# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

# DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions ofthe authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsever for any consequences for any action taken by anyone on the basis of information in theJournal.

 ISSN: 2582-6433

# EDITORIALTEAM

## EDITORS

### Dr. Samrat Datta

*Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board*

### *Dr. Namita Jain*

*Head & Associate Professor*

*School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.*

*Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019*

 ISSN: 2582-6433

# Mrs.S.Kalpana

Assistant professor of Law

*Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.*

# Avinash Kumar

*Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.*

 ISSN: 2582-6433

# ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

# DATA PRIVACY INFRINGED BY MACHINE LEARNING ALGORITHM DRIVEN PERSONALIZED ADVERTISEMENTS

AUTHORED BY - MOHAMMED SHEHIN S S
LLM Student, Christ (Deemed To Be) University, Bangalore

## ABSTRACT

As technology has drastically changed in the modern era, the usage of the user/consumer has also drastically changed. However, these machine learning algorithms obtain and examine vast amounts of user personal information to provide personalized and targeted content for their profits, which comes at a high cost to the users. Though there are advanced regulations like GDPR and CCPA that protect users' privacy, several inadequacies exist in protecting users' data. This study examines how machine learning, targeted advertising, and data privacy interact, pointing out significant legal gaps and thoroughly investigating ethical, technical, and regulatory issues. These machine-learning algorithms can benefit both the seller and the user. There are many drawbacks to using these methods, which can be bypassed by articulating companies' privacy policies using ML algorithms. The user's consent must be obtained by elaborating on the privacy policy and training the AI on diverse data sets to reduce discrimination and allow the machine learning algorithms and natural language processing to collect only necessary data for providing personalized advertisements. The paper promotes a balanced strategy that preserves user privacy without hindering ad tech innovation by implementing regulatory reforms, privacy-preserving solutions, and international cooperation. The paper emphasizes the necessity of flexible regulatory frameworks, enhanced algorithmic decision-making transparency, and global standards to guarantee that personalized advertising and machine learning developments comply with data protection laws.

**KEYWORDS: Data privacy, consent, targeted advertisements, Jurisdictions, Data misuse**

 ISSN: 2582-6433

## INTRODUCTION

Digital marketing has undergone a fundamental transformation due to targeted advertising, which uses information about users to personalize ads and enhance interaction. This method involves monitoring user activity online, including purchases, social media interactions, and browsing patterns, to present ads customized to the user's tastes. Although the end effect is an enhanced user experience, privacy issues and the degree of personal data collection without express authorization are brought up. Introducing machine learning (ML) to the advertising industry has raised the bar for personalization. Marketing professionals can precisely target specific individuals via machine learning algorithms that process and analyze large databases to forecast user behavior. These systems constantly improve, adjusting their targeting strategies in response to real-time input. As a result, customized advertising is now more effective and valuable for companies. Nevertheless, there are privacy-related issues with this data-centric approach. Data privacy is a significant concern due to the use of massive volumes of personal data to train machine learning algorithms. Users need more control over how their data is used or shared and frequently share it without realizing it across sites. Because ML algorithms are opaque, users cannot understand the extent of the data analysis that takes place, which worsens the problem. This presents moral and legal dilemmas, particularly in areas with inadequate or lacking data protection regulations. Even though machine learning has potential for the advertising sector, many legal gaps still prevent users from being protected. The complexity of machine learning algorithms is too much for the regulatory frameworks that are in place, so new technologies that protect privacy and data protection must be implemented.

## THE CURRENT STATE OF TARGETED ADVERTISING AND MACHINE LEARNING ALGORITHM

Personal information gathered from several sources, such as websites, social media platforms, and mobile apps, is necessary for targeted advertising to function. These strategies include contextual targeting, in which adverts are shown based on the material users are now interacting with, and behavioral targeting, which concentrates on users' previous actions (such as searches, purchases, etc.)[1]. Data-driven advertising is expanding its reach beyond statistics to offer hyper-targeted advertisements that anticipate personal desires. With machine learning at its core, marketers can now adjust personalized marketing in real time. Large datasets are analyzed

[1] Gao, B., Wang, Y., Xie, H., Hu, Y., & Hu, Y. (2023). Artificial Intelligence in Advertising: Advancements, Challenges, and Ethical Considerations in Targeting, Personalization, Content Creation, and Ad Optimization. Sage Open, 13(4).

