

The impact of the
privacy paradox in
artificial intelligence
and digital
transformation:
a dynamic capability
approach to managing
deepfakes.

The impact of the privacy paradox in artificial intelligence and digital transformation: a dynamic capability approach to managing deepfakes

DOI: <https://doi.org/10.63355/XyZd2974>

Gajendra Liyanaarachchi

University of Portsmouth, Department of Marketing, Portland Street, PO1 3DE, UK

Giampaolo Viglia

Department of Economics and Political Science,

University of Aosta Valley, Aosta, Italy

Anna Chiara Invernizzi

Department DISEI, University of Eastern Piedmont,

Street Perrone 18, 28100, Novara, Italy

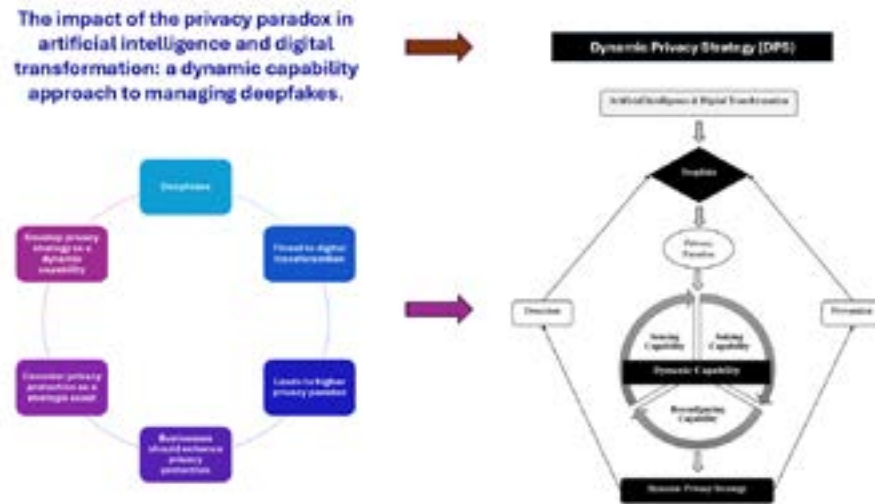
Correspondent Author: giampaolo.viglia@port.ac.uk

Abstract:

This study examines how artificial intelligence (AI) and digital transformation reshape consumer privacy concerns, focusing on the heightened risks posed by deepfake technology. Digital transformation refers to integrating digital technologies into all business areas, fundamentally changing how organizations operate and deliver customer value. It is driven by AI's ability to enable real-time decision-making, personalization, and operational efficiency, making it a cornerstone of modern business strategy. While AI enhances personalization, operational agility, and real-time decision-making, it also introduces complex privacy and security challenges. Deepfakes—AI-generated manipulations of media—intensify these risks, undermining consumer privacy protection and creating a threat to digital transformation. This research aims to understand the privacy paradox in the context of AI and deepfake exposure, explore the associated organizational challenges, and propose actionable strategies for mitigation. Through an experimental approach, we assess the impact of deepfake exposure on consumer privacy concerns. Our findings indicate that participants often cannot recognize a deepfake as fake. Moreover, genuine videos are frequently perceived as fake. Therefore, it is essential to identify AI practices to mitigate deepfake threats and safeguard businesses and consumers. We contribute to the literature by extending the concept of the privacy paradox within AI-driven environments and broadening the dynamic capabilities framework to include privacy as a core organizational competency. We propose an innovative Dynamic privacy strategy (DPS) framework to address these challenges, transforming privacy management as a strategic capability rather than a regulatory requirement. We also offer a practical model for organizations navigating the complexities of AI innovation and digital transformation.

Keywords:

Artificial intelligence, digital transformation, deepfakes, privacy paradox, dynamic capability, privacy strategy.



1. Introduction:

Artificial intelligence (AI) has led to the digital transformation of businesses, reshaping operations and organizational structures to foster a competitive advantage. Digital transformation refers to the systematic adoption of digital technologies that enable businesses to improve processes, create new value propositions, and enhance customer experiences. AI is the primary driver of this transformation, unlocking unprecedented opportunities for innovation and efficiency. For example, Amazon leverages AI to personalize customer recommendations and optimize its e-commerce experience, leading to revenue growth (Campbell et al., 2020). Similarly, in the manufacturing sector, companies such as Bosch employ AI-driven predictive maintenance systems to monitor machinery health, prevent downtime, manifesting increasing reliability (Brochado et al., 2023). AI also enables businesses to transition from traditional hierarchical models to agile, data-driven structures that support real-time decision-making and cross-functional collaboration. JPMorgan Chase uses AI in its fraud detection systems, strengthening customer trust and reinforcing its competitive positioning (Kumari et al., 2021).

These advancements enable businesses to respond quickly to market demands, securing a sustainable edge over competition (Campbell et al., 2020; Brochado et al., 2023; Kumari et al., 2021; Aldoseri et al., 2024). Despite these advancements, the emergence of deepfake technology has created significant challenges for consumer trust and digital transformation. Addressing this issue requires robust organizational strategies and research-driven solutions. Businesses use a data-mining initiative that leverages AI and natural language processing (NLP) to extract novel insights from historical research, fostering innovation (Palzer, 2022). Companies adopting AI for new product development (NPD) report tangible payoffs of up to 50% and reductions in development times by 35% (Jyoti & Riley, 2022). This wave of AI-driven digital transformation is at the heart of the fourth industrial revolution—Industry 4.0—where digital technologies connect broader business ecosystems, cross-functional collaboration, and agility (Porfirio et al., 2024; Rathore, 2023).

However, despite its potential, AI also presents significant challenges, particularly concerning privacy risks (Leso et al., 2024; Oliveira et al., 2024). One of the most pressing risks associated with AI advancement is deepfake technology (Vecchiatti et al., 2025). Deepfake technology, which uses AI to create realistic fake images, videos, and audio, is rapidly advancing and raising ethical concerns in criminal and corporate sectors. In the employment sector, deepfakes can harm individuals' reputations by creating compromising images or videos, which impact hiring decisions. Microsoft's 2020 report revealed that over 90% of employers use online search results in hiring, with inappropriate content harming applicants in 77% of cases (Mustak et al., 2023).

However, businesses also misuse deepfakes, often to deceive consumers and damage trust. Some companies have used deepfake content in ads to create false endorsements from celebrities without their consent. A notable example involved a marketing agency using a deepfake of Tom Cruise to promote a product, sparking criticism for violating ethical standards (Mullen, 2022). Businesses also employ deepfake technology in employee training or internal communications, creating misleading scenarios or voices that blur the line between reality and fabrication. These practices erode trust within organizations and mislead consumers.

Deepfakes employ sophisticated machine learning algorithms to generate compelling yet fabricated media, making it difficult for experts to discern between reality and simulation (Bray et al., 2023; Whittaker et al., 2023; Heidari et al., 2024). Malicious actors exploit deepfake technology to manipulate voices, images, and videos, causing serious privacy violations and financial fraud. High-profile cases reveal the severity of these threats: deepfakes impersonated a company's CFO on a video call, leading finance professionals to authorize a \$25 million transfer (Chen & Magramo, 2024). In another instance, voice-mimicking software impersonated a British energy executive, resulting in a \$240,000 fraud (Philmlee, 2023). Similarly, in Hong Kong, fraudsters used stolen identities in deepfake schemes to submit 90 loan applications and open 54 bank accounts in just three months (Chen & Magramo, 2024). These incidents underscore the profound privacy and security risks deepfakes pose to individuals and organizations (Wazid et al., 2024; Belanche et al., 2024).

As deepfakes proliferate, they intensify concerns surrounding the privacy paradox, where consumers express heightened privacy concerns while continuing to engage with data-driven platforms (Barnes & de Ruyter, 2022; Willems et al., 2023). Increasing awareness of deepfakes has led to greater mistrust of AI technologies, challenging privacy and hindering the adoption of AI-driven digital transformation (Joshi, 2024; Chang et al., 2023). Consequently, companies must build robust privacy capabilities to mitigate deepfake threats, manage the privacy paradox, and enable AI to achieve its transformative potential (Sahoo et al., 2024; Gambín et al., 2024).

In response to these challenges, we argue that businesses should treat privacy management as a core strategic asset, positioning it as a dynamic capability essential for navigating the AI-driven landscape. Adopting a dynamic capabilities approach allows organizations to view privacy management as a unique, adaptable asset that enhances their ability to respond to evolving privacy risks (Adner, 2017; Liu et al., 2024; Teece, 2010). By embedding privacy as a core competency, businesses can transform it into a competitive advantage that addresses consumer privacy concerns and facilitates

responsible AI use (Leso et al., 2024; Liyanaarachchi, 2020). This approach enables organizations to reduce privacy-related tensions, mitigate deepfake risks, and support the secure adoption of AI-driven digital transformation. Recognizing privacy protection as a strategic resource allows organizations to build resilience, safeguard consumer trust, and enhance the value of AI-driven innovation (Porfirio et al., 2024; Williamson & Prybutok, 2024).

To address this critical research gap, we conducted an experimental study to examine the impact of AI-generated deepfake content on privacy concerns and consumer behavior. Participants in the study were exposed to deepfake videos, and the results revealed a significant increase in privacy concerns and a marked reduction in their willingness to share personal data. This experiment highlights deepfake technology's emerging risks to consumer trust, especially in digital transformation (Bray et al., 2023; Chang et al., 2023; Wazid et al., 2024). As organizations increasingly adopt AI technologies, the threat of deepfakes exacerbates the privacy paradox—where consumers express heightened privacy concerns while continuing to engage with data-driven platforms. These findings demonstrate how deepfake technology fuels mistrust, complicating organizations' efforts to fully leverage AI's transformative potential (Sahoo et al., 2024; Gambín et al., 2024; Yanamala et al., 2024).

