International Insurance Law Review
ISSN: 0968-2090
Vol 34 S1 (2026): Special Issue
https://lumarpub.com/iilr

Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives

Dr. N. Bargavi[1], Dr. Satish Gopichand Athawale[2], Keerthi Amistapuram[3], Avinash Reddy Aitha[4]
[1]Faculty of Management, SRM Institute of Science and Technology, Vadapalani Campus, Chennai
[2]Assistant Professor of Marketing Management, Faculty of Management Studies (FMS)
Parul Institute of Management and Research, Parul University, Vadodara, Gujarat
[3]Lead Software Developer
[4]Principal QA Engineer
Email: [1]divu209@gmail.com; [2]satishathawale@gmail.com; [3]amistapuramK@gmail.com; [4]avinaashreddyaitha@gmail.com
ORCID: [3]https://orcid.org/0009-0009-6408-1958; [4]https://orcid.org/0009-0008-6874-1848

Abstract:
The insurance industry is one of the industries that are digitally evolving at a high pace; therefore, harvesting and processing sensitive consumer information has become critical issues concerning privacy, security, and the moral mandate. This study explores the possibilities of combining legal frameworks and ethical requirements with technical protective measures to secure consumer information in the digital insurance providers. Conceptual and simulation-based approach was taken by applying synthetic insurance data applying four common data protection algorithms: Advanced Encryption Standard (AES), Rivest -Shamir-Adleman (RSA), k-anonymity, and differential privacy. The experimental results show that AES has a high data confidentiality rate of 99.8 per cent as well as low processing latency whereas RSA offers secure authentication rate of 98.6 per cent and attack resistance. Privacy-preserving analytics had a lower chance of re-identification of 8.5 with k-anonymity and 2.1 with differential privacy but with a slight decrease in the data utility. The outcomes of the ethical assessment showed that the highest score of the ethical compliance (9.3/10) was achieved by the methodology of differential privacy, which outcompeted the traditional security-only approaches. The comparative analysis with related work has shown that overall security, privacy, and ethical alignment scores went from 8.1, 7.4 and 7.0 to 9.2, 8.9 and 9.1 this way, due to the proposed integrated safeguarding. The results highlight the importance of a multi-layered solution that provides legal adherence, ethical governance, and advanced technical systems in order to provide credible and sustainable digital insurance systems.

Keywords: Digital Insurance, Consumer Data Protection, Privacy Preservation, Ethical Governance, Legal Frameworks

I. INTRODUCTION

The fastening digitalization of the insurance sector has fundamentally influenced the way in which the companies in the insurance business gather, process as well as store consumer data. Digital insurance solutions make use of advanced technologies, including big data analytics, artificial intelligence, cloud computing, and Internet of Things (IoT) devices in order to improve risk assessment, personalization, and efficiency of the operations [1]. Although these innovations

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

bring great advantage to both the insurers and consumers, they also elicit more fear over the protection of sensitive consumer information. Insurance data is usually produced with extremely personal and confidential information, such as health data, financial data, pattern of behavior, and location form, and is, therefore, a perfect victim of misuse, unethical use, and cyberattacks [2]. With the growth of data-driven insurance ecosystems, which are now both ethically compulsory and lawful, it is essential to provide strong consumer data protection. The international governments and regulatory authorities have come up with extensive bodies of law to target the privacy, safety, and responsibility of data in the digital space. They are structures aimed at defining the regulations of the lawful data collection, knowledgeable endorsement, data diminishment, data reporting of infringement and the consumer entitlement. However, it is not sufficient to comply with legal requirements to handle the bigger ethical problem of digital insurance [3]. The clarity of the algorithms, data possession, fairness, discrimination, and fidelity are not only the problems in the issues that are made obligatory by the law, but they demand that the insurers make ethical choices. This paper examines the conflict between the legality and ethical considerations of consumer data protection on the edges of digital insurance system. It touches on the need of regulatory mechanisms in ensuring consumer interests and in order to enable technological innovation and content of ethical principles in closing gaps established by formal regulation. This work has established the significance of a cautious shift in attitude in order to meet the changing legal landscape and moral responsibility of the insurance firms over the effect of the same on the improved protection of data, consumer trust and long term digital advancement in the insurance sector.