 ISSN: 2582-6433

by algorithms like collective filtering and deep learning models, which produce prediction models of user behavior. They process data at a rate that is faster than human capacity, enabling effective targeted ad placement. The algorithms get better at predicting the kind of product or content that a user will find interesting as they gain experience, which makes advertisements more relevant and raises the possibility that a user will interact with the ad. For machine learning algorithms to work well, they need a range of personal data. This information may consist of Search terms and websites visited during browsing, previously made purchases, and preferred products; mobile devices are used to track movements in geography and comments, shares, and likes on various social media platforms. The ability of algorithms to create thorough user profiles based on such precise data improves the customization of advertisements. Advertisers can achieve improved conversion rates using cost-effective ad targeting made possible by machine learning's precision. By presenting users with relevant material, ML algorithms improve the user experience for platforms and increase user engagement. Because customized ads frequently increase clicks and purchases and maximize the return on advertising spending, both parties gain monetarily.[2] A global survey conducted in 2023 found that 4.8 billion individuals utilize social media, highlighting the platform's importance for businesses and wide range of demographic appeal. It has been demonstrated that personalized advertisements on these platforms enhance the probability of a purchase, as 80% of consumers react positively to personalized encounters. However, the emergence of personalized advertising has also raised privacy concerns, most notably privacy fatigue, a phenomenon where users get disinterested in privacy concerns and stop taking security precautions. A lack of optimism and emotional exhaustion are symptoms of privacy fatigue, significantly influencing user behavior more than privacy concerns alone. Users' Information Privacy Awareness (IPA) and personality attributes are factors that affect their level of privacy fatigue. Users' perceptions of the gathering, use, and consequences of their data are reflected in IPA. The "big five" personality qualities include conscientiousness, agreeableness, openness, neuroticism, and extraversion. While privacy fatigue has been the subject of a few studies, machine learning (ML) has been used increasingly to predict actions related to privacy concerns[3].

[2] **Pamela Samuelson**, Privacy as Intellectual Property?, 52 **STAN. L. REV.** 1125, 1143 (2000).
[3] Ghosh Debasis, International Journal of Applied Business and Economic Research Volume 14, Issue 10, Pages 7089 - 7102 (2016)

 ISSN: 2582-6433

## DATA PRIVACY CONCERNS AND INFRINGEMENTS

Numerous privacy issues are brought up by machine learning algorithms' widespread usage of personal data in advertising.[4] Businesses frequently gather more information than is required, and consumers are ignorant of the extent to which their data is being mined. Using behavioral data, in-depth, sometimes intrusive user profiles are created. Privacy violations are more likely when data is routinely shared with third parties without explicit user authorization. The public's lack of confidence in tech businesses has increased due to growing awareness of data privacy issues. According to surveys, many people find the amount of tracking associated with targeted advertising to be unsettling. Calls for tighter restrictions and increased transparency have arisen due to the backlash against exploitative data practices. Personalized advertising presents severe ethical problems. When targeted advertisements are aimed at vulnerable groups like children or those with addictive tendencies, they have the potential to be deceptive and take advantage of users[5]. The results show that although high-end and low-end devices generally provide more protection, there are significant security and privacy issues with both types of devices. These problems show how quickly regulations are needed to guarantee that wearables adhere to strict security and privacy requirements, especially for devices used by children. The research adds crucial new information to the continuing conversation about wearable security by highlighting the significance of creating a solid framework for assessing and guaranteeing the safety of wearable technology in the marketplace.[6]

Moreover, people need to be made aware of how their data is being utilized and how much their online behavior is being affected due to the opaque nature of algorithms, which raises ethical concerns. Online marketing has grown in popularity as e-commerce grows because businesses realize how effective and widespread it is. India offers a distinct market for online ads due to its fast-expanding internet user population, especially among the younger generation (Y generation). This survey aims to understand better how young Indian customers feel about online advertisements, which are gradually replacing conventional marketing strategies.[7] A 21-item questionnaire was used to survey 149 young consumers in order to determine their