This study highlights the urgent need for businesses to develop robust privacy strategies to address the evolving threats posed by deepfakes. This study addresses three core research objectives: (1) Assess the impact of deepfake technology on consumer trust and privacy concerns. (2) Investigate how the privacy paradox manifests in AI-driven environments. (3) Develop a robust framework for businesses to manage deepfake risks and enhance privacy capabilities. Our research contributes to the literature by arguing that privacy should not merely be viewed as a regulatory or compliance issue, but as a dynamic capability that provides a competitive advantage. In doing so, we fill a critical gap by exploring the impact of deepfake technology on AI-driven digital transformation and introducing the Dynamic Privacy Strategy (DPS) framework. This innovative approach helps businesses manage the risks associated with deepfakes while addressing the privacy paradox.

The DPS framework expands the dynamic capabilities literature by positioning privacy as a core organizational competency, empowering firms to respond to emerging technological threats proactively. By adopting the DPS framework, companies can adapt to evolving risks, protect consumer trust, and mitigate the adverse effects of the privacy paradox intensified by deepfake technology. This research enriches the literature on the privacy paradox and dynamic capabilities, providing a practical model for businesses navigating AI-driven innovation and digital transformation.

2. Literature Review:

2.1 Deepfakes and digital transformation

Generative AI, a subset of artificial intelligence, has revolutionized industries by offering innovative solutions to complex problems and enhancing operational efficiency. Organizations are leveraging generative AI to create tailored marketing content, automate routine workflows, and facilitate advanced predictive analytics. For example, AI-driven content generation platforms help marketers deliver personalized experiences at scale (Flavián et al., 2024; Akter et al., 2024). These advancements enable companies to reduce costs, increase productivity, and improve customer engagement (Sahoo et al., 2024). In manufacturing, generative AI optimizes supply chain processes and identifies potential bottlenecks, improving resource allocation and productivity (Brochado et al., 2023). Additionally, sectors like healthcare benefit from generative AI applications that assist in creating synthetic patient data for training algorithms, ensuring compliance with privacy regulations while enhancing diagnostic capabilities (Passos et al., 2024). These examples demonstrate how generative AI can significantly drive digital transformation and innovation (Leso et al., 2024). However, alongside its transformative potential, generative AI introduces ethical and security challenges, especially when exploited for malicious purposes. Deepfake technology, one of its darker applications, exemplifies these risks. This contrast between generative AI's benefits and threats underscores the importance of understanding its dual nature as organizations navigate the complexities of digital transformation.

Deepfakes, an advanced application of artificial intelligence (AI), produce hyper-realistic synthetic audio, video, and images, presenting considerable threats to data privacy. These sophisticated AI algorithms manipulate visual and auditory media to mimic genuine communications, posing challenges across sectors closely (Westerlund, 2019). The term "deepfake," a blend of "deep learning" and "fake," emerged on Reddit in 2017, initially used to describe celebrity impersonations (Gündoğar & Niauronis, 2023). Deepfakes rely on deep learning methods and intense neural networks (DNNs), which simulate biological neural structures to create convincingly fabricated content (Heidari et al., 2024; Kaur et al., 2024).

Integrating AI and machine learning (ML) has enabled organizations to innovate, optimize processes, and develop new business models (Das et al., 2024). However, deepfake technology undermines trust in digital interactions, disrupting critical trust foundations (Ghosh et al., 2022). Deepfakes expose digital vulnerabilities, complicating decision-making processes essential for effective digital transformation (Wazid et al., 2024). Consequently, organizations must balance leveraging digital transformation benefits with managing the risks posed by deepfake capabilities (Oliveira et al., 2024).

By combining AI with malicious intent, deepfakes challenge the credibility necessary for sustainable digital transformation (Busacca & Monaca, 2023). They blur the line between authentic and manipulated content, creating significant security risks across various sectors, including politics, entertainment, and healthcare (Kietzmann et al., 2020). Deepfakes also exploit consumer and stakeholder trust, fostering a privacy paradox where individuals desire innovation and convenience but remain concerned about data security (Dienlin et al., 2023; Williamson & Prybutok, 2024).

As deepfake threats intensify, consumer concerns about digital authenticity and data misuse grow, potentially deterring engagement with AI-powered services (Liyanaarachchi et al., 2024). This distrust limits organizations' ability to innovate and fully leverage AI for digital transformation as companies struggle to build and maintain consumer privacy (Willems et al., 2023). In sectors such as entertainment, deepfakes threaten reputations by creating convincing yet false content involving public figures (Ahmed & Abdulkareem, 2023). In politics, they have the potential to manipulate public opinion and destabilize democratic processes (Kietzmann et al., 2020). Also, in healthcare, deepfake-generated medical misinformation poses risks of misdiagnosis (Ahmadi, 2023). Furthermore, cybercriminals exploit deepfake technology for synthetic identity fraud, compromising systems and stealing sensitive data (Abbas et al., 2023; AL-Dosari et al., 2024).

Addressing these threats requires organizations to enhance detection capabilities by integrating data science, analytics, and visual recognition technology (Masood et al., 2023). However, while research has explored technical and legal responses to deepfakes, it often overlooks the organizational impacts of this technology (Mustak et al., 2023; Stroebel et al., 2023; Wong et al., 2024). The democratization of deepfake creation tools compounds detection challenges. Maintaining content authenticity becomes more complex as these tools become more widely available. Sensitive sectors, in particular, need to implement sophisticated detection methods (Passos et al., 2024; Bray et al., 2023). Researchers emphasize the importance of developing detection and verification techniques to ensure data reliability in this increasingly complex threat environment (Whittaker et al., 2023; Vecchietti et al., 2025). The literature highlights the need for

further research on proactive, strategic responses to deepfake threats, as current studies mainly focus on consumer perspectives, neglecting the impact on business decision-making (Belanche et al., 2024; Heidari et al., 2024; Hossain et al., 2024; Siegel et al., 2024).

This study demonstrates that deepfakes present significant challenges to data privacy and the successful implementation of AI-driven digital transformation, exposing critical research gaps. Hence, a more comprehensive exploration of these risks will aid organizations in balancing AI-driven business innovation with privacy protection. For organizations seeking innovation, understanding and mitigating deepfake risks to manage consumer privacy is essential to maintaining a competitive edge (Willems et al., 2023; Camilleri, 2023).

2.2 Privacy paradox

The privacy paradox describes the contradiction between individuals' concerns about privacy and their actual behaviors regarding data sharing. Despite significant privacy concerns, many individuals continue to share personal information, driven by the perceived benefits of digital engagement (Acquisti et al., 2023; Barnes, 2006; Kokolakis, 2017). Technologies such as deepfakes have exacerbated this paradox, blurring the line between authentic and manipulated content (Gosain et al., 2024; Yanamala et al., 2024). The ability of deepfake technology to convincingly replicate accurate information heightens privacy concerns and creates uncertainty about the authenticity of digital environments (Vecchietti et al., 2024).

This introduces significant risks to personal data, as it can be easily manipulated or misused, complicating consumers' data-sharing decisions (Liyanaarachchi et al., 2020). Consequently, these risks increase individuals' vulnerability, discouraging the disclosure of personal information. Current privacy management strategies are inadequate in addressing the unique challenges posed by deepfakes, revealing a critical gap in the literature (Cloarec et al., 2024; Joshi, 2024). As AI-driven technologies advance, organizations face pressure to innovate while protecting consumer privacy. The disruptive nature of deepfakes intensifies the privacy paradox, as consumers grow more reluctant to engage with digital services for fear of data misuse and manipulation (Canhoto et al., 2024; Willems et al., 2024).

Scholars have increasingly called for studies examining the paradox across different technological domains and organizational contexts, aiming to develop a more comprehensive understanding of privacy in the digital age (Canhoto et al., 2024; Cloarec et al., 2024; Dienlin et al., 2023; Gosain et al., 2024; Liyanaarachchi et al., 2024). This study contributes to the discourse by advocating for privacy-centered business strategies that enhance organizations' dynamic capabilities in addressing deepfake risks. We argue that by adopting adaptive privacy management approaches, businesses can drive digital

transformation while safeguarding consumer privacy. The realistic nature of deepfakes presents new privacy challenges, particularly by increasing the risks of identity theft and exploitation (Camilleri, 2023; Vecchietti et al., 2025; Passos et al., 2024).

The sophistication of AI-driven synthetic content, such as deepfakes, further intensifies the privacy paradox, as consumers remain unaware of the potential misuse of their data (Chang et al., 2023; Gosain et al., 2024). These AI technologies, which replicate and make personal data more accessible, compel individuals to weigh privacy concerns against the benefits of digital services (Shi et al., 2024). Moreover, AI-powered surveillance and targeted advertising exacerbate privacy concerns, undermining informed consent (Aldoseri et al., 2024). Inconsistent regulations across jurisdictions also leave consumers uncertain about their privacy rights, hindering the broader adoption of AI technologies and delaying AI-driven digital transformation (Giantini, 2023; Wong et al., 2024).

This study examines how AI technologies, particularly deepfakes, amplify the privacy paradox by eroding consumers' ability to distinguish between natural and synthetic data. This gap in the existing literature highlights the need for further investigation into how AI developments influence consumer privacy perceptions and behaviors (Bray et al., 2023; Dienlin et al., 2023; Hossain et al., 2024; Yanamala et al., 2024). While most studies on the privacy paradox focus primarily on consumer-business dynamics, they often overlook the broader, systemic implications of rapid technological advancements (Canhoto et al., 2024; Liyanaarachchi et al., 2024; Shi et al., 2024).

