Advances in Consumer Research
https://acr-journal.com/
Volume-3 | Issue-4 |April 2026
Original Researcher Article

Ensuring Data Privacy And Ethical Customer Consent In Digital Marketing Against Data Breaching And Cyber Crime

Dr.M. Lavanya[1], Ms.E.Asha Elumalai [2], Ms.Jetty Tanuja [3] Mr.G.Karthikeyan [4], Mr.W.Jerry Jabez [5]
[1]Associate Professor, School of Management Studies, Sathyabama Institute of Science and Technology Chennai, Tamilnadu, South India
Email:ID: lavanya.soms@sathyabama.ac.in
ORCID ID: 0000-0002-7367-7413
[2]PG Student, School of Management Studies, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, South India
Email:ID: ashaelumalai21@gmail.com
ORCID ID: 0009-0000-8235-8986.
[3]PG Student, School of Management Studies, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, South India
Email:ID: jettytanuja1234@gmail.com
ORCID ID: 0009-0002-7348-0482
[4]PG Student, School of Management Studies, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, South India
Email:ID: Karthiksurya200322@gmail.com
ORCID ID: 0009-0009-7501-9332
[5]PG Student, School of Management Studies, Hindustan Institute of Science and Technology,
Chennai, Tamil Nadu, South India
Email:ID: jerryjabez10@gmail.com
ORCID ID: 0009-0004-0705-4236

ABSTRACT
The research explores how businesses can balance effective marketing strategies with responsible data protection. Through statistical analysis using SPSS, the study investigates the connection between proper data security practices and growing customer trust. With a sample of 300 customers, the study examines key factors such as data breach incidents, transparency in data use, customer consent, and encrypted storage. Social media has become a powerful tool for reaching large audiences, but concerns remain about how the information shared and collected is being managed. This paper highlights the importance of strong security measures and clear customer consent when using personal data in digital marketing. It emphasizes the need to guard against cyber threats by adopting tools like encryption and two-factor authentication, which not only strengthen data security but also improve customer satisfaction. The results underline the critical role of ethical standards and preventive security measures in safeguarding customer information. It confirms that maintaining strong data security is essential for building lasting customer relationships and achieving long-term success in the digital marketing space. Ultimately, this research sheds light on the ethical challenges surrounding data privacy and stresses the importance of transparency and responsible data handling in today's digital world
Keywords: Data security, digital marketing, customer consent, encryption, customer trust

INTRODUCTION:

In today's digital world, businesses rely heavily on technology to strengthen their marketing strategies. Digital marketing has become one of the most effective tools for reaching large, diverse audiences. A big part of this involves collecting and analyzing customer data to better understand their preferences, behaviors, and shopping habits. However, focusing solely on customer data raises serious concerns about privacy and security. One of the biggest challenges for companies is not just how they use customer information, but how they protect it from data breaches and cyber threats. To address this, businesses need to follow strict security measures like encryption and two-factor authentication to keep personal data safe.

In the digital marketing space, using consumer data is key to delivering targeted ads and personalized experiences. But as data breaches become more common, ethical questions about privacy, consent, and responsible data use are more important than ever. This paper explores how digital marketers can handle customer data ethically while staying compliant with legal standards. Specifically, this research aims to understand how customers' views of a company's data privacy practices influence their trust in that brand. It's essential for companies to be transparent about how they use customer data and to reassure clients that their information won't be misused or sold. The study also looks at key ethical concerns in collecting consumer data online — asking what the ethical responsibilities are, and what best practices companies should follow to protect customer data and get proper consent for

marketing purposes. It further highlights the challenges of data management in digital marketing and suggests strategies to enhance data security and defend against cyberattacks.

REVIEW OF LITERATURE

Martin (2018) highlights that customer data has become the backbone of digital marketing, helping companies understand customer preferences, behaviors, and purchasing habits. This allows firms to tailor marketing communications effectively for different audience segments. However, constant data collection brings serious ethical concerns, especially relating to privacy and security. **Martin (2018)** stresses that transparency is a crucial factor in building trust between brands and consumers. When companies openly communicate how data is collected, used, and shared with third parties, it boosts customer confidence. Supporting this, **Madden (2014)** emphasizes the importance of clarity about data sharing practices, and **Baruh et al. (2017)** found that consumers are more willing to share their personal data when they are well-informed.

