

DATA PRIVACY RISKS AND AI – A BIBLIOMETRIC ANALYSIS OF FIVE FORMS OF AI FROM A CONSUMER PERSPECTIVE

Irina Bojescu^{1*}, Giulia Kondort², Roxana Cioc³, Maria Barbul⁴

¹⁾²⁾³⁾⁴⁾ The Bucharest University of Economic Studies, Romania

Abstract

Privacy has become one of the central concerns in the relationship between consumers and artificial intelligence, yet the notion of artificial intelligence covers technologies that differ considerably in the way they handle personal data. This paper examines how the academic literature connects five forms of artificial intelligence, namely artificial intelligence in the broad sense, service robots, chatbots, virtual assistants and generative artificial intelligence, with privacy risks. The academic literature on each of these technologies was identified through separate searches in the Web of Science database, combining the terms privacy risks and consumer with the corresponding technology, and subsequently analyzed using VOSviewer to identify the most frequently associated terms and the main themes emerging from the literature. The results indicate a substantial increase in research interest over recent years, together with growing attention to the privacy implications of generative artificial intelligence in particular. Across the five categories, the associated terms consistently gather around trust, acceptance, technology adoption and data confidentiality, while the specific privacy risks differ from one technology to another. These findings support the treatment of each form of artificial intelligence separately when studying consumer privacy concerns and offer a conceptual basis for future research on consumer attitudes towards artificial intelligence.

Keywords

Artificial intelligence, privacy risks, consumers, robots, chatbots, virtual assistants, generative artificial intelligence.

JEL Classification

M10, M15, M30

* Corresponding author, Irina Bojescu – irina0927@yahoo.com

1. Introduction

Research on consumer privacy in the context of artificial intelligence has grown rapidly over the past few years. However, artificial intelligence includes a wide range of technologies that differ considerably in how they interact with consumers and in the kinds of data they collect. Recent reviews note that the consumer-facing AI literature remains fragmented: many studies talk about artificial intelligence as if it were a single concept, when in fact they examine one particular application, like chatbots, recommendation systems, virtual influencers or generative AI tools (Morales-Muñoz et al., 2026). Reviews focusing on specific AI applications, such as anthropomorphic chatbots, reach much the same conclusion (Greilich et al., 2025).

This distinction is particularly important for the present analysis. Different artificial intelligence applications rely on different forms of consumer data and operate in different settings, so privacy concerns cannot be assumed to look the same across technologies. Before performing the keyword analysis, it is therefore necessary to be explicit about what AI means in each search. For this reason, the review focuses on the five categories that dominate consumer-facing research, namely artificial intelligence in the broad sense, service robots, chatbots, virtual assistants and generative AI, and examines how each of them has been linked to privacy risks in studies indexed in Web of Science.

This analysis is important considering how research on consumer privacy and artificial intelligence has developed over time. Studies in this area come from different fields, including marketing, information systems, tourism, healthcare, and law, and often focus on specific forms of artificial intelligence. Therefore, existing research is divided across several areas of study. A bibliometric analysis based on keyword co-occurrence provides a systematic and replicable way to bring this research together and identify the main topics related to each form of artificial intelligence, the links between these topics, and how research interest has changed over time.

It is also important to examine different forms of artificial intelligence separately, because they interact with consumers and process personal data in different ways. Service robots may use cameras and sensors in the physical environment, chatbots process personal information shared during conversations, and virtual assistants may process voice data from everyday interactions. Generative AI brings additional privacy concerns related to the information provided by users and the data used to develop these systems. Analyzing all these technologies together could therefore make it difficult to identify the differences between them and to understand the specific privacy concerns associated with each form of artificial intelligence.

This article begins with a review of the literature on privacy risks related to each of the five forms of artificial intelligence, followed by a description of the research methodology. This section explains the data collection process, based on five separate searches conducted in the Web of Science database, and the keyword co-occurrence analysis performed using VOSviewer. The results and discussion section then presents the number of publications identified for each search and their development over time, the main keyword groups associated with each form of artificial intelligence, and a comparison of the results across the five forms. This article concludes by presenting the main findings of the study and discussing their implications for the financial sector.

2. Review of the scientific literature

2.1. Artificial Intelligence and consumer privacy

In its broadest sense, artificial intelligence refers to computer systems able to perform tasks normally associated with human intelligence: recognizing patterns, making predictions, supporting decisions or generating recommendations by learning from large volumes of data (Davenport et al., 2020). In consumer settings, these capabilities appear mostly in digital marketing and retail, where they are delivered through machine learning and advanced analytics (Spais & Chryssochoidis, 2025).

From a privacy perspective, much of what artificial intelligence offers-personalisation, real-time prediction, automated interaction rests on the collection and processing of detailed consumer data. Martin and Zimmermann (2024) suggest that AI continues the long expansion of data collection that information technologies began, while pushing its depth, breadth and scope further. They also distinguish process-oriented AI, centered on collecting and processing data, from outcome-oriented AI, centered on producing outputs, and show that the two interact differently with the mechanisms consumers rely on when making privacy decisions, including the privacy calculus, psychological ownership and social influence.

Empirical studies suggest that consumers are beginning to recognize this distinction. Specifically, they increasingly distinguish between privacy concerns associated with the organizations collecting their data and those associated with the AI systems that subsequently process and use them. The second tends to be perceived as the more threatening of the two, because the workings of AI are harder to understand and to check (Martin & Zimmermann, 2024; Menard & Bott, 2025; Pelau et al., 2024).

Building on this idea, Menard and Bott (2025) propose a new construct, “concern for information privacy under AI misuse”, which captures fears such as data being reused for other purposes, the AI drawing inferences the user never authorised, and a gradual widening of how data are used over time. Similar findings come from AI-driven marketing and AI-based fraud detection, where consumers feel particularly exposed because the models are opaque and the data needed to train them are highly sensitive (Alhitmi et al., 2024; Awosika et al., 2024; Siminica et al., 2025).

A second line of research asks how consumers actually decide whether to share data with a system based on artificial intelligence. The classical answer is that users weigh the expected benefits of sharing against its expected costs. Shin (2025) argues that this trade-off no longer works well in AI environments: users simply cannot see how their data will be transformed by downstream algorithms, so their risk assessments end up biased. Frank (2024) reaches a compatible conclusion in a cross-segment study, showing that preferences for AI-enhanced products depend heavily on individual privacy literacy and trust, with effects that differ markedly from one consumer group to another.

These findings have important practical implications. Drawing on expert interviews, Akakpo et al. (2025) argue that the standard notice-and-consent approach is no longer adequate once artificial intelligence is involved, and call instead for privacy-by-design principles, with protection built into the model from the outset. From a legal perspective, Takhshid (2024) reframes the problem: AI-trained models can reproduce

identifying features of individuals even after the original data have been formally anonymised.

Technology-adoption studies finally confirm that privacy concern is a persistent barrier to the use of artificial intelligence, though its weight varies with the application. Sebastián et al. (2022) and Pal et al. (2021) both find that perceived privacy risk lowers the intention to adopt virtual assistants and smart voice assistants, but the negative effect weakens when the service is seen as clearly useful or trustworthy. From a more critical perspective, Véliz (2023) and Elliott & Soifer (2022) provide a broader perspective on these findings, suggesting that business models based on extensive data collection create structural pressures that individual privacy decisions alone cannot resolve. What emerges from this body of work is that artificial intelligence does not create a single new privacy risk, but amplify and accelerate risks already present in digital consumer environments (Martin & Zimmermann, 2024; Das, 2023).

2.2. Service robots and privacy concerns

Service robots are a more specific form of artificial intelligence. Unlike purely software-based systems, they have a physical body, interact with consumers face-to-face, and carry out service tasks on their own (Chuah et al., 2021; Lin et al., 2024). Their physical presence distinguishes service robots from other forms of artificial intelligence. By combining AI-based algorithms with cameras, microphones, proximity sensors and biometric scanners, service robots can continuously collect data from their surrounding environment, potentially capturing information about individuals who are not directly interacting with the robot and who have not explicitly consented to such data collection (Hu et al., 2023; Song & Ahn, 2024).

