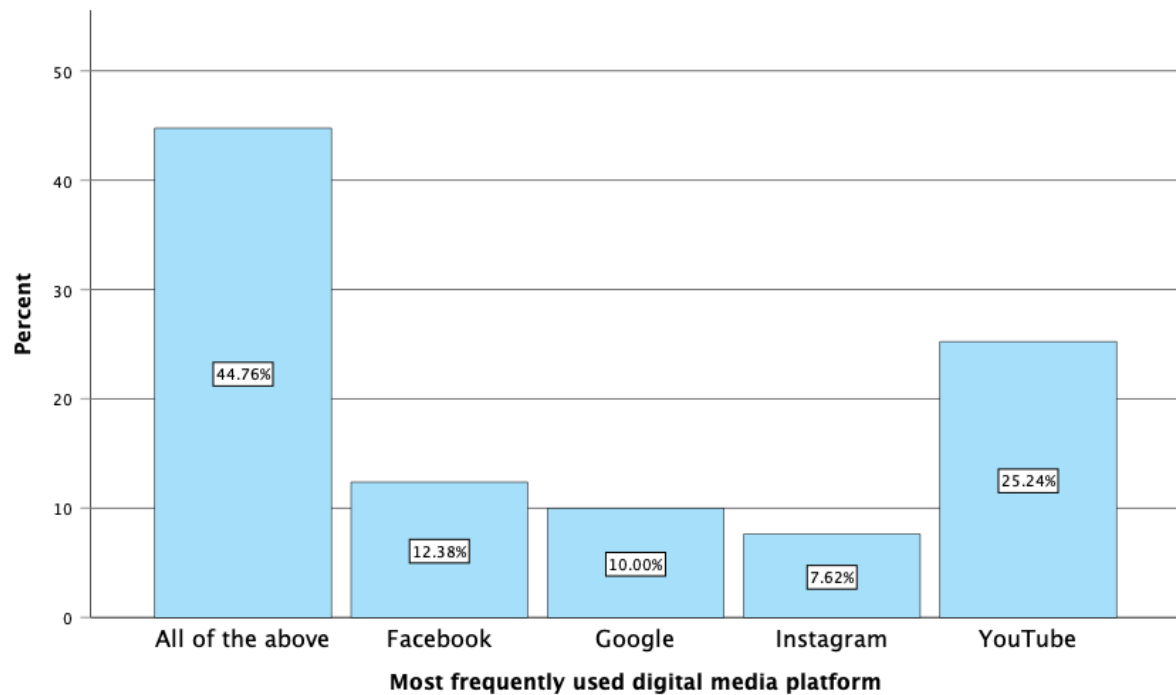
LEGEND: Figure 4 shows the occupation of the sample respondent



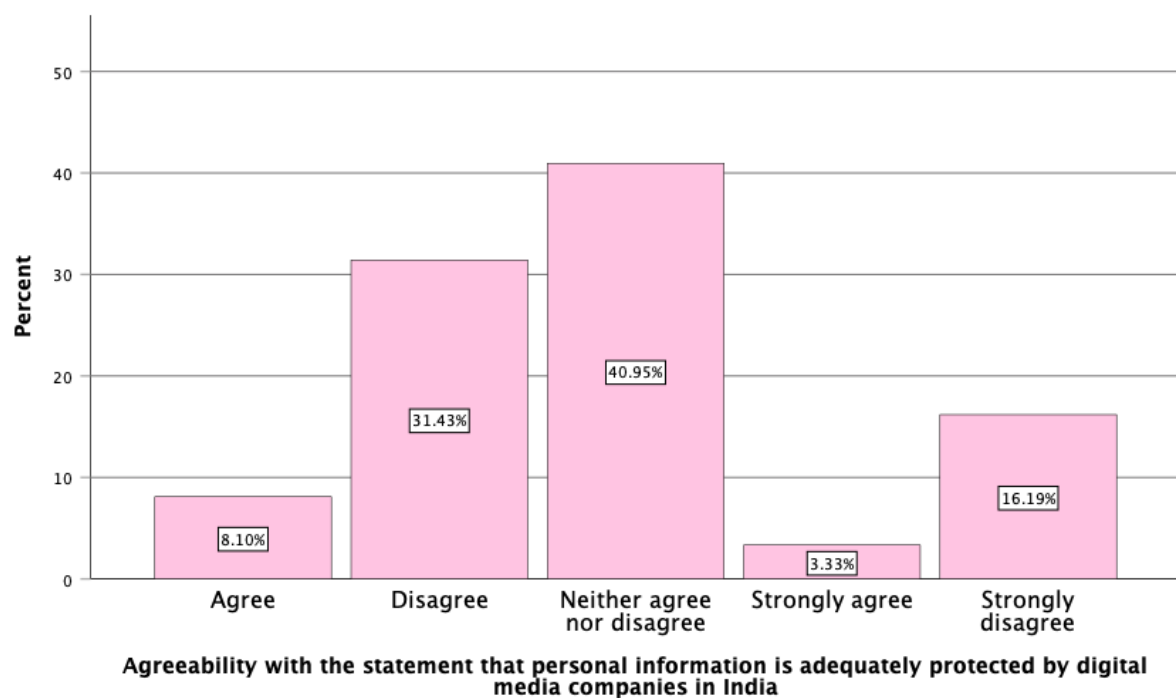
LEGEND: Figure 5 shows the place of residence of the sample respondents