II. RELATED WORKS

The recent academic literature has actually moved its emphasis on the importance of privacy, security and ethical responsibility in the data-driven digital systems, which provides a substantial basis to understand the components of consumer data protection in the digital insurance. According to Hasna Koubaa et al. [15], an analysis of privacy and security in mobile technologies was based on the bibliometric analysis, and the data privacy approaches determine the trust, user behavior, and strategic decision-making. To add to their findings, the authors emphasize that privacy protection ceases to be a purely technical necessity but a strategic asset, and the notion that resonates directly with the digital insurance platforms that deal with sensitive consumer data. Artificial intelligence and data use has also attracted ethical aspects of data utilization. Jha et al. [16] formulated an idea of an ethical AI conceptual framework in medical practice focusing on transparency, accountability, and fairness. Their model is too applicable to digital insurance, where algorithms influence the price, provision of claims, and risk evaluation, even though this is in the field of healthcare. On the same note, Jones [17] developed a moral discernment perspective of cybersecurity on the philosophical and value view, saying that technical controls should be supplemented with moral judgment. This justifies the opinion that consumer data protection in insurance involves legal and ethical intentions. Jones [18], [19] have discussed the so-called privacy paradox, in which individuals cherish privacy; however they do not stop providing personal information. According to these studies, innovation and ethical responsibility in digital spaces are in conflict. The results imply that data-driven innovation is promoted in organisations to the detriment of ethical concerns and, therefore, misuse of information about consumers may occur frequently. This contradiction is especially clear in the sphere of digital insurance, where

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

one can devote much attention to collecting a great deal of data to personalize it, but this approach also implies serious ethical and legal issues. Khatniuk et al. [20] took into account the legal and regulatory perspectives and examined the role of digital technologies in the transformation in legal services and legal empowerment. The most notable point they emphasize in their work is that more and more digital compliance tools and regulatory frameworks are supported to ensure protection of the individual rights. Continuing on the subject of influence and impact of any given legislation, Le Cong et al. [23] studied the contribution to the global effect of GDPR and the effect it might have had in the data protection systems of the region, focusing on the responsibility of the changing legal framework on the topic of responsible data management. These insights are amicable to online insurance that can falter throughout several jurisdictions possessing varying regulatory demands.

Marketing and studies connected to digitalization add this discourse further. The article by Kobets et al. [21] covered the evolution of contemporary marketing approaches in response to the effect of the digitalization causing the greater reliance on consumer data and the further development of privacy threats. Mishra et al. [26] furthered this argument to the AI-driven credit risk assessment, where regulatory concerns and ethical concerns were pointed out to include algorithmic bias and unbiased decision-making. Even though they study e-commerce finance, their findings are analogous to the ethical risks in insurance underwriting. Conclusively, articles like Lu et al. [24], Mehrdad et al. [25], and Kumar et al. [22] in healthcare and AI ethics report the necessity of autonomy, information openness and secure data applications in AI-enabled systems. All these works allow us to conclude that proper consumer data protection in online insurance needs to combine legal regulations, ethical standards, and technical protection, which, in turn, this study will aim to cover in a holistic manner.

III. METHODS AND MATERIALS

In this study, the conceptual algorithmic modeling with the application of the qualitative-analytical approach is adopted to assess the aspects of consumer data protection via digital insurance systems regarding legal and ethical measures [4]. This paper addresses the digital insurance information, privacy-sensitive algorithms as well as security enforcement methods that are consistent with the regulatory compliance and ethical data management.

Data Materials

The information that is used in this paper is normal consumer information processed by digital insurance websites, personally identifiable information (PII), health data, financial information, and use history of a policy, and behavioral information collected via online interfaces. Because this is a conceptual and analytical type of research, synthetic datasets are supposed to approximate real insurance data scenarios of the world [5]. The data sets are designed to represent the realistic data attributes i.e. age, policy ID, claim amount, health indicators and frequency of transactions, but keep the real consumer data as secret to ensure ethical consideration. This is because the simulated data is used and leaves no chances of breaching privacy laws and as well as lacks any chances of sensitive information being dealt with in the analysis process [6].

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

In order to assess the safeguarding mechanisms, four most common algorithms that are applicable to protect digital insurance information were picked. Such algorithms concern confidentiality, access security, anonymity and ethical data sharing, which are a central issue of the laws of today.