Most empirical work on this subject comes from hospitality and tourism, for a simple reason: hotels and restaurants were among the first industries to place service robots in everyday settings such as check-in desks, guest rooms and dining areas, all of them socially sensitive spaces (Song & Ahn, 2024; Lin et al., 2024; Du et al., 2025).

Privacy risk is described rather differently in this stream than in the broader AI literature. Hu et al. (2023) introduce the useful notion of a “watching-eye effect”: merely seeing cameras and sensors in a robot makes consumers feel observed and more self-aware, even when no data are actually being collected. The perception of being watched is enough, in itself, to raise privacy concerns, whatever the robot does with the data. Song & Ahn (2024) build on this with a privacy trade-off model developed specifically for hospitality robots, finding that the decisive factor in whether people will use a robot is the loss of control over physical space and personal information, which matters even more than the purely informational concerns that dominate online settings. Chien et al. (2025) push the idea further by comparing humanoid robots with tablet-based service interfaces: a human-like body intensifies privacy concerns because consumers start attributing intentions, and sometimes hidden motives, to the machine.

However, privacy concerns are not the whole story. Trust and ethical perceptions can mitigate these concerns. Using a comparative analysis of consumer profiles, Chuah et al. (2021) identify combinations of trust, ease of use and perceived usefulness that are enough to overcome privacy hesitation. Lin et al. (2024) go a step further, showing that consumers' ethical judgements of autonomous service robots are largely independent of

how useful the robot is; when it comes to robots, privacy seems to be treated as a moral question rather than a practical one. Salih and Alsmairat (2025) add that trust acts as a bridge between privacy risk and the willingness to keep using AI-enabled services. The literature on service robots indicates that privacy risks are highly context-dependent, varying according to the environment in which the robot operates, the sensors it uses and the characteristics of the social setting. This perspective differs from the more abstract and predominantly information-based understanding of privacy found in research on non-physical forms of artificial intelligence (Hu et al., 2023; Kim et al., 2022).

2.3. Chatbots and privacy risks

Chatbots are conversational agents designed to interact with consumers primarily through text-based communication. Early chatbots relied on predefined rules and scripted responses, while more recent systems use large language models to engage in more complex and open-ended conversations (Cheng & Jiang, 2020; Greilich et al., 2025; Prakash et al., 2023). They are now common in customer service, e-commerce and banking, and increasingly present in mental healthcare.

What makes chatbots distinctive from a privacy perspective is the kind of information they collect. During these interactions, users may voluntarily disclose personal information such as names, preferences, complaints or symptoms, while chatbots can also infer additional information from conversational cues, including writing style, tone and emotional state (Kronemann et al., 2023; Prakash et al., 2020; Sobowale et al., 2025). In their systematic review of consumer responses to human-like chatbots, Greilich et al. (2025) identify a notable paradox: design features intended to enhance user engagement, such as human-like language, expressions of empathy and proactive questioning, may also encourage consumers to disclose more personal information than they would through conventional digital channels.

Several empirical studies have examined the factors that shape privacy concerns in chatbot interactions. Cheng & Jiang (2020) show that perceived privacy risk can weaken the positive effects of chatbot interactions on user experience, particularly when the chatbot is perceived as intrusive. Li & Zhang (2023) find that communication quality and trust influence the relationship between chatbot use and privacy concerns. Complementing these findings, Prakash et al. (2023) identify credibility, perceived humanness and perceived security as key factors contributing to trust in AI-based customer service and healthcare chatbots.

An important aspect of privacy in chatbot interactions is their dynamic nature, as users' willingness to disclose personal information may evolve throughout the conversation. In two related studies on service recovery, Song et al. (2022a, 2022b) show that chatbot responses to service failures, including apologies, transfer to a human agent or compensation, can influence users' subsequent willingness to disclose personal information and their overall satisfaction with the interaction.

Kronemann et al. (2023) offer one of the clearest demonstrations of how disclosure works in this context. When chatbots are designed to feel more human and personalised, consumers become much more willing to share "secrets", that is, sensitive personal or financial information. Social presence makes the exchange feel like a conversation with

a person rather than with a company, and users lower their guard accordingly. Bhojwani and Ranjan (2026) and Puertas et al. (2024) confirm that in shopping contexts, chatbots cut both ways: they raise purchase intention and privacy concern at the same time, with the final balance depending on how trust is managed over the course of the relationship. The effect is considerably stronger in sensitive domains such as healthcare and mental health. Sobowale et al. (2025) and Prakash et al. (2020) show that generative AI psychotherapy and health chatbots are increasingly used by vulnerable groups, among them, young people, who hand over clinically sensitive information to systems whose data practices they rarely understand. This mix of attractive design and vulnerable users has led researchers to call for chatbot-specific privacy notices that acknowledge the conversational, cumulative and relational nature of the data being collected (Gupta et al., 2025; Alt et al., 2021).

2.4. Virtual assistants and privacy disclosure

Virtual assistants, also referred to as smart voice assistants, voice agents or intelligent personal assistants, are systems based on artificial intelligence that interact with consumers through voice communication and are commonly integrated into devices such as smart speakers, smartphones and in-vehicle systems (Pal et al., 2021; Calahorra-Candao & Martín-de Hoyos, 2024; Henkens et al., 2026).

From a privacy perspective, virtual assistants differ from other forms of artificial intelligence as they rely on continuous listening to detect activation commands such as “Alexa” or “Hey Siri”. Therefore, these devices can process sounds from the surrounding environment beyond those intentionally directed at them. The associated privacy concerns therefore differ from those of screen-based chatbots, as data collection can extend to the broader household environment and potentially include individuals who are not directly interacting with the device.

Research on virtual assistant adoption identifies privacy concerns as a key factor affecting consumers’ continued use of these technologies. Pal et al. (2021) find that perceived privacy risk reduces users’ intention to continue using smart voice assistants, alongside factors such as perceived ease of use and enjoyment. Sebastián et al. (2022) show that users’ awareness of continuous listening can increase privacy concerns, which can outweigh the enjoyment associated with using these devices. Calahorra-Candao and Martín-de Hoyos (2024), examining the transition from text-based to voice-based interaction in online shopping, find that consumers are more willing to use voice interfaces in private settings, such as their homes, than in public spaces, where privacy concerns may be greater.

Other studies focus on the use of virtual assistants in commercial and service-related contexts. Yang and Wang (2025) and Henkens et al. (2026) find that the perceived quality of artificial intelligence voice agents can contribute to brand loyalty, while this relationship may vary according to consumer innovation and perceptions of brand ethicality. Aiolfi et al. (2023) and Guerreiro et al. (2022) examine commercial content delivered through smart speakers, including shopping recommendations and voice advertising, and highlight the importance of trust and transparency regarding data use in shaping consumer acceptance. In the absence of these factors, advertising delivered

through voice-based channels may be perceived as more intrusive than advertising presented through screen-based channels.

Research on related technologies provides additional information on these privacy concerns. Focusing on wearable devices, Cho et al. (2018) identify a privacy trade-off in which consumers balance the benefits of continuous personalisation against concerns associated with the ongoing disclosure and collection of personal information. Bandara et al. (2020) and Anic et al. (2019) indicate that privacy concerns associated with online environments are also relevant to voice-based interactions. However, voice data introduce an additional privacy dimension, as human voice can function as both a biometric identifier and a source of information about an individual's emotional state, making such data potentially more sensitive than text-based information.

2.5. Generative AI and Emerging Privacy Concerns

Generative AI refers to a category of foundation models, primarily large language models and image generation models, that produce new content, including text, images, code and audio, based on patterns learned from large-scale training datasets (Wang et al., 2025; Salih & Alharthi, 2026). Consumer applications of generative AI, including ChatGPT and AI-based health assistants, have become increasingly integrated into everyday activities. This growing adoption is also reflected in the substantial increase in publications addressing privacy risks for consumers and generative AI identified in the present study (Dahabiyeh & Bouteraa, 2026; Arce-Urriza et al., 2025).