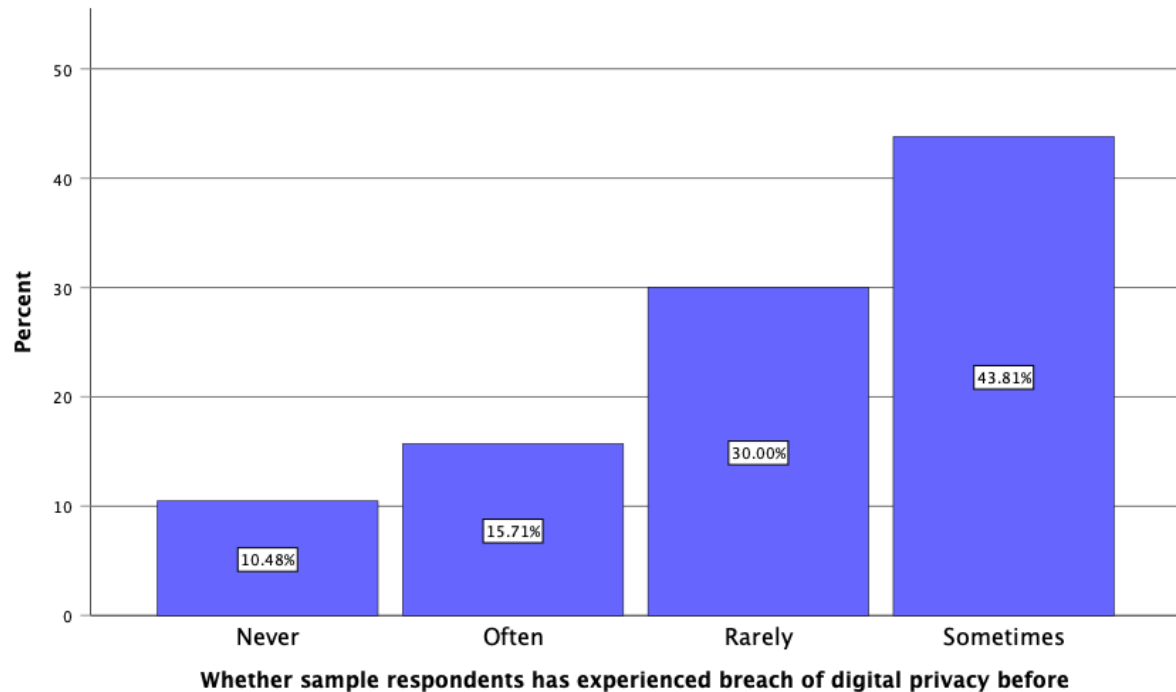
LEGEND: Figure 6 shows the frequency of usage of digital media among sample respondents