Harris et al. (2019) point out key ethical challenges like accountability, legitimacy, and consent in data collection. Problems arise when companies gather excessive data without clarifying how it will be used, stored, or who will access it. In some cases, firms pursue aggressive sales strategies using poor data acquisition methods, risking customer data leakage. This leads to ethical dilemmas about limiting data collection and preventing data misuse. **Harris et al. (2019)** argue that ethical concerns in digital marketing go beyond mere legal compliance. They suggest companies should prioritize consumer welfare, fairness, and respect for personal rights. Their research indicates that firms following ethical practices not only avoid legal trouble but also enhance brand image and build lasting customer relationships

Baruh et al. (2017) explain the importance of informed consent in digital marketing. Legal frameworks like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) mandate that companies must clearly inform customers about how their data will be collected and used. However, Madden (2014) notes that businesses often overcomplicate consent procedures, causing customers to unknowingly agree to practices they might not support.

Stiglic et al. (2018) discuss the increasing risks of data breaches and cyberattacks in digital marketing environments. These incidents can lead to the unauthorized access, theft, or loss of customer data — severely damaging both the business and its customers. Companies suffer financial losses, legal actions, and reputational harm, while customers face privacy violations and identity theft. **Stiglic et al. (2018)** emphasize the importance of implementing advanced security measures like encryption and secure storage to protect consumer data from unauthorized access. **Li et al. (2020)** found that customers are more likely to trust firms that show a strong commitment to data protection. Conversely, weak security can result in severe financial and reputational losses.

RESEARCH METHODOLOGY

OBJECTIVES OF THE STUDY:

1. To investigate the ethical dimensions of data privacy and customer consent in digital marketing, emphasizing the consequences of data breaches and the importance of transparent data handling.
2. To highlight the significance of adopting ethical practices for safeguarding customer data and building trust in digital marketing activities.
3. To provide strategic recommendations for improving ethical standards related to data privacy and customer consent within digital marketing environments.

A. RESEARCH DESIGN:

This study includes quantitative and qualitative method for accomplishing its objectives which aims aim is to explore how maintaining privacy and obtaining customer consent have become crucial concerns in digital marketing, particularly in preventing data breaches and ensuring customer satisfaction. Surveys were used as the primary tool to gather data, as they offer measurable and generalizable insights into consumer attitudes and behaviors, this is why descriptive and analytical research designs were employed. The steps include describing problem, selecting variables to be used in the study, selecting the participant, collecting data and analyzing the findings of research.

B. SAMPLING DESIGN:

The sampling methods used are convenient sampling and purposive sampling to collect responses from 300 customers were selected using a practical sampling technique of Chennai, through social media. Random sample was selected in each stratum. The inclusion criteria must be above 18 years of age. The survey is computer based Google form. To guarantee representation across several demographics, a stratified random sampling technique is used.Data was collected through a structured, computer-assisted questionnaire survey combined with face-to-face interviews. This sampling design helped improve the representativeness and generalizability of the findings.

C. DATA COLLECTION DESIGN:

The study uses primary and secondary data. Structured Questionnaire is the primary instrument. Through online and offline surveys a breakdown and explanation were given to 300 customers in Chennai. To increase the level of accuracy a face to face interview was done with the selected respondents in a manner that encourages illative questioning. Websites, review of literatures, industry reports, government publications are used as secondary sources. The combination of primary and secondary data collection enhanced the depth and context of the study.

D. STATISICAL TOOLS FOR ANALYSIS:

Data was collected using survey questionnaire and analyzed using SPSS software. The main statistical tools that used for analysis are Descriptive statistics, percentage analysis, ANOVA test, t test, Correlation Analysis,

Multiple Regression Analysis, to indentify association among variables and draw conclusions.

These tools helped identify trends, relationships, and patterns related to data privacy, customer satisfaction, and data breach incidents in digital marketing. The analysis revealed that customers who believed companies adequately protect their personal information showed a positive attitude toward digital marketing communications. In contrast, those who had personally experienced data breaches or heard about such incidents displayed lower levels of trust.

A. QUESTIONNAIRE DESIGN

Ethical considerations were prioritized throughout the research process. Participants were invited to take part voluntarily, with **informed assent forms** explaining the study's purpose, use of results, participant rights, and the option to withdraw at any time.The **questionnaire consisted of 10 thematic questions** targeting participants' awareness, perceptions, and attitudes towards data privacy in digital marketing, as well as their understanding of how companies obtain and manage customer consent.

Three demographic questions were also included to gather background information and assess whether respondents' profiles influenced their perceptions and responses.