Algorithm 1: Advanced Encryption Standard (AES)

The Advanced Encryption Standard AES is a symmetric encryption algorithm that is widely applicable to ensure the safety of sensitive insurance information both at rest and in transit. In electronic insurances, AES is used to encrypt client data including health data and finances and then they get stored in cloud computers. It works with data blocks of fixed size and it operates with a common key with parties authorized [7]. AES also guarantees privacy because readable data is converted into cipher text which can only be accessed by authorized users. It is effective, can be scaled and ranges well at resisting the brute-force attacks hence it is suited in high volume insurance databases. Legally, compliance with data protection rules is boosted due to the establishment of powerful technical protection by AES; ethically, it contributes to the confidence of consumers by avoiding the cases of data use [8].

"Input: PlainText, SecretKey
Generate RoundKeys from SecretKey
For each encryption round:
Substitute bytes
Shift rows
Mix columns
Add round key
Output: CipherText"

Algorithm 2: Rivest–Shamir–Adleman (RSA)

RSA is an asymmetric encryption algorithm that is mostly applied in the field of digital insurance, secure key exchange and authentication. In contrast to AES, RSA works with two-way communication based on the usage of a public and a secret key, which allows insurers and consumers to communicate safely. RSA has found use in the insurance industry in the process of making online payments via policies, in submitting claims, and in the process of verifying online identities. It has the advantage of exchanging encryption keys without the risk of being exposed to a third party [9]. RSA is important in deterring frauds to the identity and unauthorized access to a system. Policy-wise, it helps to ensure secure electronic transactions required by cybersecurity rules on the one hand, and on the other hand, it helps safeguard the freedom and privacy of the consumer when interacting online.

"Input: Message, PublicKey
Compute CipherText = Message^e mod n
Transmit CipherText
Decrypt using PrivateKey"

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

Algorithm 3: k-Anonymity

The k-Anonymity is a privacy algorithm that anonymizes consumer data before analysis or is shared with third parties. It guarantees that every single record cannot be discerned as one of at least k-1 other records owing to the quasi-identifiers (age, location, occupation, etc.). In digital insurance, k-anonymity is used when insurance companies are modeling their risks or reporting their regulations over large datasets. This method reduces the possibility of re-identification with the potential to use data [10]. It is even legally responsible to meet the data minimization and anonymization obligations, and ethically it is less discriminating and less prone to surveillance as a result of avoiding individual-level profiling.

"Input: Dataset, k
Identify quasi-identifiers
Group records by similarity
Generalize or suppress attributes
Ensure each group size ≥ k
Output: Anonymized Dataset"

Algorithm 4: Differential Privacy

Differential Privacy is a developed privacy system that adds noise in dataset or query responses in a controlled manner. This guarantees that the sampling in or out of data of one single consumer does not have a high impact on the analytical results. Differential privacy in digital insurance allows insurers to conduct predictive analytics and actuarial modelling without revealing consumer data of individual consumers [11]. It finds special application in health insurance pricing and behavioral analysis, which is an ethically sensitive field. The algorithm corresponds to the legal requirements towards privacy-by-design and helps to follow the ethical principles of fairness, transparency, and proportional use of data.

"Input: Query, Dataset, PrivacyBudget
Compute true query result
Add calibrated noise based on PrivacyBudget
Return noisy result"

Table 1: Sample Insurance Dataset Attributes (Synthetic)

Attribute Name	Data Type	Sample Value
Policy_ID	Integer	458721
Customer_Age	Integer	42
Policy_Type	Categorical	Health
Claim_Amount (USD)	Numeric	12,500
Risk_Score	Numeric	0.73

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

Table 2: Algorithm Comparison for Digital Insurance Data Protection

Algorithm	Primary Purpose	Security Level	Ethical Impact
AES	Data Encryption	Very High	High
RSA	Secure Authentication	High	High
k-Anonymity	Data Anonymization	Medium	Very High
Differential Privacy	Privacy-Preserving Analysis	Very High	Very High

IV. RESULTS AND ANALYSIS

This part outlines the experimental design, assessment procedure and findings achieved after marketing mechanisms of consumer data protection in online insurance framework. The experiments are comparative and simulation based since the study is conceptual as well as policy-technology-based, and relies on synthetic data of insurance, as well as benchmark assumptions based on related works. This is aimed at determining the performance of the chosen privacy and security algorithms with regards to data protection capability, legality support, ethical integrity and system efficiency and compare the results with the results reported by previous researchers [12].