Compared to previous forms of artificial intelligence, generative AI introduces several distinct privacy risks. Personal data can be included in training datasets without the explicit or informed consent of the individuals concerned; models may retain elements of such data and reproduce them in generated outputs; and users may disclose sensitive information through their prompts, which can be stored by providers and potentially used for further model development or training (Wang et al., 2025; Alzoubi et al., 2025; Takhshid, 2024).

Wang et al. (2025) provide a comprehensive overview of these privacy risks, classifying them into three main categories: data leakage from training datasets, model inversion attacks and inference attacks aimed at identifying sensitive personal attributes from model outputs. The relevance and implications of these risks may vary depending on the specific application of the consumer. Alzoubi et al. (2025) discuss differential privacy as a potential technical approach to mitigating such risks, while noting that its implementation in consumer-oriented generative AI systems often lacks transparency and remains difficult for users to assess or verify.

From a consumer perspective, awareness of these privacy risks remains limited. Dahabiyeh & Bouteraa (2026) investigate privacy awareness among ChatGPT users and find that even frequent users have a limited understanding of how their data are collected and processed, while greater awareness does not necessarily translate into protective behavior. These findings are consistent with the privacy paradox identified in previous research, although the discrepancy between privacy awareness and actual behavior may be particularly relevant in the context of generative AI due to the limited transparency surrounding how these systems process and use personal data.

In several sectors, privacy concerns are becoming an important factor influencing the adoption of generative AI. Arce-Urriza et al. (2025) show that incorporating privacy risk into consumer adoption models can improve their ability to explain and predict the acceptance of generative AI. In healthcare and mental healthcare, privacy concerns become particularly significant due to the sensitive nature of the information involved. Sobowale et al. (2025) find that the perceived benefits of continuous access to personalized medical or psychological information may be reduced by uncertainty regarding how disclosed data are stored, processed and subsequently used. Wamba-Taguimdje et al. (2024), Salih and Alharthi (2026) and Fakfare et al. (2025) identify similar considerations in marketing, hospitality and digital commerce, where consumer evaluations of generative AI are influenced not only by the quality of generated content but also by perceptions of how the underlying data are collected and managed.

Regulatory and critical perspectives provide additional insights into these privacy concerns. Carter (2025) describes generative AI as a new form of artificial intelligence surveillance and emphasizes the need for individuals to have greater control over their personal information, while Rosic and Schieke (2024), Shumate (2025) and Akakpo et al. (2025) address the legal and governance challenges associated with the use of generative AI in healthcare and mental healthcare contexts. Overall, these studies indicate that generative AI presents a distinct set of privacy concerns related to training data, the disclosure of personal information through prompts and the potential memorization of data by models based on artificial intelligence. These emerging concerns may not be fully addressed by existing privacy frameworks developed in the context of earlier applications based on artificial intelligence (Shin, 2025; Das, 2023; Martin & Zimmermann, 2024).

2.6. Privacy risks across the five AI categories

Comparative analysis of the five categories reveals a consistent pattern: privacy risk emerges as an important factor influencing consumer attitudes and behaviour, although its specific nature varies between technologies. Therefore, each form of AI is associated with a distinct privacy risk profile.

Non-physical AI, considered in broad terms, raises concerns primarily related to large-scale data aggregation, the opacity of algorithmic decision-making and the potential use of personal data for purposes beyond those initially disclosed (Martin & Zimmermann, 2024; Menard & Bott, 2025; Shin, 2025). Service robots introduce an additional physical dimension to these concerns. Their use of cameras, microphones and other sensors, combined with their presence in the consumer's immediate environment, can create a continuous observation that more closely resembles surveillance than conventional data processing (Hu et al., 2023; Song & Ahn, 2024; Lin et al., 2024).

In chatbots' case, privacy concerns are shaped by the dynamic nature of the interaction. Users' willingness to disclose personal information may evolve throughout the conversation, particularly when chatbots integrate humanlike characteristics that can encourage greater levels of self-disclosure (Kronemann et al., 2023; Greulich et al., 2025; Cheng & Jiang, 2020). Virtual assistants introduce additional privacy concerns related to voice data and the surrounding environment, as the collection and processing of voice data may also capture information related to tone and sounds from the

surrounding environment, introducing privacy considerations that are less prominent in screen-based interactions (Pal et al., 2021; Calahorra-Candao & Martín-de Hoyos, 2024; Guerreiro et al., 2022). Generative AI introduces additional privacy risks at multiple stages of data processing, including model training, user prompts and generated outputs. These risks are further intensified by the limited transparency surrounding the development of foundation models and the ways in which user data are collected, processed and potentially retained (Wang et al., 2025; Dahabiyeh & Bouteraa, 2026; Alzoubi et al., 2025).

The differences identified across the five categories demonstrate that privacy risks vary according to the characteristics and modes of interaction associated with each form of artificial intelligence. This supports the separate analysis of the five categories of artificial intelligence in the present study, as examining them collectively could obscure important differences in the nature and sources of privacy concerns. The theoretical perspectives discussed in this section provide the conceptual foundation for interpreting the VOSviewer keyword analysis presented in the following section.

3. Research methodology

The objective of this research is to evaluate the different directions and keyword associations of published articles related to privacy risks and different forms of AI. In order to achieve this objective, 5 searches were performed on the Web of Science based on the keywords “privacy risks”, “consumer” and one of the following AI types: “artificial intelligence”, “robots”, “chatbots”, “virtual assistants” and “generative AI”.

The search resulted in 293 documents (7.04.2026) for the key terms “privacy risks”, “consumers” and artificial intelligence”, 102 documents (7.04.2026) for the key term combination “privacy risks”, “consumers”, and “robots”, 121 documents (7.04.2026) for the key term combination “privacy risks”, “consumers” and “chatbots”, 113 documents (7.04.2026) for the key word combination “Privacy risks”, “consumers” and “virtual assistants” and 127 documents (7.04.2026) for the key word combination “privacy risks”, “consumers”, “generative AI”. The search for the keyword service robots indicated similar results as in the case of robots, and for this reason they were not analyzed as a separate category.

The results were exported from Web of Science and analyzed with the help of VOSviewer. For all five search results, the VOS analysis was performed based on keyword co-occurrence. Using full counting, only keywords with 5 appearances were considered.

The VOS Viewer analysis indicated that for the keyword combination “privacy risks”, “consumers” and artificial intelligence”, out of the 1529 key words, only 93 reached the threshold of 5 appearances. For the key word combination “privacy risks”, “consumers”, and “robots”, out of the 454 key words, only 21 reached the threshold of 5 appearances. This shows a higher dispersion of key words and research directions. For the key words “privacy risks”, “consumers” and “chatbots”, out of the 633 key words, only 40 reached the threshold of 5 appearances, having a similar result as in the case of robots. For “privacy risks”, “consumers” and “virtual assistants”, out of the 652 key words, only 43 reached the threshold of 5 appearances, while for “privacy risks”, “consumers”, “generative AI”, out of the 609 key words, only 25 reached the threshold

of 5 appearances. In the following, we present a deeper analysis of the results is presented. The number of articles and keywords used for each of the five analyses are presented in Table no. 1.

