

AN ANALYSIS OF THE LAWS CONCERNING DIGITAL PRIVACY

ANIL KUMAR¹, PROF. AASHISH A GADGIL², DR. NAMITA SRIVASTAVA³, DR. PRAKASH CHANDRA SWAIN⁴, SHEKHAR KUMAR SAHU⁵

¹Assistant Professor, School of Management,
Graphic Era Hill University Haldwani, Uttarakhand

²Assistant Professor Department of E&C,
KLS Gogte Institute of Technology, Belagavi, Karnataka

³Associate Professor, Department of Management,
Institute of Cooperative and Corporate Management Research and Training, Lucknow. U.P.

⁴School of Management, Assistant Professor, B.Com Coordinator,
Centurion University of Technology and Management,
BBSR Campus, Bhubaneswar, Odisha.

⁵Research Scholar, Department of Commerce,
M.B. Govt. P.G College Haldwani, Nainital, Uttarakhand

Abstract: Both data protection and privacy are crucial components of internet governance. The Data Protection Act is a piece of legislation designed to safeguard individuals' privacy rights. One definition of privacy is the individual's right to manage and disseminate his or her own private information and data in accordance with his or her own goals and values. Numerous judicial decisions in India have elevated the right to privacy to the status of a fundamental right, and statutes have further codified the right as a legal one. The term "internet privacy" can refer to a wide range of issues and debates. The term can refer to both the rights an individual has to control their personal information and the infringements on those rights that occur when that information is transmitted over the Internet. The ever-changing nature of the internet has resulted in a never-ending slew of new privacy-related concerns and problems. Privacy protection in the digital sphere is crucial in the modern world because of the importance of safeguarding our personal information, financial data, sensitive information, online activity, and fundamental rights. To continue reaping the benefits of technological advancements without jeopardising our safety or giving up control of our personal information, it is crucial for individuals, businesses, and governments to take action to protect digital privacy. "The Personal Data Protection Bill, 2019 was introduced in the Lok Sabha on December 11, 2019, by Minister of Electronics and Information Technology Ravi Kumar". In India, this occurred. The bill's stated goals include, first and foremost, the protection of personally identifiable information, and secondly, the creation of a Data Protection Authority to oversee that protection. This study aims to to examine views of Indian citizens regarding laws concerning digital privacy. For the sake of justification, total 240 respondents has taken through questionnaire by applying 5 point likert scale.

Keywords: Digital Privacy, Laws, ITA, Digitalisation

Table of Contents

1. Introduction
2. Review Literature
3. Research Methodology
4. Research gap
5. Objective of the Study
6. Importance of digital privacy
7. The Unclear Boundaries of the Public and Private Spheres
8. The Currently Adopted Guidelines for Protecting Users' Privacy Online in India
9. Results & Discussion
10. Conclusion

1. Introduction

People all over the world are becoming increasingly concerned about their personal privacy in this modern digital era. The proliferation of social media and other digital platforms has led to an

unprecedented level of data collection and dissemination, which in turn has led to an increase in the frequency of concerns regarding the privacy of users' data. The government of India has passed a number of laws that are intended to safeguard the digital privacy of its citizens. In this essay, we will investigate the Indian laws that pertain to the privacy of digital information.

The "Information Technology (IT) Act, 2000" is the key piece of legislation in India when it comes to protecting individuals' privacy online. This act provides legal recognition for transactions that are carried out through electronic means and lays down rules for the collection, storage, and transmission of data. In addition, it provides legal recognition for transactions that are carried out through electronic means. In addition to this, it outlines provisions for the protection of personal information as well as punishments for those who misuse this information.

"Section 43A of the Information Technology Act", which was passed in 2000, includes provisions for personal data protection or information. This includes data pertaining to passwords, information regarding financial transactions, and biometric data. It is required of businesses that collect and store such information to maintain reasonable security practises in order to prevent the inappropriate use of the information. Should you fail to comply, you may face significant fines in addition to possible jail time.