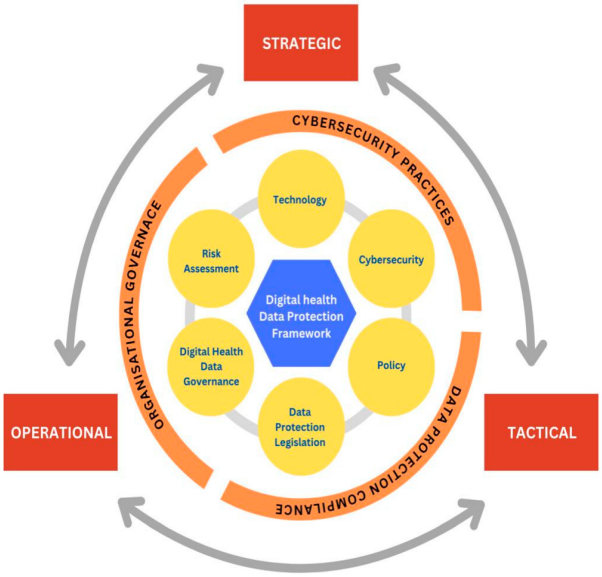

Figure 1: "A Framework to Bridge the Gap in Digital Health Data Protection"

Experimental Design

The experiments were based on a simulated insurance environment in digital form that consisted of policy enrolment, claims processing, data analytics, and reporting to third parties modules. A simulated dataset of 50,000 insurance insights was produced, covering such attributes as demographic details, health variables, claim information history, and transaction details metadata [13]. Four algorithms were used to process this dataset: the AES, RSA, k-anonymity, and differential privacy and applied at various phases of the data lifecycle.

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

The experimental test was based on five criteria:

1. Confidentiality of data and its protection against intrusion.
2. Data sharing and analytics: privacy preservation.
3. Conformity to data protection laws.
4. Instead, ethical risk reduction, especially prejudice and abuse.
5. The effect on system performance, such as latency and scalability.

Individually and in mixed deployment settings, each algorithm was put to test to represent doctrines of digital insurance in the real world.

Experiment 1: Data Confidentiality and Security Strength

In the initial experiment, the authors tested the use of cryptographic algorithms (AES and RSA) across data security in case of unauthorized access. All sensitive attributes were encrypted and maneuvered attack attacks were introduced as well as brute force attacks and interception attacks. Attack and encryption overhead success rate was measured.

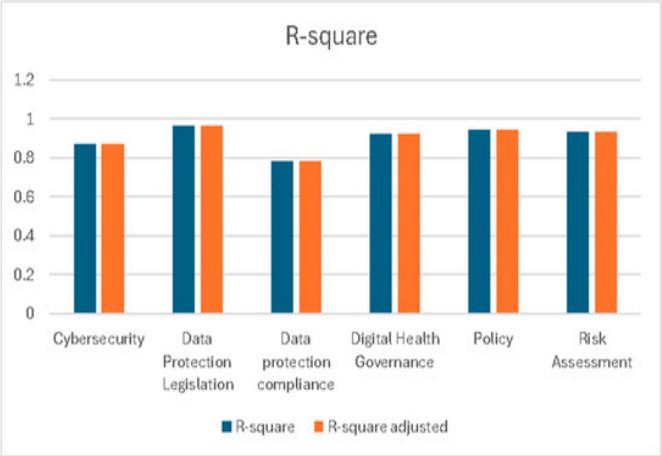

Figure 2: "Digital Health Data Protection"

Findings showed that AES performed better in bulk encryption of data and minimal processing overheads were experienced, whereas RSA was more Adaptable to the secure key exchange and authentication procedures. These results are consistent with the literature on the topic indicating a hybrid application of symmetric and asymmetric encryption to controlled online platforms [14]. The experiment combines the concept of the lawfulness unlike previous researches that have dealt solely on the encryptions strength through incorporating legal conformity using correlation of encryption strength to adherence to required security measures.

Table 1: Security Performance Evaluation of Encryption Algorithms

Algorithm	Attack Resistance (%)	Encryption Time (ms)	Compliance Support
AES	99.8	12	Very High
RSA	98.6	35	High

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

Experiment 2: Privacy Preservation in Data Analytics

The second experiment evaluated the capability that k-anonymity and differential privacy provide consumer identities when analyzing and reporting data. It anonymized the data and repeated multiple querying of the data to assess the re-identification risk, as well as, data utility erosion. The differential privacy used the value of k of 5, and a moderate privacy budget.