Table no. 1. Number of articles used in the VOS Viewer analysis

Keyword combination	Articles resulted from Web of Science search (7.04.2026)	Keywords based on full counting in VOSviewer	Keywords with a minimum of 5 appearances
Privacy risks, consumers, AI	293	1529	93
Privacy risks, consumers, robots	102	454	21
Privacy risks, consumers, chatbots	121	633	40
Privacy risks, consumers, virtual assistants	113	652	43
Privacy risks, consumers, generative AI	127	609	25

Source: Author's own research

4. Results and discussions

The analysis starts with a comparative analysis of the number of articles published based on the keyword combination “privacy risks”, “consumer” and topics such as artificial intelligence, robots, chatbots, virtual assistants and generative AI. With the help of Figure 1, we observe that, starting in 2021, more and more articles were published for the different types of AI, but most of them were on the topic of artificial intelligence. We can see that the interest in artificial intelligence and certain types of artificial intelligence has increased over the years. It can also be seen that in 2025 the number of publications on the topic of artificial intelligence reached its highest level ever. Today, artificial intelligence is increasingly used in more and more fields, and the interest in this topic is growing more and more.

The number of publications with keywords “privacy risks”, “consumer” and “artificial intelligence” has increased significantly in the last 5 years, showing increased interest in this topic. In 2025, it reached its highest peak with a number of 89 publications. The large number of publications in this field is not accidental because in the last 5 years, artificial intelligence has developed at an accelerated pace, bringing with it both opportunities and risks for consumers. Now AI is present almost everywhere, collecting more and more personal data about users, which poses a risk to their privacy because AI not only collects personal data, it also creates complex reasoning for them, which can lead to increased dangers when it comes to user privacy.

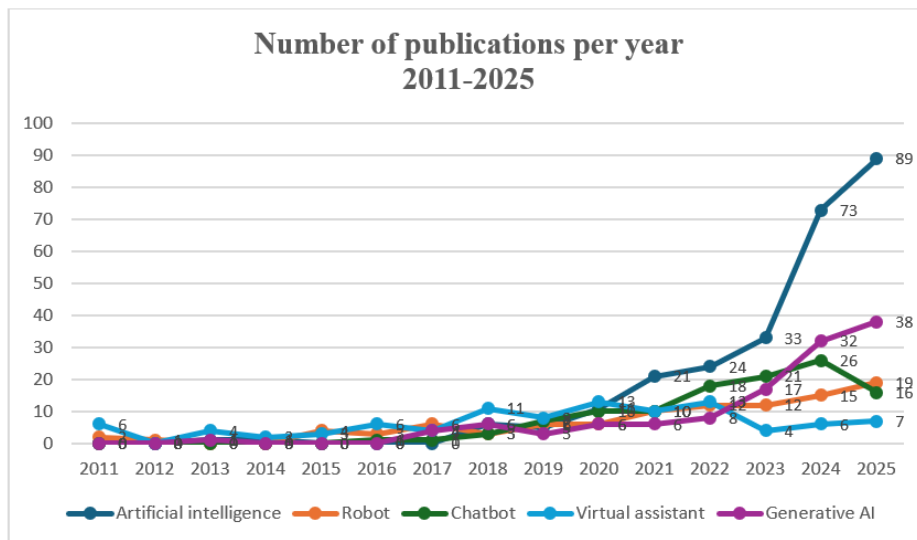


Figure no. 1: Number of publications per year (2011-2025) for the keyword combination “privacy risks”, “consumer” and one form of AI

Source: Author’s own research

The number of publications for the keyword combination “privacy risks”, “consumers” and “robots” has grown in recent years. Starting from 2011 and up to 2025, we observe that the number of publications on different types of AI has increased steadily, as the technology has developed more and more rapidly. At the same time, the increased interest in research in this field has been stimulated by the expansion of AI into more and more fields, with companies investing more in different types of AI. After 2022, the introduction of Generative Artificial Intelligence models (example: ChatGPT), has considerably stimulated scientific curiosity, leading to a rapid expansion of publications. The interest in the topic of “privacy risks”, “consumers” and “chatbots” has also increased since 2018, leading to more published articles. Chatbots and virtual assistants are increasingly being used in customer interactions, making this topic of great interest to researchers. With the increasing use of these types of AI by consumers, various researchers have begun to study the effects of these technologies on personal data security, information protection and user trust. With the rapid advancement of generative artificial intelligence models, concerns about privacy, data use and ethical consequences have also intensified, which has led researchers to study and publish more and more on this topic.

The number of publications based on “privacy risks”, “consumer” and “virtual assistants” has fluctuated from year to year. Here we can no longer talk about an increase in interest in this topic, because these fluctuations result from the phases of development and curiosity around virtual assistants. Initially, when virtual assistants were introduced, their use was limited, which restricted research in this area. With the emergence and widespread adoption of virtual assistants (such as Siri, Alexa, etc.), there

has been an increase in the number of studies, against the backdrop of issues related to personal data protection, security, and consumer trust. When an innovation or debate appears in the field of virtual assistants, researchers' interest in this topic increases, and when it is considered that virtual assistants have already become better known and everything is stable, interest in this field decreases.

The number of publications on the topic of “privacy risks”, “consumer” and “generative AI” have also grown and it can be observed that in 2025 most articles on this topic were published (38 articles). During the period 2004–2026, different types of AI developed rapidly and AI-based applications were used more frequently by consumers. As mentioned above, after 2022 several models of generative artificial intelligence were developed, which made this topic of great interest to researchers. With this development, there was an increase in interest in concerns related to personal data protection, privacy, information security and responsible use of AI-generated content. These challenges have stimulated researchers' interest in analyzing risks to privacy and consumer behavior, which has led to a significant increase in the number of publications in this field.

In the following, the word clusters for each of the five types of analysis are presented. Figure 2 represents a concept map extracted from VOSviewer for combining the terms “privacy risks”, “consumer” and “artificial intelligence”. This map was created based on the terms that appear most frequently. Analyzing Figure no 2, it can be observed that the larger nodes are associated with keywords that appear more often in publications on this topic. The connections also show how strong the link between these concepts is. Terms such as “artificial intelligence”, “technology”, “trust”, and “risk” are the most frequently used in the analyzed literature.

Based on the results, we found 5 clusters of keywords associated with “privacy risks”, “consumer”, and “AI”, which are depicted in Figure no 2 and Table no 2. In the middle of the network is the keyword “artificial intelligence,” which has the most connections to the other key terms. The red cluster is related to privacy and data protection containing key terms such as “privacy”, “data protection”, “security”, “ethics”, “machine learning”. The blue cluster focuses on customers, trust, and technology integration containing keywords such as “trust”, “technology”, “consumer”, “chatbots”, “voice assistants”. The green cluster highlights user behavior and information exchange processes and it includes keywords such as “consumers”, “information”, “perceptions” or “disclosure”. The yellow cluster focuses on technology acceptance and adoption patterns, including key terms like “user acceptance” or “information technology”. The five clusters of keywords emphasize how consumers interact with artificial intelligence, how much trust they can have in it, and how confidential the data it takes over are.

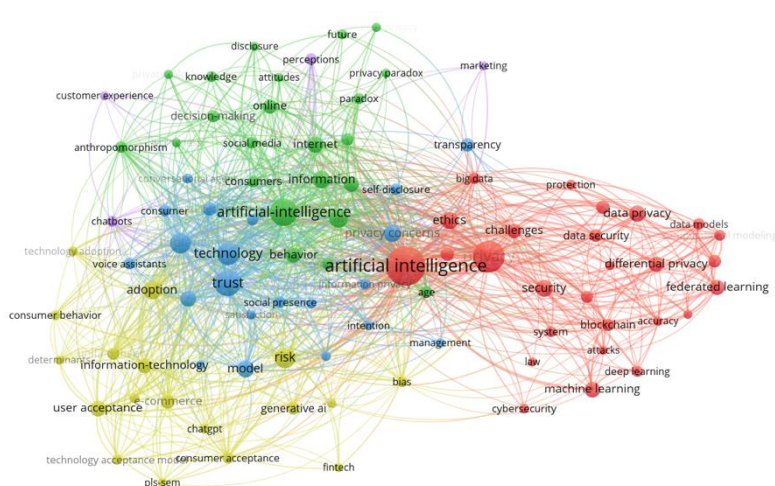


Figure no. 2: VOSviewer results based on the keyword combination "privacy risks", "consumer" and "artificial intelligence"