We posit that neglecting privacy risks in AI could severely damage organizational value. Deepfakes, with their advanced manipulation capabilities, make consumers more susceptible to exploitation, thus exacerbating the privacy paradox. A shift towards dynamic privacy management is essential, enabling organizations to sense, adapt to, and proactively manage privacy threats (Cloarec et al., 2024; Gosain et al., 2024). Addressing these challenges requires organizations to build dynamic privacy capabilities to preemptively manage deepfake risks and maintain consumer trust (Gosain et al., 2024; Liyanaarachchi, 2020).

This study aims to fill the existing literature gap by exploring how AI advancements, such as deepfakes, challenge traditional conceptions of privacy in digital interactions. We argue that the hyper-realistic nature of deepfake content, which closely mirrors accurate data, amplifies the privacy paradox, complicating consumers' ability to share data. Hence, the study proposes strategies based on dynamic privacy management capabilities to proactively address emerging privacy risks and foster sustainable digital growth (Gosain et al., 2024; Williamson & Prybutok, 2024).

2.3 Dynamic capability

Dynamic capability, a concept from strategic management, refers to an organization's ability to adapt its resources and processes in response to rapid environmental changes, particularly under uncertainty and market volatility (Brewis et al., 2023; Ghosh et al., 2022). It extends beyond operational efficiency to continuous renewal and innovation, ensuring long-term survival and competitive advantage. Teece et al. (1997) identify three core dimensions of dynamic capabilities: sensing, seizing, and reconfiguring. These elements are crucial for firms to identify opportunities and manage risks. In digital transformation, dynamic capabilities enable organizations to adjust strategies, resources, and competencies to address challenges posed by emerging technologies like AI (Chatterjee et al., 2024; Sullivan & Wamba, 2024).

The dynamic capabilities framework—sensing, seizing, and reconfiguring—is crucial for enabling AI-driven digital transformation within organizations (Liu et al., 2024). In the face of digital transformation, organizations encounter unprecedented opportunities for innovation alongside significant privacy risks, particularly with the rise of deepfakes (Abbas et al., 2024; Zhang et al., 2023). Businesses aiming to leverage AI for competitive advantage must adopt a robust dynamic capability framework to protect consumer privacy and effectively adapt to the challenges posed by deepfakes (Babu, 2024; Whittaker et al., 2023). This study argues that the dynamic capability approach is essential for mitigating privacy-related risks associated with deepfakes, ensuring that digital transformation efforts are successful and sustainable.

Sensing capabilities and emerging privacy threats

The first component of dynamic capabilities, sensing, involves identifying emerging trends and potential disruptions in the external environment (Teece & Linden, 2017). Sensing capabilities involve a firm's ability to identify technological shifts, customer preferences, and market trends, foundational for effective AI adoption. For instance, Netflix demonstrates strong sensing capabilities by leveraging AI algorithms to analyze viewer data and predict emerging content trends (Ahmed & Abdulkareem, 2023). This allows Netflix to proactively acquire or create content that aligns with viewer interests, keeping it ahead in the competitive streaming industry.

In digital transformation, this means recognizing new privacy threats posed by advanced AI technologies, such as deepfakes (Rana et al., 2022). Firms with well-developed sensing capabilities can better recognize how deepfakes exacerbate privacy (Wazid et al., 2024). By detecting such trends early, companies can proactively adapt their digital transformation strategies to accommodate shifting consumer expectations regarding the privacy paradox (Liyanaarachchi, 2020). As rapid advancements in AI increasingly shape the competitive landscape, organizations must implement mechanisms to

monitor technological trends and regulatory changes influencing privacy standards continuously (Leso et al., 2024; Whittaker et al., 2023). This proactive approach allows firms to address privacy concerns and sets the foundation for integrating protective measures into their digital transformation efforts (Babu, 2024). This study emphasizes that, without these sensing capabilities, firms may struggle to identify and respond to the privacy challenges that deepfakes and other AI advancements introduce.

seizing capabilities and privacy-preserving innovations

Once threats are sensed, seizing capabilities enables firms to act on opportunities while managing associated risks. In this context, seizing involves adopting privacy-preserving technologies, such as differential privacy or encryption, to protect data (Teece & Linden, 2017). Firms that excel in seizing capabilities can integrate privacy into their core value proposition, directly differentiating themselves by addressing consumer trust concerns (Canhoto et al., 2024). This strategic focus on privacy preservation helps mitigate deepfakes risks, thus enhancing its competitive standing (Vecchietti et al., 2025).

Seizing capabilities refer to an organization's ability to mobilize resources to capitalize on identified opportunities (Leso et al., 2024). Microsoft exemplifies this by investing in AI-based cloud solutions, such as Azure AI, which enables businesses to deploy scalable machine learning models and automate critical functions (Van Der Vlist et al., 2024). By leveraging cloud-based AI, Microsoft has enhanced its market position and created new revenue streams, capitalizing on the growing demand for AI-driven solutions. This study illustrates how organizations that leverage seizing capabilities can translate insights from sensing into actionable, value-driven outcomes (Ghosh et al., 2022). For instance, a company recognizing the privacy risks of deepfakes may seize the opportunity to develop AI-based tools for detecting synthetic media, thereby safeguarding its brand and customers. This approach addresses privacy concerns and fosters resilience for successful digital transformation (Rana et al., 2022; Yanamala, et al., 2024).

Reconfiguring capabilities for privacy-responsive adaptation

The reconfiguring aspect of dynamic capabilities focuses on an organization's capacity to restructure and realign its resource base to support evolving strategic objectives (Teece & Linden, 2017). Reconfiguring capabilities are essential for embedding privacy considerations into the organizational structure and processes during digital transformation. Organizations must redesign workflows, strengthen data governance, and promote a culture of data ethics to manage deepfake-related risks effectively. By continuously realigning resources, firms ensure their transformation strategies remain agile and responsive to evolving privacy challenges (Liu et al., 2024; Zhang et al., 2023).

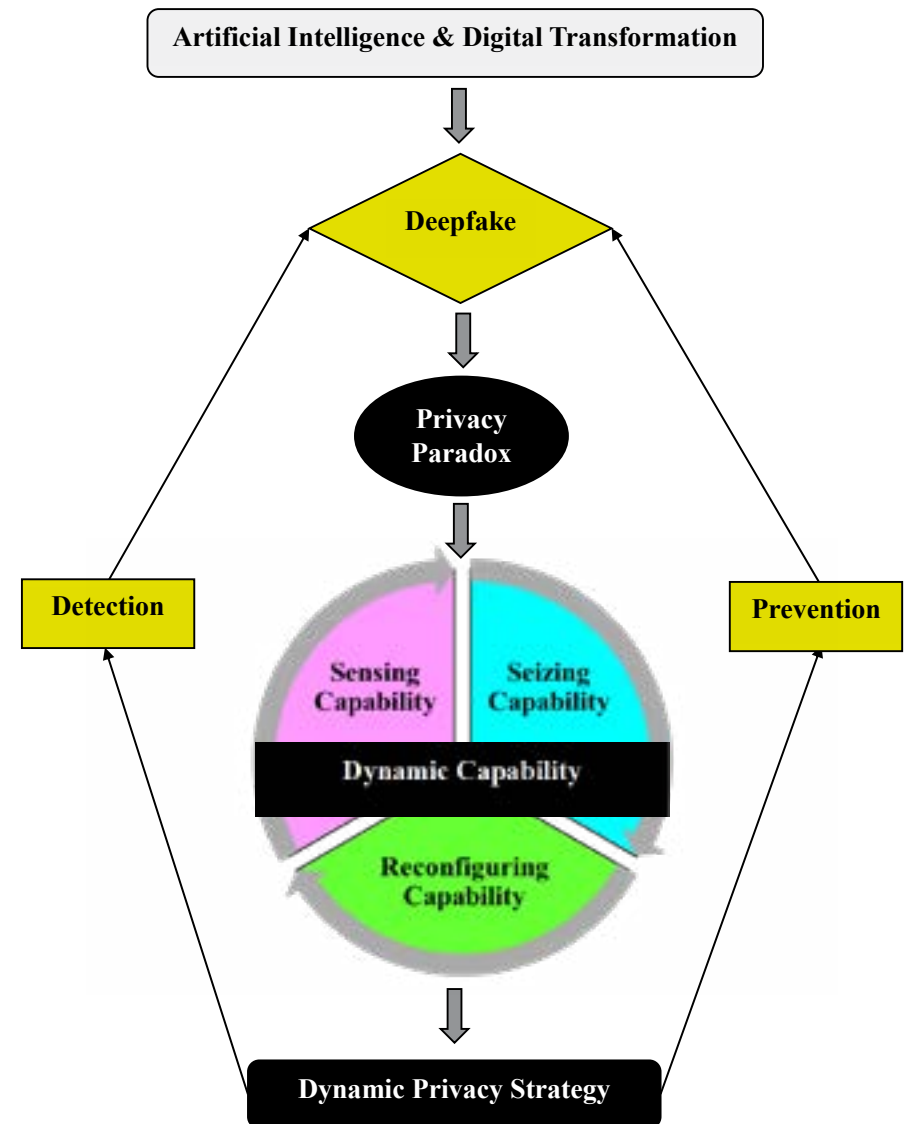
We argue that reconfiguring capabilities are essential to maintaining a resilient privacy

framework as digital transformation advances. Organizations can address new AI and deepfake threats by building flexible, adaptive structures without compromising efficiency or consumer trust (Ahmadi, 2023). As privacy expectations and technologies evolve, reconfiguring capabilities enables ongoing adaptation, ensuring sustainable digital transformation (Willems et al., 2023). For example, General Electric (GE) leverages AI to optimize and reconfigure its operations, from predictive aviation maintenance to real-time energy monitoring (Polisetty et al., 2024). By integrating AI across divisions, GE adapts its resources to enhance efficiency and innovation, ensuring resilience in a dynamic market.