To maintain **confidentiality and anonymity**, all survey data was securely stored in password-protected media. The study's ethical structure ensured that participants' rights and data privacy were respected throughout the research.

DATA ANALYSIS AND INFERENCE

Table.4.1.Table Indicating Multiple Regression Test

Variable	Unstandarized coefficient(B)	Standardized Coefficients	t-value	p-value
Constant	3.50		6.00	0.001
Customer Consent	0.70	0.40	5.00	0.001
Experiences of data breaches	0.40	0.30	3.50	0.015
Data Storage perceptions	0.80	0.35	2.20	0.003

H_{02}: Obtaining customer consent, experiences of data breaches, and perceptions of encrypted data storage have no significant impact on transparency in data use.

H_{12}: Obtaining customer consent, experiences of data breaches, and perceptions of encrypted data storage have a significant impact on transparency in data use.

INFERENCE:

From the table 4.1, it is inferred that the multiple regression analysis clearly highlights the critical role that ethical data practices play in shaping consumer perceptions of transparency in digital marketing. The results show that when companies actively seek and obtain customer consent before collecting or using their personal data, it significantly improves how informed and secure customers feel about the process. This positive relationship is evident with a strong, statistically significant increase in transparency scores. Additionally, customers who believe their data is stored securely using encryption tend to perceive a higher level of transparency in how their data is handled. This finding reinforces the importance of investing in visible and trustworthy security measures to reassure customers. Conversely, the analysis reveals that customers who have personally experienced data breaches report a noticeable decline in their perception of transparency. These negative experiences create distrust and make consumers more cautious about how businesses use their information. Together, these three factors obtaining consent, incidents of data breaches, and perceptions of encrypted data storage explain approximately 35% of the variation in customer perceptions of transparency. This substantial figure demonstrates that while other factors may also play a role, ethical practices around data privacy and security remain central to building and maintaining customer trust in today's digital marketing environment.

Table.4.2.Table Indicating Analysis Of Variance (Anova)

Variables	Sources of Variation	D.F	'F'	P
Customer Consent	Between Groups	2	5.75	0.020
	Within Groups	298		
	Total	300		
Experiences of Data Breaches	Between Groups	2	3.12	0.053
	Within Groups	298		
	Total	300		
Data Storage perceptions	Between Groups	4	14.80	0.002
	Within Groups	296		
	Total	300		

H_{02}: There is no significant difference in perceived transparency in data use based on obtaining customer

consent, experiences with data breaches, and perceptions of encrypted data storage.

H_{12}: There is a significant difference in perceived transparency in data use based on obtaining customer consent, experiences with data breaches, and perceptions of encrypted data storage.

INFERENCE:

From the table 4.2, it is inferred that the study tested whether transparency in data use differs based on three key factors: whether respondents had given consent, whether they had experienced data breaches, and their perceptions of encrypted data storage. The results showed significant differences in all three cases. Firstly, respondents who had provided consent reported feeling more informed about how their data was used ($F= 5.75$, $p = 0.020$). Secondly, those who had experienced data breaches felt less transparency compared to those who had not ($F= 3.12$, $p = 0.053$). Lastly, perceptions of encrypted data storage strongly influenced transparency, with respondents who believed their data was securely encrypted reporting higher levels of transparency ($F = 14.80$, $p < 0.002$). Since all p-values were below 0.05, the null hypotheses were rejected, confirming that obtaining consent, experiences with data breaches, and beliefs about data encryption significantly affect how transparent people perceive digital data practices to be. These findings highlight how ethical data management directly shapes consumer trust in digital marketing.

Table.4.3.Table Indicating T Test

Group	N	Mean	t-value	df	p-value
Customer Consent(Yes)	170	5.20	6.50	300	0.001
Customer Consent (No)	130	4.50			
No Data Breach	220	3.90	5.20	300	0.001
Experiences of data breaches	80	3.20			

H_{03}: There is no significant difference in transparency in data use between respondents who obtained consent and those who did not, as well as between those who have experienced data breaches and those who have not.

H_{13}: There is a significant difference in transparency in data use between respondents who obtained consent and those who did not, as well as between those who have experienced data breaches and those who have not.

