IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Guardians Of The Digital Vault: Analyzing The Right To Privacy Under The Indian Constitution In The Age Of Digital Personal Data

Shubhangi Arde

Research Scholar

Chatrapati Shivaji Maharaj University, Panvel

Abstract

In an era defined by the ubiquity of personal data in the digital realm, the right to privacy has taken on paramount significance. This research paper, titled "Guardians of the Digital Vault: Analyzing the Right to Privacy under the Indian Constitution in the Age of Digital Personal Data," embarked on a comprehensive exploration to delve into the status of the right to privacy within the context of the Indian Constitution and its alignment with the evolving landscape of digital personal data. The first objective of this study was to gauge the level of awareness among Indian citizens concerning their right to privacy. Findings from descriptive statistics and correlation analysis underscored the critical nature of this inquiry. The study discovered a statistically significant relationship between Indian citizens' awareness levels and their right to privacy. This suggests that an informed citizenry is more inclined to assert and safeguard their privacy rights, accentuating the importance of educational and awareness initiatives on this critical topic. The second objective was to evaluate the alignment between digital platforms, government policies in India, and the constitutional provisions pertaining to the right to privacy. Results from regression analysis, as presented in the model summary, ANOVA, and coefficients, painted a picture of persistent misalignment. Data security, public awareness, and constitutional provisions exerted limited influence on digital platforms and government policies concerning privacy protection. In summation, the right to privacy in the digital era is a multifaceted and dynamic challenge that demands sustained attention and concerted efforts from all stakeholders. As technology advances and personal data assumes a central role in our lives, the preservation of privacy remains a fundamental aspect of safeguarding individual liberties and upholding democratic values in the digital age.

Keywords: Digital Vault; Right to Privacy; Indian constitution; Privacy rights; Data protection.

1. Introduction

It is incredibly challenging to retain privacy and secure personal data in the digital era since it may be accessed by a number of persons and used for a variety of purposes. For instance, by the government for monitoring or even by private companies for profit-making. Companies like this leverage the public availability of people's personal information on the internet, including their name and contact information, likes, dislikes, habits, and interests, as well as their medical and financial histories, to boost their revenues. In addition to the information that people freely post online, there are various ways to get personal information about a person without that person's knowledge or agreement. These methods include data mining, clustering, geotagging, and geocoding (Donnelly 2020). The information gathered may be used for either personal or commercial purposes, including sending unsolicited business ads. In reality, when the twenty-first century arrived and technical advancement accelerated, privacy worries about emerging technology appeared to grow. As a result, it is conceivable to assert that new technologies increase the accessibility and usability of personal data. Therefore, it is essential to establish a strong and trustworthy legislative framework for data protection in order to guarantee consistency between innovation and the protection of privacy (Hildebrandt, et al., 2013). There are always conflicts between what should be kept private and what should be made public when it comes to personal data (Kumar 2019). One of those legal notions, privacy, might appear in a number of ways depending on the situation, the time of day, the topic at hand, and even who is presenting the case (Dewan, 2022; Khare K. and Mishra D. 2016).

- **Right to Privacy under the Indian constitution**

In one way or another, privacy protection is provided by constitutional documents all throughout the world (Chinchure 2021). The Fourth Amendment to the US Constitution is one of the most prominent examples of this (Corwin 2008),Human Rights in Articles 17 and 8 of the European Covenant on Civil and Political Rights and the International Covenant on Civil and Political Rights (Egli 2007).The right to privacy was seen to be a penumbra of the Bill of Rights even at the lowest point in American constitutional law, if not an essential component or a substantive right in and of itself (Griswold 1965).However, the development of privacy law in India has gone entirely in a different direction (Bisht A. and Sreenivasulu N. 2022). Despite the fact that it has been discussed in a range of constitutional and non-constitutional settings (RajaGopal 1994), The reality remains that, taken on its own, privacy is nearly unimaginable in Indian law (Behera 2021). India cannot argue that the right to privacy derives from a specific text like other states may (Michael and Charles 1998). A broad reading of Article 21, which states that the right to life and personal liberty can only be taken away through a legally defined mechanism, has proven to be the best path out of this mess thus far (Goyal and Kumar 2016). In fact, Indian law has a long history of seeking to construe Article 21 to create a rather solid right to privacy. The police surveillance of people with criminal histories (also known as "history shelters") is the subject of the first significant "privacy" issues under Indian constitutional law. In **Kharak Singh v. State of Uttar Pradesh**, (Handler 1964) The petitioner alleged that police monitoring of history shelters, notably overnight residence visits, violated Article 21 (Singh S. and Bose M. 2021). The Supreme Court ruled that a right to privacy was

implied in Article 21's rights of personal liberty, citing a great deal of American legal precedent in its decision (Goel 2021).