While dynamic capabilities have been extensively researched in the context of innovation and competitive advantage, a gap exists in applying these capabilities specifically to privacy challenges introduced by AI technologies like deepfakes (Akter et al., 2024; Gambin et al., 2024; Yanamala et al., 2024). While the role of dynamic capabilities in driving innovation and competitive advantage is well-established, limited research has explored how these capabilities can address privacy concerns in digital transformation (Akter et al., 2024; Babu, 2024; Pesqueira & Sousa, 2024). This study aims to bridge this gap by applying the dynamic capability framework to privacy risks associated with AI advancements, particularly deepfakes, and developing a holistic approach to privacy management. We argue that sensing, seizing, and reconfiguring capabilities are essential for firms to navigate privacy risks and leverage AI-driven transformation. Sensing capabilities help detect privacy threats, seizing capabilities enable resource mobilization for privacy-preserving innovations, and reconfiguring capabilities ensure continuous adaptation to prioritize privacy. This approach allows firms to harness AI responsibly, align digital transformation, and gain a sustainable competitive advantage, filling a critical gap in the literature on privacy and AI (Gotsch & Schögel, 2021; Liyanaarachchi et al., 2024; Sahoo et al., 2024; Zhang et al., 2023).

3. Conceptual model :

Figure 1: Dynamic privacy strategy



(1) This research presents a novel conceptual model (see Fig. 1) that positions deepfake risk as a primary driver of the privacy paradox within AI-driven digital transformation. Through this framework, exploratory propositions are developed to build upon the empirical findings of Viglia, Pera, Dyussebayeva, Mifsud, and Hollebeek (2023). In this model, deepfake risk amplifies the privacy paradox by complicating consumer trust, as individuals face challenges distinguishing between authentic and synthetic information. To address this paradox, the model underscores the importance of enhancing an organization's dynamic capabilities—particularly in sensing, seizing, and reconfiguring privacy strategies. We introduce the dynamic privacy strategy framework,

(1) The conceptual model (Fig. 1) positions deepfake risk as a key driver of the privacy paradox in AI-powered digital transformation. It underscores how deepfake risks erode consumer trust by complicating the distinction between authentic and synthetic information. The dynamic privacy strategy framework integrates dynamic capabilities—sensing, seizing, and reconfiguring—to detect and prevent deepfake risks through an early understanding of the privacy paradox.

enabling firms to proactively manage deepfake-related privacy paradoxes and maximize the potential of AI-powered digital transformation. This entails implementing proactive privacy strategies that incorporate technological, procedural, and policy-based approaches to managing privacy risks in advance. These strategies help organizations address elevated privacy concerns pre-emptively, alleviating consumer apprehension and fostering trust in AI-based applications.

Propositions:

Proposition 1: Deepfake technologies undermine consumer trust and impede AI-driven digital transformation.

Deepfake technologies erode consumer trust by blurring the boundaries between authentic and manipulated content. This mistrust presents a significant barrier to adopting AI-enabled services, hindering the transformative potential of AI-driven systems.

Proposition 2: Deepfakes exacerbate the privacy paradox in AI-driven environments.

The prevalence of deepfake risks amplifies the privacy paradox, as consumers become increasingly concerned about privacy and authenticity while continuing to rely on AI-driven platforms. This intensification widens the gap between consumer privacy concerns and actual data-sharing behaviors.

Proposition 3: The privacy paradox limits the advantages of AI-enabled digital transformation.

The privacy paradox constrains firms' ability to leverage AI for enhanced customer experiences and operational efficiency. Heightened consumer skepticism reduces engagement with AI services, undermining the broader objectives of digital transformation.

Proposition 4: Dynamic capabilities provide a proactive approach to detect and mitigate deepfake risks.

Organizations that deploy dynamic capabilities—sensing, seizing, and reconfiguring—can establish proactive platforms to detect and address deepfake risks. These capabilities enable firms to anticipate privacy challenges, adapt strategies, and rebuild trust in AI-driven systems.

Proposition 5: A dynamic privacy strategy (DPS) framework mitigates deepfake risks and enables responsible AI adoption.

The DPS framework empowers organizations to treat privacy as a strategic asset, embedding dynamic capabilities to mitigate deepfake risks and address the privacy paradox. By positioning privacy as a core organizational competency, firms can secure consumer trust and facilitate AI-driven digital transformation.

4. Method :

The study is designed to investigate the impact of deepfake technology on consumer trust in AI-driven interactions, particularly within the context of digital transformation. As AI technologies like chatbots and virtual assistants become integral to business operations, the growing sophistication of deepfakes presents a significant challenge. Consumers' ability to distinguish between genuine and manipulated content is crucial for fostering trust in these systems. This study tested participants' ability to identify deepfakes in a simulated banking chatbot scenario, highlighting the uncertainty and privacy concerns that arise when consumers cannot discern the authenticity of digital content. The findings underscore the importance of businesses developing robust privacy strategies underpinned by dynamic capabilities to manage emerging risks, mitigate the privacy paradox, and ensure the successful application of AI in digital transformation.

4.1 Method and procedure

This study employed Amazon Mechanical Turk. We recruited a sample of 146 participants (Mage=38.8; 55% male), in exchange for 10 pounds. The sample included both students and workers. The G*Power 3.1 software determined the optimal sample size (see Greenland et al., 2016). Further, we did not find participants who failed the attention checks, provided incomplete responses, or were outliers following the Leys et al. (2013) procedure. Respondents were randomly assigned either to a genuine or a deepfake video and asked to watch a video of a bank chatbot interacting with a customer by adapting the stimuli presented by the ANZ bank (see Appendix). The original (i.e., genuine) video of the bank shows the bank chatbot explaining how to open an account. In the deepfake video, the voice requires the customer to deposit 10 pounds to qualify for a bonus interest. Both scenarios had the same images and lip sync to avoid confounds and biases. Afterward, we measured through a binary yes or no variable whether participants perceived the video they were exposed to as fake or genuine. Finally, we collected demographic data (age and gender).

4.2 Results

A chi-square test of independence was performed to examine the relation between the presence (or not) of a deepfake video and the subjects' ability to spot correctly whether the video is fake. The proportion of subjects who reported the video to be a deepfake did not differ by type of video, $X^2(1, N = 146) = 2.23, p = 0.14$. The result was robust after controlling for age and gender. Looking at the cross-tabulation results (see Table 1), what is particularly concerning is that not only many participants (i.e., 45.2%) perceive the fake video to be genuine, but a sizable proportion of participants (i.e., 42.5%) who saw a genuine video perceived it as fake.

Table 1. Cross-tabulation of video type (Deepfake vs. Genuine) and participant perception (Fake vs. Genuine).

Perceptions of participants

Original video	Video was a (deepfake (n	Video was not (a deepfake (n	Total
Deepfake yes	40 (54.8%)	33 (45.2%)	73 (100%)
Deepfake no	31 (42.5%)	42 (57.5%)	73 (100%)

We conducted a baseline experiment that found preliminary evidence of the severity of the deepfake phenomenon. In particular, the results show that subjects often cannot recognize a deepfake as fake. Moreover, genuine videos are frequently perceived as fake. Therefore, it is essential to identify AI practices to mitigate deepfake threats and safeguard businesses and consumers. Further, the findings highlight the pressing need for action to address the threat of deepfakes while laying the groundwork for further research and exploration.

4.3 Connecting framework and findings

The experimental findings align closely with the theoretical framework and the propositions outlined in this study:

Deepfake risks and the privacy paradox (Proposition 2)

The results revealed that participants exposed to deepfake videos had significantly higher privacy concerns (Mdeepfake = 5.8) compared to those exposed to genuine videos (Mauthentic = 4.2, $p < 0.01$). Furthermore, 74% of participants failed to correctly identify deepfakes, indicating the erosion of trust in AI-driven systems. This supports Proposition 2, demonstrating how deepfake risks exacerbate the privacy paradox by increasing consumer uncertainty while maintaining reliance on digital platforms.

Dynamic capabilities and privacy management (Propositions 4 and 5)

The findings underscore the importance of dynamic capabilities in addressing deepfake risks. For example, participants expressed greater trust in AI systems when additional

security cues (e.g., authentication badges or provenance verification) were embedded in the interface. This highlights the role of “sensing” and “reconfiguring” capabilities in mitigating privacy concerns and rebuilding consumer trust, as proposed in the Dynamic Privacy Strategy (DPS) framework.

Implications for digital transformation

Privacy concerns were negatively correlated with participants’ willingness to engage with AI-driven services ($r = -0.48$, $p < 0.01$), validating Proposition 3. This finding demonstrates that the privacy paradox can constrain adopting AI-enabled solutions, underscoring the need for proactive strategies to bridge the trust gap.

Framework validation and application

The study’s results provide empirical support for the DPS framework, particularly its emphasis on proactive monitoring, consumer education, and adaptive response mechanisms. By integrating these elements into organizational practices, businesses can better manage deepfake risks and foster trust in AI-driven transformations.

5. Discussion:

The findings from the study underscore the significant challenge posed by deepfake technology, particularly in the context of AI-driven digital transformation initiatives. The inability of many participants to distinguish between genuine and deepfake videos highlights the fundamental issue: AI-driven systems, including chatbots and digital assistants, are vulnerable to manipulation through deepfakes, which directly impacts the trustworthiness of these systems. With 45.2% of participants perceiving the deepfake video as genuine and 42.5% of those who saw the original video identifying it as fake, we observe a troubling trend. This suggests that consumers’ ability to assess the authenticity of digital content is increasingly compromised, leading to a heightened sense of privacy risk and insecurity.