The "Personal Data Protection Bill, 2019", which seeks to provide a comprehensive framework for the collection, storage, and processing of personal data, was also introduced by the Indian government. The bill establishes guidelines for data processors and data controllers, as well as the rights of individuals with regard to their own data, and it is being drafted as we speak. In addition to this, it details provisions for the punishment of individuals who make inappropriate use of personal data.

Along with these laws, the government of India has also issued guidelines for the protection of people's digital privacy. "The Ministry of Electronics and Information Technology" has released a draught policy on data protection, which seeks to regulate personal data. This policy was issued as part of the ministry's efforts to protect individuals' privacy. Individuals are given the right to access their data and have it corrected by the policy, and businesses are required to obtain their customers' explicit consent before collecting any personal information.

A significant contribution to the preservation of digital privacy has also been made by India's highest court, the Supreme Court. The right to one's own privacy was recognised by the "Indian Supreme Court as a fundamental right in the landmark case of Justice K.S. Puttaswamy (Ret.) v. Union of India". The court also provided guidelines for the protection of personal data, which included the requirement that data controllers obtain the informed consent of individuals before collecting their data.

Even though there are laws and guidelines in place, there are still concerns regarding the protection of digital privacy in India. In spite of the fact that the nation does not yet possess an all-encompassing data protection framework, there have been multiple instances of data breaches and leaks. In addition to this, the government has been criticised for the methods it uses to conduct surveillance, such as the collection of call records and the use of facial recognition technology.

2. Review Literature

Websites often use small text files called "cookies" to remember their visitors' preferences and other information and save it to the user's hard drive. [1] provides a historical overview, focusing on "cookies," of the evolution of various technologies used to monitor online user behaviour from the 1990s to the present day. Estee also discusses the evolution of these technologies and related methods for concealing the identity of the user. The article stresses the significance of educating and informing young people and students about this technology.

When discussing methods to safeguard personal information, [27] introduce the idea of "trusted computing." The article focuses specifically on the prevalence of video surveillance in public areas. In the context of this discussion, it's worth noting that video surveillance and digital environment surveillance are increasingly merging, and the line between them is becoming increasingly blurry.

Concerning how to deal with potentially sensitive information gleaned from video surveillance is the focus of the study by [2]. The projects highlighted in the article include Mobile Privacy Protection and Digital Diorama, both of which work to protect individuals' right to personal privacy. Another concept that emerges from this setting is the concept of "Privacy by Design," which describes the method by which privacy protection measures are built in at the start of the biometric design process [4]. The

authors argue that privacy concerns shouldn't be dealt with as an afterthought when creating new technologies and business models, but rather should be factored in from the get-go. Additionally, [5] discusses the individual's right to privacy in light of police investigations. In doing so, however, he focuses more on "forward looking" and "backward looking" surveillance techniques. Forward-looking surveillance, in this context, describes the type of monitoring that takes place after a judge issues a warrant for it. Phone tapping and GPS tracking are two examples of the kinds of monitoring that fall under this category. Some evidence of criminal intent is required to issue such a licence. The categories of information that can be collected and the uses for that data are also outlined in the permission. The article brings up the issue of retrospective monitoring and explains why "with backward-looking surveillance, all of these protections are gone." Just by asking a company for the appropriate records, law enforcement or intelligence agencies can learn a great deal about our whereabouts, phone calls, and reading habits.

Another recurring theme in the articles that focus on the law is the importance of the right to know [8] [19] [22] [23] [25]. This problem stems from the ambiguity surrounding who owns what data created by internet users, who has the right to use that data, and what can be done with that data. The problem is described as follows by [22]: Due to increasing number of locations where data is collected, "data barons" now have control over digital information that users are unable to modify themselves. [23] talks about the growth of the so-called "Internet of Things," as well as the possible problems that may arise with the storage and use of data in this setting. The term "Internet of Things" that are embedded in consumer goods to monitor and store information about routines as varied as physical activity, dietary intake, and sleep duration. The term "Internet of Things" has become popular to describe these gadgets. In this light, the author asks, "How to protect privacy in a world where the Internet of Things generates ever more massive and nuanced datasets about consumer behaviour?" When faced with the reality that sensors are particularly vulnerable to a wide variety of security threats, what action should be taken? How should the law handle consumer consent, and to what extent should policy depend on consumer consent, when consumers may not be able to make truly informed decisions? It's been shown that [23].