2. Review of Literature

Khan S., et al., (2023) examined the foundation of the nation's human resource growth has been provided by Indian universities and research institutions, which have fostered brilliant minds and developed tomorrow's leaders. In addition to empowering individuals, their persistent dedication to excellence in research and education has made a substantial contribution to the country's overall development. The quantity of patent applications filed and the commercialization of awarded patents both behind many industrialized countries, not with standing the substantial advancements achieved by Indian universities and research organizations. With over 750 Universities and close to 40,000 colleges in India, 34 percent of students choose STEM-related disciplines, therefore the concentration of patent applications in just a few of the top 10 universities was concerned. Modern economic growth and development were mostly driven by innovation and technical improvement. In order to better understand the intellectual property landscape of Indian universities and research institutions, the study looked at supply and demand in relation to innovations and ideas. The study aimed to shed light on the current situation of intellectual property generation in the nation's academic and research ecosystem by probing the dynamics of patent filing and innovation trends.

Thomas S. and Ravindra M. (2023) focused the necessity of a privacy bill had been generally acknowledged in India, and many experts and stakeholders had asked for the adoption of a thorough privacy legislation that offered unambiguous principles and protections for people's personal data. Additionally, the necessity of a privacy bill was also widely acknowledged in the US. The essay made the case that a thorough privacy legislation was essential for safeguarding individual privacy rights and fostering confidence in the digital economy. The study emphasized the needed for privacy legislation in India and offered recommendations based on privacy laws in other countries, such as the personal data protection and electronic documents acted of Canada and the "general data protection regulation, also known as the GDPR", of the European union. The studied offered some ideas that might serve as a roadmap for Indian officials as they worked to develop and passed a privacy law. These suggestions were based on best practices that had been used throughout the globe.

Mallikarjun G. and Irfan B. (2022) asserted data protection and individual privacy were linked and unalienable concepts. Key information belonging to a person or an organization that was not safeguarded and was readily available to the public creates privacy invasion issues. Therefore, it was crucial to protected each person's personal information and stopped it from being made public. A person's or any organization's information could have been legally secured through data protection in the online and virtual communication environment. By enacting the information technology acted of 2000 and a later revision, India formally recognized the needed for data privacy protection. The information technology acted of 2000 and the information technology (reasonable security practices and procedures and personal data that was sensitive or information) laws of 2011 did not adequately addressed data protection issues in India. On December 11, the personal data protection bill 2019

was presented in the lok sabha and had since been passed. An individual's privacy was always at danger in the present digital world because to the numerous e-surveillance tactics, digital communication interceptions, and the collection of personal data in various formats and at various stages by several authorities. As a result, the author made an effort to draw attention to concerns liked surveillance, censorship, and the interception of digital communications in the article and how they influence the right to privacy, as well as how much the present bill would safeguard personal data and uphold individual privacy.

Chowdhury G. (2021) stated in the modern day, technological advancement and the dynamism of the legal system offered a viewpoint on issues with data security and privacy. Privacy was a concept that doesn't conflict with the interests of other individuals. Because of technological advancement, everyone now prioritized privacy and placed a strong premium on information security. People's freedom was emphasized by data protection, and the freedom was challenged by outside intrusion. By every means necessary, the interaction of the stranger with the person must been stopped. The constitution could have been used to establish any new phenomena as a basic legal needed. The study aimed to sparked a serious debate on data security and the right to privacy from an Indian perspective. Despite not being explicitly stated in the constitution, the right to privacy was implied as a fundamental human freedom under article 21. Data protection and the right to privacy were inherently at odds. Data protection may have covered sensitive information, business proposals, health information, and financial facts. The information technology (amendment) acted of 2008 did not fully addressed data protection and privacy. The IT acted was insufficient for data protection; hence separate legislation was required in this area.

Kira B., et al., (2021) asserted data processing and collecting was the backbone of quickly expanding business planned, supporting the operations of technology businesses and serving as a source of competitive advantage. Due to the critical role that data played in the fiercely competitive environment of digital ecosystems, there had been much discussion on the actual linkages that exist between competition law and data protection law, which had brought these two legal disciplines closer together. Researcher compare the legal restrictions imposed by the competition policy and data protection legislation after outlining the particular ways in which data grew and drove digital ecosystems and analyzing the consequences of digital privacy (or the absence of it) on consumer welfare. Then, researcher map the interfaces between these two branches of law and critically assess the locations where they substantively overlap. Researcher demonstrate that although these two frameworks were often in sync, applying competition and data protection laws individually could occasionally result in the opposite effects. Researcher argued that in ordered to promote beneficial synergies and resolve any conflicts, these two legal tools should have been seen as overlapping regions of a regulatory continuum. Researcher demonstrate that there was a sizable opportunity for institutions and competition policy players to meaningfully integrate data privacy concerns into their decision-making practiced, and that this integration may strengthen and informed the implementation of competition legislation. Researcher suggested an integrated strategy to safeguard consumers and the competitive process, foster innovation, and more effectively managed digital platform ecosystems.