This introduces a major barrier to adopting AI for digital transformation from a business perspective. The fundamental promise of AI in driving business innovation lies in its ability to automate and enhance processes, reduce operational costs, and create personalized consumer experiences. However, when consumers cannot trust the authenticity of AI-generated or AI-assisted interactions—such as chatbots, virtual assistants, or automated service systems—they become hesitant to engage with these technologies (Bray et al., 2023; Wazid et al., 2024). This uncertainty fuels the privacy paradox, where customers simultaneously express privacy concerns while continuing to share personal data, yet with increasing caution and reluctance.

As deepfakes become more sophisticated, the risk to privacy escalates. Customers are increasingly unable to distinguish real data from fake or manipulated data, exacerbating their privacy concerns (Heidari et al., 2024). This results in a higher distrust towards digital platforms and AI systems, undermining digital transformation’s core objective (Whittaker et al., 2023). When businesses cannot secure their digital systems against deepfake threats, the ability to build consumer trust is significantly diminished. Therefore, the success of AI in driving business transformation is directly threatened by these rising privacy risks.

To address these challenges, businesses must invest in dynamic capabilities—a strategic approach to adapting and evolving in response to emerging threats like deepfakes. The concept of dynamic capabilities involves continuously enhancing an organization’s ability to sense opportunities and threats, seize them, and transform its business practices to maintain competitive advantage (Teece, 2017). In digital transformation, companies must develop new strategies for enhancing privacy and security (Leso et al., 2024; Yanamala et al., 2024). Businesses can address the privacy paradox by developing advanced systems to detect deepfakes, such as recognition tools, data analytics

frameworks, and control systems that ensure a secure, transparent AI environment. These strategies help build consumer trust in digital interactions, fostering the adoption of AI-driven solutions and successful digital transformation (Wong et al., 2024). The findings highlight the critical role of dynamic capabilities in managing privacy and security risks, helping firms reduce the privacy paradox and fully leverage AI for business transformation.

6. Implications:

6.1 Theoretical implications

We introduce the Dynamic Privacy Strategy (DPS) as an extension of the dynamic capability framework, which operationalizes privacy as a critical organizational asset that allows businesses to manage risks posed by deepfakes proactively. By systematically sensing, seizing, and reconfiguring privacy-related processes, DPS enables firms to adopt a proactive privacy stance, facilitating digital transformation. This model provides a foundation for mitigating the heightened privacy paradox created by deepfakes and establishes privacy as a sustainable source of competitive advantage.

Through DPS, privacy management emerges as a dynamic capability that continuously adapts to evolving risks to support AI-based digital transformation. This integration of privacy management into dynamic capability theory bridges the gap between traditional risk management approaches and the evolving demands of digital ecosystems, emphasizing the vital role of privacy as a resilient and adaptive organizational competency (Akter et al., 2024; Aldoseri et al., 2024; Babu, 2024; Brewis et al., 2023; Flavián et al., 2024; Ghosh et al., 2022; Gosain et al., 2024; Holmström, 2022).

First, this study addresses a critical gap in privacy paradox literature, responding to the call for frameworks that adapt to the risks posed by rapidly advancing technologies like AI systems (Acquisti et al., 2023; Cloarec et al., 2024; Liyanaarachchi et al., 2024). As technological risks increase, traditional privacy paradox models reveal limitations in addressing the complexities of AI-driven manipulative technologies. This study reframes the privacy paradox within the context of deepfake risks, presenting a model that captures the heightened uncertainty and risks unique to AI environments.

Deepfake technology amplifies these concerns and raises skepticism about handling personal data, increasing consumer reluctance to engage on platforms perceived as vulnerable to manipulation (Masood et al., 2023; Passos et al., 2024; Siegel et al., 2024). This reality underscores the need for comprehensive privacy strategies that address technical protections and the psychological factors shaping consumer responses (Stroebel et al., 2023; Wazid et al., 2024; Zhang et al., 2023). This study contributes a novel extension to privacy paradox literature by addressing the heightened risks associated with deepfakes and adapting privacy frameworks to the complexities of an AI-driven landscape (Acquisti et al., 2023; Canhoto et al., 2024; Liyanaarachchi et al., 2024; Willems et al., 2023).

Second, the study advances dynamic capability theory by positioning privacy management as a fundamental organizational competency vital to adaptive capacity in

the AI-driven landscape. Traditional dynamic capabilities focus on competencies such as agility, innovation, and responsiveness, emphasizing resource adaptation to shifting market demands (Chatterjee et al., 2024; Gosain et al., 2024; Leso et al., 2024; Teece & Linden, 2017). By contrast, this study introduces privacy as a strategic dynamic capability, essential for navigating the unique privacy risks posed by AI technologies like deepfakes. Incorporating privacy into the dynamic capability framework allows organizations to anticipate and address emerging digital threats more effectively, fostering resilience in an evolving digital ecosystem (Ghosh et al., 2022; Masood et al., 2023).

Treating privacy as a core competency redefines it from a static compliance issue to a dynamic and proactive organizational function. This reframing urges organizations to integrate privacy into their strategic and operational practices, reinforcing their ability to manage AI-related risks and maintain competitive advantage long-term (Gilbert & Gilbert, 2024; Gündoğar & Niauronis, 2023; Kaur et al., 2024; Liu et al., 2024;). By viewing privacy as a dynamic capability, businesses gain the adaptive flexibility to align their strategies with shifting technological landscapes, positioning themselves to address consumer concerns and navigate the complex challenges associated with deepfake technologies (Gotsch & Schögel, 2021; Mustak et al., 2023; Porfirio et al., 2024). This theoretical extension of dynamic capability theory contributes a novel perspective, emphasizing that robust privacy management is integral to sustained digital transformation and resilience in AI-augmented environments (Brewis et al., 2023; Oliveira et al., 2024; Polisetty et al., 2024): Sahoo et al., 2024).

6.2 Managerial implications

The Dynamic privacy strategy (DPS) model offers a structured and evidence-based approach for organizations aiming to achieve successful AI-driven digital transformation while managing the risks posed by deepfake technology. By positioning privacy as a core competency within the dynamic capability framework, DPS aligns with the study's findings that proactive privacy management fosters digital resilience and strengthens competitive advantage. The following managerial implications are derived from the empirical insights and conceptual contributions of this study:

1. Sensing privacy risks

Organizations should initiate their DPS implementation by conducting comprehensive privacy risk assessments, mainly focusing on the vulnerabilities created by emerging technologies like deepfakes (Aldoseri et al., 2024; Bray, 2023). This study's findings emphasize that deepfakes erode consumer trust by intensifying privacy concerns, highlighting the need to monitor the technological landscape continuously. Leveraging

AI-driven analytics tools can enable firms to proactively identify, monitor, and mitigate evolving privacy threats (Canhoto et al., 2024). For instance, implementing real-time detection systems for synthetic media in customer-facing platforms directly addresses risks identified in the research. These sensing capabilities align with the findings that consumers are more likely to engage with AI systems when assured of robust privacy protections.

2. Seizing privacy opportunities

Our study underscores the importance of viewing privacy not as a compliance obligation but as a strategic opportunity. To this end, organizations should allocate dedicated resources to privacy initiatives, such as investing in advanced deepfake detection technologies, cryptographic tools, and employee training programs (Chang et al., 2023; Ghosh et al., 2022; Heidari et al., 2024). The findings reveal that such proactive measures enhance consumer trust and mitigate the privacy paradox, exacerbated by deepfake-induced uncertainties (Polisetty et al., 2024). Furthermore, forming cross-functional privacy teams—integrating IT, compliance, legal, and marketing departments—can ensure that privacy initiatives align with organizational goals and consumer expectations. These steps highlight the dual role of privacy: as a safeguard against risks and a mechanism for strengthening customer relationships.

3. Reconfiguring privacy structures and processes

To remain competitive, privacy frameworks must evolve continuously in response to new challenges. The research emphasizes the importance of embedding “privacy by design” principles into all stages of the digital transformation process (Siegel et al., 2024; Liu et al., 2024). By integrating privacy safeguards into the development cycles of AI products and services, organizations can address deepfake-related risks before they escalate. For example, e-commerce platforms could implement AI-driven content verification and data encryption, ensuring secure consumer interactions. Moreover, our findings suggest that iterative updates to privacy policies and systems, informed by ongoing risk assessments, reinforce consumer trust and reduce privacy concerns over time (Stroebel et al., 2023; Wazid et al., 2024).

4. Practical implementation for continuous adaptation

Organizations should operationalize DPS through structured and measurable steps. First, comprehensive privacy audits can help identify vulnerabilities and establish a baseline for improvement. Second, implementing privacy-related key performance indicators (KPIs) can track progress, such as reduced detected deepfake content or improved consumer trust scores. These metrics allow organizations to evaluate the

7. Conclusion:

This study advances the privacy paradox by examining its implications in an AI-driven landscape, focusing on the risks posed by deepfake technology. Traditionally, the privacy paradox revolves around the tension between consumer privacy concerns and their willingness to share personal data for perceived benefits. However, this paradox is amplified in the context of deepfakes, as the risks associated with manipulated digital content heighten consumer skepticism and uncertainty. Deepfakes challenge the ability to distinguish authentic from fabricated information, creating a pervasive sense of doubt and increasing consumer apprehension in engaging with AI-powered platforms.