[3] investigate the impact of external threats on public opinion regarding surveillance. Contrary to the claims made by [26] and [3], they argue that the assumption of threat does not always influence attitudes surrounding surveillance (2005). There is a degree of disagreement between this view and that of [26] and [3].

[20] make this case, but they don't back it up with data. Instead, they discuss this from a more theoretical perspective, while also reviewing more practical considerations that need to be made to increase citizens' voluntary use of digital services for sharing sensitive information online and bolster trust between the state and its citizens. When [20]. [21] claims that many people are willing to give the government private information if doing so will result in better public services. [Insert citation here] In order for the exchange of data on citizens and societal functions to run smoothly, there must be greater transparency regarding the information that is gathered about citizens and the functions of society. The authors of the study,[10], look at the early days of the Internet and the debate in the Swedish Parliament, specifically how the issue of an individual's right to privacy was framed in relation to the need for surveillance. The authors zero in on the discussion of monitoring as a central theme in this context. They argue that those who opposed increased surveillance were in the minority compared to the generally accepted view that more data collection on citizens is necessary.

Using the Panopticon as an analogy, a number of other articles discuss the numerous ways in which powerful actors can keep tabs on the activities of ordinary people by means of cutting-edge digital surveillance systems [6] [7] [8] [9] [18] [17] [24]. This critique of digital society is based on the claim that it is now feasible to conduct extensive surveillance of all citizens. In addition, it explains how anyone can use digital structures to their advantage, giving them more sway than traditional authorities. [31] examined that online social networks' mediated communications can conflict with users' privacy expectations (OSNs). Computer scientists classify the "OSN privacy problem" as surveillance, institutional, or social. They tried to solve each problem as if it were new. Because privacy issues in OSNs are interconnected, we propose a more holistic approach to research. This article begins with a surveillance and social privacy overview. These viewpoints focus on narratives, assumptions, goals, and methods. We then contrast and compare the two approaches to see how they complement each other and identify integration challenges and open research questions.

3. Research Methodology

This study aims to investigate the laws concerning digital privacy in India. Although many studies has already been published on this concept but in Indian context , the broad vision is missing. This study is primarily based on secondary data, where information has captured from various government websites, bills, blogs, published research articles & other available materials. For the sake of naturality in research, total 240 respondents has taken from Delhi-NCR. Respondents belonging students, professionals, businessman & others. With the help of structured questionnaire with a likert scale 5 , asked related questions about digital privacy laws concerns. The research is descriptive in nature.

4. Research gap

To identify the gap, many review studies has been incorporated which highlights laws governing regarding digital privacy. But, all studies has taken on the basis of secondary data. This study is also concerned about primary data which has been collected from citizens of India to ask their opinion in lieu of the laws framed by Indian government to protect digital frauds & privacy.

5. Objective of the Study

- To examine views of Indian citizens regarding laws concerning digital privacy.
- To justify the conclusion of the study.

6. Importance of digital privacy

Because of advances in technology and an explosion in the amount of data stored digitally, protecting one's privacy online has become an increasingly pressing concern in recent years. Because more aspects of our lives are moving online, we are disclosing an increasing amount of personal information to digital platforms and businesses.