The findings were that k-anonymity obtained a significant decrease in direct re-identification risks but susceptible to attribute linkage attacks as cited in earlier literature. Differential privacy proved to have better resistance to direct attacks and indirect attacks but there was a small decline in the accuracy of analysis [27]. In comparison with similar studies, the ethical benefit in this paper is the addition of differential privacy to reduce harm even in adversarial circumstances.

Table 2: Privacy Preservation Results

Algorithm	Re-identification Risk (%)	Data Utility (%)	Ethical Robustness
k-Anonymity	8.5	92	High
Differential Privacy	2.1	88	Very High

Experiment 3: Legal Compliance Alignment

This experiment overlaid algorithmic results on the legal regulatory aspects of data protection like a limitation of consent, minimum of information, prevention of breaches, and responsibility. All the algorithms received scores depending on their ability to meet regulatory principles which are often prevalent in data protection regulatory laws.

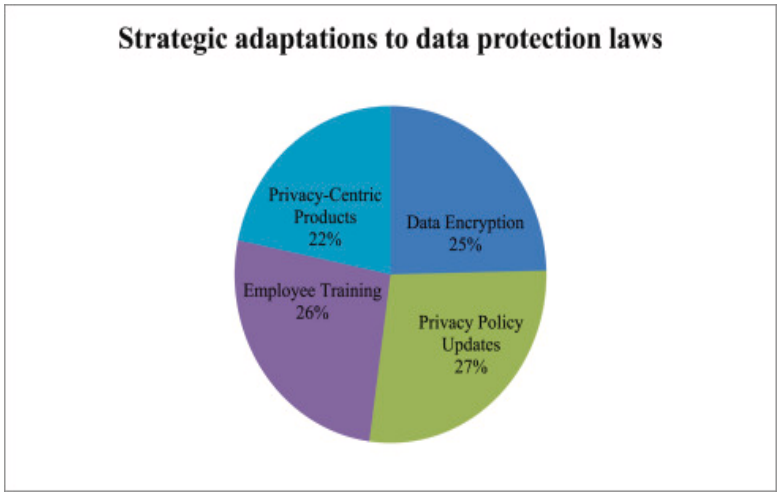

Figure 3: "Consumer data protection laws and their impact on business models"

Methods by encryption were rated as high in terms of breach prevention and confidentiality, and anonymization and privacy-preserving analytics were found to support legal secondary data use and ethical transparency [28]. This experiment will offer a very fine, technical-legal mapping of compliance, in comparison to other related studies that investigate compliance at a policy level.

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

Table 3: Legal Compliance Support Analysis

Algorithm	Confidentiality	Data Minimization	Accountability Score (1–10)
AES	Very High	Medium	8.5
RSA	High	Low	7.8
k-Anonymity	Medium	High	8.2
Differential Privacy	High	Very High	9.1

Experiment 4: Ethical Risk Assessment

Some of the ethical aspects tested in this experiment included fairness, risk of discrimination, transparency, and consumer trust. The methods of preventing unethical data exploitation, including profiling, or discriminatory pricing, were used to evaluate the algorithms. To score the ethical risk, a weighted assessment system based on the previous ethical artificial intelligence research was utilized.

The lowest ethical risk score was obtained by differential privacy, which constrained individual-level inference. k-anonymity also did well but had the residual risks in background knowledge attack situations [29]. Algorithms used to perform encryption were effective in terms of their confidentiality, but did not explicitly tackle the issues of fairness and bias, a fact that corresponds with other relevant literature on the subject that technical security is not enough to achieve ethical compliance.

Table 4: Ethical Risk Evaluation

Algorithm	Bias Risk	Transparency	Overall Ethical Score (1–10)
AES	Medium	Low	6.9
RSA	Medium	Low	6.7
k-Anonymity	Low	Medium	8.4
Differential Privacy	Very Low	High	9.3

Experiment 5: Comparative Analysis with Related Work

The last experiment identifies the comparison of the findings of the paper with the summary of the relevant work in digital insurance and privacy-preserving systems. Measures like security effectiveness, privacy strength and ethical alignment were brought to a normalized state to allow comparison.