Rai N. (2020) examined the development of technology had been extremely beneficial to humans. But as technology advances, many of our freedoms were now under danger. As the digital era developed and contained data that was routinely collected and sold in the new economy, there was rising worry over the right to privacy. Technology advancement had led to the emergence of additional criminal behaviors including identity theft, prank phoning, online victimization, etc. When people provided their personal information to websites liked social media, marketing companies, communication surveillance companies, government stakeholders, and others, it was usually vulnerable to exploitation. The collection, preservation, monitoring, intercepting, obtaining, analysis, used, retention, etc. of data was not specifically regulated by law in India. The current study looked at how data analysis and the right to privacy interact in contemporary society. Users' personal information was routinely misused by marketing companies, communication surveillance companies, government and private interests, and other websites. The collection, storage, monitoring, interception, acquisition, analysis, used, and retention of data, among other activities, were not specifically governed by law in India. In the study, researcher tried to looked into the current issues with data analysis and privacy rights. The applicability of the laws to each of these sectors had been compared and contrasted because data collection occurs equally in the public and private sectors. Under the supervision of former supreme court justice b. N. Sri Krishna, experts appointed by the ministry of technology and electronics were now drafting a data protection law. The personal data protection bill, 2018, was a drafting bill that was made. But because it couldn't have been submitted, the personal data protection bill 2019 was introduced to the lok sabha on December 11. The goal of the current study was to examine the bill and determine how far the rights to privacy and data protection may been advanced. Additionally, the draught bills of 2018 and 2019 had been contrasted. Thus, the study's overall goal was to analyses the gaps in India's data protection laws as well as what adjustments may been made to ensured that both current and future regulations were implemented correctly.

Mohsin K. (2020) affirmed there were always indications of digital activity. Researcher released personal information into cyberspace each time you entered a website, submit contact, financial, or debit or credit card information, register for an account, sent an email, filled out an online form, post on social media, or put files in cloud storage. There were several sources for cyberattacks, all of which attempted to obtain or utilize personally identifiable information (PI). There was a needed for stronger internal and regulatory defenses as incursions got more complicated. With more and more individuals gone online, there was a feeling of constant monitoring or a fear of losing privacy. Privacy and surveillance provided people the power to decided what data was available and gathered.

Chatterjee S., et al., (2018) examined the entire world worked to provided its citizens with modern infrastructure and cutting-edge services. In ordered to establish smart cities or turn existing cities or major cities into smart cities, efforts were being done all over the world. The majority of nations strive to offered top-notch amenities to their residents, and India was also making preparations to saw the success of its smart city initiative. To accomplish this aimed, government agencies, businesses, and individuals were all attempting to collaborate. The top leveled of the Indian government's urban development ministry had recommended the creation of 100 "smart cities" around the country, where inhabitants might have had access to all current amenities, including any services that could been enabled by IT. The realization of India's aspirations for a "smart city" and the delivery of the finest IT-enabled services with the best reliability and performance depend on a variety of factors that must all been taken into consideration. The leveled of internal information technology expertise to created and maintained information technology-enabled services in the recommended smart city environments, as well as the participation of the public to use the services made possible by IT in a focus on the subject of security and privacy, had been the main topics of the paper. In comparison to studied on security and privacy concerns connected to information technology-enabled services, there was a dearth of researched on system security and privacy rules for the projected Indian smart cities, taking into consideration internal IT workers and future citizens of these proposed smart cities. The studied would contribute to our understanding of how potential residents' desire to used IT-enabled services in India's proposed smart cities was influenced by the system security and privacy policy.

3. Objectives of the Study

- To assess the level of awareness among Indian citizens regarding their right to privacy.
- To examine how misalignment between digital platforms and government policies in India and the constitutional provisions related to the right to privacy.

4. Hypotheses of the Study

Hypothesis 1: There is sig association between the levels of awareness among Indian citizens regarding their right to privacy.