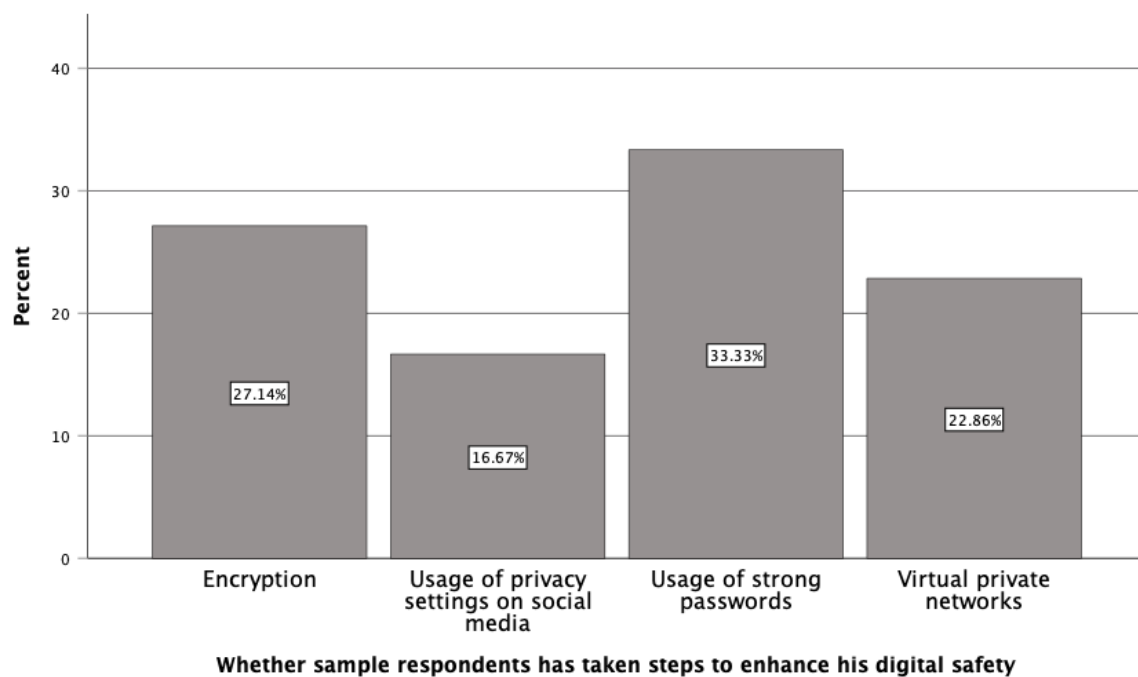
LEGEND: Figure 7 shows the most frequently used digital media platform by sample respondents



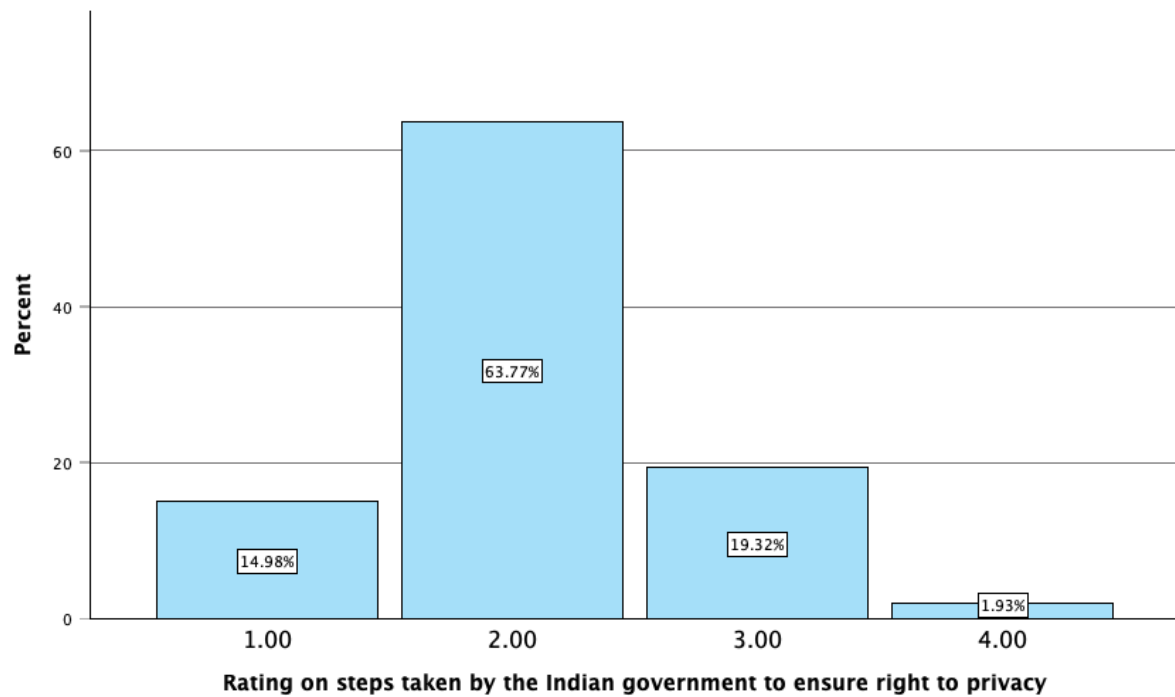
LEGEND: Figure 8 shows the agreeability with the statement that personal information is adequately protected by digital media companies in India among sample respondents