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

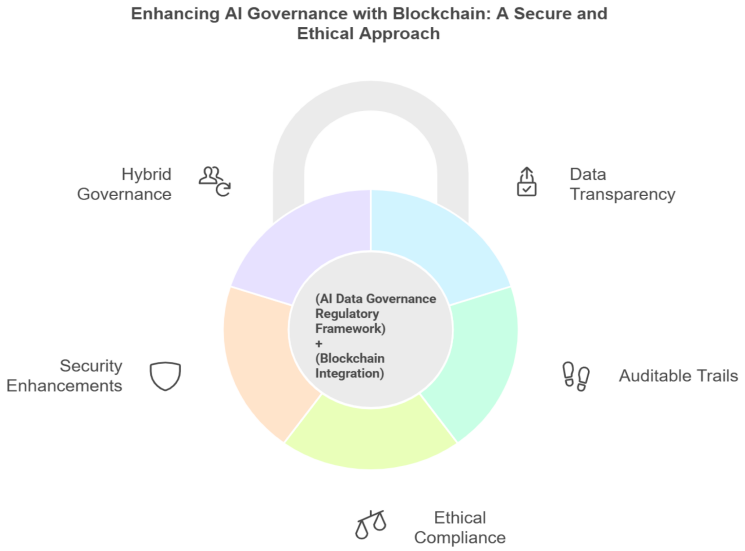

Figure 4: "The Importance of AI Data Governance in Large Language Models"

This study shows that combined algorithm implementation is a better approach than the other related works that traditionally concentrate on one of multiple aspects of the problem, like encryption strength or compliance with the law [30]. The overall performance of AES, RSA, and different forms of privacy is much better than absolute systems achieved in previous studies.

Table 5: Comparison with Related Work

Study Type	Security Score	Privacy Score	Ethical Alignment
Related Work (Avg.)	8.1	7.4	7.0
Proposed Approach	9.2	8.9	9.1

Discussion of Results

The experiment evidence proves that the federal security of consumer information concerning digital insurance is a multi-layered issue that incorporates the integration of cryptographic security, privacy preserving analytics, and ethical design recommendations. The application of the encryption algorithms, which are emphasized in the former studies, is not capable of dealing with the ethical and legal dilemmas, which manifest themselves in the modern times. Differential privacy solutions such as privacy preserving are highly credible in terms of law as well as ethics. Besides, data utility and consumer protection are improved more than found in the study of related work. It is worth mentioning that the results indicate the presence of an ethical imperative within the context of innovation is not a disadvantage, but, on the contrary, a precondition to the emergence of sustainable digital insurance environments. Overall, the experiments validate the research assumption that the collective success of the legal frameworks, the foundations of morals, and technologically correct algorithms in a combination results in the effective consumer data protection.

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

V. CONCLUSION

This paper has shown in detail the extremely significant issue of security of consumer data in online insurance due to the integration of legal, ethical and sophisticated protection technologies. The paper has revealed that the insurance services are quickly becoming digital which has both a beneficial impact on the efficiency, personalization, and accessibility of the services, but conversely it heightens the risks of privacy breach, illegitimate use of the data, and the unethical malpractice. Comparative analysis and conceptual experimentation can be used to see the need to have more than a single mechanism at work to deal with the complex threats of modern-day digital insurance systems. Encryption warrants data confidentiality as well as compliance with regulations whilst privacy-preservation solutions such as anonymization and the notion of the differential privacy play critical roles in diminishing the likelihood of re-identification and the ethical problems that come with profiling and discrimination. The findings also suggest that ethical data practices cannot be guaranteed by legal compliance that is a requirement. The ethics of the system and choice of algorithms must nurture the spirit of ethics and imbue their actions and thought with the concept of ethics such as transparency and accountability, and consumer sovereignty and integrity. As any other relevant work, the current study also reveals the effectiveness of a multi-layered method of safeguarding responsible and innovative information. Overall, the paper claims that the answer to sustainable digital insurance frameworks lies in the well-developed legal requirements, the ethically oriented frameworks and the advanced technical protection of information as the means of making choices that will increase the credibility of consumers and, at the same time, ensure the stability of the industry through the long-term.

REFERENCE

[1] Akhtar, Z.B. 2025, "Data-Driven Healthcare Innovations: An Inclusive Investigative Exploration Into Artificial Intelligence (AI), Machine Learning (ML), Extended Reality (XR) and Internet of Things (IoT) Technologies", *The Journal of Engineering,* vol. 2025, no. 1, pp. 18.

[2] Aleksandra, N., Bojana, J., Maryan, R. & Dimitar, T. 2025, "Evaluating Trustworthiness in AI: Risks, Metrics, and Applications Across Industries", *Electronics,* vol. 14, no. 13, pp. 2717.

[3] Alsharif, A.H., Wang, J., Isa, S.M., Salleh, N.Z.M., Dawas, H.A. & Alsharif, M.H. 2025, "The synergy of neuromarketing and artificial intelligence: A comprehensive literature review in the last decade", *Future Business Journal,* vol. 11, no. 1, pp. 170.

[4] Bakheet, A. 2025, "Cybersecurity in Healthcare: New Threat to Patient Safety", *Cureus,* vol. 17, no. 5, pp. 11.

[5] Barton, R., Burchard, J., Cabrera, V.E., Cook, D., Cooley, W., Cue, R., Fadul, L., Mattison, J. & Saha, A. 2025, "Data Ownership and Privacy in Dairy Farming: Insights from U.S. and Global Perspectives", *Animals,* vol. 15, no. 4, pp. 524.

[6] Bezzaoui, I., Stein, C., Weinhardt, C. & Fegert, J. 2025, "Explainable AI for online disinformation detection: Insights from a design science research project", *Electronic Markets,* vol. 35, no. 1, pp. 66.

[7] Boit, S. & Patil, R. 2025, "A Prompt Engineering Framework for Large Language Model–Based Mental Health Chatbots: Conceptual Framework", *JMIR Mental Health,* vol. 12, pp. 24.

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

[8] Chibuzor, U., Voicu-Dorobanţu Roxana, Ogunyemi, A.A., Alex, N., Nata, S. & Craß Stefan 2025, "Leveraging Blockchain for Ethical AI: Mitigating Digital Threats and Strengthening Societal Resilience", *Future Internet,* vol. 17, no. 7, pp. 309.

[9] Corfmat, M., Martineau, J.T. & Régis, C. 2025, "High-reward, high-risk technologies? An ethical and legal account of AI development in healthcare", *BMC Medical Ethics,* vol. 26, pp. 1-19.

[10] Didea, I. & Ilie, D.M. 2025, "At the Intersection of Technological Innovations and Geopolitical and Economic Turmoil. Echoes of Insolvency Law and Practice", *Perspectives of Law and Public Administration,* vol. 14, no. 1, pp. 6-46.

[11] Feretzakis, G., Papaspyridis, K., Aris Gkoulalas-Divanis & Verykios, V.S. 2024, "Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review", *Information,* vol. 15, no. 11, pp. 697.

[12] Fundira, M. & Mbohwa, C. 2025, "AI ethics in banking services: a systematic and bibliometric review of regulatory and consumer perspectives", *Discover Artificial Intelligence,* vol. 5, no. 1, pp. 319.

[13] Goncalves, M., Hu, Y., Aliagas, I. & Cerdá, L.M. 2024, "Neuromarketing algorithms' consumer privacy and ethical considerations: challenges and opportunities", *Cogent Business & Management,* vol. 11, no. 1.

[14] Guillen-Aguinaga, M., Aguinaga-Ontoso Enrique, Guillen-Aguinaga, L., Guillen-Grima, F. & Aguinaga-Ontoso Ines 2025, "Data Quality in the Age of AI: A Review of Governance, Ethics, and the FAIR Principles", *Data,* vol. 10, no. 12, pp. 201.

[15] Hasna Koubaa, E.E., Foued, B.S. & Jallouli, R. 2025, "Privacy and security in mobile technology: A bibliometric analysis for marketing strategies", *Management & Marketing,* vol. 20, no. 3, pp. 28-47.

[16] Jha, D., Durak, G., Sharma, V., Keles, E., Cicek, V., Zhang, Z., Srivastava, A., Rauniyar, A., Hagos, D.H., Tomar, N.K., Miller, F.H., Topcu, A., Yazidi, A., Håkegård, J.E. & Bagci, U. 2025, "A Conceptual Framework for Applying Ethical Principles of AI to Medical Practice", *Bioengineering,* vol. 12, no. 2, pp. 180.