INFERENCE:

From the table 4.3, it is inferred that the t-test analysis reveals significant differences in transparency in data use based on obtaining consent and incidents of data breaches. Respondents who gave consent for data usage reported a higher level of transparency (mean = 5.20) compared to those who did not provide consent (mean = 4.50), with a t-value of 6.50, $p < 0.001$, indicating that obtaining consent is associated with a clearer understanding of data practices. Additionally, individuals who have experienced data breaches reported a significantly lower level of transparency (mean = 3.20) compared to those who have not encountered such breaches (mean = 3.90), with a t-value of 5.20, $p < 0.001$. This suggests that personal experiences with data breaches negatively impact perceptions of data transparency. Overall, these findings highlight the importance of obtaining consent and ensuring robust data security practices to build trust and transparency in digital marketing, as experiences with data breaches lead to a diminished sense of being informed about how personal data is used.

Table.4.4.Table Indicating Correlation Analysis

Variables	Customer Consent	Experiences of data breaches	Data Storage perceptions	Data Storage encrypted
Customer Consent	1	0.40	0.60	0.50
Experiences of data breaches	0.40	1	0.56	0.30
Data Storage perceptions	0.60	0.56	1	0.70
Data Storage encrypted	0.50	0.30	0.70	1

H_{04}: There is no positive correlation between obtaining consent or encrypted data storage and transparency in data use, nor is there a negative correlation between incidents of data breaches and transparency in data use.

H_{14}: – There is a positive correlation between obtaining consent or encrypted data storage and transparency in data use, while there is a negative correlation between incidents of data breaches and transparency in data use.

INFERENCE:

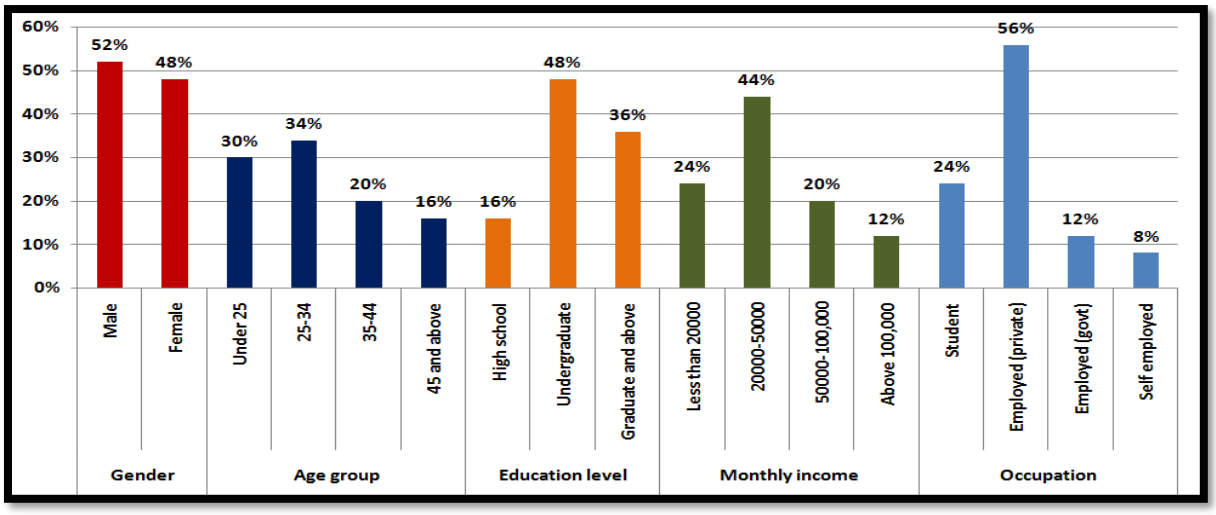
From the table 4.4, it is inferred that correlation analysis reveals significant relationships between key factors influencing transparency in data use. There is a moderate positive correlation ($r = 0.60$, $p < 0.001$) between obtaining consent and transparency in data use, indicating that respondents who provided consent generally perceive a higher level of transparency regarding how their data is used. Conversely, incidents of data breaches show a moderate negative correlation ($r = 0.56$, $p < 0.001$) with transparency in data use, meaning that those who have experienced data breaches or are aware of such breaches tend to feel less informed and more skeptical about how their data is managed. On the other hand, there is a strong positive correlation ($r = 0.70$, $p < 0.001$) between perceptions of encrypted data storage and transparency,

with respondents who believe their data is securely encrypted reporting significantly higher levels of perceived transparency. These findings emphasize that obtaining consent and ensuring data encryption are crucial factors in fostering transparency and building consumer trust, while incidents of data breaches can diminish trust and transparency in digital marketing practices.