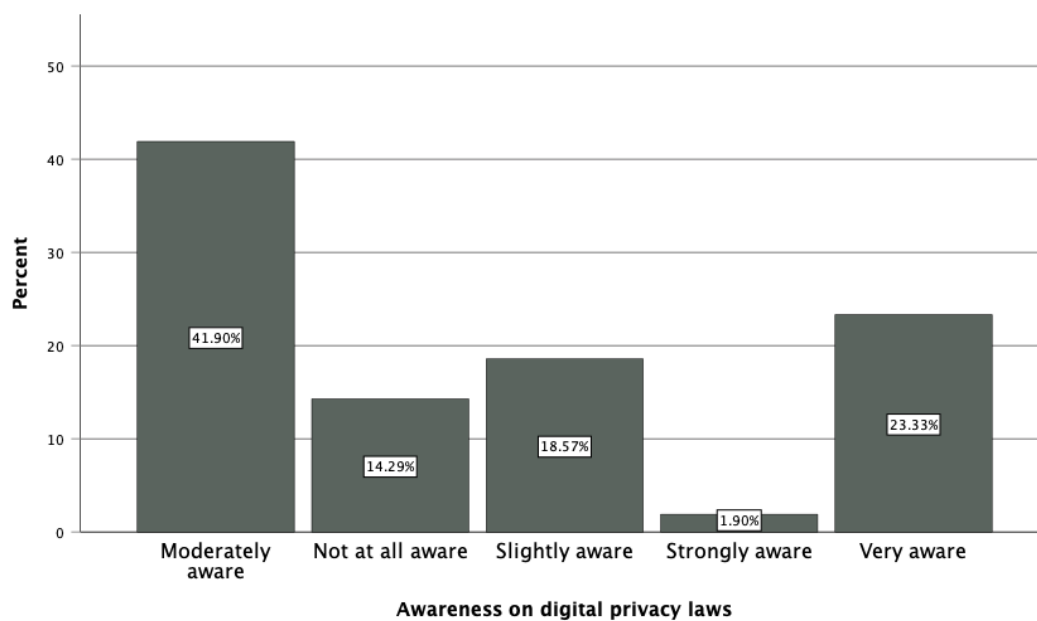
LEGEND: Figure 9 shows whether sample respondents have experienced data breach



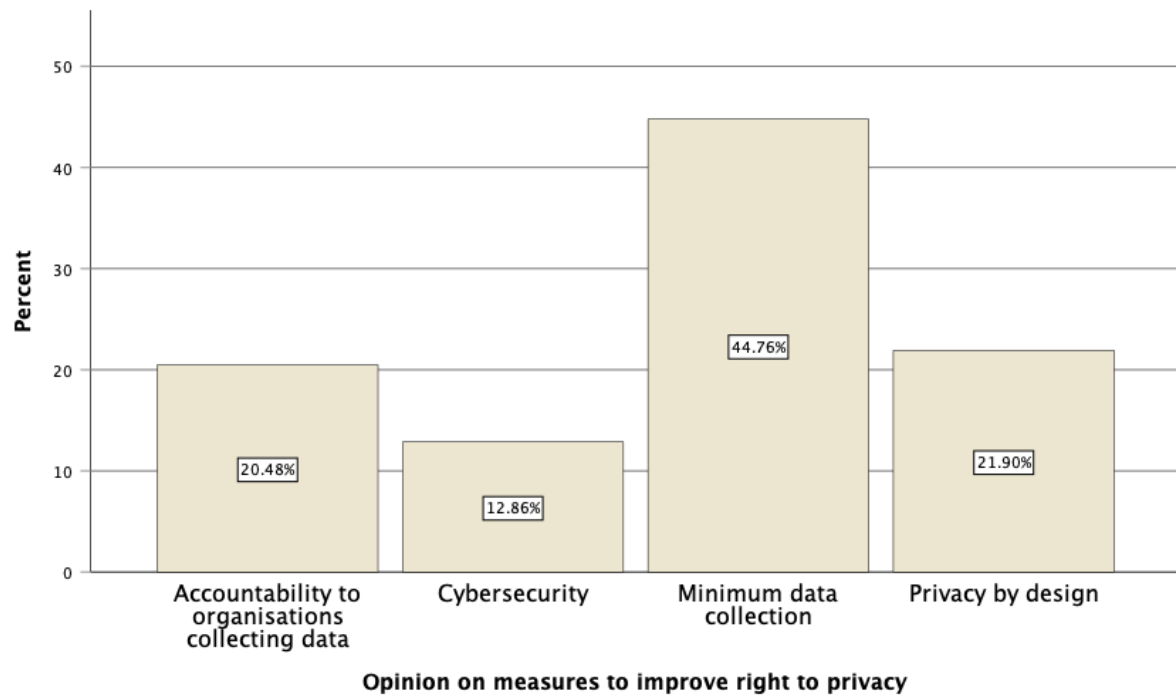
LEGEND: Figure 10 shows whether sample respondents have taken steps to enhance digital safety



