Journal of Organizational and End User Computing
Volume 35 • Issue 1

Uncovering the Dark Side of Artificial Intelligence in Electronic Markets:
A Systematic Literature Review

Yunfei Xing, Jilin University, China

Lu Yu, Zhejiang University, China

Justin Z. Zhang, University of North Florida, USA*

https://orcid.org/0000-0002-4074-9505

Leven J. Zheng, Hong Kong Metropolitan University, Hong Kong

ABSTRACT

The dark sides of artificial intelligence (AI) have attracted immense attention in recent years. This study produces a synthesis of current research on six dark sides of AI in electronic markets through a systematic literature review. The authors searched five different databases and summarized the dark sides of AI in electronic markets from six aspects: privacy concerns, security issues, ethical challenges, criminals and terrorists enabled by AI, trust issues between humans and machines, and AI biases. The literature review presented in this study has provided a rigorous and structured overview of research on AI's dark sides in the electronic markets through a combination of quantitative and qualitative analysis of the AI literature. As AI has made rich contributions to a variety of applications in electronic markets, special care should be taken regarding the dark side of AI. Governments and policymakers are recommended to establish legislation to ensure that AI-powered innovation and implementation are beneficial to the social good while limiting the threats caused by the dark side of AI.

KEYWORDS

AI, Biases, Dark Side, Electronic Market, Privacy, Security

Artificial intelligence (AI) has attracted immense attention in recent years. The term was first coined by Prof. John McCarthy for a conference on the subject held at Dartmouth in 1956. McCarthy defines AI as the "science and engineering of making intelligent machines, especially intelligent computer programs". Nilsson (1971) referred to AI as machines performing interacting, learning, and problem-solving functions associated with human minds. AI is revolutionizing the way many industries operate, including electronic markets and smart services (Chang et al., 2022; Du et al., 2022; Dubey et al., 2022; Hossain et al., 2022; Huang et al., 2021; Lee, 2022; Paul et al., 2022; Qiu,

DOI: 10.4018/JOEUC.327278

*Corresponding Author

2022; Shrivastav, 2022; Wu, 2021; Wu et al., 2021; Xing et al., 2022). An electronic market refers to a virtual trading environment that integrates buyers and sellers through dynamic web applications and other applications based on Internet communication technology (Tan et al., 2019). By integrating market and competition orientation, e-commerce enterprises can enhance their understanding of customer needs, identify market opportunities, promote product development, and increase innovation success by accessing a wider range of market information (Jebarajakirthy et al., 2022; Li, Du et al., 2022; Raisch & Krakowski, 2021; Sun & Li, 2022; Sun & Wang, 2022; Yu & Yu, 2022; Zhang, 2022). Numerous digital business companies and retailers, such as Amazon, leverage AI to enhance sales, attract and retain customers and improve profitability (Zheng et al., 2023) through optimized marketing strategies and streamlined business processes (Bai & Lin, 2022; Li & Feng et al., 2022; Liu & Li, 2022; Liu et al., 2022; Kozinets & Gretzel, 2020; Ma & Zhang, 2022; Rashidin et al., 2022; Shankar, 2020; Varsha et al., 2021; Wang et al., 2022). Simultaneously, utilizing AI introduces many new challenges that span ethical, legal, social, and technological dimensions (Trappey et al., 2022; Akter et al., 2021; Xu et al., 2022). As outlined by Kozinets and Gretzel (2020), a predicament arises when implementing AI technologies in the market: While AI-driven marketing campaigns can generate substantial sales and revenue, marketers face diminishing opportunities to establish meaningful customer relationships.

The rising adoption of a new generative AI technology, ChatGPT, in the electronic market is notable due to its transformative impact on customer interactions and overall business operations. While ChatGPT offers significant potential for the electronic market—such as improved customer support, streamlined sales and trading, scalability, cost-effectiveness, and competitive advantage—it is essential to recognize that it can also introduce specific adverse effects. First, ChatGPT's ability to generate text can be exploited to spread disinformation or manipulate market conditions. Malicious actors could use the technology to disseminate misleading product descriptions, manipulate stock prices, or deceive customers. Second, while ChatGPT can provide automated customer support, it may lack the empathy and nuanced understanding that human agents possess. This can lead to frustrated customers and negative experiences, potentially affecting trust and loyalty in the e-market. Moreover, implementing ChatGPT may require substantial resources, giving larger companies with greater financial capabilities an advantage over smaller competitors. This could lead to increased market consolidation and reduced competition. ChatGPT may exhibit biases in the training data if not adequately trained and monitored, leading to unfair or discriminatory outcomes in the electronic marketplace. This can perpetuate existing inequalities and hinder equal access and opportunities for all participants. It is, therefore, essential to mitigate these adverse effects by implementing robust safeguards, responsible use guidelines, and thorough testing and auditing processes. Continuous monitoring and improvement of AI systems can help address these concerns and promote the responsible and ethical use of ChatGPT in the electronic market.

Despite the rich opportunities AI offers, it is evident that AI is not a panacea that can address every problem facing individuals, organizations, and society. On April 21, 2021, the European Union (EU) published strict regulations governing the use of AI. This first-of-its-kind policy outlines how companies and governments can use a technology seen as one of today's most significant but ethically fraught scientific breakthroughs (Li, Yu, et al., 2019). According to the EU's strategic policy, AI can be used, but the application of AI technology must be limited. If AI technology is abused, it will significantly impact the financial order of the electronic market and cause an imbalance in the financial chain, thus hindering the development of the electronic market (Brynjolfsson & Mitchell, 2017). A thorough review of the benefits and challenges of using AI in the electronic marketplace is needed to help marketers, business managers, entrepreneurs, and researchers leverage AI for maximum benefit while mitigating its potential risks, harms, and other dark aspects.

Systematic reviews on a topic can provide a comprehensive, synthesized understanding of academic knowledge and contribute to its domain. In this research, we conduct a systematic literature review (SLR) on the dark side of AI in the electronic market by combining qualitative and quantitative analysis methods. Our research follows the procedures adopted by previous reviews (e.g., Cooper, 1988; Alavi & Carlson, 1992) in combination with the research methodologies by Webster and Watson (2002) and Vom Brocke (2015). Specifically, we investigate the following three research questions in this study:

RQ 1: What types of dark sides have been identified by prior research on AI in electronic markets?
RQ 2: What are the consequences of the dark sides of AI in electronic markets and the solutions provided by prior research?
RQ 3: What are the research gaps and future research opportunities for AI's dark sides in electronic markets?

In addition to offering a general overview of the prior research and identifying gaps for future research regarding the dark sides of AI in electronic markets, we discuss the social consequences of AI's dark sides and the managerial strategies to cope with them. We hope to inspire researchers and practitioners to exploit the benefits of AI while reducing its potential risks in electronic markets.

The paper proceeds with the following structure. Section 2 provides the background. Section 3 introduces the review methodology. Section 4 details the results of the review. Section 5 discusses the essential findings and offers suggestions for future research directions. Section 6 provides the theoretical and practical implications, and Section 7 concludes the paper.

BACKGROUND

In the literature addressing the dark sides of AI (see Table 1), Roche (2016) was the first to identify five conditions related to AI's dark side: the destruction of employment, stimulating societal instability, enabling criminal and terrorist activities, losing autonomy and privacy, and fuelling a cyber arms race. Cheng et al. (2021) uncovered both the bright and dark sides of AI by identifying two primary concerns: uncertainty and the invasion of privacy. In an extensive and comprehensive study on AI techniques, Jabbarpour et al. (2021) found the following negative aspects: energy consumption, data issues, security and trust, privacy, fairness, safety, predictability, explainability, complexity, monopoly, and responsibility.

AI has revolutionized the field of e-commerce. Despite the positive values being created, negative impacts arise when customers interact with AI technologies. Humans and machines jointly produce values, which can also be destroyed in human–computer interactions. The autonomy of AI should be questioned if technology is misused in unexpected ways or if companies' illegal or unethical actions involve using data without users' knowledge. For instance, in an overview of AI challenges in public management, Wirtz et al. (2020) categorized AI's dark side from societal, legal, and ethical perspectives. Exploring the co-destruction of values between humans and machines, Castillo et al. (2020) identified the top five reasons for customers' failure in interacting with chatbots: authenticity issues, cognition challenges, affective issues, functionality issues, and integration conflicts. Esmaeilzadeh (2020) summarized the significant factors contributing to the perceived risks of AI use from technological, ethical (trust factors), and regulatory perspectives.

Through a comprehensive examination of the existing literature, we observed a significant lack of scholarly attention to the negative aspects of AI in the electronic market (Yang et al., 2021). E-commerce plays a crucial role in facilitating online transactions and overseeing the entire service process, encompassing various functions, such as advertising, consultation and negotiation, online ordering, payment processing, electronic account management, service delivery, consultation, and transaction management. E-commerce activities demonstrate distinct characteristics, including integration, expansibility, security, and coordination (Raisch & Krakowski, 2021). The emergence of transformative technologies, including AI, has greatly enhanced these characteristics. Nonetheless, using AI to process personal data within a trading platform can raise privacy violations and system

Table 1. Dark sides of AI summarized in previous research

Author	Year	Challenges or Dark Sides of AI	Contribution
Roche	2016	● Destruction of employment ● Stimulating societal instability ● Enabling criminal and terrorist activities ● Losing autonomy and privacy ● Fuelling a cyber arms race	● Discussing both good and bad downstream consequences of AI
Wirtz et al.	2020	● AI society (workforce substitution & transformation; social acceptance & trust in AI; transformation of H2M interaction) ● AI law and regulation (AI rulemaking for human behavior; moral dilemmas; AI discrimination) ● AI ethics (privacy & safety; responsibility & accountability; governance of autonomous intelligence systems)	● Outlining the current state of AI governance ● Giving an overview of AI challenges and risks for public administration as well as previous AI governance or regulation frameworks ● Developing an integrated AI governance framework that organizes the key aspects of AI governance and regulation
Castillo et al.	2020	● Authenticity issues ● Cognition challenges ● Affective issues ● Functionality issues ● Integration conflicts	● Discussing how AI is transforming the service industry ● Exploring the theoretical concept of value co-destruction by adopting an S-D logic lens ● Discussing the proposed conceptualization of co-destruction in AI service settings
Esmaeilzadeh	2020	● Technological concerns (perceived performance anxiety; perceived communication barriers) ● Ethical concerns (perceived social biases; perceived privacy concerns; perceived mistrust in AI mechanisms) ● Regulatory concerns (perceived unregulated standards; perceived liability issues; perceived risks)	● Developing a model mainly based on value perceptions due to the specificity of the healthcare field ● Examining the perceived benefits and risks of AI medical devices with clinical decision support (CDS) features from consumers' perspectives ● Using an online survey to collect data from 307 individuals in the United States
Cheng et al.	2021	● Uncertainty ● Invasion of privacy	● Uncovering the interplay between the dark and bright sides of big data analytics and AI and the underlying mechanisms of cognitive appraisals for user behavior in ridesharing
Jabbarpour et al.	2021	● Energy consumption ● Data issues ● Security and trust ● Privacy ● Fairness ● Safety ● Beneficial ● Predictability ● Explainable AI ● The complexity issue ● Monopoly ● Responsibility challenges	● Discussing the general concepts of the CS problem and its variations ● Conducting an extensive and comprehensive study on the dark sides of AI techniques to extract the main technical dark sides ● Proposing a novel framework for the CS problem of ISs that considers the dark sides of AI

security issues (Li, Chu, et al., 2022). In addition, the prevalence of AI technology in e-commerce has opened the door to numerous criminal economic activities, posing a threat to the overall security of e-commerce. As AI empowers machines to acquire the ability to perform tasks traditionally performed by humans, ethical concerns surrounding its use and the extent to which we can trust AI have come to the forefront of the public consciousness (Wu, 2021).

METHODOLOGY

Search Strategies

AI research spans various disciplines, making it non-restrictive regarding discipline or field when gathering AI literature. To collect AI literature for our study, we conducted searches on two reputable databases, Web of Science and Elsevier. Our study exclusively considered publications written in English. The search strategy for each database was developed based on keywords identified from the literature and rules for subject headings in each. The keyword search query was constructed as follows: TS=("electronic markets" OR "electronic commerce") AND TS=("artificial intelligence" OR "machine learning") AND TS=("dark side" OR "negative impact" OR risks OR disadvantage OR problems).

The first author used a structured form to extract information from eligible papers, including author, publication year, journal title, organization type, country/region of the first author, research question, theoretical basis, core opinion, primary findings, and conclusions/comments. Two other authors subsequently validated this data set. The search yielded a total of 3,541 publications from the two databases.