[4] Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2056 (2004), https://doi.org/10.2307/4093335.
[5] Fúster, J., Solera-Cotanilla, S., Pérez, J. et al. Analysis of security and privacy issues in wearables for minors. Wireless Netw 30, 5437–5453 (2024). https://doi.org/10.1007/s11276-022-03211-6
[6] Kiersten E. Todt, Data Privacy and Protection: What Businesses Should Do, 4 Cyber Def. Rev. 39 (2019), https://www.jstor.org/stable/26843891
[7] Marc Rotenberg, Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), 2001 STAN. TECH. L. REV. 1, ¶¶ 92–97

 ISSN: 2582-6433

sentiments. Four significant dimensions—usefulness, interaction and awareness, promises and enjoyment, catchy persuasion, and easy contact—influenced positive attitudes through factor analysis. The most important of these was the effectiveness of internet advertisements. Prominent data privacy violations highlight the dangers of using machine learning in advertising. For example, the Cambridge Analytica[8] controversy exposed the unapproved use of Facebook data to influence political outcomes. In a different instance, Google's DoubleClick business was penalized for breaking privacy agreements by combining customer data from multiple platforms.[9] These incidents show how data privacy infractions can have far-reaching effects.

## THE LEGAL GAP IN EXISTING REGULATION

Regulations like the California Consumer Privacy Act (CCPA) in the US and the General Data Protection Regulation (GDPR) in the EU largely control the present legal environment for data privacy, particularly with regard to machine learning (ML) and targeted advertising[10]. Considerable progress has been made in protecting user data with this legislation. For example, the GDPR[11] gives users the right to removal, enabling them to control and remove their personal data if they want, and mandates that businesses get informed permission and follow data minimization guidelines. Similarly, users can choose not to share their personal information by using the CCPA, which gives Californians the right to know what personal data is being gathered and if it is being sold. Though these laws offer a solid basis for safeguarding personal information, they need to address the complex issues brought forth by machine learning algorithms, especially regarding advertising. The incapacity of existing legislation to handle the dynamic nature of machine learning algorithms is one of their main drawbacks. Because these algorithms are constantly changing, there may be changes in the way data is handled and used in the future. Because of this, it is challenging for regulators to monitor the use of personal data and determine whether it complies with the law.

Furthermore, there's typically no oversight of cross-platform data sharing, which is a standard

[8] Cambridge Analytica Scandal: https://www.bbc.com/news/uk-43480048
[9] Shraddha Kulhari, Data Protection, Privacy and Identity: A Complex Triad, in Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity 23, 37 (1st ed. Nomos Verlagsgesellschaft mbH 2018), http://www.jstor.org/stable/j.ctv941qz6.7.
[10] Soini, E., Hallinen, T., & Martikainen, J. (2022). RWD31 Secure Processing Environments (SPE) Are Needed for the Cybersecure Collection and Secondary Use of Personal, Health, and Social Data. Value in Health. https://doi.org/10.1016/j.jval.2022.09.2256
[11] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

 ISSN: 2582-6433

practice in targeted advertising. Users might not completely understand how their information is merged, sold, or used for other purposes as it moves from one platform to another. The difficulties in enforcing existing laws also contribute significantly to their limited effectiveness. Regulators need help to keep up with the rapid advancement of technology, which results in inadequate enforcement and uneven implementation of the law in various jurisdictions. The fact that machine learning algorithms are "black boxes" presents another significant difficulty. Since these algorithms are frequently opaque, not even the businesses creating them completely comprehend the processes by which they arrive at particular results. It is extremely difficult to hold companies accountable for privacy violations due to this lack of transparency. Lawmakers have an even harder time controlling this sector because laws usually don't keep up with technology developments[12]. By the time a law is passed, the underlying technology has advanced, rendering some provisions of the law ineffective or obsolete. Moreover, the legal environment is dispersed across international borders. The CCPA[13] is one of the several state laws with different degrees of protection that are in place in other regions, including the United States, while the European Union has imposed strict regulations through the GDPR. Users in developing nations like India are particularly susceptible to privacy violations since comprehensive data privacy policies are still being developed in these areas.[14] The absence of global standards makes things much more complicated because multinational corporations frequently have to reconcile competing regulatory obligations, which makes it challenging to protect user data consistently across national borders.