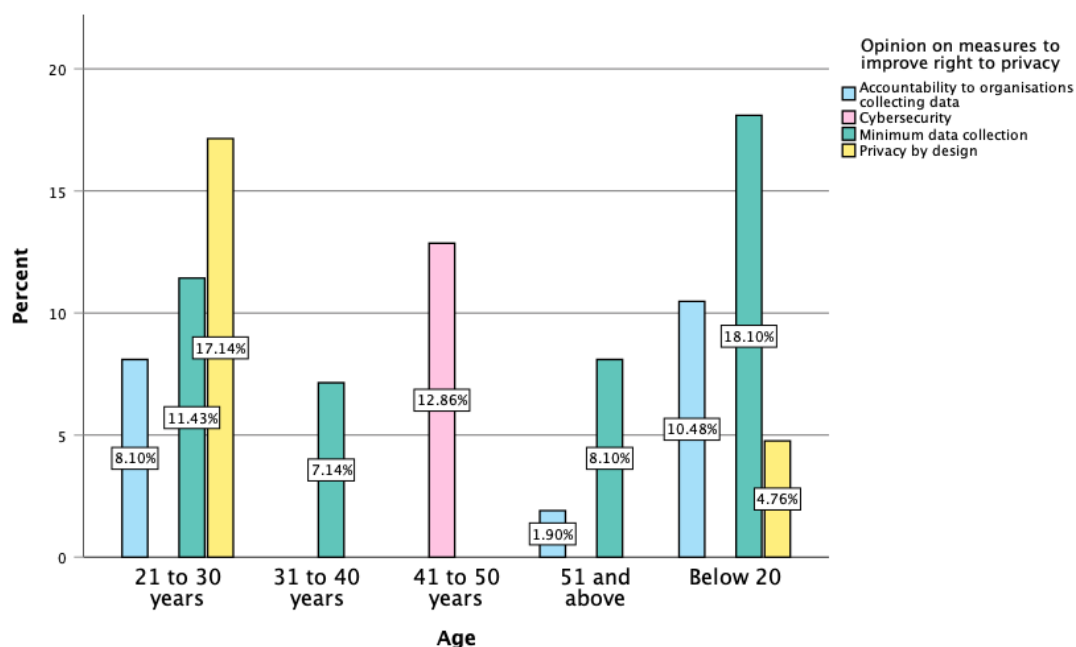
LEGEND: Figure 11 shows the rating of steps taken by government to ensure to privacy of users



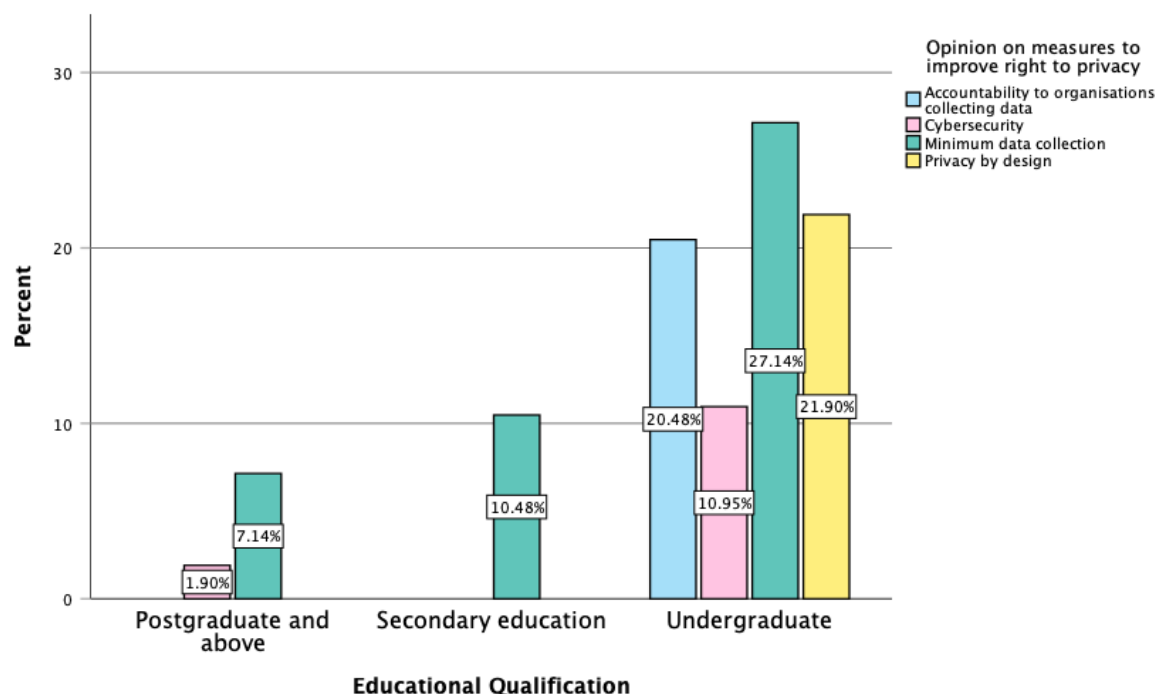
LEGEND: Figure 12 shows the awareness of digital privacy laws among sample respondents



LEGEND: Figure 13 shows the opinion of sample respondents on how companies can improve the right to privacy.