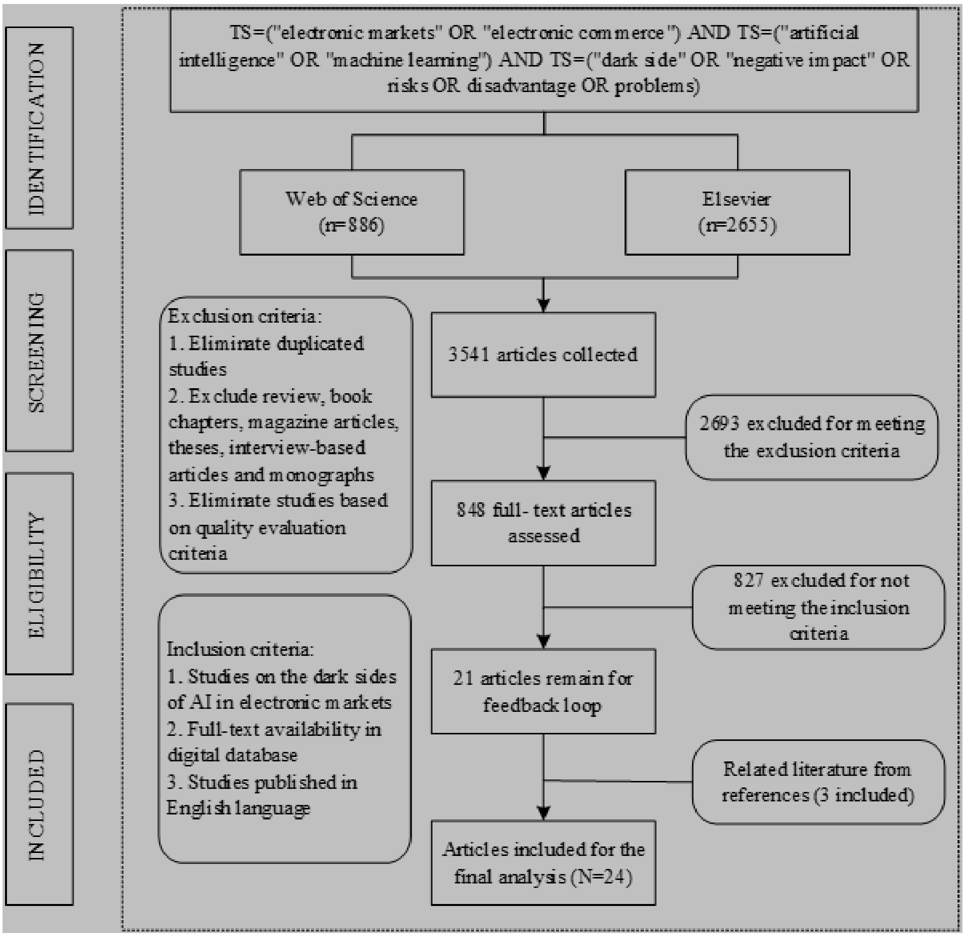
Article Screening and Selection

We applied some exclusion and inclusion criteria based on the entire paper (see Figure 1). We first excluded articles based on the following exclusion criteria: duplicated studies and certain article types, namely reviews, book chapters, magazine articles, theses, and interview-based studies. Each study was then evaluated through an initial screening that examined the title and abstract. Articles that did not specifically mention "artificial intelligence" or "electronic market" in the abstract were excluded from the dataset. Article type was also restricted for full-text evaluation. Books, doctoral dissertations, book reviews, letters, and announcements were excluded from the dataset. We also used quality criteria to evaluate the articles to ensure they presented unbiased and transparent results. The quality criteria included the article's length, the journal's rank, the research scope regarding AI dark sides, and the research topic.

In this nascent and evolving field of research, we faced difficulties pinpointing relevant papers within our scope, prompting us to employ a manual search approach for obtaining search results. We established three key inclusion criteria to filter out articles. The primary criteria entailed choosing articles based on their theme and topics associated with the negative aspects of AI in electronic markets. For instance, while some articles discussed the theme of trust in AI within the electronic market, they primarily focused on fostering customer trust in e-commerce. Similarly, other articles offered only a scant mention, perhaps a sentence or two, of the negative implications of AI, leading us to exclude these articles from our dataset. Following this, two examiners independently reviewed the full-text articles. The classification was primarily based on keywords such as "ethical," "security," "privacy," "risks," "bias," "misuse," and "dysfunction." Factors such as the authorship, journal, and publication year were not concealed. In summary, we performed a comprehensive retrospective and prospective analysis of a selected sample of papers in our dataset to uncover additional relevant research. We carefully checked the references for the retrospective review to ensure that no relevant studies were overlooked. Thus, our final collection consists of 24 articles.

Upon examining our compiled literature set, we noticed a significant emphasis on the exploration, application, and progression of AI over the past decade. However, the challenges arising from the integration of AI into the electronics market have primarily been highlighted by researchers in more recent years. The literature review revealed that investigations into the negative implications of AI in electronic markets have only surfaced in the past seven years. These adverse aspects of AI in electronic markets can be placed into six categories: privacy concerns, security dilemmas, ethical dilemmas, potentially criminal and terrorist activities facilitated by AI, trust issues between humans and machines, and biases inherent in AI.

Figure 1. Flow of information through different phases of the systematic review


IDENTIFICATION
SCREENING
ELIGIBILITY
INCLUDED
TS=("electronic markets" OR "electronic commerce") AND TS=("artificial intelligence" OR "machine learning") AND TS=("dark side" OR "negative impact" OR risks OR disadvantage OR problems)
Web of Science (n=886)
Elsevier (n=2655)
Exclusion criteria:
1. Eliminate duplicated studies
2. Exclude review, book chapters, magazine articles, theses, interview-based articles and monographs
3. Eliminate studies based on quality evaluation criteria
3541 articles collected
2693 excluded for meeting the exclusion criteria
848 full- text articles assessed
827 excluded for not meeting the inclusion criteria
Inclusion criteria:
1. Studies on the dark sides of AI in electronic markets
2. Full-text availability in digital database
3. Studies published in English language
21 articles remain for feedback loop
Related literature from references (3 included)
Articles included for the final analysis (N=24)

RESULTS

This section discusses the findings of this study and presents their implications in detail. We count the number of studies by publication year and frequency by country. The results showed that publications on AI's dark side in electronic markets emerged within the last seven years, between 2016 and 2022 (see Figure 2). A notable surge in articles was observed in 2019, 2020, and 2021, with six papers published each year. However, the volume of publications on this subject declined in 2022.

The analysis indicates that the authors of the reviewed articles are associated with institutions spanning ten countries. As suggested by Figure 3, scholars from the United States are the most productive, contributing most of the published articles on the dark aspects of AI in electronic markets, with seven articles to their credit. German scholars come in second, trailed by their counterparts from the UK and China. Collectively, these four countries—the United States (with seven articles), Germany (with five articles), and the United Kingdom and China (each with three articles)—account for 75% of the sample representation. This distribution could be attributed to the fact that these countries, being global economic powerhouses, are predominantly impacted by the adverse effects of rapid technological growth and AI advancements. Interestingly, we observe that among high-output countries, US authors have placed significant emphasis on AI privacy; German researchers have

Figure 2. Number of studies by year of publication

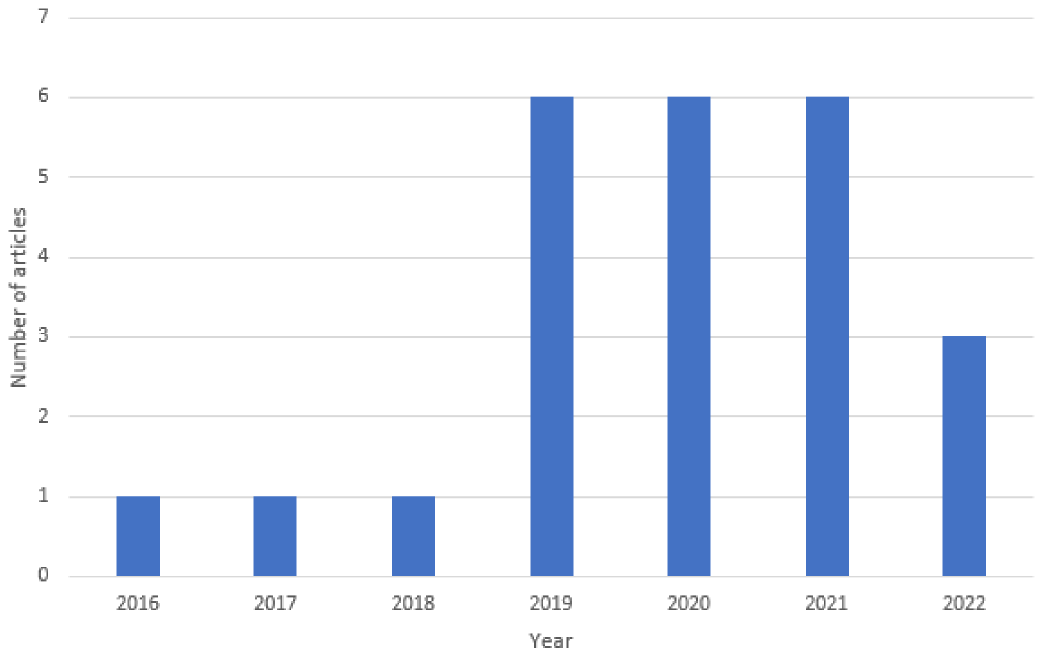
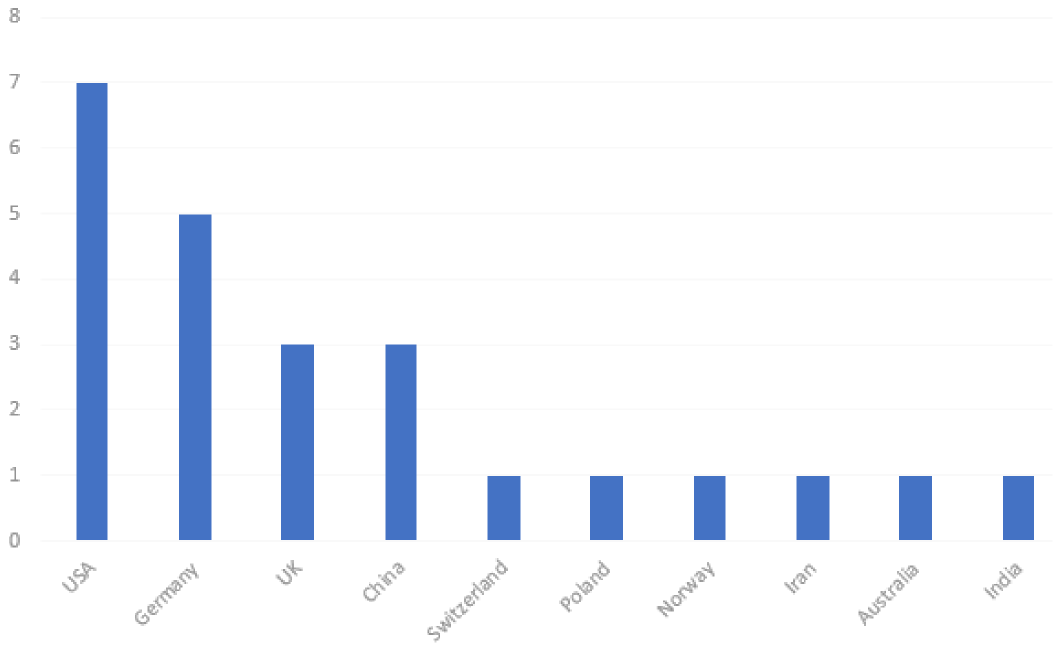
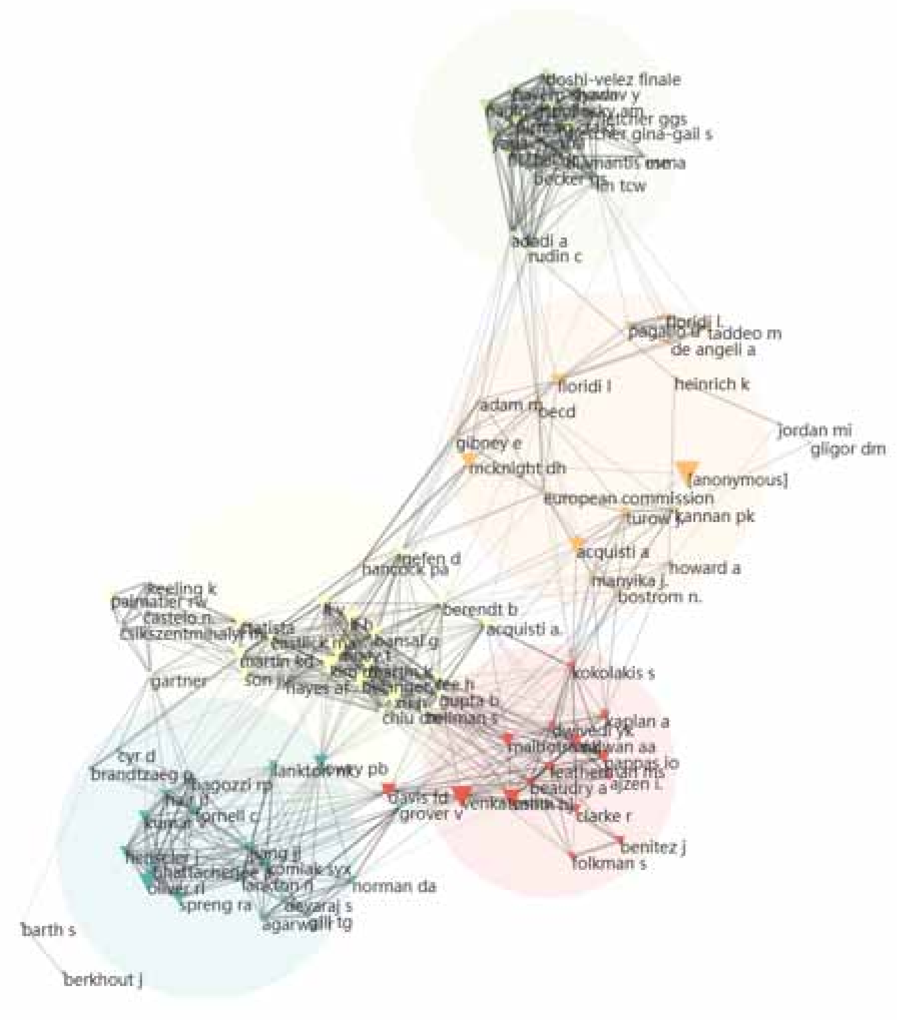


Figure 3. Publications by country (note: The institute location belongs to the first author)



delved into both privacy concerns and trust issues between humans and machines; UK researchers have focused more on AI security threats and associated criminal activities; and Chinese researchers have demonstrated a heightened focus on ethical issues and privacy concerns related to AI.