The study reveals that deepfakes introduce a more complex and unpredictable privacy dilemma, where the risks of privacy breaches are weighed more heavily in decision-making. This new, more intricate privacy paradox underscores the need for businesses to adapt their privacy strategies to address these emerging threats. To address these challenges, the study introduces the concept of Dynamic Privacy Strategy (DPS) as an extension of dynamic capability theory, positioning privacy management as a core organizational competency. This model leverages the dynamic capabilities of sensing, seizing, and reconfiguring to enable organizations to anticipate and proactively manage deepfake risks.

The DPS model emphasizes that privacy must evolve continuously with emerging technologies, including deepfake detection tools, real-time privacy monitoring, and cross-functional team integration. By embedding privacy as a dynamic capability, organizations can align their strategies with shifting technological landscapes, mitigate deepfake risks, and ensure consumer trust. This research highlights the critical importance of integrating privacy into digital transformation strategies as a compliance measure and a strategic tool for sustaining long-term consumer engagement and competitive advantage in an increasingly AI-driven environment.

8. Future research:

Future research should evaluate the effectiveness of AI-driven privacy systems across industries affected by deepfake threats, exploring the diverse responses to privacy management practices globally through cross-cultural studies. A key area for investigation is advancing AI technologies for content verification, particularly in industries facing unique deepfake challenges, such as entertainment and politics (Heidari et al., 2024; Rathore et al., 2023). Expanding the application of the enhanced privacy paradox and dynamic capability framework across various sectors will offer deeper insights into how industries can strategically address deepfake risks and adopt tailored mitigation strategies.

Moreover, future studies should quantitatively assess the enhanced privacy paradox model about consumer trust and data integrity in the context of AI and immersive digital platforms. Research should also incorporate the perspectives of cybersecurity professionals and management decision-making processes, providing a comprehensive understanding of organizational adaptations to emerging risks (Shi et al., 2024). Additionally, exploring the psychological and social dimensions of consumer privacy decision-making in AI-driven environments will shed light on how privacy concerns impact digital engagement, especially in high-risk contexts. Finally, the impact of deepfakes on business operations and corporate strategies warrants further exploration, as it remains an under-examined area in the literature.

Table 1: Future research agenda

<p>AI-Induced privacy</p> <ul style="list-style-type: none"> ● How does the ambiguity between authentic and AI-manipulated content intensify traditional privacy paradox issues, impacting consumer engagement with digital services? ● To what extent do consumers' perceptions of privacy costs change in response to deepfake risks, affecting their willingness to share personal data? ● What psychological mechanisms contribute to privacy concerns as consumers encounter AI-generated content that challenges perceptions of authenticity and security? ● How can transparency initiatives, such as labelling or content verification, help mitigate privacy concerns in an era of AI-driven media?
<p>Consumer digital vulnerability in AI-driven environments</p> <ul style="list-style-type: none"> ● How do AI applications like deepfakes affect consumer trust, particularly in discerning real versus manipulated content? ● How does exposure to deepfakes influence consumer trust in digital interactions and perceptions of content authenticity? ● What individual traits (e.g., digital literacy, technology anxiety) affect privacy perceptions amid deepfake risks and digital transformation? ● What measures can businesses implement to mitigate reputational damage from deepfake risks and build consumer trust?
<p>Dynamic capabilities and privacy</p> <ul style="list-style-type: none"> ● What frameworks or adaptive models enable businesses to manage AI-induced privacy risks continuously, building resilience? ● How does managing deepfake risks contribute to competitive advantage and organizational resilience, especially as privacy becomes a core competency? ● How can businesses leverage advanced AI detection algorithms to create proactive defense systems against deepfake risks?

<p>Cultural impact in AI privacy perceptions</p> <ul style="list-style-type: none"> ● How do cultural values shape consumer responses to deepfake-related privacy risks, and how might these vary across regions? ● How do different data privacy regulations influence consumer trust and perceptions of AI-related privacy risks, especially with deepfakes? ● Can cultural differences impact the effectiveness of dynamic capabilities in managing privacy within AI-driven transformations? ● What role do cross-cultural privacy expectations play in developing adaptive privacy strategies for AI technologies?
<p>Deepfake risks and ethical considerations in AI transformation</p> <ul style="list-style-type: none"> ● How do deepfakes challenge ethical considerations in AI-driven transformations, especially concerning authenticity and integrity? ● What ethical frameworks can guide businesses in responsibly handling deepfake technology and minimizing consumer manipulation? ● What strategies can be applied to ensure ethical use of AI and deepfake technologies while preserving consumer trust? ● How do evolving ethical standards influence corporate responsibility in mitigating AI-related risks, particularly deepfake concerns?

Table 2: Results and implications

Key results	Implications and recommendations for business management
Participants exposed to deep-fakes had higher privacy concerns	Organizations must prioritize consumer trust by implementing advanced detection systems, e.g., real-time authentication and content verification.
Privacy concerns negatively correlated with AI service engagement	Develop proactive privacy strategies (e.g., “privacy by design”) to reduce skepticism and promote adopting AI-enabled solutions.
74% of participants failed to identify deepfakes	Enhance consumer education campaigns to improve awareness of deepfake risks and foster informed decision-making in AI-enabled environments.
Dynamic capabilities (e.g., sensing and reconfiguring) build trust when security cues are present.	Invest in dynamic capabilities like real-time monitoring and adaptive privacy features (e.g., authentication badges) to mitigate privacy concerns.
Deepfake risks intensify the privacy paradox.	Address consumer uncertainty by embedding transparency and accountability into AI operations, bridging the trust gap in digital ecosystems.
Proactive measures increase trust and mitigate the privacy Paradox	Allocate resources for advanced privacy technologies, such as deepfake detection and cryptographic safeguards, to differentiate from competitors.
Iterative updates to privacy policies reinforce trust.	Continuously refine privacy structures through ongoing risk assessments and align them with consumer expectations and regulatory requirements.
Empirical validation of the dynamic privacy strategy (DPS) framework	Treat privacy as a strategic asset by integrating dynamic capabilities into organizational frameworks, enabling proactive risk management.

References :

- Acquisti, A., Adjerid, I., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., ... & Wilson, S. (2023). Nudges (and deceptive patterns) for privacy: six years later. In *The Routledge Handbook of Privacy and Social Media* (pp. 257269-). Routledge.
- Ahmadi, S. (2023). Open AI and its Impact on Fraud Detection in Financial Industry. *Open AI and its Impact on Fraud Detection in Financial Industry. Journal of Knowledge Learning and Science Technology* ISSN, 29596386-.
- Ahmed, A., & Abdulkareem, A. M. (2023). Big data analytics in the entertainment Industry: audience behavior analysis, content recommendation, and Revenue maximization. *Reviews of Contemporary Business Analytics*, 6(1), 88102-.
- Akter, S., Mohiuddin Babu, M., Hossain, T. M. T., Dey, B. L., Liu, H., & Singh, P. (2024). Omnichannel management capabilities in international marketing: the effects of word of mouth on customer engagement and customer equity. *International Marketing Review*, 41(1), 4273-.
- Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2024). Methodological approach to assessing the current state of organizations for AI-Based digital transformation. *Applied System Innovation*, 7(1), 14.
- Babu, C. S. (2024). Adaptive AI for Dynamic Cybersecurity Systems: Enhancing Protection in a Rapidly Evolving Digital Landscap. In *Principles and Applications of Adaptive Artificial Intelligence* (pp. 5272-). IGI Global.
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9).
- Belanche, D., Belk, R. W., Casaló, L. V., & Flavián, C. (2024). The dark side of artificial intelligence in services. *The Service Industries Journal*, 44(3172-149), (4-.
- Bray, S. D., Johnson, S. D., & Kleinberg, B. (2023). Testing human ability to detect ‘deepfake’ images of human faces. *Journal of Cybersecurity*, 9(1), tyad011.
- Brewis, C., Dibb, S., & Meadows, M. (2023). Leveraging big data for strategic marketing: A dynamic capabilities model for incumbent firms. *Technological Forecasting and Social Change*, 190, 122402.
- Brochado, A. F., Rocha, E. M., Almeida, D., de Sousa, A., & Moura, A. (2023). A data-driven model with minimal information for bottleneck detection-application at Bosch thermotechnology. *International Journal of Management Science and Engineering Management*, 18(4), 318331-.

12. Busacca, A., & Monaca, M. A. (2023). Deepfake: Creation, Purpose, Risks. In *Innovations and Economic and Social Changes due to Artificial Intelligence: The State of the Art* (pp. 5568-). Cham: Springer Nature Switzerland.
13. Canhoto, A. I., Keegan, B. J., & Ryzhikh, M. (2024). Snakes and ladders: Unpacking the personalisation-privacy Paradox in the context of AI-Enabled personalisation in the physical Retail Environment. *Information Systems Frontiers*, 26(3), 10051024-.
14. Camilleri, M. A. (2023). Artificial intelligence governance: Ethical considerations and implications for social responsibility. *Expert Systems*, e13406.
15. Campbell, C., Sands, S., Ferraro, C., Tsao, H. Y. J., & Mavrommatis, A. (2020). From data to action: How marketers can leverage AI. *Business horizons*, 63(2), 227243-.
16. Chang, J. Y. S., Konar, R., Cheah, J. H., & Lim, X. J. (2023). Does privacy still matter in smart technology experience? A conditional mediation analysis. *Journal of Marketing Analytics*, 116-.
17. Chatterjee, S., Mikalef, P., Khorana, S., & Kizgin, H. (2024). Assessing the implementation of AI integrated CRM system for B2C relationship management: integrating contingency theory and dynamic capability view theory. *Information systems frontiers*, 26(3), 967985-.
18. Chen, H. & Magramo, K. (2024), Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'. Retrieved 15.03.2024 From <https://edition.cnn.com/2024/04/02/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>
19. Cloarec, J., Meyer Waarden, L., & Munzel, A. (2024). Transformative privacy calculus: Conceptualizing the personalization privacy paradox on social media. *Psychology & Marketing*.
20. Flavián, C., Belk, R. W., Belanche, D., & Casaló, L. V. (2024). Automated social presence in AI: Avoiding consumer psychological tensions to improve service value. *Journal of Business Research*, 175, 114545.
21. Das, R., Ahmed, W., Sharma, K., Hardey, M., Dwivedi, Y. K., Zhang, Z., ... & Filieri, R. (2024). Towards the development of an explainable e-commerce fake review index: An attribute analytics approach. *European Journal of Operational Research*. <https://doi.org/10.1016/j.ejor.2024.03.008>.
22. Dienlin, T., Masur, P. K., & Treppe, S. (2023). A longitudinal analysis of the privacy paradox. *New Media & Society*, 25(5), 10431064-.
23. Gambín, Á. F., Yazidi, A., Vasilakos, A., Haugerud, H., & Djenouri, Y. (2024). Deepfakes: current and future trends. *Artificial Intelligence Review*, 57(3), 64.