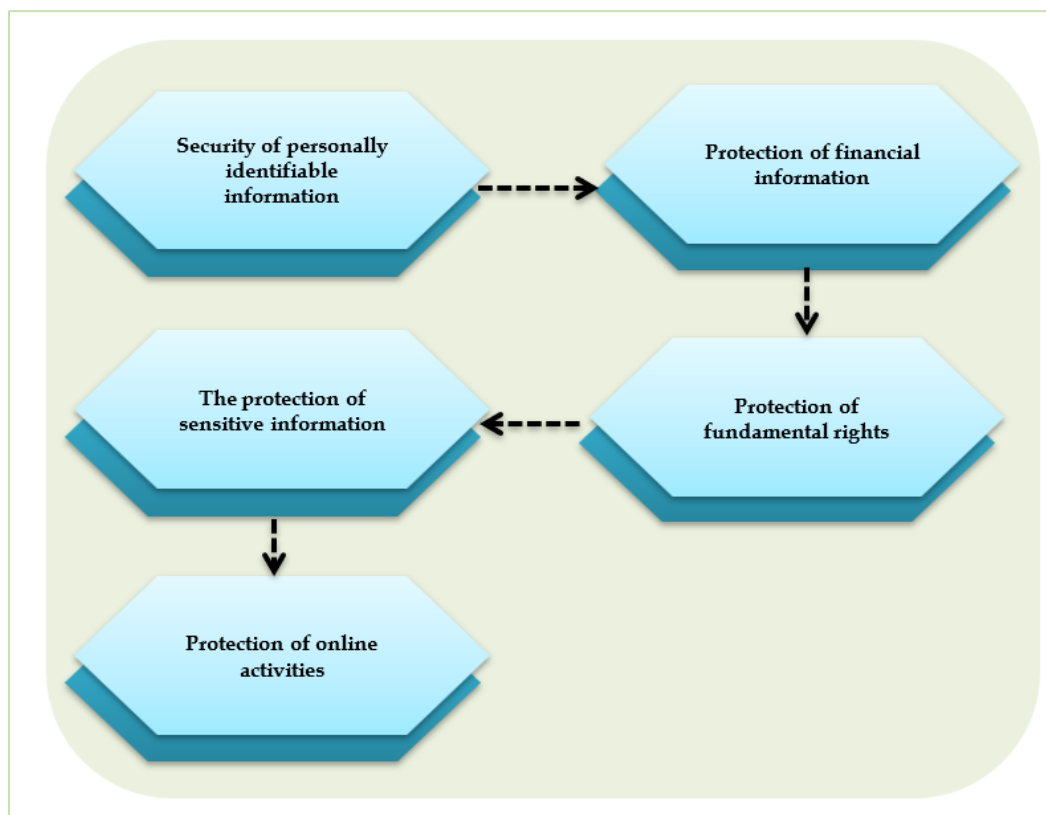


Figure 1 : Importance of Digital Privacy

These platforms and businesses are then more susceptible to data breaches and improper use of the information. In today's world, maintaining one's privacy online is critically important for a variety of reasons, including the following:



Security of personally identifiable information: The protection of our personal information from unauthorised access or use by third parties is one of the primary reasons why digital privacy is so essential. It is possible for someone to commit identity theft or fraud using our personal information, such as our name, address, phone number, and email address. This information can also be used to stalk or harass us.

Protection of financial information: We also store our financial information online, including details about our bank accounts and credit cards. These details, which can be exploited by hackers or cybercriminals if our digital privacy is not protected, include our bank account information and credit card information.

The protection of sensitive information: Sensitive personal information, such as our medical history, sexual orientation, religious beliefs, or political affiliations, can be exploited for inappropriate purposes if it is obtained by the wrong parties. The confidentiality of this information must be maintained at all costs if we are to avoid being persecuted, harassed, or discriminated against on the basis of the personal beliefs that we hold.

Protection of online activities: Having control over our digital privacy is essential if we want to prevent our online activities from being watched or recorded by third parties. Numerous businesses and government agencies now keep tabs on their customers' activities online in order to learn more about their preferences, routines, and behaviours, as well as to better target them with advertising or surveillance.

Protection of fundamental rights: Finally, protecting our right to freedom of speech, assembly, and association requires that we maintain our digital privacy. This is the final reason why protecting our digital privacy is important. It is possible that we will be less likely to freely express ourselves if our online activity is monitored and censored. This can have a negative impact on both our society and our democracy.