LEGEND: Figure 14 shows the age of sample respondents in relation to opinion on how companies can improve right to privacy



LEGEND: Figure 15 shows the educational qualification of sample respondent in relation to opinion on measures companies can take to improve right to privacy

RESULTS:-

It is revealed that 34.31% of sample respondents are of ages 21 to 30 years, 7.84% 31 to 40, 16.67% 41 to 50, 13.42% above 50 years, 27.94% below 20 years(**Figure 1**)

It is revealed that 61.27% of sample respondents are females, and 38.73% of sample respondents are males (**Figure 2**)

It is revealed that 72.06% of sample respondents are postgraduates, 22.55% have completed secondary school, and 5.39% are undergraduates (**Figure 3**)

It is revealed that 8.33% of sample respondents work in Government sector, 32.84% work in private sector, 13.73% are self-employed, and 45.1% yet to be employed (**Figure 4**)

It is revealed that 24.51% of sample respondents are from semi-urban regions, 75.49% are from urban regions (**Figure 5**)

It is revealed that 1.90% of sample respondents say they do not use digital media at all, 42.86% of sample respondents use social media often, 40.48% of sample respondents use social media sometimes, 14.76% of sample use social media very often. **(Figure 6)**

It is revealed that 25.24% of sample respondents use YouTube the most, 12.38% of sample respondents use facebook the most, 10% of sample respondents use google the most, 7.62% of sample respondents use Instagram the most, 44.76% use all of the above **(Figure 7)**

It is revealed that 8.10% of sample respondents Agree with the statement that personal information is adequately protected by digital media companies in India, 31.43% of sample respondents with the statement that personal information is adequately protected by digital media companies in India, 40.95% of sample respondents neither agree nor disagree with the statement that personal information is adequately protected by digital media companies in India, 3.33% of sample respondents strongly Agree with the statement that personal information is adequately protected by digital media companies in India, and 16.19% of sample respondents strongly disagree with the statement that personal information is adequately protected by digital media companies in India **(figure 8)**

It is revealed that 10.48% of sample respondents have never experienced breach of their digital privacy, 15.71 % of sample respondents have often experienced breach of their digital privacy, 30% of sample respondents have rarely experienced breach of their digital privacy, 43.81% of sample respondents have sometimes experienced breach of their digital privacy **(figure 9)**

It is revealed that 27.14% of sample respondents have taken the step of encryption for enhancement of digital privacy, 16.67%% of sample respondents have taken the step of Usage of privacy settings for enhancement of digital privacy 33.33%, % of sample respondents have taken the step of usage of strong password for enhancement of digital privacy, 22.86% of sample respondents have taken the step of VPN for enhancement of digital privacy **(figure 10)**

It is revealed that 14.98% of sample respondents rate $\frac{1}{5}$ of steps taken by the government to ensure to privacy of users, 63.77%% of sample respondents rate $\frac{2}{5}$ of steps taken by the government to ensure to privacy of users, 18.32% of sample respondents rate $\frac{3}{5}$ of steps taken by government to ensure to privacy of users, 1.93 % of sample respondents rate $\frac{4}{5}$ of steps taken by government to ensure to privacy of users. **(figure 11)**

It is revealed that 18.57% of sample respondents are slightly aware of digital privacy laws, 14.29% of sample respondents are Not at all aware of digital privacy laws, 41.90% of sample

respondents are moderately aware of digital privacy laws, 1.90% of sample respondents are strongly aware of digital privacy laws, 23.33% of sample respondents are very aware of digital privacy laws. (**figure 12**)

It is revealed that 20.48% of sample respondents have said accountability to organisations collecting data as a measure to ensure the right to privacy, 12.86 % of sample respondents have said Cybersecurity as a measure to ensure the right to privacy, 44.76% of sample respondents have said minimum data collection as a measure to ensure the right to privacy, 21.90% of sample respondents have said Privacy by design as a measure to ensure the right to privacy, (**figure 13**)

It is revealed that 8.1% of sample respondents of ages 21 to 30 answer accountability to organisations collecting data as opinion for ways to improve right to privacy, 11.43% minimum data collection, 17.14% privacy by design; 7.14% of sample respondents of ages 31 to 40 minimum data collection; 12.86% of sample respondents of ages 41 to 50 cybersecurity; 1.9% of sample respondents of ages 51 and above accountability to organizations collecting data, 8.1% minimum data collection; 10.48% of sample respondents of ages below 20 accountability to organisations collecting data, 18.1% minimum data collection, 4.76% privacy by design(**Figure 14**)