Figure 4. Co-citation relationship diagram on the dark sides of AI in electronic markets



We drew a co-citation relationship diagram based on the references of the 24 articles to see which articles were more important in the field of AI's dark side in the electronic market (see Figure 4). Influential references in the dark side of technology and AI field include Acquisti et al.'s (2015) research published in "*Science*" (cited four times), which connected insights from the social and behavioral sciences by taking advantage of uncertainty about the consequences of privacy behavior, the situational dependence of concerns, and the extent to which business and government interests can manipulate privacy issues. Acquisti et al. (2016) published another article in the *Journal of Economic Literature*, which summarized and drew links between theoretical and empirical studies of different schools of privacy economics. Other influential articles include McKnight et al.'s (2002) study in *Information Systems Research*, Son and Kim's (2008) research in *MIS Quarterly*, Podsakoff et al.'s (2003) paper in the *Journal of Applied Physiology*, Smith et al.'s (1996) research in *MIS Quarterly*, and Martin and Murphy's (2017) study in the *Journal of the Academy of Marketing Science*. These studies, despite discussing the dark side of AI, were excluded from our sample because they did not specifically address the electronic market domain. These studies were merely cited by researchers investigating the adverse effects of AI in e-commerce. While no direct positive correlation can be drawn between author influence and citation count, a high citation rate does suggest the significant value and pioneering nature of research on the dark side of AI in the e-marketplace.

We have distilled the research topics that are prevalent in the selected articles. As per Table 2, the dominant themes related to the negative aspects of AI in electronic markets include consumer privacy concerns (covered by 45.83% of the selected literature), AI's ethical challenges, trust issues between humans and machines, and security concerns (each featured in 33.33% of the studies). Sundar Pichai (2018), Google's CEO, proposed a set of ethical principles for AI development, which included being socially beneficial, avoiding the creation or reinforcement of unfair bias, and being accountable to people. Our findings highlight a strong correlation between AI ethics research and the issue of unfair bias. Privacy is interwoven with multiple challenges, such as online security, fraud, and trust issues, which can threaten the growth of e-commerce. We observed a convergence between the literature addressing privacy concerns related to AI, and that focused on security in the electronic market. This is because privacy concerns are invariably linked to the disclosure of personal profiles and data security. In turn, research investigating individual privacy concerns often intersects with research on AI ethics within e-commerce. This is because privacy issues often challenge fundamental human ethics. Much of the discussion surrounding AI bias stems from these ethical studies. On another note, only four articles explore AI's role in "facilitating criminal and terrorist activities" (16.67%), and six delve into "AI biases" in the electronic market (25%). As a result, we infer that the most prominent negative aspects of AI in electronic markets are privacy concerns, security issues, and AI bias, followed by ethical challenges. By contrast, research has devoted little attention to AI's role in "criminal and terrorist activities" and trust issues between humans and machines.

DISCUSSION

To help understand these issues better, in this section, we detail each of the dark sides identified in these articles, including research gaps and related further research opportunities.

Privacy Concerns

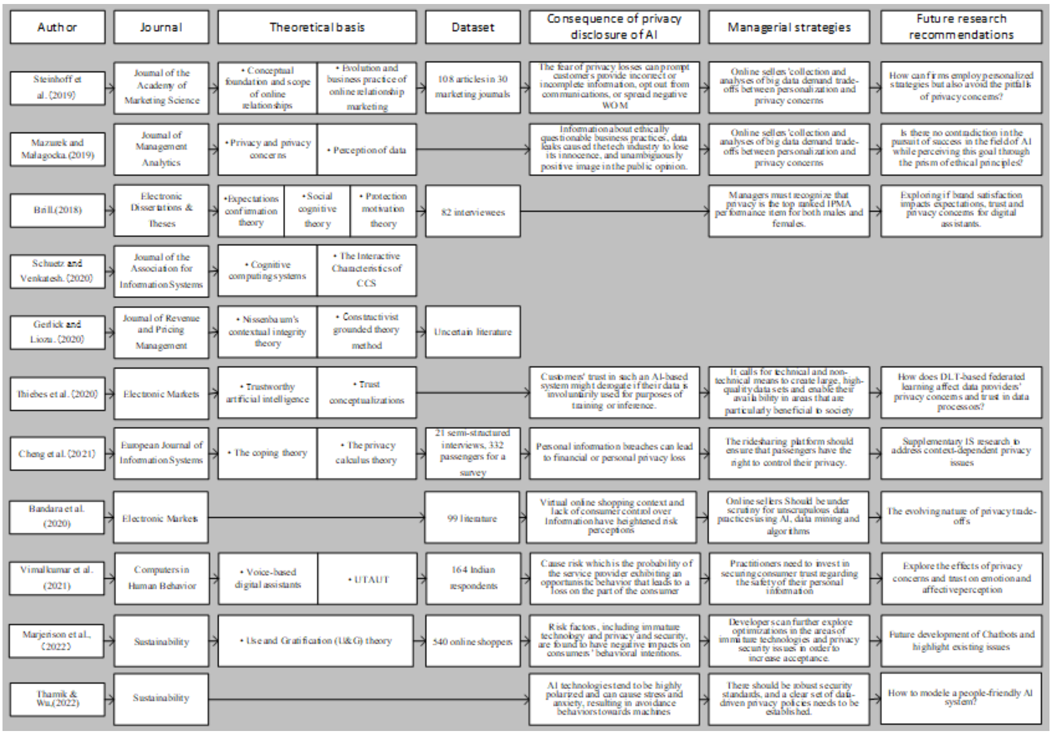
Eleven of the publications we reviewed concentrated on privacy issues related to AI in the electronic market. Details, including the authors, journals, theoretical frameworks, datasets, key findings, implications of AI privacy disclosure, proposed solutions, and recommendations for future research, are illustrated in Figure 5. The theoretical foundations that have been shown to address privacy disclosure problems of AI in electronic markets effectively include expectation confirmation theory, social cognitive theory, protection motivation theory (Brill et al., 2019), coping theory, privacy calculus theory (Cheng et al., 2021), Nissenbaum's contextual integrity theory, and constructivist grounded theory method (Gerlick & Liozu, 2020). In terms of research methodologies, Steinhoff et al. (2019), Gerlick and Liozu (2020), Bandara et al. (2019), and Thamik and Wu (2022) each carried out literature reviews to encapsulate how AI has infringed upon privacy, leading to data breaches and misuse in electronic markets. Vimalkumar et al. (2021) conducted a noteworthy quantitative study utilizing the UTAUT2 model, focusing on perceived privacy concerns, perceived privacy risks, and perceived trust. Marjerison et al. (2022) adopted uses and gratification (U&G) theory to investigate consumer acceptance of applied AI, specifically in the form of chatbots, within the context of online shopping in China. Brill et al. (2019) and Cheng et al. (2021) delved into online consumers' privacy concerns as influenced by AI development. They employed semi-structured interviews and questionnaire surveys to underscore the crucial role of customer satisfaction (Brill et al., 2019) and the gathering of personal biometric information using big data analytics and AI technologies, particularly in the context of participation in ridesharing (Cheng et al., 2021; Haverila et al., 2022; Xie et al., 2022). The other studies discussed privacy issues through theoretical analyses (Mazurek & Małagocka, 2019; Schuetz & Venkatesh, 2020; Thiebes et al., 2020).

Table 2. Classification of research themes

Authors	Privacy Concerns	Security Issues	Ethical Challenges	Enabling Criminal and Terrorist Activities	Trust Issues Between Humans and Machines	AI Biases
Coeckelbergh, 2016			√			
Howard et al., 2017						√
Motlagh & Bardsir, 2018		√				
Steinhoff et al., 2019	√				√	
Mazurek & Małagocka, 2019	√		√			
Brill et al., 2019	√					
Bandara et al., 2019	√	√			√	
Lauterbach, 2019		√	√			√
Yeoh, 2019		√		√		
Schuetz & Venkatesh, 2020	√				√	
Gerlick & Liozu, 2020	√		√			√
Thiebes et al., 2020	√		√		√	√
Kaloudi & Li, 2020		√				
Toader et al., 2020					√	
King et al., 2020		√		√		
Cheng et al., 2021	√					
Wing et al., 2021			√			
Vimalkumar et al., 2021	√				√	
Gligor et al., 2021					√	
Fletcher, 2021				√		
Janiesch et al., 2021						√
Thamik & Wu, 2022	√	√	√		√	√
Marjerison et al., 2022	√	√				
Azzutti, 2022			√	√		
Quantity statistics	11	8	8	4	8	6
Proportion	45.83%	33.33%	33.33%	16.67%	33.33%	25.00%

Studies have revealed that adequate privacy protection helps people maintain personal dignity, maintain a comfortable mood, and promote overall development. In contrast, perceived privacy intrusion would affect consumers' trust and usage (Esmaeilzadeh, 2020). However, motivated by interest, many e-commerce companies overuse consumer information. Scandals involving privacy infringement in AI marketing have become a universal phenomenon (Bandara et al., 2019; Thamik & Wu, 2022). The disclosure of private information by AI would cause severe consequences in electronic markets. Fear of a loss of privacy can trigger adverse reactions from customers. For example, they may provide incorrect or incomplete information, choose not to participate in communication, or even spread negative information by word of mouth (Karwatzki et al., 2017). In addition, ethically questionable business practices, data breaches, and social and economic side effects could cause the tech industry to lose its positive image in public opinion (Mazurek & Małagocka, 2019; Zheng, Wang et al., 2023). Therefore, the creation of professional, comprehensive, and high-quality data sets and the enhancement of their availability (proprietary or open access) are particularly beneficial for

Figure 5. Studies on the privacy of AI in electronic markets



Author	Journal	Theoretical basis	Dataset	Consequence of privacy disclosure of AI	Managerial strategies	Future research recommendations
Steinhoff et al. (2019)	Journal of the Academy of Marketing Science	• Conceptual foundation and scope of online relationships • Evolution and business practice of online relationship marketing	108 articles in 30 marketing journals	The fear of privacy losses can prompt customers provide incorrect or incomplete information, opt out from communications, or spread negative WOM	Online sellers 'collection and analyses of big data demand trade-offs between personalization and privacy concerns	How can firms employ personalized strategies but also avoid the pitfalls of privacy concerns?
Mazurek and Malagocka.(2019)	Journal of Management Analytics	• Privacy and privacy concerns • Perception of data		Information about ethically questionable business practices, data leaks caused the tech industry to lose its innocence, and unambiguously positive image in the public opinion.	Online sellers 'collection and analyses of big data demand trade-offs between personalization and privacy concerns	Is there no contradiction in the pursuit of success in the field of AI while perceiving this goal through the prism of ethical principles?
Brill.(2018)	Electronic Dissertations & Theses	•Expectations confirmation theory •Social cognitive theory • Protection motivation theory	82 interviewees		Managers must recognize that privacy is the top ranked IPMA performance item for both males and females.	Exploring if brand satisfaction impacts expectations, trust and privacy concerns for digital assistants.
Schuetz and Venkatesh. (2020)	Journal of the Association for Information Systems	• Cognitive computing systems • The Interactive Characteristics of CCS				
Gerlick and Liozu. (2020)	Journal of Revenue and Pricing Management	• Nissenbaum's contextual integrity theory • Constructivist grounded theory method	Uncertain literature			
Thiebes et al. (2020)	Electronic Markets	• Trustworthy artificial intelligence • Trust conceptualizations		Customers' trust in such an AI-based system might derogate if their data is involuntarily used for purposes of training or inference.	It calls for technical and non-technical means to create large, high-quality data sets and enable their availability in areas that are particularly beneficial to society	How does DLT-based federated learning affect data providers' privacy concerns and trust in data processors?
Cheng et al. (2021)	European Journal of Information Systems	• The coping theory • The privacy calculus theory	21 semi-structured interviews, 332 passengers for a survey	Personal information breaches can lead to financial or personal privacy loss	The ridesharing platform should ensure that passengers have the right to control their privacy.	Supplementary IS research to address context-dependent privacy issues
Bandara et al. (2020)	Electronic Markets		99 literature	Virtual online shopping context and lack of consumer control over Information have heightened risk perceptions	Online sellers Should be under scrutiny for unscrupulous data practices using AI, data mining and algorithms	The evolving nature of privacy trade-offs
Vimalkumar et al. (2021)	Computers in Human Behavior	• Voice-based digital assistants • UTAUT	164 Indian respondents	Cause risk which is the probability of the service provider exhibiting an opportunistic behavior that leads to a loss on the part of the consumer	Practitioners need to invest in securing consumer trust regarding the safety of their personal information	Explore the effects of privacy concerns and trust on emotion and affective perception
Marjerison et al., (2022)	Sustainability	• Use and Gratification (U&G) theory	540 online shoppers	Risk factors, including immature technology and privacy and security, are found to have negative impacts on consumers' behavioral intentions.	Developers can further explore optimizations in the areas of immature technologies and privacy security issues in order to increase acceptance.	Future development of Chatbots and highlight existing issues
Thamik & Wu.(2022)	Sustainability			AI technologies tend to be highly polarized and can cause stress and anxiety, resulting in avoidance behaviors towards machines	There should be robust security standards, and a clear set of data-driven privacy policies needs to be established.	How to modele a people-friendly AI system?