## THE DIGITAL PERSONAL DATA PROTECTION BILL, 2023

The Digital Personal Data Protection Bill of 2023 is an upcoming law in India that aims to rectify several of the current legal environment's flaws. Stricter guidelines for the collection, storage, and use of personal data by companies are anticipated as a result of this new rule, especially when it comes to advanced technologies like machine learning. The bill's emphasis on data localization, which mandates that businesses retain vital data inside India's borders, is one of its main features.[15] This action attempts to provide Indian customers with more control over their personal data while safeguarding national security objectives. In addition, the law

[12]Ananya Mohapatra, Artificial Intelligence and Privacy of Digital Consumers, 24 SUPREMO AMICUS [344] (2021).
[13] California Consumer Privacy Act (CCPA): California Civil Code §§ 1798.100 - 1798.199.
[14] Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 Geo. L.J. 2381, 2385 (1996).
[15] "Making Sense of the Law: An Overview of the Digital Personal Data Protection Bill, 2023" by Dr. Kriti Singh, published in the Indian Journal of Law and Legal Research, Volume 5, Issue 4, 2023.

 ISSN: 2582-6433

clarifies permission and data processing principles, bringing them into compliance with international norms like the GDPR while also being adapted to India's unique requirements. In order to ensure accountability among data controllers, fines for non-compliance are also created, and the Data Protection Authority (DPA) is given the authority to implement the regulations. The Digital Personal Data Protection Bill has many benefits. One benefit is that it offers legal clarity in a field that has historically been characterized by ambiguity, especially in relation to permission and cross-border data transfers. Additionally, by explicitly granting users rights over their data, such as the option to have their data corrected, erased, and transferred, the measure aims to empower users. These rights are fundamental when it comes to machine learning algorithms, which frequently rely on enormous datasets that are incomprehensible to the general public. The law may reduce the privacy dangers connected to ML-based personalized marketing by granting people control over their personal data. The creation of the Data Protection Authority, which will act as an enforcement body to make sure businesses follow the new legislation, is another critical benefit. With the DPA in place, India can increase accountability by monitoring and punishing companies that violate data protection laws more effectively. Furthermore, the bill's requirements for data breach notifications guarantee greater transparency in the event that businesses misuse or misplace personal data.[16] This is especially important when people are frequently unaware that their information has been misused and data breaches are happening more frequently. While existing data privacy rules such as the CCPA and GDPR offer a solid framework, they need to adequately address the issues raised by machine learning algorithms, particularly with regard to targeted advertising.[17] A potential remedy is provided by the establishment of India's Digital Personal Data Protection Bill, which emphasizes user participation, localization of data, and strong enforcement measures.[18] Nonetheless, international collaboration and standardization are still necessary to provide a unified legal framework that safeguards users everywhere[19].

## SUGGESTED REMEDIES TO BRIDGE THE LEGAL GAP

The first solution would be to improve the existing regulatory framework. To bridge the gaps in data privacy protection, governments must prioritize algorithmic accountability and

[16] Developments in the Law—The Law of Cyberspace, 112 Harv. L. Rev. 1574, 1634–49 (1999).
[17] "The Missing Privacy by Design in the Draft Digital Personal Data Protection Bill of India" by Avinash Koli, 2023.
[18] Paul M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices, 2000 Wis. L. Rev. 743, 744.
[19] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

 ISSN: 2582-6433

transparency. A more transparent environment can be achieved by requiring companies to reveal the data they use and how their algorithms operate. To guarantee adherence to privacy regulations, machine learning systems should undergo mandatory audits on a regular basis. Another solution suggests technical Solutions for Privacy-Preserving Machine Learning. Developments in machine learning methods that protect privacy, such as federated learning and differential privacy, can lessen privacy issues.[20] While machine learning models can be trained on decentralized data sources, federated learning reduces the need for central data collection by enabling algorithms to analyze data without disclosing individual data points[21]. Using these strategies, user privacy and personalization demands can be better balanced. The companies can self-regulate data misuse. Privacy by The principles of design should be implemented by the advertising sector as a means of self-regulation. Businesses can make sure that privacy concerns are taken into account from the beginning while developing algorithms. The industry might also create best practices for managing personal data and establishing guidelines above and beyond the law mandates. This would lessen the possibility of privacy abuses while also fostering consumer trust.[22] The existing privacy issues can also be overcome by consumer education and Empowerment. To enable customers to make wise decisions, it is essential to inform them about the collection and use of their data. Simplified privacy policies and public awareness campaigns can aid in educating people about the dangers of targeted advertising. Furthermore, granting consumers more authority over their data—for example, by enabling them to refuse tracking—can aid in resolving privacy issues[23].