It is revealed that 1.9% of sample respondents who have completed postgraduate and above are of the opinion that cybersecurity is a measure to improve right to privacy, 7.14% minimum data collection; 10.48% of sample respondents who have completed secondary education say minimum data collection; 20.48% of sample respondents who are undergraduates say accountability to organisations collecting data, 10.95% cybersecurity, 27.14% minimum data design, 21.9% privacy by design(**Figure 15**)

DISCUSSION:

In **figure 5**, we see that a significant majority of the population use digital media often this shows how digital media has become a integral part of our lives and how The widespread availability of the internet and the proliferation of smartphones have significantly increased connectivity and accessibility. People can easily access social media platforms from their devices, fostering a global network of communication. Social media platforms provide a convenient and immediate means of communication. Users can stay in touch with friends, family, and colleagues, share updates, and engage in real-time conversations, fostering a sense of connectedness. The usage of social media involves the generation and collection of vast

amounts of user data. This data can be utilized for various purposes: Social media platforms leverage user data to provide targeted advertisements based on users' interests, behaviours, and demographics. While the collection and use of data contribute to the functionality and profitability of social media platforms, it also raises concerns about user privacy and the responsible handling of personal information

In **Figure 8**, we see that a majority of the population neither agrees nor disagrees on whether digital media companies protect data of its uses, this can show either lack of awareness of the topic or can also show an ignorance as to how the collected data is used, Social networking businesses gather private information on people's activities, passions, traits, political opinions, shopping preferences, and internet behaviours. Social media companies' enormous repositories of user information are open to hacking, data breaches, and scraping, especially if they neglect to implement essential security controls and access limitations. The information at danger can vary depending on the network and include location data, health data, sexual orientation, religion, facial recognition images, private messages, and more. The repercussions of disclosing this information can be dire, ranging from forced LGBTQ individual outings to stalking to the revelation of one's religious beliefs and movements.

In **Figure 10**, shows that all of the sample respondents have taken some step of the other to protect their data on digital media platforms, some more steps that can be taken are, Enablement of Two-Factor Authentication (2FA), being wary of Third-Party Apps, Educate Themselves on Phishing, Limit Personal Information Sharing, Understand and Manage Cookies, Regularly Audit Friends and Followers, Report Suspicious Activity.

In **Figure 11**, we see a significant majority of the population do not consider the Indian governments action on data protection adequate, but India now has a data privacy law for the first time thanks to the 2023 act. Prior to processing personal data, consent must be obtained, and the legislation explicitly lists a limited number of exceptions. Along with the right to nominate, it gives customers the ability to see, update, modify, and remove their data. It adds further security measures to the way children's data is processed. It imposes duties on organisations to provide notice of data collection and processing, limit its use, and ensure security measures. Businesses are required by law to establish grievance redress processes. In addition, the DPB will manage grievances and complaints and has the authority to impose penalties for breaking the law. India now has a regulatory framework for data protection for

the first time. The existence of the law will eventually cause companies that gather data to gradually establish minimum standards of conduct and compliance.

In **Figure 12** we see that a significant majority of people are moderately aware of data protection laws, this shows the lack of awareness among individuals about their rights, this can be improved by Launch comprehensive educational campaigns through various mediums, including social media, television, radio, and print media. Conduct workshops and training sessions in schools, colleges, workplaces, and community centres. Tailor the content to the specific audience, addressing concerns and practices relevant to each group. Integrate data protection and privacy awareness into legal literacy programs. Empower individuals with knowledge about their rights, legal remedies, and how to exercise them.

LIMITATIONS: The study uses a convenient sampling method.

CONCLUSION:

In conclusion, the effect of digital media on India's right to privacy is a complex and dynamic issue that necessitates careful evaluation of sociological, legal, technological, and historical aspects. The creation, sharing, and consumption of information have all changed as a result of the digital revolution, posing both benefits and threats to privacy. India has taken attempts to address the complications coming from the digital age, with recent legislative efforts including the Personal Data Protection Bill, 2019, and its constitutional acknowledgment of the right to privacy. But considering the speed at which technology is developing and the fluidity of digital media, the efficacy of these steps is still being evaluated. The legal landscape has historically been shaped by significant judgements and rulings from the judiciary, such as the Supreme Court's recognition of privacy as a basic right. However, there are still issues that need to be resolved, such as the requirement for a specific surveillance statute and the delicate balancing of individual rights with the needs of national security. The complex dynamics of the digital privacy discourse are influenced by events like government spying, data breaches, and the blurring of public and private borders in social media. The commoditization of user data for financial benefit and the ubiquitous effect of surveillance capitalism exacerbate privacy issues. In the modern world, digital literacy, education, and user awareness stand out as essential elements in enabling people to safeguard their privacy. Legal frameworks are important, but user-centric measures are even more important for reducing risks. Examples of these include enhancing privacy settings, maintaining good online hygiene, and being aware of the consequences of sharing data. The critical analysis essentially highlights the necessity of an

all-encompassing and dynamic strategy for digital privacy in India—one that incorporates strong legislative frameworks, proactive government, and empowered individuals. Policymakers, engineers, legal experts, and the public must keep talking as the digital ecosystem develops in order to achieve a balance between the advantages of digital media and the protection of individual privacy rights.