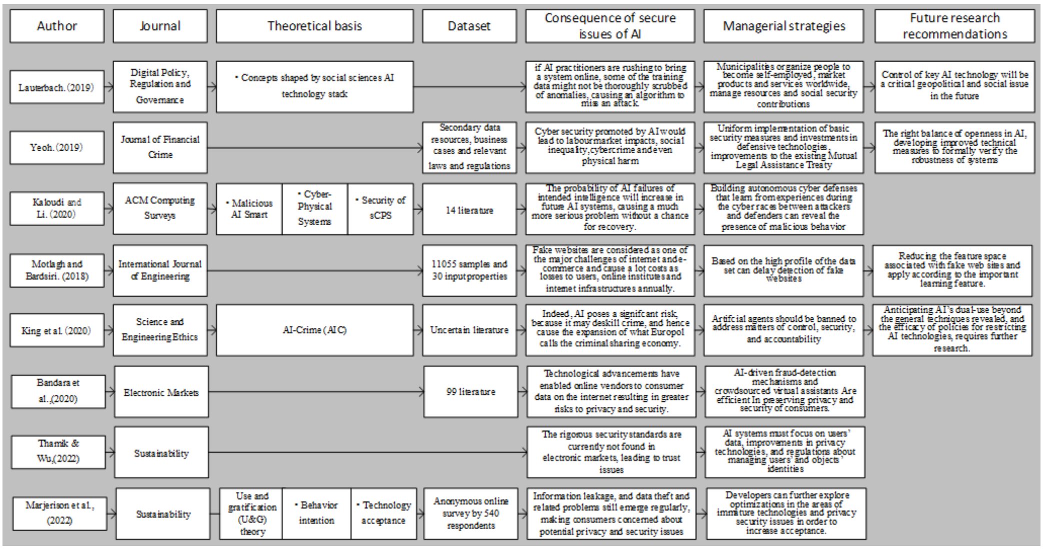
online privacy protection, developing privacy standards, and making sure the online platform allows customers the right to control their privacy (Cheng et al., 2021; Thamik & Wu, 2022).

Regarding research gaps and opportunities for further research on this dark side, the most recent research on privacy has focused on the factors influencing user privacy awareness and their impact on AI marketing adoption and disclosure behavior. Prior studies have also identified the existence of privacy fatigue, which means that people are beginning to be indifferent to their privacy rights. If this phenomenon continues, people will lose their trust in society (Bandara et al., 2019; Brill et al., 2019). Therefore, future research needs to explore the causes of this phenomenon more deeply to find more effective solutions (Mazurek & Małagocka, 2019; Thiebes et al., 2020). In addition, research has found that rigorous privacy policies can hinder the development of AI technologies and economies; future research should seek effective ways to balance technology and legal formulation (Gerlick & Liozu, 2020).

Security Issues

Eight articles addressed the security issues of AI in the electronic market, as shown in Figure 6. Researchers have used theoretical analysis methods to illustrate the security issues arising from the development of AI, especially cybersecurity in e-commerce environments (Ifinedo et al., 2022). Two articles explored existing AI-based cyber attacks and provided insight into new threats through a literature review (Kaloudi & Li, 2020; King et al., 2020). They found that with the development of technology, the danger of AI marketing is much more severe than in a traditional marketing environment (Motlagh & Bardsir, 2018). The development of AI results in more variants of viruses with shorter cycles, leading to additional virus solutions and new attack methods (Yeoh, 2019). Moreover, unlike traditional crimes, cybercrimes are easier to replicate since the developed hacking techniques are

Figure 6. Studies on the security topic of AI in electronic markets



Author	Journal	Theoretical basis	Dataset	Consequence of secure issues of AI	Managerial strategies	Future research recommendations
Lauterbach. (2019)	Digital Policy, Regulation and Governance	• Concepts shaped by social sciences AI technology stack		if AI practitioners are rushing to bring a system online, some of the training data might not be thoroughly scrubbed of anomalies, causing an algorithm to miss an attack.	Municipalities organize people to become self-employed, market products and services worldwide, manage resources and social security contributions	Control of key AI technology will be a critical geopolitical and social issue in the future
Yeoh. (2019)	Journal of Financial Crime		Secondary data resources, business cases and relevant laws and regulations	Cyber security promoted by AI would lead to labourmarket impacts, social inequality,cybercrime andeven physical harm	Uniform implementation of basic security measures and investments in defensive technologies, improvements to the existing Mutual Legal Assistance Treaty	The right balance of openness in AI, developing improved technical measures to formally verify the robustness of systems
Kaloudi and Li. (2020)	ACM Computing Surveys	• Malicious AI Smart • Cyber-Physical Systems • Security of sCPS	14 literature	The probability of AI failures of intended intelligence will increase in future AI systems, causing a much more serious problem without a chance for recovery.	Building autonomous cyber defenses that learn from experiences during the cyber races between attackers and defenders can reveal the presence of malicious behavior	
Motlagh and Bardsiri. (2018)	International Journal of Engineering		11055 samples and 30 input properties	Fake websites are considered as one of the major challenges of internet and e-commerce and cause a lot costs as losses to users, online institutes and internet infrastructures annually.	Based on the high profile of the data set can delay detection of fake websites	Reducing the feature space associated with fake web sites and apply according to the important learning feature.
King et al. (2020)	Science and Engineering Ethics	AI-Crime (AIC)	Uncertain literature	Indeed, AI poses a signifcant risk, because it may deskill crime, and hence cause the expansion of what Europol calls the criminal sharing economy.	Artifcial agents should be banned to address matters of control, security, and accountability	Anticipating AI's dual-use beyond the general techniques revealed, and the efficacy of policies for restricting AI technologies, requires further research.
Bandara et al.,(2020)	Electronic Markets		99 literature	Technological advancements have enabled online vendors to consumer data on the internet resulting in greater risks to privacy and security.	AI-driven fraud-detection mechanisms and crowdsourced virtual assistants Are efficient In preserving privacy and security of consumers.	
Thamik & Wu,(2022)	Sustainability			The rigorous security standards are currently not found in electronic markets, leading to trust issues	AI systems must focus on users' data, improvements in privacy technologies, and regulations about managing users' and objects' identities	
Marjerison et al., (2022)	Sustainability	Use and gratification (U&G) theory • Behavior intention • Technology acceptance	Anonymous online survey by 540 respondents	Information leakage, and data theft and related problems still emerge regularly, making consumers concerned about potential privacy and security issues	Developers can further explore optimizations in the areas of immature technologies and privacy security issues in order to increase acceptance.	

often shared in hacker communities (Bandara et al., 2019). The lowering of technological barriers is likely to lead to more AI-based crime.

Extensive and in-depth deployments of AI technologies are found in marketing, and the extent to which security risks may be enhanced depends significantly on how well the action is embedded in a computational environment, mainly using cloud or edge computing. Moreover, as AI marketing involves a lot of important information and trading activities, once security is challenged, significant harm could come to a country's personal or economic safety (Yeoh, 2019). Therefore, it is crucial to identify the security risk factors associated with AI marketing to defend against cybercrime and risks from developed systems.

Hazardous activities in AI marketing occur mainly through two channels. First, the attacker can destroy or control the AI marketing system or intentionally change the input, such as interfering with sensors to change data input or using malware to inject malicious data so the system can make the decision the attacker wants (Lauterbach, 2019). Second, the attacker may steal the confidential data used to train the AI system or extract the AI model (Huawei, 2018). In particular, most current AI marketing systems use open-source software and architectures, which have many security vulnerabilities.

For enterprises, it is necessary to improve security by strengthening the architecture's security, enhancing the model's robustness, and strengthening real-time monitoring (Polasik et al., 2015). First, organizations must increase the security of edge computing and systems through early-stage secure deployment. Adopting the necessary verification and rigorous audit programs, AI software and hardware environments should be carefully evaluated, such as servers and clients, software configurations, load management, patch management, and runtime configuration management for real-time monitoring. Specifically, algorithms such as deep learning can be used to implement malware characterization and detection in edge computing security (Yuan et al., 2016).

In terms of the research gaps and further research opportunities regarding security issues, we found that a large number of scholars have explored how to adopt technical means to discover and solve the problems of data security and system security in AI marketing (King et al., 2020; Nilashi et al., 2015). More effective technology remains the dominant direction of further exploration, and how to implement these technologies has become a more prominent issue (Bandara et al., 2019; Lauterbach, 2019). For example, ways to truly apply blockchain technology to achieve security in e-commerce deserve further study. Managers should also pay special attention to organizational-related security issues arising from AI marketing. For example, how multinational e-commerce companies resolve the differences in AI security standards in different countries or regions matters (Yeoh, 2019).

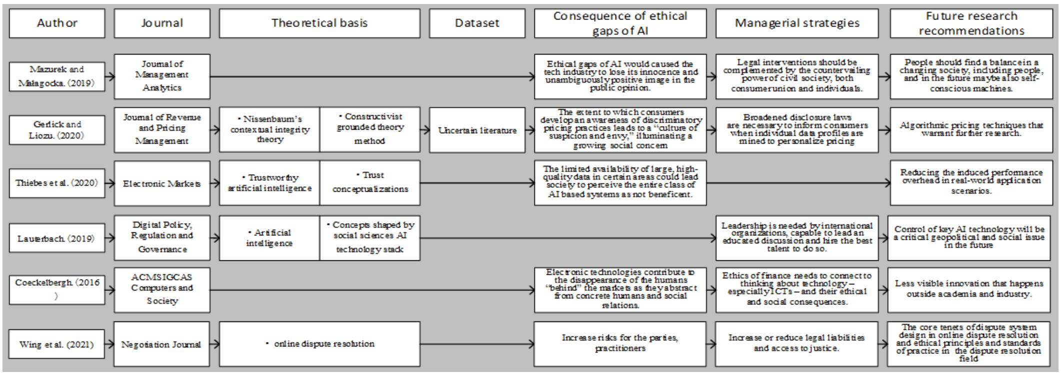
Ethical Challenges

Six articles examined the ethical challenges of AI in the electronic markets, as shown in Figure 7. All of these studies used theoretical analysis to explore the ethical issues raised by AI. The authors presented a similar opinion on the importance of AI ethics management, the effect of ethical deficiencies on society and country, and how urgently the problem needs to be solved through countries in electronic markets. Thiebes (2020) argued that when AI is developed, deployed, and used in a way that ensures compliance with all relevant laws and regulations and adheres to general ethical principles, users (e.g., consumers, organizations, and societies) will find it trustworthy. Mazurek (2019) maintained that it could only be a metaphor if the transparency of AI processes can be implemented and ethical norms can be applied in practice rather than just in theory.

Ethical issues related to data science and AI are frequently discussed. Organizations in online markets and trading platforms should address the ethics of the use of data and algorithms. Ethics is embedded in the design and development process of online trading. A human-centered, ethical AI should be designed and developed to be consistent with the values and ethical principles of the online communities it affects (Li, Deng, et al., 2019; Wing et al., 2021). Interpretability is needed to build consumer confidence in AI disruptive technologies in the electronics market, promoting safer practices and broader social adoption (Lauterbach, 2019). AI may have to make ethical value decisions but is subject to algorithmic bias (Zhao, 2021). Analysis exploring the ethical dimension can provide stakeholders insight into business value creation and confidence in their decisions (Vanderelst & Winfield, 2018; Vidgen et al., 2020). When AI helps consumers make sensitive decisions, it should explain why it makes such recommendations, what data was used, and the reasoning steps or processes behind them. In practice, AI ethics is often considered an "add-on" to technical concerns.