Source: Author's own research

Table no. 2. VOSviewer clusters for keyword combination “privacy risks”, “consumer” and “artificial intelligence”

	Word clusters for “privacy risks”, “consumer” and “artificial intelligence”
Cluster 1 (27 items)	accuracy, artificial intelligence, attacks, big data, blockchain, challenges, computational modelling, consumer electronics, cybersecurity, data models, data privacy, data protection, data security, deep learning, differential privacy, ethics, federated learning, framework, internet of things, law, machine learning, privacy, privacy protection, protection, security, system, training
Cluster 2 (23 items)	age, AI, anthropomorphism, artificial intelligence, attitudes, behavior, consumer privacy, consumers, decision-making, disclosure, future, impact, information, internet, knowledge, online, paradox, personalization, privacy calculus, privacy paradox, services, social media, willingness
Cluster 3 (21 items)	acceptance, antecedents, artificial intelligence, consumer, conversational agent, electronic commerce, engagement, information privacy, intention, management, model, perceived risk, privacy concerns, quality, satisfaction, self-disclosure, social presence, technology, transparency, trust, voice assistants
Cluster 4 (18 items)	adoption, bias, chatgpt, consumer acceptance, consumer behavior, determinants, e-commerce, fintech, generative AI, information-technology, pls-sem, privacy risk, risk, technology acceptance, technology adoption, unified theory, user acceptance
Cluster 5 (4 items)	chatbots, customer experience, marketing, perceptions

Source: Author's own research

Based on the results obtained from VOSviewer, we created a co-occurrence map based on the combination of “privacy risks”, “consumer” and “robots”. It can be seen that terms such as “privacy”, “trust”, “human-robot interaction”, and “acceptance” are most

frequently in the analyzed literature. The analysis revealed 3 clusters of keywords associated with the search terms “privacy risks”, “consumers” and “robots”, which we can see in Figure no 3 and Table no. 3. The red group emphasizes key words such as “privacy”, “technological innovation”, “ethical principles” and “acceptance models”. The blue cluster emphasizes the importance of “trust”, “social robots” and “user availability”. The green cluster focuses on “artificial intelligence”, “data protection”, “human-robot interactions” and “information transfer”. The yellow group links the dimensions related to “acceptance of technologies” and “artificial intelligence”.

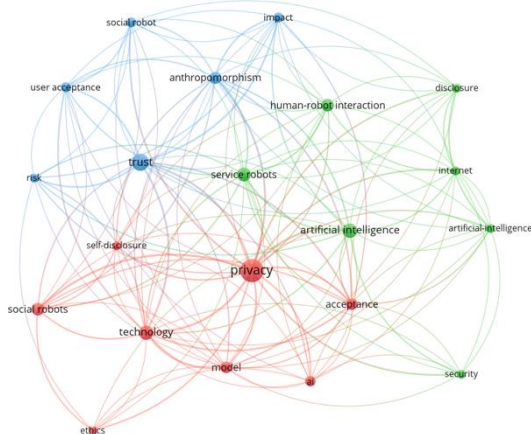


Figure no. 3: VOSviewer results based on the keyword combination "privacy risks", "consumer" and "robots"

Source: Author's own research

Table 3: VOSviewer clusters for keyword combination "privacy risks", "consumer" and "robots"

Word clusters for "privacy risks", "consumer" and, robots"	
Cluster 1 (8 items)	acceptance, AI, ethics, model, privacy, self-disclosure, social robots, technology
Cluster 2 (7 items)	artificial intelligence, artificial-intelligence, disclosure, human-robot interaction, internet, security, service robots
Cluster 3 (6 items)	anthropomorphism, impact, risk, social robot, trust, user acceptance

Source: Author's own research

The next co-occurrence map refers to the keyword combination “privacy risks”, “consumer”, “chatbots”. It can be seen that terms such as “acceptance”, “trust”, “perceived risk”, “artificial intelligence”, “chatbot”, “technology” are most frequently used in the analyzed literature. Based on the results, we discovered 4 clusters of keywords associated with these search terms, and they can be seen in Figure no 4 and Table 4. The green cluster focuses on “chatbots”, “artificial intelligence”, “ChatGPT”

and “generative AI”, highlighting the growing interest in AI-based communication technologies. The red cluster focuses on privacy issues, including keywords like “privacy concerns”, “social presence” and “technological issues” related to the use of chatbots. The blue cluster highlights factors affecting user adoption and satisfaction, such as “trust level”, “perceived risk” and “willingness to use”. The yellow cluster encompasses concepts related to “technology acceptance”, “consumers and information systems”.

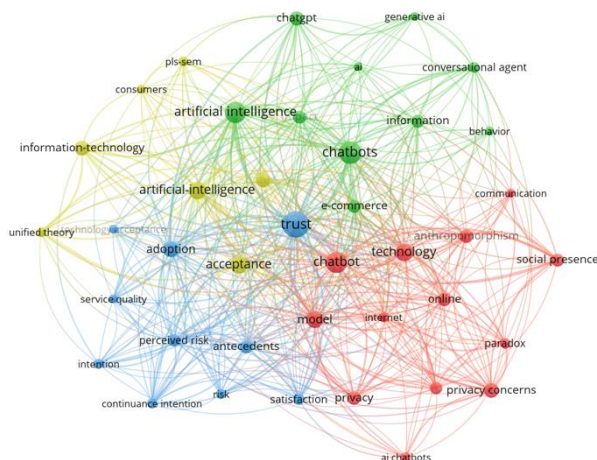


Figure 4. VOSviewer results based on the keyword combination "privacy risks", "consumer" and "chatbots"

Source: Author's own research

Table 4: VOSviewer clusters for keyword combination "privacy risks", "consumer" and "chatbots"

Word clusters for "privacy risks", "consumer" and, chatbots"	
Cluster 1 (13 items)	AI chatbots, anthropomorphism, chatbot, communication, internet, model, online, paradox, privacy, privacy concerns, self-disclosure, social presence, technology
Cluster 2 (10 items)	AI, artificial intelligence, behavior, chatbots, chatgpt, conversational agent, e-commerce, generative AI, impact, information
Cluster 3 (10 items)	adoption, antecedents, continuance intention, intention, preceived risk, risk, satisfaction, service quality, technology acceptance, trust
Cluster 4 (7 items)	acceptance, artificial intelligence, consumers, information-technology, pls-sem, unified theory, user acceptance

Source: Author's own research

The co-occurrence results for the keywords “privacy risks”, “consumer” and “virtual assistants” show that terms such as “privacy”, “trust”, “personalisation”, “adoption”, “model”, “data privacy” are the most frequently used in the analyzed literature. Based on the results, we discovered 4 clusters of keywords that can be seen in Figure no 5 and

Table 5. The red cluster focuses on “data security”, “protection”, “information disclosure” and “consumer privacy”. The green cluster focuses on “user trust”, “user behavior” and the “privacy paradox”. The blue cluster gathers ideas about “technology acceptance”, “e-commerce” and “perceived risks”. Finally, the yellow cluster integrates aspects related to “information management”, “communication” and the effect on users.