## ISSUES AND CONSIDERATIONS FOR IMPLEMENTATION

Finding a balance between innovation and privacy protection is one of the most challenging tasks in tackling data privacy concerns in machine learning-based targeted advertising. Since machine learning algorithms depend on data, restricting user data access might hinder ad tech progress. However, users remain open to abuse without strong and transparent data privacy safeguards. Legislators must design rules that safeguard privacy while allowing technology to grow, especially in advertising. Utilizing technologies that protect privacy, such as differential

[20] Thomas G. Donlan, Freedom of Information: The Right to Privacy Must Be Maintained by Private Effort, BARRON'S, June 21, 1999, at 62, Westlaw (WL-BARRONS 19353447).
[21] Ghaffari, A., Jelodari, N., pouralish, S. et al. Securing internet of things using machine and deep learning methods: a survey. Cluster Comput (2024)
[22] Paul M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices, 2000 Wis. L. Rev. 743, 744.
[23] Yu-Qian Zhu, Kritsapas Kanjanamekanant, No trespassing: exploring privacy boundaries in personalized advertisement and its effects on ad attitude and purchase intentions on social media, Information & Management, Volume 58, Issue 2, 2021

 ISSN: 2582-6433

privacy, might provide a way forward where privacy and innovation coexist. Implementing stricter laws would have Economic Impacts on the Advertising Industry[24]. More rigid laws governing the gathering and use of data may affect the advertising sector's profitability because customized advertisements significantly depend on comprehensive data profiles. Reduced ad targeting efficacy could lead to better click-through and conversion rates for businesses if data collection is unrestricted or user consent is obtained more rigorously.

On the other hand, companies that put privacy first might eventually win over customers' trust, boosting user engagement and brand loyalty.[25] Another would be Enforcement Mechanisms. For privacy laws to be successful, robust enforcement measures are required. To ensure businesses using machine learning algorithms adhere to data protection regulations, regulators should be able to audit such applications. Fines or limitations on the use of data are examples of penalties for non-compliance that need to be specified precisely and enforced consistently.[26] Companies should also be held responsible for any violations pertaining to data breaches and cross-border data movements, especially when third-party advertising is involved. Global cooperation and standardization can also be implemented. The global reach of digital advertising necessitates international collaboration in developing uniform data privacy regulations. Variations in national legislation give rise to vulnerabilities that multinational corporations might exploit, resulting in uneven user safeguards.[27] Closing these gaps and guaranteeing a consistent approach to data privacy across jurisdictions can be achieved by creating international standards for data protection modeled after the GDPR. Effective enforcement and compliance in cross-border data flows depend on this cooperation.

## CONCLUSION

Targeted advertising powered by machine learning is a two-edged sword: while it presents tremendous difficulties to data privacy, it also offers notable improvements in user engagement and advertising efficiency. Due to the overwhelming amount of personal data needed for precise forecasts and the opaque decision-making processes of many machine learning (ML) algorithms, individuals may be subject to privacy violations beyond the purview of the laws in

[24] Ghosh Debasis, International Journal of Applied Business and Economic ResearchVolume 14, Issue 10, Pages 7089 - 7102 (2016)
[25] Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 STAN. L. REV. 1373, 1423–28 (2000).
[26] Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 Vand. L. Rev. 1609 (1999).
[27] Anita L. Allen, Coercing Privacy, 40 WM. & MARY L. REV. 723, 750–57 (1999).

 ISSN: 2582-6433

place. While offering an essential degree of protection, current rules such as the CCPA and GDPR frequently fall short in addressing the particular and changing threats that the advertising industry faces from sophisticated algorithms. There is an urgent need for action as these technologies advance since there is a growing gap between what is technologically and legally permitted. This study emphasizes how important it is to implement a mix of technological advancements, international collaboration, and legal changes to guarantee that the digital advertising sector may grow without violating consumers' fundamental right to privacy. Regulations must change to reflect the complexity of machine learning by requiring increased accountability and openness from companies utilizing these systems. Technical solutions that protect user privacy, such as machine learning, can help lower the risks involved in data collecting while still enabling businesses to profit from targeted advertising. International cooperation is necessary since the digital world is transnational and calls for global data privacy rules that impose accountability on enterprises regardless of their location.