Table 4.5.Table Indicating Demographic Details Of The Respondents

Demographic variable	Category	Frequency	Percentage	Mean	Standard deviation
Gender	Male	156	52%	2.97	1.21
	Female	144	48%		
Age group	Under 25	90	30%	3.52	1.35
	25-34	102	34%		
	35-44	60	20%		
	45 and above	48	16%		
Education level	High school	48	16%	2.98	1.15
	Undergraduate	144	48%		
	Graduate and above	108	36%		
Monthly income	Less than 20000	72	24%	2.57	1.20
	20000-50000	132	44%		
	50000-100,000	60	20%		
	Above 100,000	36	12%		
Occupation	Student	72	24%	2.42	1.25
	Employed (private)	168	56%		
	Employed (govt)	36	12%		
	Self employed	24	8%		

Chart 4.5.Chart Representing Demographic Details Of The Respondents



INFERENCE

It is inferred from table 4.5 that the majority 34% belonging to the 25 – 34 age group, reflecting a savvy population. Majority of the respondents are male with 52%. Majority 48%are undergraduates. Majority 56% are private employed.Majority 44%are earning monthly income from Rs.20,000 – 50,000.

DISCUSSION AND RECOMMENDATION

- ✓ Businesses should implement clear and easy-to-understand consent processes, ensuring customers fully understand how their data will be used. This includes using plain language and providing simple opt-in/opt-out options.
- ✓ Transparency should be a priority, with companies regularly updating customers about how their data is used and the measures taken to protect their information, helping to build trust.
- ✓ Organizations should invest in advanced security measures such as encryption and two-factor authentication to protect data and minimize the risk of breaches, with regular audits to ensure ongoing security.
- ✓ Educating customers about data privacy and security through informative content like webinars and workshops can empower them to make informed decisions about their data.
- ✓ In the event of a data breach, businesses should have a clear response plan that includes prompt notifications to affected customers, outlining corrective actions and offering support.
- ✓ Protecting personal data through encryption and two-factor authentication is essential for maintaining trust in digital marketing and ensuring customers feel their data is safe.
- ✓ Companies should develop a comprehensive data protection policy, including risk assessments and incident response plans, to proactively address potential vulnerabilities.
- ✓ Building partnerships with third-party vendors that follow strong data security protocols ensures that all parties involved in the data collection and storage process maintain high standards of protection.
- ✓ Businesses should engage in continuous monitoring and improvement of their data security systems to adapt to emerging cyber threats and ensure sustained protection.
- ✓ Regularly conducting audits and seeking external certifications for data protection can demonstrate a company's commitment to maintaining high security standards and enhance consumer confidence.

VI.CONCLUSION

This research underscores the deep connection between customer trust, data security, and digital marketing. It highlights how vital it is for businesses to adopt strong data protection strategies like encryption and two-factor authentication to keep customer information safe and avoid potential breaches. The findings show that customers who feel their data is secure are more likely to trust the businesses they interact with, which in turn boosts satisfaction and loyalty. The study also reveals how essential it is for businesses to be transparent with customers about how their data is used and to obtain clear consent before using it, as this significantly influences customer perceptions. On the flip side, customers who have experienced data breaches tend to feel less trust and transparency from companies, which signals a need for businesses to act swiftly to protect customer data. By following the recommendations—such as improving consent processes, enhancing transparency, investing in security, and educating customers—companies can build a reputation of ethical data usage. This not only helps them meet legal requirements but also gives them a strategic edge, strengthening relationships with their customers. As the digital world continues to grow, prioritizing data privacy will be crucial for businesses that want to maintain consumer trust and succeed in the future.

ACKNOWLEDGEMENT

The authors sincerely express their gratitude to the School of Management Studies, Sathyabama Institute of Science and Technology, for providing the academic environment and institutional support necessary for carrying out this study. The authors extend their heartfelt thanks to Dr. Lavanya M., Associate Professor, School of Management Studies, Sathyabama Institute of Science and Technology, for her valuable guidance, encouragement, and academic support throughout the course of this research work. The authors also wish to thank all the respondents who participated in the study and contributed their valuable time and insights. Special appreciation is extended to the faculty members, peers, and well-wishers whose suggestions and support helped in the successful completion of this work.

ABBREVIATIONS

Abbreviation	Full Form
ANOVA	Analysis of Variance
SPSS	Statistical Package for the Social Sciences
SPSS	Statistical Package for the Social Sciences
IV	Independent Variable
DV	Dependent Variable
MV	Mediating Variable

AUTHOR CONTRIBUTION

Dr. Lavanya M., Associate Professor, School of Management Studies, Sathyabama Institute of Science and Technology, contributed to the conceptual guidance, overall supervision, review of the manuscript, and academic refinement of the study.

Ms.E.Asha Elumalai , Ms.Jetty Tanuja, Mr.G.Karthikeyan , Mr.W.Jerry Jabez , students of the School of Management Studies contributed to literature collection, questionnaire preparation, data collection, analysis support, interpretation of results, and manuscript drafting. All authors contributed to the final preparation of the manuscript and approved the final version for submission.

ETHICAL CONSIDERATIONS

The study was conducted in accordance with ethical research standards. Informed consent was obtained from all participants prior to data collection. Respondents were assured of confidentiality and anonymity, and participation was voluntary. The data collected has been used solely for academic and research purposes.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this research paper.

FUNDING

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors

REFERENCES

1. Behera, R. K., Bala, P. K., Rana, N. P., &Kizgin, H. (2022). Cognitive computing-based ethical principles for improving organisational reputation: A B2B digital marketing perspective. Journal of Business Research, 141, 685-701.
2. Brewer, R., Westlake, B., Hart, T., &Arauza, O. (2021). The ethics of web crawling and web scraping in cybercrime research: Navigating issues of consent, privacy, and other potential harms associated with automated data collection. Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches, 435-456.
3. Economides, N., &Lianos, I. (2021). Restrictions on privacy and exploitation in the digital economy: A market failure perspective. Journal of Competition Law & Economics, 17(4), 765-847.
4. Gulyamov, S., &Raimberdiyev, S. (2023). Personal data protection as a tool to fight cyber corruption. International Journal of Law and Policy, 1(7), 17.
5. Lulandala, E. E. (2020). Facebook data breach: A systematic review of its consequences on consumers' behaviour towards advertising. Strategic System Assurance and Business Analytics, 45-68.
6. Madan, S., Savani, K., &Katsikeas, C. S. (2023). Privacy please: Power distance and people's responses to data breaches across countries. Journal of International Business Studies, 54(4), 731-754.
7. Metsiou, A., Broni, G., Papachristou, E., Migkos, S., & Kiki, M. (2023). An exploratory study on ethics on the internet. Journal of System and Management Sciences, 13(4), 624-639.
8. Ogbuke, N. J., Yusuf, Y. Y., Dharma, K., &Mercangoz, B. A. (2022). Big data supply chain analytics: Ethical, privacy and security challenges posed to business, industries and society. Production Planning & Control, 33(2-3), 123-137.
9. Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., &Bakare, S. S. (2024). Data privacy laws and their impact on financial technology companies: A review. Computer Science & IT Research Journal, 5(3), 628-650.
10. Quach, S., Thaichon, P., Martin, K. D., Weaven, S., &Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299-1323.
11. Richards, N., &Hartzog, W. (2021). A duty of loyalty for privacy law. Washington University Law Review, 99, 961-1005.
12. Saeed, S. (2023). A customer-centric view of E-commerce security and privacy. Applied Sciences, 13(2), 1020.
13. Wylde, V., Rawindaran, N., Lawrence, J.,

Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., &Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. SN Computer Science, 3(2), 127.

14. Behera, R. K., Bala, P. K., Rana, N. P., &Kizgin, H. (2022). Cognitive computing-based ethical principles for improving organisational reputation: A B2B digital marketing perspective. Journal of Business Research, 141, 685-701.
15. Brewer, R., Westlake, B., Hart, T., &Arauza, O. (2021). The ethics of web crawling and web scraping in cybercrime research: Navigating issues of consent, privacy, and other potential harms associated with automated data collection. Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches, 435-456.
16. Economides, N., &Lianos, I. (2021). Restrictions on privacy and exploitation in the digital economy: A market failure perspective. Journal of Competition Law & Economics, 17(4), 765-847.
17. Gulyamov, S., &Raimberdiyev, S. (2023). Personal data protection as a tool to fight cyber corruption. International Journal of Law and Policy, 1(7), 17.
18. Lulandala, E. E. (2020). Facebook data breach: A systematic review of its consequences on consumers' behaviour towards advertising. Strategic System Assurance and Business Analytics, 45-68.
19. Madan, S., Savani, K., &Katsikeas, C. S. (2023). Privacy please: Power distance and people's responses to data breaches across countries. Journal of International Business Studies, 54(4), 731-754.
20. Metsiou, A., Broni, G., Papachristou, E., Migkos, S., & Kiki, M. (2023). An exploratory study on ethics on the internet. Journal of System and Management Sciences, 13(4), 624-639
.