REFERENCES:

1. Lapenta, G. H., & Jørgensen, R. F. (2015, February 24). Youth, privacy and online media: Framing the right to privacy in public policy-making. *First Monday*. <https://doi.org/10.5210/fm.v20i3.5568>
2. Marmor, A. (2021, November 10). Privacy in Social Media. *Oxford Handbook of Digital Ethics*, 575–589. <https://doi.org/10.1093/oxfordhb/9780198857815.013.31>
3. Marmor, A. (2020). Privacy in Social Media. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3544764>
4. Wolf, R. D., & Heyman, R. (2015, February 11). Privacy and Social Media. *The International Encyclopedia of Digital Communication and Society*, 1–6. <https://doi.org/10.1002/9781118767771.wbiedcs118>
5. Rodríguez, E., Rodríguez, V., Carreras, A., & Delgado, J. (2010). A Digital Rights Management approach to privacy in online social networks.
6. Beigi, G., & Liu, H. (2018). Privacy in Social Media: Identification, Mitigation and Applications. *ArXiv, abs/1808.02191*.
7. <https://doi.org/10.1093/ct/qtz035>
8. Campisi, P., Maiorana, E., & Neri, A. (2009, July). Privacy protection in social media networks a dream that can come true? *2009 16th International Conference on Digital Signal Processing*. <https://doi.org/10.1109/icdsp.2009.5201125>
9. Zurbriggen, E. L., Ben Hagai, E., & Leon, G. (2016, September). Negotiating privacy and intimacy on social media: Review and recommendations. *Translational Issues in Psychological Science*, 2(3), 248–260. <https://doi.org/10.1037/tps0000078>
10. Beigi, G., & Liu, H. (2020, February 29). A Survey on Privacy in Social Media. *ACM/IMS Transactions on Data Science*, 1(1), 1–38. <https://doi.org/10.1145/3343038>
11. Raad, E., & Chbeir, R. (2013). Privacy in Online Social Networks. *Lecture Notes in Social Networks*, 3–45. https://doi.org/10.1007/978-3-7091-0894-9_1
12. Barrett-Maitland, N., & Lynch, J. (2020, September 9). Social Media, Ethics and the Privacy Paradox. *Security and Privacy From a Legal, Ethical, and Technical Perspective*. <https://doi.org/10.5772/intechopen.90906>
13. Lapenta, G. H., & Jørgensen, R. F. (2015, February 24). Youth, privacy and online media: Framing the right to privacy in public policy-making. *First Monday*. <https://doi.org/10.5210/fm.v20i3.5568>
14. Dr. Shambhu Singh Rathore. (2023). New Dimension of Right to Privacy in Social

- Media ERA. *EUROPEAN JOURNAL OF INNOVATION IN NONFORMAL EDUCATION*, 3(9), 21–51.
15. Marsoof, A. (2011, January 16). Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression. *International Journal of Law and Information Technology*, 19(2), 110–132. <https://doi.org/10.1093/ijlit/eqq018>
 16. (2015). On Privacy and Security in Social Media – A Comprehensive Study. *Procedia Computer Science*, 78, 114-119. <https://doi.org/10.1016/j.procs.2016.02.019>
 17. MODERN TECHNOLOGY AND CHALLENGES TO PROTECTION OF THE RIGHT TO PRIVACY Author(s): Ivana Stepanović Journal: Анали Правног факултета у Београду Issue Year: 63/2014 Issue No: 3 Page Range: 167-178 Page Count: 12 Language: English
 18. GÜNEŞ PESCHKE, S., & PESCHKE, L. (2013). PROTECTION OF THE MEDIATIZED PRIVACY IN THE SOCIAL MEDIA: ASPECTS OF THE LEGAL SITUATION IN TURKEY AND GERMANY. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 17(2), 857-884.
 19. Lilian Edwards, Lachlan Urquhart, Privacy in public spaces: what expectations of privacy do we have in social media intelligence?, *International Journal of Law and Information Technology*, Volume 24, Issue 3, Autumn 2016, Pages 279–310, <https://doi.org/10.1093/ijlit/eaw007>
 20. Laidlaw, Emily B. 2017. "Online Shaming and the Right to Privacy" *Laws* 6, no. 1: 3. <https://doi.org/10.3390/laws6010003>