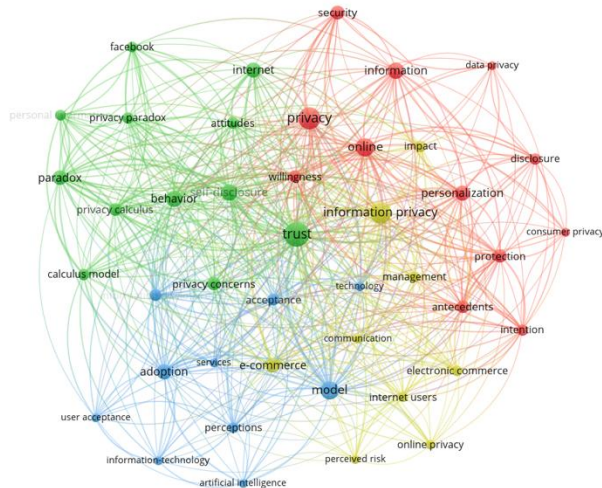


Figure no 5. VOSviewer results based on the keyword combination "privacy risks", "consumer" and "virtual assistants"

Source: Author's own research

Table 5: VOSviewer clusters for keyword combination “privacy risks”, “consumer” and “virtual assistants”

Word clusters for “privacy risks”, “consumer” and, virtual assistants”	
Cluster 1 (12 items)	antecedents, consumer privacy, data privacy, disclosure, information, intention, online, personalisation, privacy, protection, security, willingness
Cluster 2 (12 items)	attitudes, behavior, calculus model, Facebook, internet, paradox, personal information, privacy calculus, privacy, concerns, privacy paradox, self-disclosure, trust
Cluster 3 (10 items)	acceptance, adoption, artificial intelligence, information disclosure, information-technology, model, perceptions, services, technology, user acceptance
Cluster 4 (9 items)	communication, e-commerce, electronic commerce, impact, information privacy, internet users, management, online privacy, perceived risk

Source: Author's own research

The VOSviewer results for “privacy risks”, “consumer” and “generative AI” show that terms such as “privacy”, “artificial intelligence”, “trust”, “machine learning” are the most frequently used in the analyzed literature. The results reveal 4 clusters of keywords associated with the search terms “privacy risks”, “consumer”, “generative AI”, which can be seen in Figure no 6 and Table 6. The blue cluster includes keywords such as “trust”, “privacy concerns” and “information”, highlighting the significance of trust and

data management in the context of artificial intelligence usage. The green cluster relates to “machine learning”, “data privacy”, “information protection” and “differential privacy”, emphasizing concerns regarding data security and the protection of AI systems. The red cluster focuses on “generative artificial intelligence”, “ChatGPT”, “consumers” and “technology acceptance”. The yellow cluster links the concepts of “privacy” and “security”, underscoring the relevance of these topics as essential elements. The various connections between the clusters suggest that contemporary studies on artificial intelligence integrate both technical components and issues related to privacy, security, and user reception of the technology.

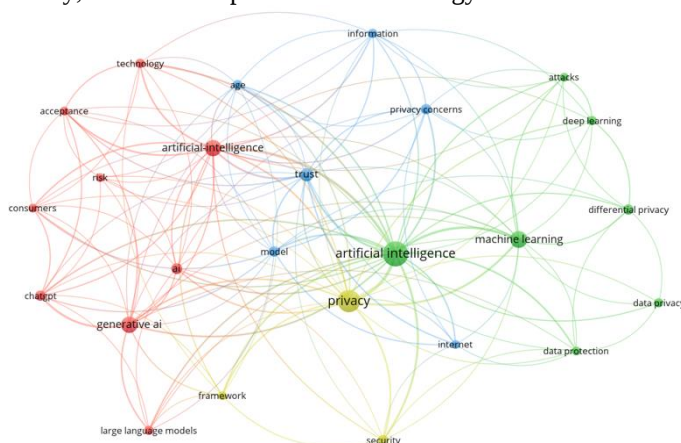


Figure 6. VOSviewer results based on the keyword combination "privacy risks", "consumer" and "generative AI"

Source: Author's own research

Table 6: VOSviewer clusters for keyword combination "privacy risks", "consumer" and "generative AI"

Word clusters for "privacy risks", "consumer" and, generative AI"	
Cluster 1 (9 items)	acceptance, AI, artificial-intelligence, chatgpt, consumers, generative AI, large language models, risk, technology
Cluster 2 (7 items)	artificial intelligence, attacks, data privacy, data protection, deep learning, differential privacy, machine learning
Cluster 3 (6 items)	age, information, internet, model, privacy concerns, trust
Cluster 4 (3 items)	framework, privacy, security

Source: Author's own research

In order to compare the results of the five analyzes, the keyword groups identified in each search were examined together. The results show several common topics across all five analyses. Keywords such as “privacy”, “trust”, “acceptance”, and “technology”, as well as terms related to artificial intelligence, appear in all five analyses. Terms related

to risk, including “risk”, “perceived risk”, and “privacy concerns”, are also found in the five groups of results. These similarities show that, regardless of the form of artificial intelligence analysed, research on privacy risks is closely linked to topics such as trust and technology acceptance. This suggests that these topics play an important role in research on consumer interactions with artificial intelligence.

At the same time, the five analyses show clear differences in the topics associated with each form of artificial intelligence. The network for robots is the only one that includes terms related to physical and social interaction, such as “human-robot interaction”, “social robots”, and “service robots”. The chatbot network includes terms related to communication and interaction, such as “social presence”, “conversational agent”, “communication”, and “satisfaction”. In virtual assistants’s case, terms such as “privacy calculus”, “privacy paradox”, “personalization”, and “information disclosure” show that the literature focuses more on the relationship between the benefits of personalization and the disclosure of personal information. The generative AI network, together with the broader artificial intelligence network, also includes a separate group of technical terms, such as “machine learning”, “deep learning”, “differential privacy”, “data protection”, and “attacks”. This shows that research on generative AI also addresses technical aspects related to data security. The terms related to humanlike interaction, such as “anthropomorphism” and “self-disclosure”, appear in artificial intelligence, robot, and chatbot networks, but not in the generative AI network, where greater attention is paid to “large language models” and the security of the data used to develop these systems.

The comparison also shows differences in the number and variety of keywords identified across the five analyses. The broader artificial intelligence search produced the largest number of keywords above the selected threshold, 93, while the robot search produced only 21. This difference shows that some forms of artificial intelligence have been studied from a wider range of perspectives than others. Another relevant result is the presence of the terms “ChatGPT” and “generative AI” not only in the generative AI network, but also in the broader artificial intelligence and chatbot networks. This suggests that generative AI is becoming increasingly present in other areas of research on artificial intelligence. Overall, the results support the decision to examine the five forms of artificial intelligence separately. Although the analyses share several common topics related to privacy, trust, acceptance, and data protection, each form of artificial intelligence is also associated with specific privacy concerns that may not be clearly identified when all five forms are analyzed together.

Conclusions

In conclusion, the results reveal that the use of artificial intelligence, chatbots, virtual assistants and generative AI is largely influenced by aspects such as user trust, data protection and acceptance of technology. Therefore, from the financial sector perspective, financial institutions should pay special attention to strengthening data protection measures, as privacy concerns are one of the most important obstacles to implementing solutions using artificial intelligence. At the same time, chatbots and virtual assistants must be implemented in an ethical manner that ensures the provision of quality services, without affecting the security of users' financial data. To create

leadership strategies and ethical principles for the application of generative artificial intelligence, to reduce the risks related to mistakes, false information and improper data manipulation, financial institutions must develop various governance and ethics policies for the use of generative AI.

In this research, we observe that trust and acceptance play a very important role for consumers, which means that financial institutions must ensure compliance with data protection and artificial intelligence regulations to guarantee that legislation is respected and to strengthen customer credibility in the field of digital financial services.

These results also have important implications for the financial sector. The terms related to trust, acceptance, and data protection, which appear in all five analyses, indicate that these factors are important for the adoption of artificial intelligence in financial services, regardless of the technology used. This is also supported by the presence of terms such as “fintech” and “e-commerce” in the broader artificial intelligence network. Banks and other financial institutions already use chatbots for customer service, virtual assistants in mobile banking, and artificial intelligence for fraud detection (Alt et al., 2021; Awosika et al., 2024). However, the differences identified across the five analyses show that privacy measures should be adapted to the type of technology used. For chatbots, it is important that customers to understand how the personal information shared during conversations is stored and used. Virtual assistants raise additional concerns related to the processing of voice data, while generative AI requires clear rules regarding the information provided by users and the content generated for customers.

Finally, we can say that the successful implementation of artificial intelligence in all areas depends on efficient management of privacy, security and ethics issues, technological performance and consumer trust.

References

- [1] Aiolfi, S., Bellini, S., & Grandi, B., 2023. How shopping habits change with artificial intelligence: smart speakers' usage intention. *International Journal of Retail & Distribution Management*, 51(9-10), 1288–1312. <https://doi.org/10.1108/IJRDM-11-2022-0441>
- [2] Akakpo, A., Gyasi, E.A., Oduro, B., & Akpabot, S., 2025. Artificial Intelligence (AI) and the Future of Information Privacy: Expert Viewpoints. *Journal of Global Information Management*, 33(1). <https://doi.org/10.4018/JGIM.383050>
- [3] Alhitmi, H.K., Mardiah, A., Al-Sulaiti, K.I., & Abbas, J., 2024. Data security and privacy concerns of AI-driven marketing in the context of economics and business field: An exploration into possible solutions. *Cogent Business & Management*, 11(1), 2393743. <https://doi.org/10.1080/23311975.2024.2393743>
- [4] Alt, M.A., Vizeli, I., & Saplacan, Z., 2021. Identifying relevant segments of potential banking chatbot users based on technology adoption behavior. *Market-Tržište*, 33(2), 165–183. <https://doi.org/10.22598/mt/2021.33.2.165>
- [5] Alzoubi, Y.I. & Mishra, A., 2025. Differential privacy and artificial intelligence: potentials, challenges, and future avenues. *EURASIP Journal on Information Security*, 18. <https://doi.org/10.1186/s13635-025-00203-9>

- [6] Anic, I.D., Budak, J., Rajh, E., Recher, V., Škare, V., & Škrinjarić, B., 2019. Extended model of online privacy concern: what drives consumers' decisions? *Online Information Review*, 43(5), 799–817. <https://doi.org/10.1108/OIR-10-2017-0281>
- [7] Arce-Urriza, M., Chocarro, R., Cortiñas, M., & Marcos-Matas, G., 2025. From familiarity to acceptance: The impact of Generative Artificial Intelligence on consumer adoption of retail chatbots. *Journal of Retailing and Consumer Services*, 84, 104234. <https://doi.org/10.1016/j.jretconser.2025.104234>
- [8] Awosika, T., Shukla, R.M., & Pranggono, B., 2024. Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection. *IEEE Access*, 12, 64551–64560. <https://doi.org/10.1109/ACCESS.2024.3394528>
- [9] Bandara, R., Fernando, M., & Akter, S., 2020. Privacy concerns in E-commerce: A taxonomy and a future research agenda. *Electronic Markets*, 30(3), 629–647. <https://doi.org/10.1007/s12525-019-00375-6>
- [10] Bhojwani, R., & Ranjan, R., 2026. Role of artificial intelligence on consumer buying behavior: the dual effects of AI-enabled features on decision-making and trust. *Journal of Research in Interactive Marketing*. <https://doi.org/10.1108/JRIM-11-2025-0702>
- [11] Calahorra-Candao, G., & Martín-de Hoyos, M.J., 2024. From Typing to Talking: Unveiling AI's Role in the Evolution of Voice Assistant Integration in Online Shopping. *Information*, 15(4), 202. <https://doi.org/10.3390/info15040202>
- [12] Carter, C., 2025. AI surveillance: Reclaiming privacy through informational control. *European Labour Law Journal*, 16(4), 492–514. <https://doi.org/10.1177/20319525241306327>
- [13] Cheng, Y., & Jiang, H., 2020. How Do AI-driven Chatbots Impact User Experience? Examining Gratifications, Perceived Privacy Risk, Satisfaction, Loyalty, and Continued Use. *Journal of Broadcasting & Electronic Media*, 64(4), 592–614. <https://doi.org/10.1080/08838151.2020.1834296>
- [14] Chien, S.Y., Lin, Y.L., Luo, J.T., & Chan, Y.C., 2025. Exploring the Antecedents and Consequences of Privacy Concerns: A Comparison of Humanoid Robot to Tablet. *Expert Systems*, 42(10), e70132. <https://doi.org/10.1111/exsy.70132>
- [15] Cho, J.Y., Ko, D., & Lee, B.G., 2018. Strategic Approach to Privacy Calculus of Wearable Device User Regarding Information Disclosure and Continuance Intention. *KSII Transactions on Internet and Information Systems*, 12(7), 3356–3374. <https://doi.org/10.3837/tjis.2018.07.022>
- [16] Chuah, S.H.W., Aw, E.C.X., & Yee, D., 2021. Unveiling the complexity of consumers' intention to use service robots: An fsQCA approach. *Computers in Human Behavior*, 123, 106870. <https://doi.org/10.1016/j.chb.2021.106870>
- [17] Dahabiyeh, L., & Bouteraa, M., 2026. Privacy awareness in generative AI: the case of ChatGPT. *Interactive Technology and Smart Education*, 23(1), 28–47. <https://doi.org/10.1108/ITSE-01-2025-0009>
- [18] Das, S., 2023. Privacy in the Age of AI. *Communications of the ACM*, 66(11), 29–31. <https://doi.org/10.1145/3625254>
- [19] Davenport, T., Guha, A., Grewal, D., & Bressgott, T., 2020. How artificial intelligence will change the future of marketing. *Journal of the Academy of Marketing Science*, 48(1), 24–42. <https://doi.org/10.1007/s11747-019-00696-0>

- [20] Du, H.Y., Xu, L., & Wang, S.B., 2025. Artificial intelligence in hospitality services: examining consumers' receptivity to unmanned smart hotels. *Journal of Hospitality and Tourism Insights*, 8(11). <https://doi.org/10.1108/JHTI-10-2024-1092>
- [21] Elliott, D., & Soifer, E., 2022. AI Technologies, Privacy, and Security. *Frontiers in Artificial Intelligence*, 5, 826737. <https://doi.org/10.3389/frai.2022.826737>
- [22] Fakfare, P., Promsivapallop, P., Ponsignon, F., Manosuthi, N., & Kim, J.J., 2025. Exploring the drivers of hospitality and tourism customer loyalty for generative artificial intelligence (AI): a multi-analytic approach. *Current Issues in Tourism*. <https://doi.org/10.1080/13683500.2025.2500726>
- [23] Frank, B., 2024. Consumer preferences for artificial intelligence-enhanced products: Differences across consumer segments, product types, and countries. *Technological Forecasting and Social Change*, 209, 123774. <https://doi.org/10.1016/j.techfore.2024.123774>
- [24] Greilich, A., Bremser, K., & Wuest, K., 2025. Consumer Response to Anthropomorphism of Text-Based AI Chatbots: A Systematic Literature Review and Future Research Directions. *International Journal of Consumer Studies*, 49(5), e70108. <https://doi.org/10.1111/ijcs.70108>
- [25] Guerreiro, J., Loureiro, S.M.C., & Ribeiro, C., 2022. Advertising acceptance via smart speakers. *Spanish Journal of Marketing - ESIC*, 26(3). <https://doi.org/10.1108/SJME-02-2022-0028>
- [26] Gupta, S., Modgil, S., & Kushwaha, A., 2025. AI feel millennials: prioritizing the intentions towards adoption of AI-enabled chatbots using fuzzy-AHP approach. *Journal of Science and Technology Policy Management*. <https://doi.org/10.1108/JSTPM-09-2023-0159>
- [27] Henkens, B., Schultz, C.D., De Keyser, A., & Mahr, D., 2026. The sound of progress: AI voice agents in service. *Journal of Service Management*, 37(1), 1–24. <https://doi.org/10.1108/JOSM-06-2025-0269>
- [28] Hu, Y.U., Min, H., & Su, N., 2023. The dark side of artificial intelligence in service: The watching-eye effect and privacy concerns. *International Journal of Hospitality Management*, 110, 103437. <https://doi.org/10.1016/j.ijhm.2023.103437>
- [29] Kim, T.W., Jiang, L., Duhachek, A., Lee, H., & Garvey, A., 2022. Do You Mind if I Ask You a Personal Question? How AI Service Agents Alter Consumer Self-Disclosure. *Journal of Service Research*, 25(4), 649–666. <https://doi.org/10.1177/10946705221120232>
- [30] Kronemann, B., Kizgin, H., Rana, N., & Dwivedi, Y.K., 2023. How AI encourages consumers to share their secrets? The role of anthropomorphism, personalisation, and privacy concerns and avenues for future research. *Spanish Journal of Marketing - ESIC*, 27(1), 3–19. <https://doi.org/10.1108/SJME-10-2022-0213>
- [31] Li, J.J., & Zhang, J., 2023. Determinants Affecting Consumer Trust in Communication With AI Chatbots: The Moderating Effect of Privacy Concerns. *Journal of Organizational and End User Computing*, 35(1). <https://doi.org/10.4018/JOEUC.328089>
- [32] Lin, B., Lee, W., Wise, N., & Choi, H.C., 2024. Consumers' Ethical Perceptions of Autonomous Service Robots in Hotels. *Journal of Hospitality & Tourism Research*. <https://doi.org/10.1177/10963480231194693>