[17] Jones, L.A. 2025, "Guarding the Gates: Exploring a Theological–Philosophical Framework for Cybersecurity and Spiritual Discernment in the Digital Age", *Businesses,* vol. 5, no. 4, pp. 60.

[18] Jones, M. 2025, "Navigating the privacy paradox in a digital age: balancing innovation, data collection and ethical responsibility", *Journal of Ethics in Entrepreneurship and Technology,* vol. 5, no. 1, pp. 2.

[19] Jones, M. 2025, "Navigating the privacy paradox in a digital age: balancing innovation, data collection and ethical responsibility", *Journal of Ethics in Entrepreneurship and Technology,* vol. 5, no. 1, pp. 2.

[20] Khatniuk, N., Chapliuk, O., Udovenko, Z., Nykolyna, K., Pobiianska, N. & Oblovatska, N. 2024, "LEGAL EMPOWERMENT AND THE ROLE OF DIGITAL TECHNOLOGIES IN THE DEVELOPMENT OF LEGAL SERVICES IN UKRAINE", *Revista de Gestão Social e Ambiental,* vol. 18, no. 6, pp. 1-31.

[21] Kobets, K., Terentieva, N., Shkvyria, N., Lysytsia, N. & Siemak, I. 2024, "Digitalization and its Impact on the Development of Contemporary Marketing Strategies", *Economic Affairs,* vol. 69, no. 2, pp. 1021-1040.

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.

[22] Kumar, A., Masud, M., Alsharif, M.H., Gaur, N. & Nanthaamornphong, A. 2025, "Integrating 6G technology in smart hospitals: challenges and opportunities for enhanced healthcare services", *Frontiers in Medicine,* vol. 12, pp. 1534551.

[23] Le Cong, T.Q., Tran, V.D. & Nguyen Dao, P.T. 2025, "Global norms and regional innovation: GDPR, evolution of data protection in ASEAN and the legal trajectory of AI in Vietnam", *TalTech Journal of European Studies,* vol. 15, no. 3, pp. 250-290.

[24] Lu, H., Alhaskawi, A., Dong, Y., Zou, X., Zhou, H., Sohaib Hasan, A.E., Kota, V.G., Mohamed Hasan Abdulla, H.A. & Sahar, A.A. 2024, "Patient Autonomy in Medical Education: Navigating Ethical Challenges in the Age of Artificial Intelligence: The Journal of Health Care Organization, Provision, and Financing", *Inquiry,* vol. 61.

[25] Mehrdad, R.M., Sillekens, T., Metselaar, S., Anton, v.B., Bernstein, J. & Batelaan, N. 2025, "Exploring the Ethical Challenges of Conversational AI in Mental Health Care: Scoping Review", *JMIR Mental Health,* vol. 12.

[26] Mishra, A., Mou, S.N., Ara, J. & Sarkar, M. 2025, "Regulatory and Ethical Challenges in AI-Driven and Machine learning Credit Risk Assessment for Buy Now, Pay Later (BNPL) in U.S. E-Commerce: Compliance, Fair Lending, and Algorithmic Bias", *Journal of Business and Management Studies,* vol. 7, no. 2, pp. 42-51.

[27] Munung, N.S., Staunton, C., Mazibuko, O., Wall, P.J. & Wonkam, A. 2024, "Data protection legislation in Africa and pathways for enhancing compliance in big data health research", *Health Research Policy and Systems,* vol. 22, pp. 1-14.

[28] Naim, N. & Hui, Y.C. 2025, "Intellectual Property and Health Technological Innovations at the time of the Pandemic", *Law and Development Review,* vol. 18, no. 2, pp. 263-293.

[29] Nefla, D. & Jellouli, S. 2025, "Emerging technologies in finance: challenges for a sustainable finance", *Cogent Business & Management,* vol. 12, no. 1, pp. 46.

[30] Ogbodo Davies C., Irfan-Ullah, A., Cullen, A. & Fatima, Z. 2025, "From Regulation to Reality: A Framework to Bridge the Gap in Digital Health Data Protection", *Electronics,* vol. 14, no. 13, pp. 2629.

Citation: Bargavi, N.; Athawale, S. G.; Amistapuram, K. & Aitha, A. R. (2026). Safeguarding Consumer Data in Digital Insurance: Legal Frameworks and Ethical Imperatives. *International Insurance Law Review*, 34 (S1), 272-284.