Regarding the gaps and further research opportunities regarding this dark side, ethical considerations must be a vital component of any AI policy in the electronic market. The current frameworks on AI ethics focus on society's ethical concerns (Mazurek & Małagocka, 2019), but notable gaps remain. For example, the environmental impacts associated with data processing and storage, the unfairness of the unequal distribution of benefits, and the potential exploitation of employees are all likely to raise ethical issues in terms of AI (Lauterbach, 2019; Thiebes et al., 2020). Thus, we need new strategies to transition to a fair AI-driven economic environment (Coeckelbergh, 2016). On the other hand, while questions about the ethical principles of AI are critical to the future

Figure 7. Studies on the ethical challenges of AI in electronic markets



Author	Journal	Theoretical basis	Dataset	Consequence of ethical gaps of AI	Managerial strategies	Future research recommendations
Mazurek and Małagocka. (2019)	Journal of Management Analytics			Ethical gaps of AI would caused the tech industry to lose its innocence and unambiguously positive image in the public opinion.	Legal interventions should be complemented by the countervailing power of civil society, both consumerunion and individuals.	People should find a balance in a changing society, including people, and in the future maybe also self-conscious machines.
Gerlick and Liozu. (2020)	Journal of Revenue and Pricing Management	• Nissenbaum's contextual integrity theory • Constructivist grounded theory method	Uncertain literature	The extent to which consumers develop an awareness of discriminatory pricing practices leads to a "culture of suspicion and envy," illuminating a growing social concern	Broadened disclosure laws are necessary to inform consumers when individual data profiles are mined to personalize pricing	Algorithmic pricing techniques that warrant further research.
Thiebes et al. (2020)	Electronic Markets	• Trustworthy artificial intelligence • Trust conceptualizations		The limited availability of large, high-quality data in certain areas could lead society to perceive the entire class of AI based systems as not beneficent.		Reducing the induced performance overhead in real-world application scenarios.
Lauterbach. (2019)	Digital Policy, Regulation and Governance	• Artificial intelligence • Concepts shaped by social sciences AI technology stack			Leadership is needed by international organizations, capable to lead an educated discussion and hire the best talent to do so.	Control of key AI technology will be a critical geopolitical and social issue in the future
Coeckelbergh. (2016)	ACMSIGCAS Computers and Society			Electronic technologies contribute to the disappearance of the humans "behind" the markets as they abstract from concrete humans and social relations.	Ethics of finance needs to connect to thinking about technology – especially ICTs – and their ethical and social consequences.	Less visible innovation that happens outside academia and industry.
Wing et al. (2021)	Negotiation Journal	• online dispute resolution		Increase risks for the parties, practitioners	Increase or reduce legal liabilities and access to justice.	The core tenets of dispute system design in online dispute resolution and ethical principles and standards of practice in the dispute resolution field

global adoption of this critical technology, not all countries understand the ethics of AI in the same way (Wing et al., 2021). Therefore, a comparative study of AI ethics in electronic markets, national regulatory approaches, and consumer attitudes in different countries would provide exciting insights into ethical understandings of AI.

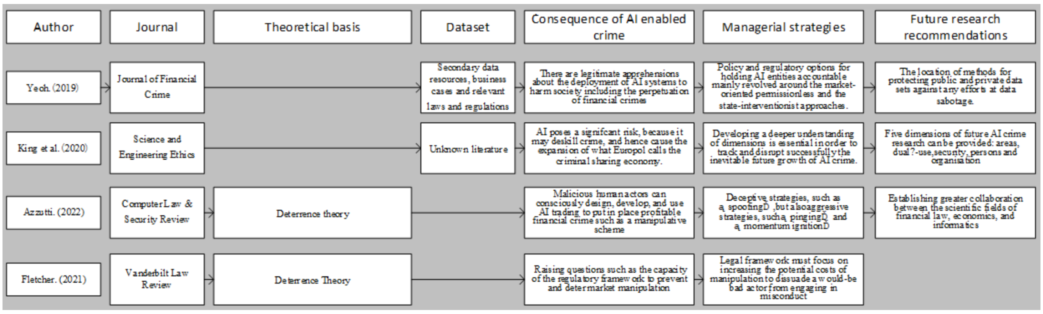
Enabling Criminal and Terrorist Activities

Only four articles dealt with the criminal and terrorist activities of AI in the electronic market. This topic has received the least attention in the literature, as seen in Figure 8. Techniques and tools developed for crime prevention and detection can be misused for criminal activities. Financial crime refers to behaviors that occur in financial activities, violate financial management laws and regulations, destroy financial management order, and should be punished according to the law (Fletcher, 2021). Money laundering and financial fraud are familiar types of financial crimes in our daily lives. Some efforts have been made to classify potential risks and threats from AI-assisted crime (King et al., 2020). AI, digital security, and physical security are closely linked. As AI systems are further developed and applied in the electronic marketplace, more sophisticated social engineering attacks that exploit these capabilities are likely to emerge (Azzutti, 2022; Li, Feng et al., 2022).

Criminals are likely to leverage AI to improve their attacks. AI-enabled crime has been on the rise recently. Criminals use AI to maximize profit opportunities and exploit more victims. Some cybersecurity experts express concerns about AI-related crimes in online markets, including AI-supported hacking, AI-assisted password guessing, insider trading, and deep fakes (Caldwell et al., 2020). More efforts and resources are needed to help mitigate these risks. Also, governments should strengthen the policy construction and supervision to hold AI entities accountable and intervene and regulate AI activities in electronic markets and online social networks (Fletcher, 2021). As a double-edged sword, AI can either curb financial crimes or accelerate them, depending on the management strategies of policymakers and regulators.

Concerning the research gaps and related research opportunities for this dark side, little attention has been paid to the criminal and terrorist activities arising from the development of AI in the electronic market. Although various criminal risks of AI and its characteristics have been addressed (Caldwell et al., 2020; Yeoh, 2019), it is still unclear to what extent those crimes affect the electronic market. In addition, the roles of employers and employees in defending against crimes have not been as well explored as would be expected (Azzutti, 2022; King et al., 2020). More broadly, research on AI crime in the electronic market is still in its infancy, and research on different dimensions of future AI criminal activity should be considered. Researchers should focus on individual factors that may create perpetrators in future e-commerce environments. Such research will help mitigate future AI crimes and terrorist activities.

Figure 8. Studies on AI crime in electronic markets



Author	Journal	Theoretical basis	Dataset	Consequence of AI enabled crime	Managerial strategies	Future research recommendations
Yeoh. (2019)	Journal of Financial Crime		Secondary data resources, business cases and relevant laws and regulations	There are legitimate apprehensions about the deployment of AI systems to harm society including the perpetuation of financial crimes	Policy and regulatory options for holding AI entities accountable mainly revolved around the market-oriented permissionless and the state-interventionist approaches.	The location of methods for protecting public and private data sets against any efforts at data sabotage.
King et al. (2020)	Science and Engineering Ethics		Unknown literature	AI poses a signifcant risk, because it may deskill crime, and hence cause the expansion of what Europol calls the criminal sharing economy.	Developing a deeper understanding of dimensions is essential in order to track and disrupt successfully the inevitable future growth of AI crime.	Five dimensions of future AI crime research can be provided: areas, dual?-use,security, persons and organisation
Azzutti. (2022)	Computer Law & Security Review	Deterrence theory		Malicious human actors can consciously design, develop, and use AI trading to put in place profitable financial crime such as a manipulative scheme	Deceptive strategies, such as ą spoofingĐ ,but also aggressive strategies, such ą pingingĐ and ą momentum ignitionĐ	Establishing greater collaboration between the scientific fields of financial law, economics, and informatics
Fletcher. (2021)	Vanderbilt Law Review	Deterrence Theory		Raising questions such as the capacity of the regulatory framework to prevent and deter market manipulation	Legal framework must focus on increasing the potential costs of manipulation to dissuade a would-be bad actor from engaging in misconduct	

Trust Issues Between Humans and Machines

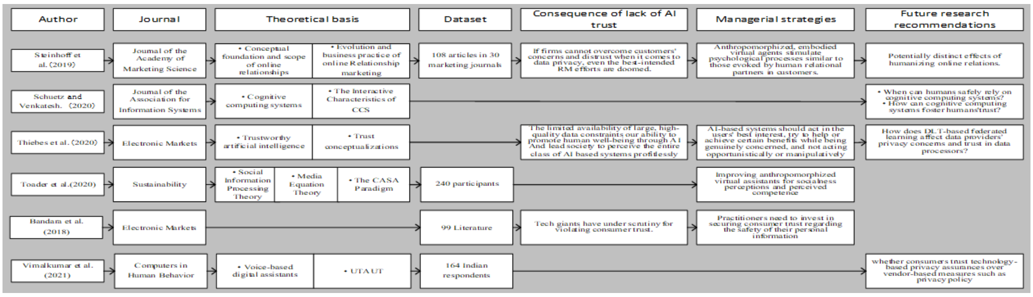
Six articles addressed trust issues between humans and machines in the electronic market, as shown in Figure 9. The trust issue is a cornerstone for AI (Schuetz & Venkatesh, 2020), and it also provides commerce with powerful competitive advantages (Karimova & Goby, 2020). Therefore, if e-commerce companies cannot effectively reduce the perceived risk while establishing trust and benefits, consumers will not accept the value delivered by AI marketing (Steinhoff et al., 2019). Furthermore, in 2019, the European Commission published ethics guidelines for trustworthy AI, stressing the importance of keeping people's trust in AI.

However, building human–AI trust in AI marketing has become a challenging problem due to the complexity and non-determinism of AI behavior. Robots with various structural, functional, social, and psychological properties have been rapidly introduced (Karimova & Goby, 2020). In addition, the objects of trust involve algorithms and systems and the organization and operation of AI marketing (Steinhoff et al., 2019). More specifically, several difficulties in trust-building have emerged in AI marketing. From a technology perspective, as most algorithms in AI marketing are uninterpretable, people will fear a lack of control, affecting trust building (Bandara et al., 2019). Moreover, consumers will doubt the goodwill behind the organization's use of AI (Thiebes et al., 2020). Consumers worry about whether AI marketers collect information about them from all over the world and whether they "look" at their faces through web cameras to read their expressions. Moreover, due to technical limitations, even if machines are equipped with a well-defined and generally accepted value system, they cannot feel the emotional consequences as people do. This may make it difficult for AI marketing systems to build trust with people.

To better establish the trust issues between machines and people, studies have explored the characteristics of the electronic markets with established trust and found that security, design, and content factors have different weights (Schuetz & Venkatesh, 2020; Vimalkumar et al., 2021). Meanwhile, scholars suggest e-commerce marketers should turn off some of the AI functions to alleviate consumers' concerns about being monitored. Moreover, empirical studies have shown that the form of AI affects the construction of trust. In AI robot design, typology, anthropomorphism, and immediate behaviors can be considered. Gligor et al. (2021) argued that in the process of building trust, electronic market participants also develop close relationships that can lead to mutually advantageous outcomes.

In terms of research gaps and further opportunities related to the dark side of AI marketing, trust is widely acknowledged to play a crucial role. However, building user trust remains a significant challenge. Although existing studies have explored the importance of website design and security in the e-commerce trust-building (Thiebes et al., 2020), few studies have considered how to change the characteristics of AI to enhance trust, especially through a detailed exploration of different AI marketing contexts (Steinhoff et al., 2019; Toader et al., 2020). Furthermore, cross-disciplinary research is needed because the interaction between AI and humans involves complex psychological

Figure 9. Studies on the AI trust in electronic markets



Author	Journal	Theoretical basis	Dataset	Consequence of lack of AI trust	Managerial strategies	Future research recommendations
Steinhoff et al. (2019)	Journal of the Academy of Marketing Science	• Conceptual foundation and scope of online relationships • Evolution and business practice of online Relationship marketing	108 articles in 30 marketing journals	If firms cannot overcome customers' concerns and distrust when it comes to data privacy, even the best-intended RM efforts are doomed.	Anthropomorphized, embodied virtual agents stimulate psychological processes similar to those evoked by human relational partners in customers.	Potentially distinct effects of humanizing online relations.
Schuetz and Venkatesh. (2020)	Journal of the Association for Information Systems	• Cognitive computing systems • The Interactive Characteristics of CCS				• When can humans safely rely on cognitive computing systems? • How can cognitive computing systems foster humans'trust?
Thiebes et al. (2020)	Electronic Markets	• Trustworthy artificial intelligence • Trust conceptualizations		The limited availability of large, high-quality data constraints our ability to promote human well-being through AI And lead society to perceive the entire class of AI based systems profitlessly	AI-based systems should act in the users' best interest, try to help or achieve certain benefits while being genuinely concerned, and not acting opportunistically or manipulatively	How does DLT-based federated learning affect data providers' privacy concerns and trust in data processors?
Toader et al.(2020)	Sustainability	• Social Information Processing Theory • Media Equation Theory • The CASA Paradigm	240 participants		Improving anthropomorphized virtual assistants for socialness perceptions and perceived competence	
Bandara et al. (2018)	Electronic Markets		99 Literature	Tech giants have under scrutiny for violating consumer trust.	Practitioners need to invest in securing consumer trust regarding the safety of their personal information	
Vimalkumar et al. (2021)	Computers in Human Behavior	• Voice-based digital assistants • UTAUT	164 Indian respondents			whether consumers trust technology-based privacy assurances over vendor-based measures such as privacy policy

and ethical issues. In addition, most research on trust in AI has focused on the individual level, while less has been done on the group, organizational, or social level. Therefore, conducting studies at different levels and even across levels of trust is an important research direction. For example, how to adopt appropriate organizational configurations to ensure that AI has a positive impact on the team is a question worth discussing.