Table-1 Descriptive Statistics

	Mean	Std. Deviation	N
Indian citizens awareness	32.5247	3.03850	223
Right to privacy	29.69	3.133	223

The above table 1 defines the descriptive statistics of the Indian citizens' awarenessand Right to privacy. The mean score and std. deviation of Indian citizen's awareness is 32.5247, 3.03850 and of Right to privacy is 29.69, 3.133.

Table-2 Correlations

		Indian citizens' awareness	Right to privacy
Indian citizens' awareness	Pearson Correlation	1	.142*
	Sig. (2-tailed)		.035
	N	223	223
Right to privacy	Pearson Correlation	.142*	1
	Sig. (2-tailed)	.035	
	N	223	223

*. Correlation is significant at the 0.05 level (2-tailed).

The above table 2 defines the correlation between "Indian citizens' awareness" and "Right to privacy". "There is statistically significant relationship between Indian citizens' awareness and Right to privacy because the sig value is 0.035 (i.e., sig value is less than 0.05)."

Hypothesis 2: Digital platforms and government policies in India exhibit an insignificant alignment with the constitutional provisions related to the right to privacy.

Table- 3 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.134	.018	.005	3.978	.018	1.350	3	220	.259

Predictors: (Constant), Constitutional Provisions, Public Awareness, Data Security

Above table "defines the model summary, indicating a significant degree of connection." The "R-value for the simple correlation is 0.134," indicating a weak positive correlation "which reflects how much of the overall variance in the dependent variable," the impact of Constitutional Provisions, Public Awareness, Data Security on Digital platforms and government policies. "The independent variable can be used to explain the results."

Table-4 ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	64.086	3	21.362	1.350	.259
	Residual	3481.467	220	15.825		
	Total	3545.554	223			

a. Dependent Variable: Digital platforms and government policies

b. Predictors: (Constant), Constitutional Provisions, Public Awareness, Data Security

The above table is an "ANOVA table that shows how well the data fits by the regression equation (i.e., predicts the dependent variable)."“This table demonstrates the reliability of the regression model's predictions for the dependent variable."“The above table 10 shows a negative significant impact of Digital platforms and government policies," as "the significance value is 0.259, which is greater than 0.05."

Table- 5 Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	24.433	2.907		8.406	.000
	Data Security	.018	.072	.017	.252	.801
	Public Awareness	-.112	.066	-.112	-1.681	.094
	Constitutional Provisions	.068	.071	.065	.965	.335

a. Dependent Variable: Digital platforms and government policies

Table 5 of "the Coefficients in the model demonstrates how data security," public awareness and constitutional provisions have impacted digital platforms and government policies. "The table highlight that the regression model shows an insignificant value of 0.259 (the significance value is less than 0.05)."

5. Conclusion

In the digital age, where personal data has become the currency of the virtual world, the right to privacy is more pertinent than ever. This research paper embarked on a comprehensive journey to scrutinize the status of the right to privacy under the Indian Constitution and assess its alignment with the evolving landscape of digital personal data. The initial objective of this study was to gauge the awareness levels among Indian citizens concerning their right to privacy. The findings, as indicated by the descriptive statistics and correlation analysis, underscored the significance of this endeavor. The study found a statistically significant relationship between Indian citizens' awareness and their right to privacy. This implies that an informed citizenry is more likely to assert and protect their privacy rights, thereby emphasizing the importance of educational and awareness campaigns on this crucial subject. The second objective of this study was to evaluate the alignment between digital platforms, government policies in India, and the constitutional provisions related to the right to privacy. The regression analysis, as indicated by the model summary and ANOVA results, revealed that the alignment between these elements remained insignificant. The coefficients further elucidated this lack of substantial impact, signifying that data security, public awareness, and constitutional provisions had limited influence on digital platforms and government policies in the context of privacy protection. These findings imply that there is still much work to be done in bridging the gap between constitutional ideals and the practical implementation of privacy safeguards in the digital realm. While the right to privacy is enshrined in the Indian Constitution, its

application and enforcement in the digital sphere remain a complex challenge. This research holds several implications for policymakers, legal scholars, and advocates of privacy rights. It underscores the necessity for more robust legal frameworks and policy measures to protect privacy in the digital age. Additionally, it highlights the need for educational initiatives to enhance public awareness and empower citizens to exercise their privacy rights effectively. Future research in this domain should delve deeper into the factors that hinder the alignment of digital platforms and government policies with constitutional provisions related to privacy. Furthermore, a comparative analysis of privacy laws and practices in different countries could offer valuable insights into best practices and potential improvements. In conclusion, the right to privacy in the digital era is a complex and evolving challenge that demands continuous attention and concerted efforts from all stakeholders. As technology advances and personal data becomes more integral to our lives, safeguarding privacy remains an essential aspect of preserving individual liberties and upholding democratic values in the digital age.