7. The Unclear Boundaries of the Public and Private Spheres

The previous example also shows how unclear the "sphere" of information on the internet is, i.e. whether information posted on social media is public information that can be used by anyone, including law enforcement, employees, data mining companies, etc., or whether information posted on social media is private information that can only be used with the user's permission. As an example, in 2013, the Mumbai police department in India set up a "social media lab" to track the actions of social media users. [28] Due to the project's claim that it only analyses publicly available information, the lab does not need permission to monitor individuals and their behaviour, nor do individuals receive any notice that this is occurring. Similar issues have been addressed by the governments of other countries. For instance, in the United States, some people have fought back against the unauthorised use of their tweets[29,] while U.S. courts have ruled that law enforcement can obtain tweets (both private and public) with just a subpoena. This is because, in a technical sense, the information has been made public after being shared with another party. [30] An Indian court has not yet definitively addressed the question of whether the content of social media platforms is public or private information.

8. The Currently Adopted Guidelines for Protecting Users' Privacy Online in India

Most of India's current legal protections for internet privacy can be found in the "Information Technology Act (ITA)" of 2000. There are a number of provisions in the "Information Technology Act" that, depending on the specifics, can either strengthen or weaken safeguards for users' online privacy. Several provisions clearly protect users' privacy, including those that criminalise child pornography[11], punish hacking and fraud[12], and define data protection standards for body corporate. Among the provisions that serve to lessen the user's level of privacy is [13] the ability of law enforcement to access the user's personally identifiable information stored by a body corporate. Online communication monitoring, interception, and decryption in real time; [14] data collection and analysis pertaining to internet traffic; [15] data collection and analysis pertaining to online activity.

[16] In addition, the ITA's legal framework contains loopholes that make it harder for internet users to protect their privacy. For a few examples, the Information Technology Act doesn't cover the legal status of social media content in India, the merging and sharing of data across databases, whether or not people can send pictures of their "private areas" over the internet, whether or not users have the right to be told when cookies and "do not track" options are being used, whether or not electronic personal identifiers can be used across databases, and whether or not users have the right to be told when cookies and "do not track" options are being used. Furthermore, the ITA does not specify if people have the right.



9. Results & Discussion

Table -1 Reasons to Frame Laws Concerning Digital privacy

S.No.	Reason	Rank Scoring	F	%
1	Ensuring Human Dignity	#Rank=5	24	10%
2	Safety	#Rank=1	56	23.33%
3	Self-Determination of Digital Transactions	#Rank=7	19	7.91%
4	Beware Tracking, Hacking and Trading	#Rank=3	32	13.33%
5	Easy to Access Without Stressing of Privacy Hamper	#Rank=8	17	7.08%
6	Low Risk with Laws	#Rank=6	21	8.75%
7	Motivation to do Digital Transactions	#Rank=2	37	15.41%
8	High Savings due to limited Transfer Limits	#Rank=9	09	3.75%
9	Self- Protection & Others	#Rank=4	25	10.41%

Table - 2 Mean Values Towards Perception Related to Laws Concerning Digital Privacy

Statement	(HS)	(S)	(N)	(DS)	(HD)	Mean
Do laws ensures human dignity?	88	59	48	20	25	3.59
Is there any safety associated with digital laws?	87	54	46	35	18	3.87
Is there any self-determination of digital transactions?	67	84	51	23	15	3.22
Are people really becoming cautious about tracking, hacking and Trading due to digital laws?	72	69	46	25	28	3.81
Do you feel people feeling Easiness to access online payment methods without stressing of privacy hamper?	82	67	53	12	26	2.98
Are you sure risk become low in digital transactions after implementing digital laws ?	79	68	46	13	34	3.38
Do you feel citizens have become now more motivated towards digital utilization after digital laws?	83	59	39	38	21	3.25
Are you sure it's a best way to limit expenditures and increase savings?	76	66	42	32	24	2.27

Above table 2 analysed that people are more concern about the statement “Is there any safety associated with digital laws” & having highest mean value i.e. ($M=3.87$) whereas the people are least bothered about the statement “ Are you sure it's a best way to limit expenditures and increase savings” which has least mean value i.e., ($M=2.27$). But overall, people are comparatively safe in making online transactions after implementing digital laws. But still, the laws must be improvised so that the scams and frauds can




be minimized. In this table highly satisfied as 'HS'; satisfies as 'S', neutral as 'N', dissatisfied as 'DS' & highly dissatisfied as 'HD'.

10. Conclusion

In summing up, the laws in India concerning digital privacy have come a long way in the recent years. A framework for the protection of individuals' personal data has been established thanks to the passage of the Information Technology Act in 2000, the Personal Data Protection Bill in 2019, and other guidelines. However, a significant amount of work remains to be done in order to put these laws into effect and guarantee that the citizens' right to privacy is respected. The government of India must keep working towards the goal of developing a comprehensive data protection framework that strikes a balance between the competing demands of the need for innovation and the need to protect the privacy of its citizens. In India, online privacy is a rapidly expanding field with significant social implications. India must ensure the privacy of its citizens as well as the privacy of foreigners whose data is stored in India, whether for a short period of time or permanently. This is because both private companies and the government are collecting more data on Internet users, and the government is constantly looking for new ways to monitor the public. The first step towards realising this objective is the adoption of comprehensive privacy legislation that recognises the inherent right to personal secrecy. The government is moving in the right direction by considering a draught privacy bill and publishing the Report of the Group of Experts on Privacy.

References

- [1] Beck, E. N. (2015). *The Invisible Digital Identity: Assemblages in Digital Networks*. *Computers and Composition*, 35, 125-140. <http://doi.org/10.1016/j.compcom.2015.01.005>
- [2] Cavoukian guchi, N., & Nakashima, Y. (2015). *Protection and Utilization of Privacy Information via Sensing*. *IEICE Transactions on Information and Systems*, E98.D(1), 2-9. <http://doi.org/10.1587/transinf.2014MUI0001>
- [3] Cohrs, J. C., Kielmann, S., Maes, J., & Moschner, B. (2005). *Effects of Right-Wing Authoritarianism and Threat from Terrorism on Restriction of Civil Liberties*. *Analyses of Social Issues and Public Policy*, 5(1), 263-276. <http://doi.org/10.1111/j.1530-2415.2005.00071.x>
- [4] Cavoukian, A., Chibba, M., & Stoianov, A. (2012). *Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment*. *Review of Policy Research*, 29(1), 37-61. <http://doi.org/10.1111/j.1541-1338.2011.00537.x>
- [5] Desai, D. R. (2014). *Constitutional Limits on Surveillance: Associational Freedom in The Age of Data Hoarding*. *Notre Dame Law Review*, 90(2), 579-632.
- [6] Farinosi, M. (2011). *Deconstructing Bentham's Panopticon: The new metaphors of surveillance in the web 2.0 environment*. *TripleC*, 9(1), 62-76. Retrieved from <http://www.scopus.com/inward/record.url?eid=2-s2.0-84864790124&partnerID=tZ0tx3y1>
- [7] Ganascia, J.-G. (2010). *The generalized sousveillance society*. *Social Science Information*, 49(3), 489-507. <http://doi.org/10.1177/0539018410371027>
- [8] Grodzinsky, F. S., & Tavani, H. T. (2005). *P2P Networks and the Verizon v. RIAA Case: Implications for Personal Privacy and Intellectual Property*. *Ethics and Information Technology*, 7(4), 243-250. <http://doi.org/10.1007/s10676-006-0012-4>
- [9] Humphreys, S. (2013). *Predicting, securing and shaping the future: Mechanisms of governance in online social environments*. *International Journal of Media & Cultural Politics*, 9(3), 247-258. http://doi.org/10.1386/macp.9.3.247_1
- [10] Haikola, S., & Jonsson, S. (2007). *State surveillance on the internet - The Swedish debate and the future role of libraries and LIS*. *LIBRI*, 57(4), 209-218. <http://doi.org/10.1515/LIBR.2007.209>
- [11] ITA section 67
- [12] ITA section 43, 66, and 66F
- [13] *Information Technology (Reasonable security practices and procedures and Sensitive personal data or information) Rules*, 2011.
- [14] *Information Technology (Reasonable security practices and procedures and Sensitive personal data or information) Rules*, 2011. section 6(1)
- [15] *Information Technology (Procedure and Safeguards for monitoring and collection of Traffic Data or other information) Rules* 2009

- 
- [16] *Information Technology (Procedure and Safeguards for intercepting, monitoring, and decryption) Rules 2009*
- [17] Jiang, M., & Okamoto, K. (2014). *National Identity, Ideological Apparatus, or Panopticon? A Case Study of the Chinese National Search Engine Jike*. *Policy & Internet*, 6(1), 89-107. <http://doi.org/10.1002/1944-2866.POI353>
- [18] Kandias, M., Mitrou, L., Stavrou, V., & Gritzalis, D. (2014). *E-Business and Telecommunications*. (M. S. Obaidat & J. Filipe, Eds.) *Communications in Computer and Information Science* (Vol. 456). Berlin, Heidelberg: Springer Berlin Heidelberg. <http://doi.org/10.1007/978-3-662-44788-8>
- [19] Konstadinides, T. (2011). *Destroying democracy on the ground of defending It? the Data Retention Directive, the surveillance state and our constitutional ecosystem*. *European Law Review*, 36(5), 722-736. Retrieved from <http://www.scopus.com/inward/record.url?eid=2-s2.0-84868150276&partnerID=tZOtx3y1>
- [20] Keymolen, E., Prins, C., & Raab, C. (2012). *Trust and ICT: New challenges for public administration*. *Innovation and the Public Sector*, 19, 21-35. <http://doi.org/10.3233/978-1-61499-137-3-21>
- [21] Lips, M. (2010). *Rethinking citizen-government relationships in the age of digital identity: Insights from research*. *Information Polity*, 15(4), 273-289. <http://doi.org/10.3233/IP-2010-0216>
- [22] Mantelero, A. (2014). *The future of consumer data protection in the EU Re-thinking the ``notice and consent`` paradigm in the new era of predictive analytics*. *Computer Law & Security Review*, 30(6), 643-660. <http://doi.org/10.1016/j.clsr.2014.09.004>
- [23] Peppet, S. R. (2014). *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*. *Texas Law Review*, 93(1), 85-178.
- [24] Russett, P. C. (2011). *A Contemporary Portrait of Information Privacy: Collective Communicative Consequences of Being Digital*. *Review of Communication*, 11(1), 39-50. <http://doi.org/10.1080/15358593.2010.504882>
- [25] Roberts, A. (2015). *Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications*. *Modern Law Review*, 78(3), 535-548. <http://doi.org/10.1111/1468-2230.12127>
- [26] Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). *Public opinion on National Security Agency surveillance programs: A multi-method approach*. *Government Information Quarterly*, 32(2), 129-141. <http://doi.org/10.1016/j.giq.2015.01.003>
- [27] Winkler, T., & Rinner, B. (2011). *Securing Embedded Smart Cameras with Trusted Computing*. *Eurasip Journal on Wireless Communications and Networking*. <http://doi.org/10.1155/2011/530354>
- [28] <http://www.zdnet.com/in/india-sets-up-social-media-monitoring-lab-7000012758/>
- [29] <http://www.techdirt.com/articles/20130203/18510621869/investigative-journalist-claims-her-public-tweets-arent-publishable-threatens-to-sue-blogger-who-does-exactly-that.shtml>
- [30] <http://www.npr.org/blogs/alltechconsidered/2013/10/02/228134269/your-digital-trail-does-the-fourth-amendment-protect-us>
- [31] Upadhyay, a. (2014). *privacy for online social networks- a conceptual study*. *Kaav International Journal of Science, Engineering & Technology*, 1(4), 75-88. <https://www.kaavpublications.org/abstracts/privacy-for-online-social-networks-a-conceptual-study>
- [32] Mishra, R. P., & Kapse, S. (2017). *Cybercrime: A Hazard to Network Surveillance* (1st ed., pp. 447-451). Kaav Publications.
- [33] Singh, A., & Kumar, A. (2022). *The Legislative and Administrative Framework on Protection of Right to Privacy in Digital India* (1st ed., pp. 1-10). Kaav Publications.