- [33] Martin, K.D., & Zimmermann, J., 2024. Artificial intelligence and its implications for data privacy. *Current Opinion in Psychology*, 58, 101829. <https://doi.org/10.1016/j.copsyc.2024.101829>
- [34] Menard, P., & Bott, G.J., 2025. Artificial intelligence misuse and concern for information privacy: New construct validation and future directions. *Information Systems Journal*, 35(4), 1341–1393. <https://doi.org/10.1111/isj.12544>
- [35] Morales-Muñoz, A., Iniesta-Bonillo, M.A., Estrella-Ramón, A., & Herrada-Lores, S., 2026. Artificial Intelligence and Consumer Behaviour in Social Media: Systematic Literature Review and Future Research Agenda. *International Journal of Consumer Studies*, 50(1), e70173. <https://doi.org/10.1111/ijcs.70173>
- [36] Pal, D., Babakerkhell, M.D., & Zhang, X.M., 2021. Exploring the Determinants of Users' Continuance Usage Intention of Smart Voice Assistants. *IEEE Access*, 9, 162259–162275. <https://doi.org/10.1109/ACCESS.2021.3131848>
- [37] Pelau, C., Dabija, D.C., & Stanescu, M. 2024. Can I trust my AI friend? The role of emotions, feelings of friendship and trust for consumers' information-sharing behavior toward AI, *Oeconomia Copernicana*, 15(2), 407–433, 3, <https://doi.org/10.24136/oc.2916>
- [38] Prakash, A.V., Joshi, A., Nim, S., & Das, S., 2023. Determinants and consequences of trust in AI-based customer service chatbots. *Service Industries Journal*, 43(9–10), 642–675. <https://doi.org/10.1080/02642069.2023.2166493>
- [39] Prakash, A.V., Das, S., & Pillai, K.R., 2020. Intelligent Conversational Agents in Mental Healthcare Services: A Thematic Analysis of User Perceptions. *Pacific Asia Journal of the Association for Information Systems*, 12(2), 1–34. <https://doi.org/10.17705/1pais.12201>
- [40] Puertas, S.M., Aguilar-Illescas, R., Molinillo, S., & Anaya-Sánchez, R., 2024. Purchase intentions in a chatbot environment: An examination of the effects of customer experience. *Oeconomia Copernicana*, 15(2), 653–686. <https://journals.economic-research.pl/oc/article/view/2914>
- [41] Rosic, A., & Schieke, S.M., 2024. Legal implications of artificial intelligence in health care. *Clinics in Dermatology*, 42(5), 451–458. <https://doi.org/10.1016/j.clindermatol.2024.08.004>
- [42] Salih, L., & Alsmairat, M.A.K., 2025. AI-Enabled Service Continuance: Roles of Trust and Privacy Risk. *Journal of Computer Information Systems*. <https://doi.org/10.1080/08874417.2025.2484928>
- [43] Salih, S., & Alharthi, S., 2026. From ideation to execution: Unleashing the power of generative AI in modern digital marketing and customer engagement - A systematic literature review and case study. *Array*, 25, 100404. <https://doi.org/10.1016/j.array.2025.100404>
- [44] Sebastián, M.G.D., Guede, J.R.S., & Antonovica, A., 2022. Application and extension of the UTAUT2 model for determining behavioral intention factors in use of the artificial intelligence virtual assistants. *Frontiers in Psychology*, 13, 993935. <https://doi.org/10.3389/fpsyg.2022.993935>
- [45] Shin, D., 2025. Privacy Decision Making in Artificial Intelligence. *Computer*, 58(9), 94–100. <https://doi.org/10.1109/MC.2024.3509498>

- [46] Shumate, J.N., 2025. Governing AI in Mental Health: 50-State Legislative Review. *JMIR Mental Health*, 12, e80739. <https://doi.org/10.2196/80739>
- [47] Siminica, M., Zaharia, A., Ladaru, G.R., Cîrciumaru, D., & Dobrota, C.E. 2025. Determinants of the actual financial knowledge – multivariate logistic regression. *Journal of Applied Economics*, 28(1). <https://doi.org/10.1080/15140326.2025.2482546>
- [48] Sobowale, K., Humphrey, D.K., & Zhao, S.Y., 2025. Evaluating Generative AI Psychotherapy Chatbots Used by Youth: Cross-Sectional Study. *JMIR Mental Health*, 12, e79838. <https://doi.org/10.2196/79838>
- [49] Song, B., & Ahn, Y., 2024. How to calculate privacy: privacy concerns and service robots' use intention in hospitality. *Current Issues in Tourism*, 27(21), 3401–3417. <https://doi.org/10.1080/13683500.2023.2265029>
- [50] Song, M., Du, J., Xing, X., & Mou, J., 2022a. Should the chatbot "save itself" or "be helped by others"? The influence of service recovery types on consumer perceptions of recovery satisfaction. *Electronic Commerce Research and Applications*, 55, 101199. <https://doi.org/10.1016/j.elerap.2022.101199>
- [51] Song, M., Xing, X., Duan, Y., Cohen, J., & Mou, J., 2022b. Will artificial intelligence replace human customer service? The impact of communication quality and privacy risks on adoption intention. *Journal of Retailing and Consumer Services*, 66, 102900. <https://doi.org/10.1016/j.jretconser.2022.102900>
- [52] Spais, G., & Chryssochoidis, G., 2025. Trends and future of artificial intelligence (AI), machine learning (ML) algorithms, and data analytics and their applications and implications for digital marketing and digital promotions. *Journal of Marketing Analytics*, 13(2). <https://doi.org/10.1057/s41270-025-00406-6>
- [53] Takshid, Z. (2024). Data as Likeness. *Georgetown Law Journal*, 112(5), 1061–1121.
- [54] Véliz, C. (2023). Artificial Intelligence and Data Harvesting: An Interview with Carissa Véliz. *Think - Philosophy for Everyone*, 22(65), 33–39. <https://doi.org/10.1017/S1477175622000215>
- [55] Wamba-Taguimdje, S.L., Wamba, S.F., Kamdjoug, J.R.K., & Tchatchouang Wanko, C.E., 2024. Why Should Users Take the Risk of Sustainable Use of Generative Artificial Intelligence Chatbots: An Exploration of ChatGPT's Use. *Journal of Global Information Management*, 32(1). <https://doi.org/10.4018/JGIM.365600>
- [56] Wang, T., Zhang, Y., Qi, S., Zhao, R., Xia, Z., & Weng, J., 2025. Security and Privacy on Generative Data in AIGC: A Survey. *ACM Computing Surveys*, 57(4), 101. <https://doi.org/10.1145/3703626>
- [57] Yang, M., & Wang, M., 2025. How AI service quality influence brand loyalty: moderating effects of innovativeness, brand ethicality, and privacy concern. *Journal of Brand Management*, 32(4), 282–297. <https://doi.org/10.1057/s41262-025-00383-2>