References:

i. Behera, N. (2021). *Legal Protection of Right to Privacy in Cyberspace* (Doctoral dissertation, National Law School of Indian University, Bengaluru).

ii. Bisht, A. K., & Sreenivasulu, N. S. (2022). Clause 35 of the Personal Data Protection Bill, 2019: Whether a Reasonable Restriction or a Withering Away of Fundamental Right to Information Privacy? *Issue 2 Int'l JL Mgmt. & Human.*, *5*, 1745.

iii. Chatterjee, S., Kar, A. K., & Gupta, M. P. (2018). Alignment of IT authority and citizens of proposed smart cities in India: System security and privacy perspective. *Global Journal of Flexible Systems Management*, *19*, 95-107.

iv. Chinchure, A. D. (2021). Right to Privacy-A Judicial View. *Issue 3 Int'l JL Mgmt. & Human.*, *4*, 5221.

v. Chowdhury, G. R. (2021). Right to Privacy and Data Protection in India. *Issue 4 Int'l JL Mgmt. & Human.*, *4*, 2602.

vi. Corwin, E. S. H. (2008). *Edward S. Corwin's Constitution and What It Means Today: 1978 Edition*. Princeton University Press.

vii. Dewan, Y. (2022). An Analysis of Digital Privacy Laws. *Issue 6 Indian JL & Legal Rsch.*, *4*, 1.

viii. Donnelly, D. L. (2020). *Privacy by (re) design: a comparative study of the protection of personal information in the mobile applications ecosystem under United States, European Union and South African law* (Doctoral dissertation).

ix. Egli, P. (2007). Protocol No. 14 to the European Convention for the Protection of Human Rights and Fundamental Freedoms: Towards a More Effective Control Mechanism. *J. Transnat'l L. & Pol'y*, *17*, 1.

x. Goel, S. (2021). Right to Privacy: A Critical Analysis. *Issue 3 Int'l JL Mgmt. & Human.*, *4*, 2117.

xi. Goyal, G., & Kumar, R. (2016). The Right to Privacy in India: Concept and Evolution. Partridge Publishing.

xii. Griswold, V. (1965). Connecticut, 381 US 479, 85 S. *Ct*, *1678*, 14.

xiii. Handler, P. (1964). Resource Letter Scr-1 on Semiconductors. *American Journal of Physics*, *32*(5), 329-333.

xiv. Hildebrandt, M., O'Hara, K., & Waidner, M. (Eds.). (2013). *Digital enlightenment yearbook 2013: The value of personal data*. IOS Press.

xv. Khan, S., Sharma, S. K., & Laha, A. K. (2023). From Misalignment to Synergy: Analysis of Patents from Indian Universities & Research Institutions. *arXiv preprint arXiv:2304.12176*.

xvi. Khare, K., & Mishra, D. (2016). Contextualising the Right to Be Forgotten in the Indian Constitution: Juxtaposing Right to Privacy and Right to Free Speech. *CALJ*, *3*, 70.

xvii. Kira, B., Sinha, V., & Srinivasan, S. (2021). Regulating digital ecosystems: bridging the gap between competition policy and data protection. Industrial and Corporate Change, 30(5), 1337-1360.

xviii. Kumar, A. (2019). The Right to Be Forgotten in Digital Age: A Comparative Study of the Indian Personal Data Protection Bill, 2018 & the GDPR. *Shimla Law Review*, *2*.

xix. Mallikarjun, G., & Irfan, B. M. (2022). Right to Privacy in India: The Technical and Legal Framework. Journal of Positive School Psychology, 6(3), 5785-5790.

xx. Michael, D., & Charles, S. (1998). A Constitution of Democratic Experimentalism. *Cornell Law Review*, *98*(2), 267-473.

xxi. Mohsin, K. (2020). Right to Privacy in Digital Era. Available at SSRN 3678224.

xxii. Rai, N. (2020). Right to Privacy and Data Protection in the Digital Age-Preservation, Control and Implementation of Laws in India. Indian JL & Just., 11, 115.

xxiii. Rajagopal, R. (1994). *Evaluation of the reciprocating plate column for treating petroleum waste waters* (Doctoral dissertation, Oklahoma State University).

xxiv. Singh, S., & Bose, M. M. (2021). Right to Privacy: An Indian for its Inherent Right. *Journal of Human Rights Law and Practice*, *4*(1), 13-17.

xxv. Thomas, S. V., & Ravindra, M. (2023). Right to Privacy in the Digital Era. *Issue 1 Indian JL & Legal Rsch.*, *5*, 1.