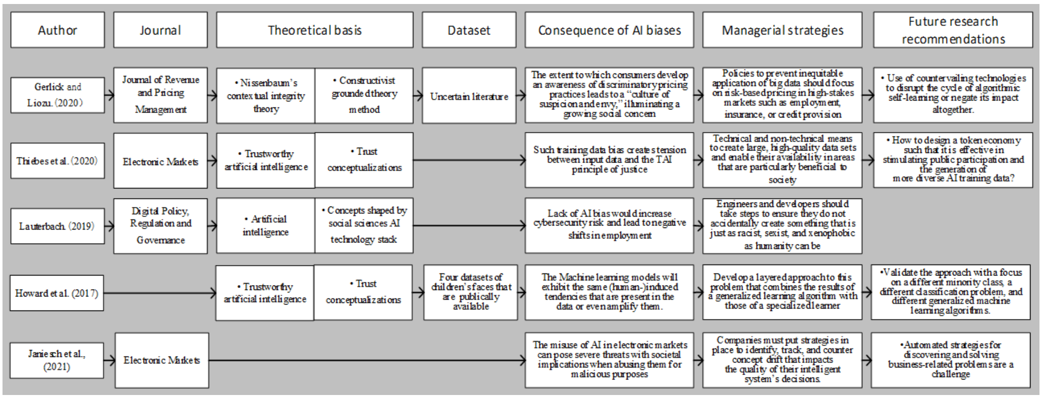
AI Biases

Four articles discussed the bias problems of AI in the electronic market, closely related to AI ethics (see Figure 10). AI decision quality is adversely affected by algorithmic bias. Bias issues grow exponentially when e-marketers rely primarily on their own data to train their algorithms. Organizations' AI algorithms are heavily biased toward what they have done in the past (Vidgen et al., 2020). When training an AI algorithm, it depends on the input data. This is especially true in business environments, where the purpose of AI may be to interact with customers, manage automated systems, or mimic human decisions (Chen et al., 2022). Crucially, the results match the goals. However, companies must be able to address any biases that might distort the way AI responds to commands or requests (Thiebes et al., 2020).

Bias can be a stumbling block in electronic markets. Potential flaws and biases in the algorithms used by AI may disproportionately impact diverse populations (Howard et al., 2017; Zheng, Zheng et al., 2022). If the underlying AI algorithm favors certain demographics over others, the results can be biased and unfair to specific populations (Janiesch et al., 2021). Furthermore, the training data sets for the AI algorithms are often not large enough or representative of the general population (Esmaeilzadeh, 2020; Gerlick & Liozu, 2020). This could put underrepresented and underserved groups at a systematic disadvantage.

Marketers should consider multiple complementary models to reduce AI biases (Thiebes et al., 2020). Combining multiple models and inputs is likely to result in richer insights. In addition, companies need to be mindful of the data sources, avoiding misrepresentative or inapplicable data sets since the integrity of the algorithms behind AI depends on the quality of the training datasets (Gerlick & Liozu, 2020; Kumar et al., 2022). If a model is trained to predict the future online market, the training data upon which it is built must accurately reflect that online market. Conversely, AI algorithms could lead to biased or wrong predictions (Lavorgna et al., 2020). Another good way to mitigate AI biases is by maintaining the right level of human interaction in the AI decision-making process while scrutinizing the data sources (Howard et al., 2017). Other strategies include capturing training data from a pool that provides quantity, quality, and diversity. Without diversity in the training

Figure 10. Studies on the AI bias in electronic markets



Author	Journal	Theoretical basis	Dataset	Consequence of AI biases	Managerial strategies	Future research recommendations
Gerlick and Liozu. (2020)	Journal of Revenue and Pricing Management	• Nissenbaum's contextual integrity theory • Constructivist grounded theory method	Uncertain literature	The extent to which consumers develop an awareness of discriminatory pricing practices leads to a "culture of suspicion and envy," illuminating a growing social concern	Policies to prevent inequitable application of big data should focus on risk-based pricing in high-stakes markets such as employment, insurance, or credit provision	• Use of countervailing technologies to disrupt the cycle of algorithmic self-learning or negate its impact altogether.
Thiebes et al. (2020)	Electronic Markets	• Trustworthy artificial intelligence • Trust conceptualizations		Such training data bias creates tension between input data and the TAI principle of justice	Technical and non-technical means to create large, high-quality data sets and enable their availability in areas that are particularly beneficial to society	• How to design a token economy such that it is effective in stimulating public participation and the generation of more diverse AI training data?
Lauterbach. (2019)	Digital Policy, Regulation and Governance	• Artificial intelligence • Concepts shaped by social sciences AI technology stack		Lack of AI bias would increase cybersecurity risk and lead to negative shifts in employment	Engineers and developers should take steps to ensure they do not accidentally create something that is just as racist, sexist, and xenophobic as humanity can be	
Howard et al. (2017)		• Trustworthy artificial intelligence • Trust conceptualizations	Four datasets of children's faces that are publically available	The Machine learning models will exhibit the same (human-)induced tendencies that are present in the data or even amplify them.	Develop a layered approach to this problem that combines the results of a generalized learning algorithm with those of a specialized learner	•Validate the approach with a focus on a different minority class, a different classification problem, and different generalized machine learning algorithms.
Janiesch et al., (2021)	Electronic Markets			The misuse of AI in electronic markets can pose severe threats with societal implications when abusing them for malicious purposes	Companies must put strategies in place to identify, track, and counter concept drift that impacts the quality of their intelligent system's decisions.	•Automated strategies for discovering and solving business-related problems are a challenge

data, the algorithm will not identify a wide range of possibilities, making the algorithm ineffective (Lam et al., 2022; Li, Yu et al., 2019).

Concerning research gaps and opportunities for further research on AI bias, the discipline of AI bias in electronic markets should be filled, maintained, and utilized. While researchers across disciplines have made some progress in figuring out how to reduce AI disparities caused by human bias and how to deploy AI more equitably, further exploration is needed. Although there are many methods for mitigating bias, which methods perform best is still inconclusive (Thiebes et al., 2020). To deal with biases, different application areas and real-world challenges that manifest themselves should be covered by benchmark datasets. Finally, AI developers and customers involved in the decision-making process in the electronic market should be aware of AI bias issues and the impact of their choices in using AI.

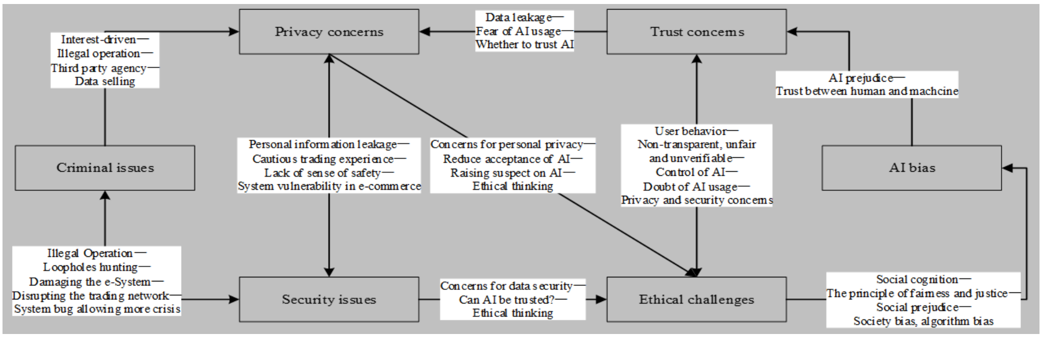
Correlations of the Dark Sides of AI in Electronic Markets

Having discussed the six adverse aspects of AI in electronic markets, we then examined the interrelationships among these aspects by constructing a relational graph through content analysis, as depicted in Figure 11. The arrowhead signifies that the source issue could potentially trigger or lead to the target issues. The double-headed arrow indicates a reciprocal relationship between two issues, suggesting that their coexistence could intensify the challenges posed by AI systems in electronic markets. For example, the criminal issues of AI in e-commerce are implemented by illegal organizations. They prey on online economic vulnerabilities, damage electronic systems for profit, disrupt trading networks, threaten online trading networks, and cause security problems through AI technologies. On the other hand, those electronic bugs allow for more crises in return, creating a vicious cycle for malicious AI in e-commerce. The relationships between the associations are indicated in the literature. For example, Gligor et al. (2021) proposed that the demotivation arising from a lack of personal interactions and emotional exchanges can lead to a decline in affective commitment, thereby fueling organizational inertia. Similarly, blockchain can enhance trust within the system (Teoh, 2022). Too much trust can lead to a lack of information search and complacency. New technologies can lead to inertia by limiting creativity, fueling demoralization among employees, and creating too much trust within the system. Graphically, privacy concerns and ethical challenges are at the center. They are considered primary issues of AI usage in the electronic market and require close attention from governments and societies. Less significant AI challenges include security issues and trust concerns between humans and machines. Finally, criminal issues and AI bias in e-commerce still need to be brought to the forefront of AI governance. The correlation graph suggests that the government and related institutes are aware of the situation of malicious AI. It also guides the management of AI usage in the electronic market.

Privacy concerns, security issues, ethical challenges, criminal and terrorist activities enabled by AI, trust issues between humans and machines, and AI biases introduced in electronic markets are significantly correlated with each other. These factors have both direct and indirect effects on each other; for instance, privacy breaches can lead to compromised security (Azzutti, 2022; Thamik & Wu, 2022). Ethical challenges arise in electronic markets through the use of AI, particularly regarding data handling, algorithmic fairness, and potential unintended consequences (Marjerison et al., 2022). The exploitation of AI technologies by criminals and terrorists poses additional security risks and ethical dilemmas. Trust issues can arise between humans and machines when AI systems fail to meet expectations or when biases in the algorithms are perceived as unfair or discriminatory (Howard et al., 2017). It is crucial to address these complex correlations to facilitate the responsible and sustainable use of AI technologies in the electronics market.

In addition to the six dark sides discussed in this paper, other concerns exist regarding the development of AI. First, AI models the data through self-training. Therefore, its models lack theories to support them (Lavorgna et al., 2020). Their understanding may deviate from reality in exceptional circumstances, leading them to make poor judgments. Second, the volume of AI-based transactions is

Figure 11. Correlations among six dark sides of AI in electronic markets



still small compared to the size of the electronic market. The use of AI in e-commerce could potentially create liquidity risks in some small-scale markets. Third, many countries have incomplete or even inaccurate credit entry data. It is difficult to guarantee that spurious data will not mislead models of AI techniques. Solutions to these problems remain unclear.

IMPLICATIONS

This paper has presented and extracted six dark sides of AI in electronic markets. Assessing and using AI, such as ChatGPT, in electronic markets can yield significant advantages, including increased efficiency, improved decision-making, and enhanced customer experiences.

To ensure the future adoption of AI in electronic markets, it is vital to identify key areas of AI applications. These may include customer service, where AI chatbots such as ChatGPT can be utilized, as well as price optimization, demand forecasting, supply chain management, and fraud detection. To effectively evaluate AI models, testing them using real-world data and examining related metrics, such as accuracy and recall, for a given task is crucial. Stringent data privacy and security measures must be in place, especially when dealing with sensitive information with AI systems to prevent potential data breaches. Moreover, it is crucial to ensure that AI solutions such as chatbots are user-friendly and provide a positive customer experience. It is essential to be mindful of the ethical implications of AI usage, which involves addressing fairness, transparency, and accountability issues. To achieve this, it is crucial to be transparent with users about when and how they interact with AI while minimizing biases in the AI-generated responses.

Before fully rolling out an AI solution, it is advisable to conduct pilot tests to assess its functionality and usefulness and identify any potential issues that need to be addressed. Finally, it is crucial to ensure that the AI system can handle increased user interactions or data processing without significant performance degradation.

Theoretical Implications

Theoretically, the literature review presented in this study has provided a rigorous and structured overview of research on AI's dark sides in the electronic markets through a combination of quantitative and qualitative analysis of the AI literature. A systematic search led to 24 publications studying any dark side of AI in electronic commerce. The theoretical basis, dataset, core opinion, consequences of AI's dark sides and the solutions, and future research recommendations were all summarized and compared among the prior studies. We also showed the correlations of the six dark sides of AI in electronic markets. Given the practices of disguising employees' and customers' concerns about privacy, security, ethics, untrusting, and bias problems, merely mining such data for research or to inform public services raises ethical challenges. This is especially true when consent has not or cannot be obtained. There is a need for further research to assess the extent to which economic measures are consistent with laws or policies and also acceptable to the stakeholders. We hope to provide the authors with an in-depth understanding of AI's dark sides in the electronic market through thorough analysis.

Practical Implications

On the practical level, we aim to provide guidance for the government and institutions for AI regulations. As technological advances in AI have made rich contributions to various applications in electronic markets, special care should be taken regarding the dark side of AI. Governments and policymakers are recommended to establish legislation to ensure that AI-powered innovation (Wang et al., 2022) and implementation are beneficial to the social good while limiting the threat posed by the dark side of AI. It is also crucial for regulations to regularly assess their AI applications, approaches, and practices to ensure proper and responsible use of AI for themselves and their customers. Governments should increase the use of information security technology in the electronic market. Taking information encryption technology as an example, when applying AI, organizations involved in the electronic market should closely combine AI with information encryption technology to improve the security of AI systems to prevent customer information from being stolen and intercepted and avoid the risk of information leakage. Appropriate laws, policies, and regulations must be developed and enforced in countries where AI is applied in the electronic market.

CONCLUSION

The application of AI has accelerated the transformation of digital services in the electronic market and provided an impetus for further growth. However, AI presents various ethical, legal, and social challenges when AI technologies are used in electronic markets. If these risks are not managed effectively, there will be serious consequences for the future growth of the electronic market.

This paper involves several limitations. Our selection was limited to English-language articles, which may have resulted in overlooking relevant articles published in other languages. Moreover, this study did not encompass the gray literature pertaining to the dark side of AI, which could have possibly offered some valuable contributions. Despite these limitations, this research has successfully provided insightful knowledge and enhanced our understanding of the dark side of AI in the electronic market, as well as strategies to address these challenges.

Future research could delve into other negative aspects of AI in electronic markets and suggest an AI governance framework to assist governments and regulators in effectively managing these dark sides of AI. Subsequent research should take an interdisciplinary approach, bolstering research at the crossroads of people, technology, and organizations. This would aid in identifying user expectations, investigating potential privacy violations, imposing penalties for non-compliance, and discerning approaches to mitigate the risks consumers face.

ACKNOWLEDGMENT

This research is funded by the National Social Science Fund of China (22CTQ019).

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. doi:10.1126/science.aaa1465 PMID:25635091

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442–492. doi:10.1257/jel.54.2.442

Akter, S., Dwivedi, Y. K., Biswas, K., Michael, K., Bandara, R. J., & Sajib, S. (2021). Addressing algorithmic bias in AI-driven customer management. *Journal of Global Information Management*, *29*(6), 1–27. doi:10.4018/JGIM.20211101.oa3

Alavi, M., & Carlson, P. (1992). A review of MIS research and disciplinary development. *Journal of Management Information Systems*, *8*(4), 45–62. doi:10.1080/07421222.1992.11517938

Azzutti, A. (2022). Ai trading and the limits of EU law enforcement in deterring market manipulation. *Computer Law & Security Report*, *45*, 105690. doi:10.1016/j.clsr.2022.105690

Bai, R., & Lin, B. (2022). Access to credit and green innovation: Do green finance and digitalization levels matter? *Journal of Global Information Management*, *30*(1), 1–21. doi:10.4018/JGIM.315022

Bandara, R., Fernando, M., & Akter, S. (2019). Privacy concerns in e-commerce: A taxonomy and a future research agenda. *Electronic Markets*, *30*(3), 629–647. doi:10.1007/s12525-019-00375-6

BBC. (2021, April 21). EU artificial intelligence rules will ban "unacceptable" use. *BBC News*. https://www.bbc.com/news/technology-56830779

Brill, T. M., Munoz, L., & Miller, R. J. (2019). Siri, Alexa, and other digital assistants: A study of customer satisfaction with artificial intelligence applications. *Journal of Marketing Management*, *35*(15–16), 1401–1436. doi:10.1080/0267257X.2019.1687571

Brynjolfsson, E., & Mitchell, T. (2017). What can machine learning do? Workforce implications. *Science*, *358*(6370), 1530–1534. doi:10.1126/science.aap8062 PMID:29269459

Caldwell, M., Andrews, J. T., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(14), 1–13.

Castillo, D., Canhoto, A. I., & Said, E. (2020). The dark side of AI-powered service interactions: Exploring the process of co-destruction from the customer perspective. *Service Industries Journal*, 1–26.

Chang, F. K., Hung, W. H., Lin, C. P., & Chang, I. C. (2022). A self-assessment framework for global supply chain operations: Case study of a machine tool manufacturer. *Journal of Global Information Management*, *30*(1), 1–25. doi:10.4018/JGIM.298653

Chen, C. M., Cai, Z. X., & Wen, D. W. M. (2021). Designing and evaluating an automatic forensic model for fast response of cross-border e-commerce security incidents. *Journal of Global Information Management*, *30*(2), 1–19. doi:10.4018/JGIM.20220301.oa5

Cheng, X., Su, L., Luo, X., Benitez, J., & Cai, S. (2021). The good, the bad, and the ugly: Impact of analytics and artificial intelligence-enabled personal information collection on privacy and participation in ridesharing. *European Journal of Information Systems*, *31*(6221), 1–25.

Coeckelbergh, M. (2016). The invisible robots of global finance. *Computers & Society*, *45*(3), 287–289. doi:10.1145/2874239.2874280

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society*, *1*(1), 104–126. doi:10.1007/BF03177550

Du, X., Zhao, X., Wu, C., & Feng, K. (2022). Functionality, emotion, and acceptance of artificial intelligence virtual assistants: The moderating effect of social norms. *Journal of Global Information Management*, *30*(7), 1–21. doi:10.4018/JGIM.290418

Dubey, S., Salwan, P., & Agarwal, N. K. (2021). Application of machine learning algorithm in managing deviant consumer behaviors and enhancing public service. *Journal of Global Information Management*, *30*(5), 1–24. doi:10.4018/JGIM.292064

Esmaeilzadeh, P. (2020). Use of AI-based tools for healthcare purposes: A survey study from consumers' perspectives. *BMC Medical Informatics and Decision Making*, *20*(170), 1–19. doi:10.1186/s12911-020-01191-1 PMID:32698869

Fletcher, G. G. (2021). Deterring algorithmic manipulation. *Vanderbilt Law Review*, *74*(2), 101.

Gerlick, J. A., & Liozu, S. M. (2020). Ethical and legal considerations of artificial intelligence and algorithmic decision-making in personalized pricing. *Journal of Revenue and Pricing Management*, *19*(2), 85–98. doi:10.1057/s41272-019-00225-2

Gligor, D. M., Pillai, K. G., & Golgeci, I. (2021). Theorizing the dark side of business-to-business relationships in the era of AI, Big Data, and Blockchain. *Journal of Business Research*, *133*, 79–88. doi:10.1016/j.jbusres.2021.04.043

Haverila, M., Haverila, K. C., Mohiuddin, M., & Su, Z. (2022). The impact of quality of big data marketing analytics (BDMA) on the market and financial performance. *Journal of Global Information Management*, *30*(1), 1–21. doi:10.4018/JGIM.315646

Hossain, M. A., Akter, S., Yanamandram, V., & Gunasekaran, A. (2022). Operationalizing artificial intelligence-enabled customer analytics capability in retailing. *Journal of Global Information Management*, *30*(8), 1–23. doi:10.4018/JGIM.298992

Howard, A., Zhang, C., & Horvitz, E. (2017). Addressing bias in machine learning algorithms: A pilot study on emotion recognition for Intelligent Systems. In *2017 IEEE Workshop on Advanced Robotics and Its Social Impacts (ARSO)*. IEEE. doi:10.1109/ARSO.2017.8025197

Huang, C., Chou, T., & Wu, S. (2021). Towards convergence of AI and IoT for smart policing: A case of a mobile edge computing-based context-aware system. *Journal of Global Information Management*, *29*(6), 1–21. doi:10.4018/JGIM.20211101.oa2

Huawei. (2019). *AI security white paper*. Huawei Technologies Co., Ltd. https://www.huawei.com/en/trust-center/resources/ai-security-white-paper

Ifinedo, P., Mengesha, N., & Bekele, R. (2022). Effects of Personal Factors and Organizational Reinforcing Tools in Decreasing Employee Engagement in Unhygienic Cyber Practices: Perspectives From a Developing Country. *Journal of Global Information Management*, *30*(1), 1–27. doi:10.4018/JGIM.299324

Jabbarpour, M. R., Saghiri, A. M., & Sookhak, M. (2021). A framework for component selection considering dark sides of artificial intelligence: A case study on autonomous vehicle. *Electronics (Basel)*, *10*(4), 384. doi:10.3390/electronics10040384

Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. *Electronic Markets*, *31*(3), 685–695. doi:10.1007/s12525-021-00475-2

Jebarajakirthy, C., Saha, V., Goyal, P., & Mani, V. (2022). How do value co-creation and e-engagement enhance e-commerce consumer repurchase intention?: An empirical analysis. *Journal of Global Information Management*, *30*(5), 1–23. doi:10.4018/JGIM.290369

Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape. *ACM Computing Surveys*, *53*(1), 1–34. doi:10.1145/3372823

Karimova, G. Z., & Goby, V. P. (2020). The adaptation of anthropomorphism and archetypes for marketing artificial intelligence. *Journal of Consumer Marketing*, *38*(2), 229–238. doi:10.1108/JCM-04-2020-3785

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, *34*(2), 369–400. doi:10.1080/07421222.2017.1334467

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*(1), 89–120. doi:10.1007/s11948-018-00081-0 PMID:30767109

Kozinets, R. V., & Gretzel, U. (2020). Commentary: Artificial intelligence: The marketer's dilemma. *Journal of Marketing*, *85*(1), 156–159. doi:10.1177/0022242920972933

Kumar, R., Chau, K. Y., Negash, Y. T., & Tang, Y. M. (2022). Modeling business-to-business sharing drivers using a hierarchical framework under uncertainties. *Journal of Global Information Management*, *30*(1), 1–25. doi:10.4018/JGIM.301615

Lam, H. Y., Tsang, Y. P., Wu, C. H., & Chan, C. Y. (2021). Intelligent e-vendor relationship management for enhancing global B2C e-commerce ecosystems. *Journal of Global Information Management*, *29*(3), 1–25. doi:10.4018/JGIM.2021050101

Lauterbach, A. (2019). Artificial intelligence and policy: Quo vadis? *Digital Policy. Regulation & Governance*, *21*(3), 238–263. doi:10.1108/DPRG-09-2018-0054

Lavorgna, A., Middleton, S. E., Pickering, B., & Neumann, G. (2020). FloraGuard: Tackling the online illegal trade in endangered plants through a cross-disciplinary ICT-enabled methodology. *Journal of Contemporary Criminal Justice*, *36*(3), 428–450. doi:10.1177/1043986220910297

Lee, W. S. (2022). Analyzing the evolution of interdisciplinary areas: Case of Smart Cities. *Journal of Global Information Management*, *30*(1), 1–23. doi:10.4018/JGIM.304062

Li, C., Chu, J., & Zheng, L. J. (2022). Better not let me know: Consumer response to reported misuse of personal data in privacy regulation. *Journal of Global Information Management*, *30*(1), 1–22. doi:10.4018/JGIM.309377

Li, C., Feng, W. X., Han, S., Gupta, S., & Kamble, S. (2022). Digital adaptive governance, digital transformation, and service quality in logistics enterprises. *Journal of Global Information Management*, *30*(1), 1–26. doi:10.4018/JGIM.309377

Li, G., Deng, X., Gao, Z., & Chen, F. (2019). Analysis on ethical problems of artificial intelligence technology. In *Proceedings of the 2019 International Conference on Modern Educational Technology*. ICMET 2019. doi:10.1145/3341042.3341057

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1), 1–6. doi:10.1080/1097198X.2019.1569186

Li, Z., Dai, R., Feng, X., & Xiong, Y. (2022). The analysis of two-way e-commerce credit evaluation model based on the C2C mode. *Journal of Global Information Management*, *30*(11), 1–21. doi:10.4018/JGIM.305238

Liu, K. P., Chiu, W., Chu, J., & Zheng, L. J. (2022). The impact of digitalization on supply chain integration and performance: A comparison between large enterprises and SMEs. *Journal of Global Information Management*, *30*(1), 1–20. doi:10.4018/JGIM.315301

Liu, Q., & Li, J. (2022). The progress of business analytics and knowledge management for enterprise performance using artificial intelligence and man-machine coordination. *Journal of Global Information Management*, *30*(11), 1–21. doi:10.4018/JGIM.302642

Ma, X., & Zhang, Y. (2021). Digital innovation risk management model of discrete manufacturing enterprise based on big data analysis. *Journal of Global Information Management*, *30*(7), 1–14. doi:10.4018/JGIM.286761

Marjerison, R. K., Zhang, Y., & Zheng, H. (2022). AI in e-commerce: Application of the use and gratification model to the acceptance of chatbots. *Sustainability (Basel)*, *14*(21), 14270. doi:10.3390/su142114270

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. doi:10.1007/s11747-016-0495-4

Mazurek, G., & Małagocka, K. (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, *6*(4), 344–364. doi:10.1080/23270012.2019.1671243

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334–359. doi:10.1287/isre.13.3.334.81

Motlagh, F. P., & Bardsiri, A. K. (2018). Detecting fake websites using swarm intelligence mechanism in human learning. *International Journal of Engineering*, *31*(10), 1642–1650.

Nilashi, M., Ibrahim, O., Mirabi, V. R., Ebrahimi, L., & Zare, M. (2015). The role of security, design and content factors on customer trust in mobile commerce. *Journal of Retailing and Consumer Services*, *26*, 57–69. doi:10.1016/j.jretconser.2015.05.002

Nilsson, N. J. (1971). *Problem-solving methods in artificial intelligence*. McGraw-Hill.

Paul, S. K., Riaz, S., & Das, S. (2022). Adoption of artificial intelligence in supply chain risk management: An Indian perspective. *Journal of Global Information Management*, *30*(8), 1–18. doi:10.4018/JGIM.307569

Pichai, S. (2018, June 7). AI at Google: Our principles. *The Keyword*. https://blog.google/technology/ai/ai-principles/

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *The Journal of Applied Psychology*, *88*(5), 879–903. doi:10.1037/0021-9010.88.5.879 PMID:14516251

Polasik, M., Piotrowska, A. I., Wisniewski, T. P., Kotkowski, R., & Lightfoot, G. (2015). Price fluctuations and the use of bitcoin: An empirical inquiry. *International Journal of Electronic Commerce*, *20*(1), 9–49. doi:10.1080/10864415.2016.1061413

Qiu, J. (2022). Analysis of human interactive accounting management information systems based on artificial intelligence. *Journal of Global Information Management*, *30*(7), 1–13. doi:10.4018/JGIM.294905

Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation-augmentation paradox. *Academy of Management Review*, *46*(1), 192–210. doi:10.5465/amr.2018.0072

Rashidin, M., Gang, D., Javed, S., & Hasan, M. (2022). The role of artificial intelligence in sustaining the e-commerce ecosystem: Alibaba vs. Tencent. *Journal of Global Information Management*, *30*(8), 1–25. doi:10.4018/JGIM.304067

Roche, E. M. (2016). Information and communication technology still a force for good? *Journal of Global Information Technology Management*, *19*(2), 75–79. doi:10.1080/1097198X.2016.1172952

Schuetz, S., & Venkatesh, V. (2020). Research perspectives: The rise of human machines: How cognitive computing systems challenge assumptions of user-system interaction. *Journal of the Association for Information Systems*, *21*(2), 460–482. doi:10.17705/1jais.00608

Shankar, V., Kalyanam, K., Setia, P., Golmohammadi, A., Tirunillai, S., Douglass, T., Hennessey, J., Bull, J. S., & Waddoups, R. (2020). How technology is changing retail. *Journal of Retailing*, *97*(1), 13–27. doi:10.1016/j.jretai.2020.10.006

Shrivastav, M. (2022). Barriers related to AI implementation in supply chain management. [JGIM]. *Journal of Global Information Management*, *30*(8), 1–19. doi:10.4018/JGIM.296725

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals’ concerns about organizational practices. *Management Information Systems Quarterly*, *20*(2), 167–196. doi:10.2307/249477

Son, J. Y., & Kim, S. S. (2008). Internet users’ information privacy-protective responses: A taxonomy and a nomological model. *Management Information Systems Quarterly*, *32*(3), 503–529. doi:10.2307/25148854

Steinhoff, L., Arli, D., Weaven, S., & Kozlenkova, I. R. (2019). Online relationship marketing. *Journal of the Academy of Marketing Science*, *47*(3), 369–393. doi:10.1007/s11747-018-0621-6

Sun, Y., & Li, Y. (2022). The impact of risk-aware consumer trust on CB e-commerce platforms and purchase intention. *Journal of Global Information Management*, *30*(3), 1–13. doi:10.4018/JGIM.20220701.oa10

Sun, Y., & Wang, P. (2022). The e-commerce investment and enterprise performance based on customer relationship management. *Journal of Global Information Management*, *30*(3), 1–15. doi:10.4018/JGIM.20220701.oa9

Tan, X. J., Wang, Y., & Tan, Y. (2019). Impact of live chat on purchase in electronic markets: The moderating role of information cues. *Information Systems Research*, *30*(4), 1248–1271. doi:10.1287/isre.2019.0861

Teoh, S. Y. (2022). Improving shipping efficiency industry-led consortium blockchain smart contact. *Journal of Global Information Management*, *30*(1), 1–32. doi:10.4018/JGIM.313035

Thamik, H., & Wu, J. (2022). The impact of artificial intelligence on sustainable development in electronic markets. *Sustainability (Basel)*, *14*(6), 3568. doi:10.3390/su14063568

Thiebes, S., Lins, S., & Sunyaev, A. (2020). Trustworthy artificial intelligence. *Electronic Markets*, *31*(2), 447–464. doi:10.1007/s12525-020-00441-4

Toader, D.-C., Boca, G., Toader, R., Măcelaru, M., Toader, C., Ighian, D., & Rădulescu, A. T. (2019). The effect of social presence and chatbot errors on trust. *Sustainability (Basel)*, *12*(1), 256. doi:10.3390/su12010256

Trappey, A. J., Chang, A. C., Trappey, C. V., & Chien, J. Y. C. (2022). Intelligent RFQ summarization using natural language processing, text mining, and machine learning techniques. *Journal of Global Information Management*, *30*(1), 1–26. doi:10.4018/JGIM.309082

Vanderelst, D., & Winfield, A. (2018). The dark side of ethical robots. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society.* Association for Computing Machinery. doi:10.1145/3278721.3278726

Varsha, P. S., Akter, S., Kumar, A., Gochhait, S., & Patagundi, B. (2021). The impact of artificial intelligence on branding: A bibliometric analysis (1982–2019). *Journal of Global Information Management*, *29*(4), 221–246. doi:10.4018/JGIM.20210701.oa10

Vidgen, R., Hindle, G., & Randolph, I. (2020). Exploring the ethical implications of business analytics with a business ethics canvas. *European Journal of Operational Research*, *281*(3), 491–501. doi:10.1016/j.ejor.2019.04.036

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay Google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, *120*, 106763. doi:10.1016/j.chb.2021.106763

Vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., & Cleven, A. (2015). Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research. *Communications of the Association for Information Systems*, *37*(9), 205–224. doi:10.17705/1CAIS.03709

Wang, H., Zheng, L. J., Xu, X., & Hung, T. H. B. (2022). Impact of financial digitalization on organizational performance: A look at the dark side. *Journal of Global Information Management*, *30*(1), 1–35. doi:10.4018/JGIM.315307

Wang, X., Zheng, L. J., Li, P. P., & Dong, J. (2022). International Inclusive Innovation of Entrepreneurial Firms: Toward a Process Model. *Journal of Global Information Management*, *30*(1), 1–19. doi:10.4018/JGIM.315307

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *Management Information Systems Quarterly*, *26*(2), xiii–xxiii.

Wing, L., Martinez, J., Katsh, E., & Rule, C. (2021). Designing ethical online dispute resolution systems: The rise of the fourth party. *Negotiation Journal*, *37*(1), 49–64. doi:10.1111/nejo.12350

Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2020). The dark sides of artificial intelligence: An integrated AI governance framework for public administration. *International Journal of Public Administration*, *43*(9), 818–829. doi:10.1080/01900692.2020.1749851

Wu, X. (2021). Analysis of environmental governance expense prediction reform with the background of artificial intelligence. *Journal of Organizational and End User Computing*, *34*(5), 1–19. doi:10.4018/JOEUC.287874

Wu, Z., Zang, C., Wu, C. H., Deng, Z., Shao, X., & Liu, W. (2021). Improving customer value index and consumption forecasts using a weighted RFM model and machine learning algorithms. [JGIM]. *Journal of Global Information Management*, *30*(3), 1–23. doi:10.4018/JGIM.20220701.oa1

Xie, C., Xu, X., Gong, Y., & Xiong, J. (2022). Big data analytics capability and business alignment for organizational agility: A fit perspective. *Journal of Global Information Management*, *30*(1), 1–27. doi:10.4018/JGIM.302915

Xing, F., Peng, G., Wang, J., & Li, D. (2022). Critical obstacles affecting adoption of industrial big data solutions in smart factories: An empirical study in China. *Journal of Global Information Management*, *30*(1), 1–21. doi:10.4018/JGIM.314789

Xu, Z., Xiang, D., & He, J. (2022). Data privacy protection in news crowdfunding in the era of artificial intelligence. *Journal of Global Information Management*, *30*(7), 1–17. doi:10.4018/JGIM.286760

Yang, X., Li, H., Ni, L., & Li, T. (2021). Application of artificial intelligence in precision marketing. *Journal of Organizational and End User Computing*, *33*(4), 209–219. doi:10.4018/JOEUC.20210701.oa10

Yeoh, P. (2019). Artificial intelligence: Accelerator or panacea for financial crime? *Journal of Financial Crime*, *26*(2), 634–646. doi:10.1108/JFC-08-2018-0077

Yu, J., & Yu, H. (2022). Research on C2C e-commerce taxation based on mixed decision game. *Journal of Global Information Management*, *30*(3), 1–14. doi:10.4018/JGIM.20220701.oa8

Yuan, C.-H., Wu, C.-H., Wang, D., Yao, S., & Feng, Y. (2021). Review of consumer-to-consumer e-commerce research collaboration. *Journal of Organizational and End User Computing*, *33*(4), 167–184. doi:10.4018/JOEUC.20210701.oa8

Zhang, X. (2022). B2C e-commerce logistics network optimization model. *Journal of Global Information Management*, *30*(3), 1–19. doi:10.4018/JGIM.20220701.oa7

Zhao, Y. (2021). Risk prediction for Internet financial enterprises by deep learning algorithm and sustainable development of business transformation. *Journal of Global Information Management*, *30*(7), 1–16. doi:10.4018/JGIM.300741

Zheng, K., Zheng, L. J., Gauthier, J., Zhou, L., Xu, Y., Behl, A., & Zhang, J. Z. (2022). Blockchain technology for enterprise credit information sharing in supply chain finance. *Journal of Innovation & Knowledge*, *7*(4), 100256. doi:10.1016/j.jik.2022.100256

Zheng, L. J., Wang, Y. A., Lin, H. Y., & Liu, W. (2023). Understanding circular economy adoption by SMEs: A case study on organizational legitimacy and Industry 4.0. *Industrial Management & Data Systems*, *123*(4), 1157–1177. doi:10.1108/IMDS-04-2022-0266

Zheng, L. J., Zhang, J. Z., Au, A. K. M., Wang, H., & Yang, Y. (2023). Leveraging technology-driven applications to promote sustainability in the shipping industry: The impact of digitalization on corporate social responsibility. *Transportation Research Part E, Logistics and Transportation Review*, *176*, 103201. doi:10.1016/j.tre.2023.103201

Yunfei Xing is a faculty member at the School of Business and Management at Jilin University. Her research interests include social media analysis, big data, information processing, text mining, cultural analysis, and electronic business.

Lu Yu is a Ph.D. Candidate at the School of Management, Zhejiang University, China. Her research interests include information privacy, interfirm collaboration, and digital innovation. Her work has been published in such outlets as the International Journal of Information Management, the Journal of Global Information Technology Management, and Behaviour & Information Technology.

Justin Zhang is a faculty member in the Department of Management at Coggin College of Business at the University of North Florida. He received his Ph.D. in Business Administration with a concentration in Management Science and Information Systems from Pennsylvania State University, University Park. His research interests include economics of information systems, knowledge management, electronic business, business process management, information security, and social networking. He has published research articles in various scholarly journals, as well as books and conference proceedings. He is the editor-in-chief of the Journal of Global Information Management. He also serves as an associate editor and an editorial board member for several other journals.

Leven J. Zheng is an Assistant Professor of Management in the Department of Global Business and Marketing, Hong Kong Metropolitan University. He received his Ph.D. in Innovation and Entrepreneurship from the Management School at the University of Liverpool. His research interests focus on entrepreneurship, newly public firms, new product development, entrepreneurial founding teams and senior management teams as well as entrepreneurial internationalization. His research has appeared in the Journal of Business Research, Technovation, and Technological Forecasting & Social Change. He uses both qualitative and quantitative research methods. He also serves as an entrepreneurship counsellor for the ChuangPlus (student) entrepreneurship incubator at Tsinghua University, PR China, and an Entrepreneurship and Innovation Mentor at Suzhou Mudu Economic Development Zone and Suzhou Wuzhong Science and Technology Park, PR China.