## REFERENCES

1. Gao, B., Wang, Y., Xie, H., Hu, Y., & Hu, Y. (2023). Artificial Intelligence in Advertising: Advancements, Challenges, and Ethical Considerations in Targeting, Personalization, Content Creation, and Ad Optimization. Sage Open, 13(4).
2. Pamela Samuelson, Privacy as Intellectual Property?, 52 STAN. L. REV. 1125, 1143 (2000).
3. Ghosh Debasis, International Journal of Applied Business and Economic Research Volume 14, Issue 10, Pages 7089 - 7102 (2016)
4. [4] Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2056 (2004), https://doi.org/10.2307/4093335.
5. [5] Fúster, J., Solera-Cotanilla, S., Pérez, J. et al. Analysis of security and privacy issues in wearables for minors. Wireless Netw 30, 5437–5453 (2024). https://doi.org/10.1007/s11276-022-03211-6
6. Kiersten E. Todt, Data Privacy and Protection: What Businesses Should Do, 4 Cyber Def. Rev. 39 (2019), https://www.jstor.org/stable/26843891
7. Marc Rotenberg, Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), 2001 STAN. TECH. L. REV. 1, ¶¶ 92–97
8. Cambridge Analytica Scandal: https://www.bbc.com/news/uk-43480048

 ISSN: 2582-6433

9. Shraddha Kulhari, Data Protection, Privacy and Identity: A Complex Triad, in Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity 23, 37 (1st ed. Nomos Verlagsgesellschaft mbH 2018), http://www.jstor.org/stable/j.ctv941qz6.7.
10. Soini, E., Hallinen, T., & Martikainen, J. (2022). RWD31 Secure Processing Environments (SPE) Are Needed for the Cybersecure Collection and Secondary Use of Personal, Health, and Social Data. Value in Health. https://doi.org/10.1016/j.jval.2022.09.2256
11. General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
12. Ananya Mohapatra, Artificial Intelligence and Privacy of Digital Consumers, 24 SUPREMO AMICUS [344] (2021).
13. California Consumer Privacy Act (CCPA): California Civil Code §§ 1798.100 - 1798.199.
14. Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 Geo. L.J. 2381, 2385 (1996).
15. "Making Sense of the Law: An Overview of the Digital Personal Data Protection Bill, 2023" by Dr. Kriti Singh, published in the Indian Journal of Law and Legal Research, Volume 5, Issue 4, 2023.
16. Developments in the Law—The Law of Cyberspace, 112 Harv. L. Rev. 1574, 1634–49 (1999).
17. "The Missing Privacy by Design in the Draft Digital Personal Data Protection Bill of India" by Avinash Koli, 2023.
18. Paul M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices, 2000 Wis. L. Rev. 743, 744.
19. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
20. Thomas G. Donlan, Freedom of Information: The Right to Privacy Must Be Maintained by Private Effort, BARRON'S, June 21, 1999, at 62, Westlaw (WL-BARRONS 19353447).
21. Ghaffari, A., Jelodari, N., pouralish, S. et al. Securing internet of things using machine and deep learning methods: a survey. Cluster Comput (2024)
22. Paul M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices, 2000 Wis. L. Rev. 743, 744.

 ISSN: 2582-6433

23. Yu-Qian Zhu, Kritsapas Kanjanamekanant, No trespassing: exploring privacy boundaries in personalized advertisement and its effects on ad attitude and purchase intentions on social media, Information & Management, Volume 58, Issue 2, 2021
24. Ghosh Debasis, International Journal of Applied Business and Economic ResearchVolume 14, Issue 10, Pages 7089 - 7102 (2016)
25. Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 STAN. L. REV. 1373, 1423–28 (2000).
26. Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 Vand. L. Rev. 1609 (1999).
27. Anita L. Allen, Coercing Privacy, 40 WM. & MARY L. REV. 723, 750–57 (1999).