24. Ghosh, S., Hughes, M., Hodgkinson, I., & Hughes, P. (2022). Digital transformation of industrial businesses: A dynamic capability approach. *Technovation*, 113, 102414.
25. Giantini, G. (2023). The sophistry of the neutral tool. *Weaponizing artificial intelligence and big data into threats toward social exclusion. AI and Ethics*, 3(4), 10491061-.
26. Gilbert, C., & Gilbert, M. A. (2024). The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation. *International Research Journal of Advanced Engineering and Science* (ISSN: 2455181-170), (4)9, (9024-.
27. Gosain, M. T., Bhatia, M. K., Sharma, M. R., Bhanvra, M. S., Shaw, A., Singh, T., & Kashyap, B. H. (2024). Artificial Intelligence and the Privacy Paradox: Challenges and Opportunities in Legal Adaptations. *Educational Administration: Theory and Practice*, 30(5), 1038410394-.
28. Gotsch, M. L., & Schögel, M. (2021). Addressing the privacy paradox on the organizational level: review and future directions. *Management Review Quarterly*, 134-.
29. Gündoğar, A., & Niauronis, S. (2023). An Overview of Potential Risks of Artificial General Intelligence Robots. *Applied Scientific Research*, 2(1), 2640-.
30. Heidari, A., Jafari Navimipour, N., Dag, H., & Unal, M. (2024). Deepfake detection using deep learning methods: A systematic and comprehensive review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 14(2), e1520.
31. Holmström, J. (2022). From AI to digital transformation: The AI readiness framework. *Business Horizons*, 65(3), 329339-.
32. Hossain, M. T., Afrin, R., & Biswas, M. A. A. (2024). A Review on Attacks against Artificial Intelligence (AI) and Their Defence Image Recognition and Generation Machine Learning, *Artificial Intelligence. Control Systems and Optimization Letters*, 2(1), 5259-.
33. Joshi, N. (2024). Emerging Challenges in Privacy Protection with Advancements in Artificial Intelligence. *International Journal of Law and Policy*, 2(4), 5577-.
34. Kaur, A., Noori Hoshyar, A., Saikrishna, V., Firmin, S., & Xia, F. (2024). Deepfake video detection: challenges and opportunities. *Artificial Intelligence Review*, 57(6), 147-.
35. Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat?. *Business Horizons*, 63(2), 135146-.
36. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, 64, 122134-.

37. Kumari, B., Kaur, J., & Swami, S. (2021). System dynamics approach for adoption of artificial intelligence in finance. In *Advances in Systems Engineering: Select Proceedings of NSC 2019* (pp. 555575-). Springer Singapore.
38. Leso, B. H., Cortimiglia, M. N., Ghezzi, A., & Minatogawa, V. (2024). Exploring digital transformation capability via a blended perspective of dynamic capabilities and digital maturity: a pattern matching approach. *Review of Managerial Science*, 18(4), 11491187-.
39. Leys, C., Ley, C., Klein, O., Bernard, P., & Licata, L. (2013). Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median. *Journal of experimental social psychology*, 49(4), 764766-.
40. Liu, Y., Guo, M., Han, Z., Gavurova, B., Bresciani, S., & Wang, T. (2024). Effects of digital orientation on organizational resilience: A dynamic capabilities perspective. *Journal of Manufacturing Technology Management*, 35(2), 268290-.
41. Liyanaarachchi, G. (2020). Online privacy as an integral component of strategy: allaying customer fears and building loyalty. *Journal of Business Strategy*, 41(5), 47-56.
42. Liyanaarachchi, G., Mifsud, M., & Viglia, G. (2024). Virtual influencers and data privacy: Introducing the multi-privacy paradox. *Journal of Business Research*, 176, 114584.
43. Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward. *Applied Intelligence*, 53(4), 39744026-.
44. Mullen, M. (2022). A new reality: deepfake technology and the world around us. *Mitchell Hamline L. Rev.*, 48, 210.
45. Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A., & Dwivedi, Y. K. (2023). Deepfakes: Deceptions, mitigations, and opportunities. *Journal of Business Research*, 154, 113368.
46. Oliveira, M., Zancul, E., & Salerno, M. S. (2024). Capability building for digital transformation through design thinking. *Technological Forecasting and Social Change*, 198, 122947.
47. Passos, L. A., Jodas, D., Costa, K. A., Souza Júnior, L. A., Rodrigues, D., Del Ser, J., ... & Papa, J. P. (2024). A review of deep learning-based approaches for deepfake content detection. *Expert Systems*, 41(8), e13570.
48. Pesqueira, A., & Sousa, M. J. (2024). Exploring the role of big data analytics and dynamic capabilities in ESG programs within pharmaceuticals. *Software Quality Journal*, 134-.

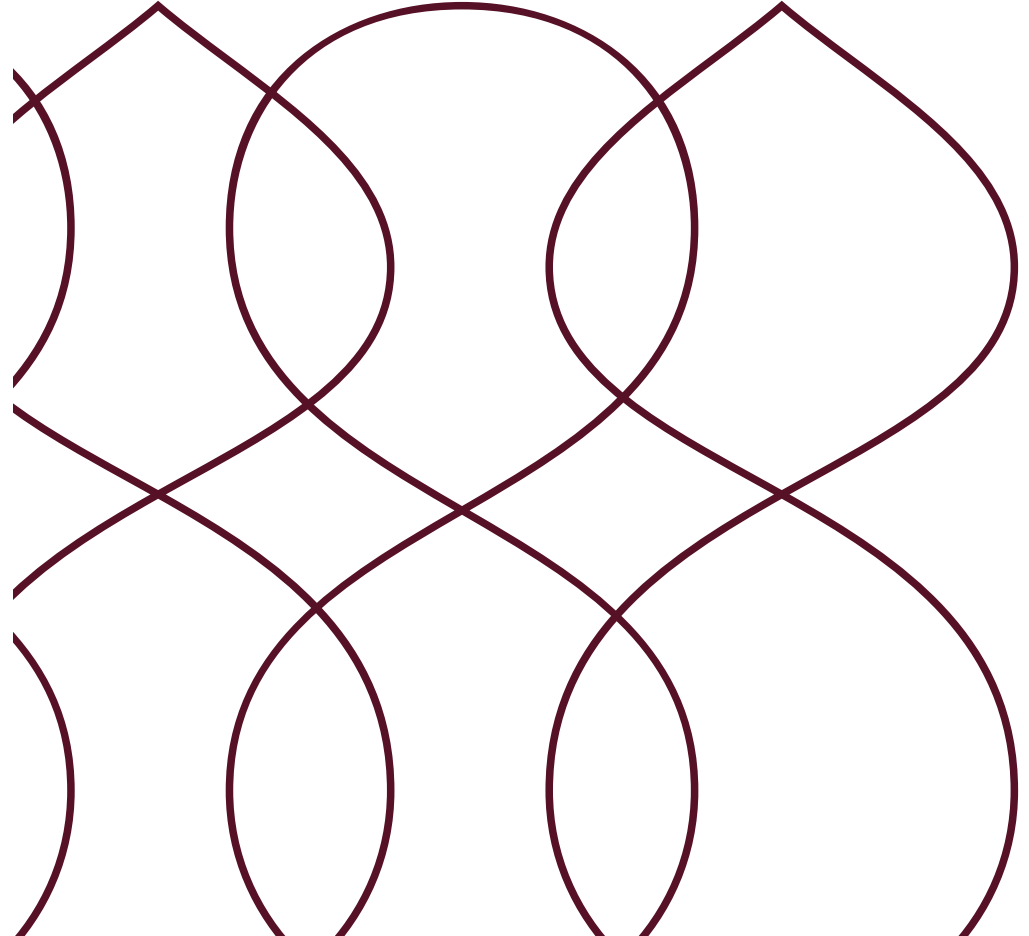
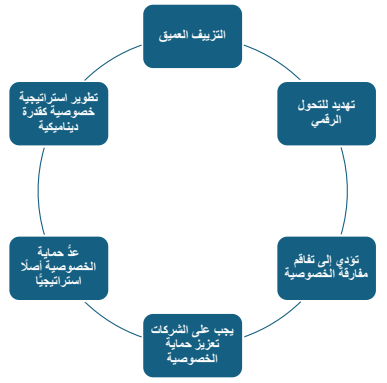
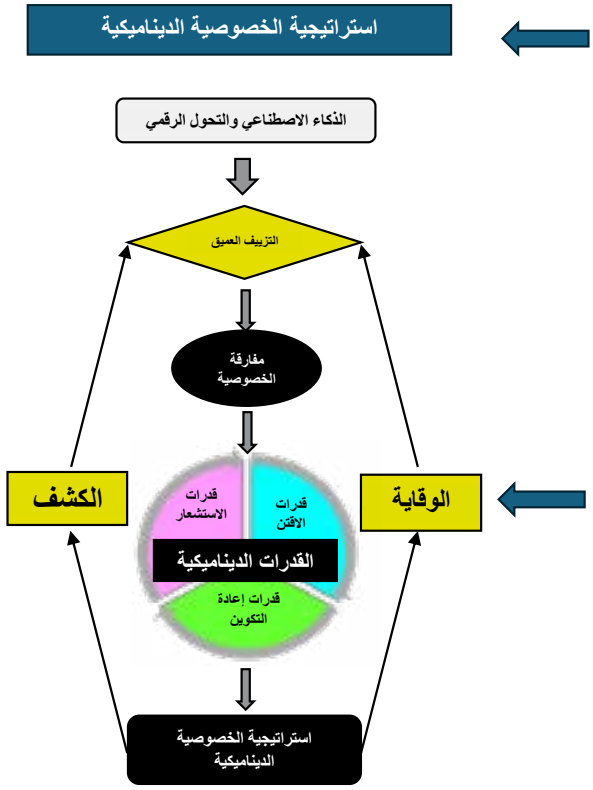
49. Polisetty, A., Chakraborty, D., Kar, A. K., & Pahari, S. (2024). What determines AI adoption in companies? Mixed-method evidence. *Journal of Computer Information Systems*, 64(3), 370387-.
50. Porfírio, J. A., Felício, J. A., & Carrilho, T. (2024). Factors affecting digital transformation in banking. *Journal of Business Research*, 171, 114393.
51. Rathore, B. (2023). Digital transformation 4.0: integration of artificial intelligence & metaverse in marketing. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, 12(1), 4248-.
52. Rana, Nripendra P., Sheshadri Chatterjee, Yogesh K. Dwivedi, and Shahriar Akter. "Understanding dark side of artificial intelligence (AI) integrated business analytics: assessing firm's operational inefficiency and competitiveness." *European Journal of Information Systems* 31, no. 3 (2022): 364387-.
53. Sahoo, S., Kumar, S., Donthu, N., & Singh, A. K. (2024). Artificial intelligence capabilities, open innovation, and business performance—Empirical insights from multinational B2B companies. *Industrial Marketing Management*, 117, 2841-.
54. Siegel, D., Kraetzer, C., Seidlitz, S., & Dittmann, J. (2024). Media Forensic Considerations of the Usage of Artificial Intelligence Using the Example of DeepFake Detection. *Journal of Imaging*, 10(2), 46.
55. Shi, Y., Lu, W., & Zhou, Y. (2024). Reconciling the personalization–privacy paradox via DoctorBots: The roles of service robot acceptance model elements and technology anxiety. *Journal of Consumer Behaviour*, 23(3), 14461462-.
56. Stroebel, L., Llewellyn, M., Hartley, T., Ip, T. S., & Ahmed, M. (2023). A systematic literature review on the effectiveness of deepfake detection techniques. *Journal of Cyber Security Technology*, 7(2), 83113-.
57. Sullivan, Y., & Wamba, S. F. (2024). Artificial intelligence and adaptive response to market changes: A strategy to enhance firm performance and innovation. *Journal of Business Research*, 174, 114500.
58. Teece, D. J., & Linden, G. (2017). Business models, value capture, and the digital enterprise. *Journal of organization design*, 6, 114-.
59. Van Der Vlist, F., Helmond, A., & Ferrari, F. (2024). Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence. *Big Data & Society*, 11(1), 20539517241232630.
60. Vecchietti, G., Liyanaarachchi, G., & Viglia, G. (2025). Managing deepfakes with artificial intelligence: Introducing the business privacy calculus. *Journal of Business Research*, 186, 115010.

61. Viglia, G., Pera, R., Dyussebayeva, S., Mifsud, M., & Hollebeek, L. D. (2023). Engagement and value cocreation within a multi-stakeholder service ecosystem. *Journal of Business Research*, 157, Article 113584.
62. Wazid, M., Mishra, A. K., Mohd, N., & Das, A. K. (2024). A Secure Deepfake Mitigation Framework: Architecture, Issues, Challenges, and Societal Impact. *Cyber Security and Applications*, 100040.
63. Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*, 9(11), 39-52
64. Willems, J., Schmid, M. J., Vanderelst, D., Vogel, D., & Ebinger, F. (2023). AI-driven public services and the privacy paradox: do citizens really care about their privacy?. *Public Management Review*, 25(11), 21162134-.
65. Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences*, 14(2), 675.
66. Whittaker, L., Mulcahy, R., Letheren, K., Kietzmann, J., & Russell-Bennett, R. (2023). Mapping the deepfake landscape for innovation: A multidisciplinary systematic review and future research agenda. *Technovation*, 125, 102784.
67. Wong, L.-W., Tan, G.W.-H., Ooi, K.-B. and Dwivedi, Y. (2024), "The role of institutional and self in the formation of trust in artificial intelligence technologies", *Internet Research*, 34(2), 343370-
68. Yanamala, A. K. Y., Suryadevara, S., & Kalli, V. D. R. (2024). Balancing Innovation and Privacy: The Intersection of Data Protection and Artificial Intelligence. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, 15(1), 143-.
69. Zhang, F., Pan, Z., & Lu, Y. (2023). AIoT-enabled smart surveillance for personal data digitalization: Contextual personalization-privacy paradox in smart home. *Information & Management*, 60(2), 103736.

Appendix. The chatbot used in Study 1.



تأثير مفارقة الخصوصية في الذكاء الاصطناعي والتحول الرقمي: نهج القدرات الديناميكية لإدارة التزييف العميق



أثر مفارقة الخصوصية في الذكاء الاصطناعي والتحول الرقمي: منهجية القدرات الديناميكية لإدارة المحتوى المزيّف

DOI: <https://doi.org/10.63355/XyZd2974>

جاديندرا ليانا أراشيا

جامعة بورتسموث، قسم التسويق، شارع بورتلاند، PO1 3DE، المملكة المتحدة

أنا كيارا إنفرنيزي

قسم دراسات الاقتصاد والأعمال، جامعة بيدمونت الشرقية، شارع بيروني 18، 28100، نوفارا، إيطاليا

جيامباولو فيغليا (المؤلف المراسل)

قسم الاقتصاد والعلوم السياسية، جامعة وادي أوستا، أوستا، إيطاليا

البريد الإلكتروني: giampaolo.viglia@port.ac.uk

المستخلص:

تبحث هذه الدراسة في كيفية إعادة تشكيل الذكاء الاصطناعي والتحول الرقمي لمخاوف المستهلكين المتعلقة بالخصوصية، مع التركيز على المخاطر المتزايدة التي تفرضها تقنية التزييف العميق. فيشير التحول الرقمي إلى دمج التقنيات الرقمية في جوانب الأعمال جميعها؛ ما يؤدي إلى تغيير جذري في كيفية تشغيل المؤسسات وتقديمها للقيمة للعملاء. ويُعزّز هذا التحول بفضل قدرة الذكاء الاصطناعي على تمكين اتخاذ القرارات في الوقت الفعلي، وتحقيق التخصيص، وزيادة الكفاءة التشغيلية؛ ما يجعله ركيزة أساسية لاستراتيجيات الأعمال الحديثة.

ومع فوائد الذكاء الاصطناعي في تعزيز التخصيص، والمرونة التشغيلية، واتخاذ القرارات الفورية؛ فإنّه يفرض أيضًا تحديات معقدة تتعلق بالخصوصية والأمان. وتُعدُّ تقنية التزييف العميق أحد أكبر هذه التحديات؛ حيث يتم استخدامها لإنشاء محتوى مزيف يُضعف حماية خصوصية المستهلك ويشكل تهديدًا للتحول الرقمي. وتهدف هذه الدراسة إلى فهم مفارقة الخصوصية في سياق الذكاء الاصطناعي والتعرض لتقنية التزييف العميق، بالإضافة إلى استكشاف التحديات التنظيمية المرتبطة بها واقتراح استراتيجيات عملية للتخفيف من مخاطرها.

ومن خلال نهج تجريبي، قُمنا بتقييم تأثير التعرض للتزييف العميق في مخاوف الخصوصية لدى المستهلكين. وتشير نتائجنا إلى أنّ المشاركين غالبًا لا يستطيعون التمييز بين مقاطع الفيديو الحقيقية والمزيفة؛ حيث يتم تصنيف مقاطع الفيديو الحقيقية أحيانًا على أنّها مزيفة والعكس صحيح. وبالتالي، من الضروري تحديد ممارسات فعالة في الذكاء الاصطناعي للحد من أخطار التزييف العميق وحماية المؤسسات والمستهلكين. تُسهم هذه الدراسة في الأدبيات العلمية من خلال توسيع مفهوم مفارقة الخصوصية ضمن البيئات التي تعتمد على الذكاء الاصطناعي، وتوسيع إطار القدرات الديناميكية ليشمل الخصوصية بَعْدَها كفاءة تنظيمية أساسية. ونقترح إطار عمل استراتيجيًا جديدًا يُعرّف باسم استراتيجية الخصوصية الديناميكية؛ الذي يهدف إلى تحويل إدارة الخصوصية من مجرد متطلب تنظيمي إلى قدرة استراتيجية أساسية. كما نقدم نموذجًا عمليًا لمساعدة المؤسسات في التعامل مع التعقيدات الناشئة عن الابتكار في الذكاء الاصطناعي والتحول الرقمي.

الكلمات المفتاحية: