Original Manuscript

Identifying and assessing the risks of artificial intelligence applications in smart libraries: Perspective of technostress

Information Development
1–25

DOI: 10.1177/02666669251329032
journals.sagepub.com/home/idv
Sage

Xu Wang
School of Economics and Management, Yanshan University, Qinhuangdao, Hebei, China

Fang Xie
School of Economics and Management, Yanshan University, Qinhuangdao, Hebei, China

Guanghui Cheng
School of Economics and Management, Southeast University, Nanjing, Jiangsu, China

Kiran Shehzadi
School of Economics and Management, Yanshan University, Qinhuangdao, Hebei, China

Abstract

In the digital & intelligent era, integrating AI technology into library services has spurred innovation but also brought potential risks. This paper identifies and assesses AI-related risks in smart libraries from a technostress perspective, proposing governance strategies to enhance service quality and provide a reference for smart library development. Using content analysis and technostress theory, potential risk sources of AI applications in smart libraries are analyzed across five dimensions: techno-overload, techno-invasion, techno-complexity, techno-insecurity, and techno-uncertainty. The Decision Making Trial and Evaluation Laboratory (DEMATEL) method is then applied to assess causal relationships among risks, revealing two categories: technical-level risks (AI malfunction, emotional disconnection, AI misjudgement, algorithmic bias, and responsibility ambiguity) and societal-level risks (security threat, fairness challenges, regulatory ambiguity, copyright concern, and occupational maladaptation). Key findings highlight AI malfunction and misjudgment as driving risks, while regulatory ambiguity and occupational maladaptation are resultant risks. The paper proposes hierarchical risk governance strategies, including prioritizing high-driven risks, managing resultant risks, and dynamically adjusting adaptation rules.

Keywords

Smart libraries, artificial intelligence, technostress, risk identification, risk assessment, risk governance, DEMATEL

Submitted: 7 February 2025; accepted: 5 March 2025

Introduction

With the development of science and technology, digital and intelligent technology drives the comprehensive transformation and upgrading of library services. The outbreak of generative AI and large language models has stunned the world, bringing opportunities for libraries while creating unprecedented challenges. How to effectively govern them has become a topic of widespread concern in academia and industry.

Smart library is an innovative library service model that integrates smart technology, smart users, and smart services (Gul and Bano, 2019). Initially, Aittola et al. (2003) defined it as a software-based, mobile library service accessed via wireless Internet

Corresponding author:
Guanghui Cheng, School of Economics and Management, Southeast University, Nanjing, Jiangsu, China.
Email: guanghui@seu.edu.cn

without the need for additional hardware support. With the wide application of information technology, library services are constantly evolving from automation to digitization and then to intelligence. The concept of smart libraries has also been gradually extended, focusing on three core components: smart technology, smart services, and smart users (Cao et al., 2018). Among them, smart technology is driven by the Internet of Things (IoT), data mining, and artificial intelligence (AI) as the core driving force; smart service focuses on user-centeredness; and smart user emphasizes the intelligence of the interaction between librarians and users in the service process. AI, as one of the key technologies of smart libraries, has been widely used in the fields of information retrieval, recommendation services, user behavior analysis, etc., and has played an important role in promoting the development of smart libraries (Huang et al., 2023).

However, while the growing popularity of AI models brings opportunities for library services, it also poses a series of ethical and legal challenges (Bradley, 2022). For example, the loss of control of technology, privacy leakage, and algorithmic bias caused by the AI technology will directly or indirectly affect the quality of library services and the user experience (Hussain, 2023). Therefore, how to effectively identify, assess, and govern the AI technology risks in the construction of smart libraries is an important topic to ensure its sustainable development.

Technostress is a negative emotional reaction that people have when confronted with emerging technologies, usually characterized by resistance or anxiety about the technology (Califf et al., 2020). Technostress has the potential to diminish the effectiveness of technology applications and even trigger more complex social issues. In the context of smart libraries, the integration of AI technology redefines the traditional human-computer interaction, with its inherent risks are ultimately mapped onto the technostress triggered during human-computer interaction. Therefore, reviewing the risk of AI technology application in smart libraries from the perspective of technostress can not only facilitates an analysis of risk origin from the psychological and behavioral levels, but also provide a theoretical foundation for risk governance at the technical and management levels.

This study employs a content analysis method based on technostress theory to systematically identify the potential risks of AI applications in smart libraries, focusing on five primary sources of stress: techno-overload, techno-invasion, techno-complexity, techno-insecurity, and techno-uncertainty. The Decision-Making Trial and Evaluation Laboratory (DEMATEL) method is then used to assess the causal relationships and structural characteristics among these risks. Furthermore, hierarchical and multifaceted risk governance strategies are proposed to offer actionable guidance for the sustainable application and management of AI technology in smart libraries.

The contributions of this study are threefold. First, it introduces technostress theory into the research on AI risks in smart libraries and comprehensively analyzes risk sources across five dimensions. Second, it applies the DEMATEL method to evaluate causal relationships between risks and identify key driving risks, such as AI malfunction and AI misjudgment. Finally, it proposes multi-level governance strategies based on risk characteristics, offering theoretical support and practical guidance for AI technology application and risk management in smart libraries. This study not only provides theoretical and practical insights into AI risk governance in smart libraries but also broadens the scope of AI risk research in other fields.

The remainder of this paper is structured as follows: Literature review reviews and synthesizes existing literature. Identifying the risks of AI applications in smart libraries identifies the risks of AI applications in smart libraries. Assessing the risks of AI applications in smart libraries assesses these risks. Discussions, countermeasures and implications discusses the results and proposes governance strategies along with theoretical and practical implications. Conclusion and future work concludes the study by addressing its limitations and outlining future research directions.

Literature review

Study on the impact generated by AI applications in smart libraries

AI has become a key technology for the construction of smart earth, digital China, and smart cities, and it is promoting the development of all fields of society in the direction of wisdom (Teddy-Ang and Toh, 2020). This includes the construction of smart libraries (Lund and Wang, 2023; Shen, 2019). In the construction of smart libraries, AI is applied to intelligent

Q&A, automatic borrowing, intelligent robots, intelligent retrieval, intelligent recommendation, and other operations in smart libraries (Cox, 2023). At present, there has been much research on AI and smart libraries. To more effectively analyze the current situation of relevant research, in the Scopus database, we conducted searches on the topics of "smart library" and "artificial intelligence", and obtained 110 articles. In addition, VOSviewer software was used to draw the knowledge mapping of the keyword co-occurrence network (Figure 1). In the figure, the node size represents the frequency of keyword occurrence, the line thickness represents the number of common occurrences of the two keywords and the closeness of the connection between the keywords, and the node color represents the year in which the keywords appear (Van Eck and Waltman, 2017).

Study on the positive impact of AI applications in smart libraries. There have been studies confirming the positive role of AI in smart libraries (Cheung et al., 2023). For example, Gul and Bano (2019) suggested that the application of AI to enhance the working capabilities of smart libraries could bridge the gap between the services offered by libraries and the rapidly changing and competing needs of humanity. Cao et al. (2018) proposed that AI is an important way to transform traditional libraries into smart libraries. Bi et al. (2022) propose that AI can promote the development of smart libraries from three aspects: intelligent service, intelligent sustainability and intelligent security. Borgohain et al. (2024) believe that AI technology supports service innovation in libraries, and AI technology opens up a new era of human-computer collaboration, diversified integration, shared construction, autonomous control of intelligent services in libraries, and enhances the ability of library intelligent services.

On the basis of this positive attitude towards AI, some scholars have tried to analyze the specific architecture of the application of AI to the construction of smart libraries in combination with cases. For example, Ekstrand and Strandberg (2023) believe that AI is one of the development trends of the Swedish medical library, and constructs the relevant technology development roadmap. Huang et al. (2023) compare the position and role of AI in the strategic development documents of academic libraries in the UK and China, and discuss how academic libraries should make good use of the development opportunities brought by AI. Asim et al. (2023) investigated the use of AI in university libraries in Pakistan and found that university libraries in Pakistan are using limited AI-based library services. These include text-to-speech and speech-to-text technologies, Google Assistant for search via voice commands, radio frequency identification (RFID) systems for self-lending, check-in and security purposes, and intelligent data analytics for collection management. Meanwhile, libraries can develop library-specific chatbots that focus on answering basic business inquiries or supporting specific workflows, such as interlibrary loan, book shelving, moving books, and book inventory checking, thus enabling them to better provide the services that users need (Cox, 2024; Wheatley and Hervieux, 2024). These studies summarized the functions of AI in the construction of smart libraries, clarified the identity and responsibilities of AI, and provided a reference for promoting the application of AI (Adetayo, 2023).

Study on risks arising from AI applications in smart libraries. Although the above research fully confirms the value of AI in the construction of smart libraries, information technology is a double-edged sword (Lee et al., 2018). AI is not only beneficial to the construction of smart libraries, but also has potential challenges and risks (Hussain, 2023). Such as copyright issues (Bradley, 2022), Privacy and confidentiality (Hamad et al., 2023), Lack of information infrastructure (Barsha and Munshi, 2023), and the technostress brought to people will be mentioned later (Bichteler, 1987). Therefore, it is necessary to objectively examine the AI technology in the smart library (Cox, 2021). Comprehensively recognize and understand the potential risks brought by AI, and adopt targeted risk management strategies, so as to ensure that AI can promote the construction of smart libraries more effectively (Panda and Kaur, 2023). For example, while the library community is actively embracing AI technology, it also needs to be alert to the risks arising from AI technology and respond to them in a timely manner. In this regard, Wu et al. (2024) advocate that the library community should focus on strengthening the standardization of business management and technology application and actively promote the updating and improvement of relevant standards, laws, and regulations in the library industry.

Study on risks of AI applications in smart libraries services from the perspective of technostress

Technostress connotations. Technostress is a negative psychological relationship between a person and the

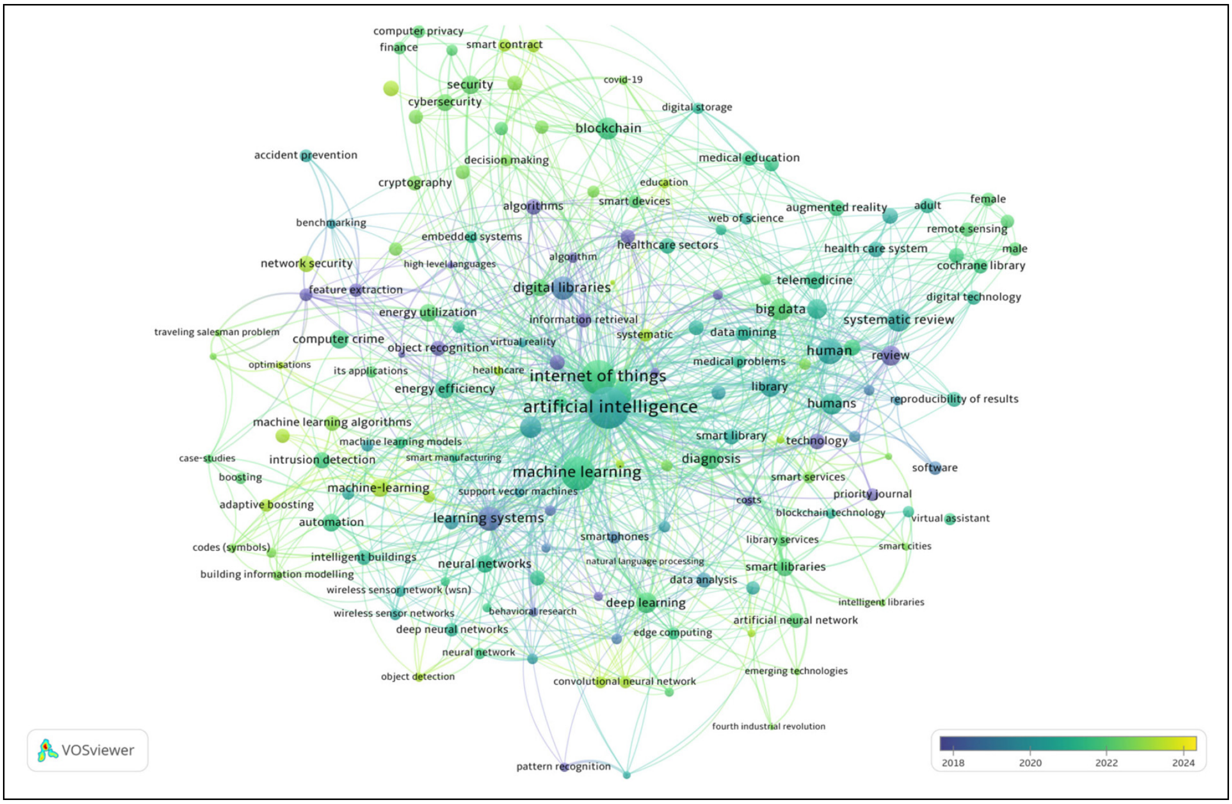

Figure 1. The keywords co-occurrence knowledge mapping of AI and smart library-related literature.
Source: Credits by authors.

introduction of new technology, initially defined by Brod (1984) as a modern adaptation disease caused by the inability to cope with new computer technology healthily, and later widely referred to as a general term for negative emotions associated with the use of technology (Weil and Rosen, 1997). Therefore, technostress can be understood as the negative impact that information technology may have on individuals (Salanova et al., 2014). From a biological point of view, it manifests as increased activity of the cardiovascular system, or increased levels of stress hormones such as adrenaline and cortisol (Riedl, 2012). This can lead to resistance to technology use (Sami and Pangannaiah, 2006).

Furthermore, The creator of technostress refers to the factors that promote the generation of technostress (Krishnan, 2017). According to the research of Tarafdar et al. (2007), the creators of technostress are divided into five aspects: techno-overload, techno-invasion, techno-complexity, techno-uncertainty and techno-insecurity. Techno-overload refers to the situation in which an individual is faced with too much information and tasks when using technology, beyond the range of effective response. Techno-invasion refers to the continuous infiltration and intrusion of technology into individual work and living space, resulting in the imbalance of work and life. Techno-complexity refers to the degree to which a technical system, application, or tool is perceived by an individual to be complex and difficult to understand. Techno-uncertainty refers to the degree of unease that people are unable to use the technology through their existing experience due to the continuous rapid update of the technology. Techno-insecurity refers to the threat of being replaced by the intelligence and automation of technology (Tarafdar et al., 2007). These five aspects cover the multiple dilemmas that individuals may face when exposed to technology, and profoundly reveal the multidimensionality of technostress generation (Ayyagari et al., 2011). Therefore, our follow-up research follows this idea and starts from these five aspects to identify the risks of AI applications in smart libraries.

Technostress in various application scenarios. Previous studies have confirmed that technostress is ubiquitous in various technical application scenarios (Self and Aquilina, 2013). For example, modern offices

(Arnetz and Wiholm, 1997), teachers in higher education Settings (Jena, 2015), students (Upadhyaya and Vrinda, 2021), work and social occasions (Brown et al., 2014; Sasidharan, 2022), hospitals (Califf et al., 2020). This includes library staff and users (Bichteler, 1987). Although Califf et al. (2020) mentioned in their research that technostress may play a double-sided role, its positive role imposes harsh conditions on people's information literacy, which is not realistic in today's society. Therefore, most studies agree that the negative effects of technostress are more significant. Technostress will reduce people's work performance (Tarafdar et al., 2015; Tiwari, 2021), satisfaction with work and life (La Torre et al., 2019; Tarafdar et al., 2010). It will also cause library staff and users to have resistance to computers (Sami and Pangannaiah, 2006), thus refusing to participate in the construction of the smart library (Lindén et al., 2018). Therefore, the existence of technostress will hinder the application of new technologies in the construction of smart libraries to a certain extent (Ahmad and Amin, 2012).

Study on risks of AI services in smart libraries from a technostress perspective. For AI, the most front-end information technology, its application will involve a large amount of data and complex deep learning algorithms, but also lead to more transactions in the library tend to be automated (R-Moreno et al., 2014). Thus, it is more likely to cause technostress (Giorgi et al., 2022). Meanwhile, technostress is an important cause of risks in the application of AI in smart libraries, so it is necessary to identify possible risks from the perspective of technostress. Applying AI to the smart library is essentially changing the way of human-computer interaction in the library. Based on the perspective of technostress, the problems and reasons for the application of AI in the smart library can be explained from the source, so as to formulate more targeted management strategies.

Studies on the potential risks triggered by AI suggest that while generative AI is evolving rapidly, society is still catching up with its ethical, political, social, cultural, and economic implications. As emphasized by Dezuanni et al. (2024), it is necessary to "strengthen the international governance of emerging technologies, including AI, for the benefit of humankind." However, while AI benefits humanity, it also raises a series of potential risks, such as copyright disputes, deep falsification, the proliferation of false information, algorithmic bias, fairness challenges and technological unemployment, among other potential risks. Among them, in the field of education, AI has raised concerns about academic plagiarism, increased errors in scientific articles, and high energy consumption while improving educational development (Lenharo, 2024). In this regard, Kwon (2024) proposed that there should be more collaboration and communication among academic publishers, technology companies, and authors to find a win-win path between the availability of AI training data and the protection of intellectual property. Meanwhile, the equity issues raised by the application of AI in public cultural services and education are universal, e.g., systematic bias, discrimination, and inequality of marginalized student populations occur from time to time (Nguyen et al., 2023). Thus, Roshanaei (2024) suggested the need to increase the diversity of AI training data, conduct regular audits and bias assessments so as to ensure that algorithms remain fair and inclusive in the long run.

From the perspective of technostress, scholars have primarily studied the risks associated with AI applications in smart library services at two levels: technical risks (self-risks) and social risks (derivative risks). At the technical risk level, scholars have conducted research on aspects such as AI runaway, AI emotional disconnection, AI algorithmic bias, AI responsibility ambiguity, and AI misjudgment. Firstly, regarding AI runaway, when libraries utilize AI for virtual reference services, subject knowledge services, and information education and training services, the algorithms inherent in AI may rank search results based on users' personal characteristics and historical records, potentially leading to some users being unable to access the most relevant information (Xu, 2024). This AI runaway behavior driven by technology development is beyond the control of librarians (Cox, 2023). Secondly, regarding emotional disconnection, the rapid advancement of technology may instill fear among librarians towards AI due to the impacts of technological changes. Particularly when librarians perceive that AI could devalue their professional identity or replace traditional roles, these negative emotions may lead to a shift in librarians' attitudes from embracing AI's potential to harboring deep-seated skepticism and alarm, resulting in an emotional disconnect (Bradley, 2022). Thirdly, regarding algorithmic bias, the application of AI in library services has raised numerous ethical concerns. There is a growing apprehension that AI might potentially replace certain aspects of librarians' roles. This development could significantly impact equality, diversity, and inclusion within the profession. In this context, the inherent algorithmic systems of AI are likely to perpetuate issues of gender discrimination and racial bias (Cox and Mazumdar, 2024). Fourthly, regarding responsibility ambiguity, when it comes to algorithmic decision-making errors or violations of user data rights resulting from AI applications in smart libraries, the responsibility should be attributed to the developers of AI models and service providers. This is because the fundamental nature of AI systems is that they are human-made artifacts, and thus accountability cannot be assigned to the machines themselves (Chesterman, 2020). Fifthly, regarding AI misjudgment, when users utilize AI for smart library services, there is a possibility of input errors that may lead to AI misinterpreting incorrect instructions during data recognition. This could result in the system outputting erroneous and misleading responses to different user groups (Yamson, 2023).

At the level of social risks (derivative risks), scholars have conducted research on aspects such as AI security threats, AI copyright concerns, AI rule ambiguity, AI vocational maladjustment, and AI fairness challenges. Firstly, regarding security threats, when library users upload required materials to the network and store them on cloud servers, there is a potential risk that AI systems identifying customer data could be vulnerable to hacker attacks on library websites due to server and network failures, thereby posing digital threats to library confidentiality or personal information (Dube et al., 2024). Secondly, regarding copyright concerns, as the core vehicle for the digital transformation of traditional libraries, smart libraries face complex copyright issues while enhancing their service efficiency. For instance, relevant copyright holders may restrict the circulation of e-book resources through technological means such as digital watermarking and access control. However, the automated services of smart libraries require moving beyond the traditional “one-to-one” authorization model, making them susceptible to compliance disputes due to technological circumvention, thereby increasing the risk of copyright infringement (Wang, 2020). Thirdly, regarding rule ambiguity, while the application of AI technology in smart libraries has brought numerous conveniences, existing regulations have certain gaps in addressing the potential risks posed by AI. This is particularly evident when AI is integrated into digital libraries, where the boundaries between AI technical failures and human operational responsibilities remain unclear (Bradley, 2022). Fourthly, concerning vocational maladjustment, as AI technology empowers library development, the rapid technological advancements can cause significant adaptation challenges for both library staff and users. Some librarians and users may hesitate to embrace new digital strategies and technologies (Hussain and Ahmad, 2021). Additionally, librarians are concerned about the potential risk of job displacement due to the wave of technological changes. In response to this, Aslam et al. (2025) proposed promoting digital literacy initiatives to help both users and librarians gain access to smart technologies and digital resources, thereby improving the accessibility of digital learning environments. Fifthly, regarding fairness challenges, scholars have raised concerns about whether the application of AI in library services might exacerbate the existing gender-based pay gap among librarians (Cox and Mazumdar, 2024; Howard et al., 2020).

Research gap

In summary, although the AI application significantly enhance convenience and efficiency in smart libraries, they may also introduce a series of potential risks that may undermine its value and effectiveness. It is particularly important to comprehensively identify and assess these risks and deeply understand their generation mechanisms and interactions. By employing technostress theory as a framework, this paper reveals the root causes of AI application risks from the perspective of human-computer interaction and focuses on the influence of technology on users and staff at the micro level. Furthermore, by refining the categorization of AI risks, this study provides a theoretical foundation for the governance of AI technology risks in smart libraries.

Specifically, this paper first adopts the content analysis method to introduce and explain the five main sources of technostress, conducting an in-depth analysis of the self-risks and derivative risks that may be triggered by AI in intelligent libraries; secondly, it employs the DEMATEL analysis method, portrays the causal relationship and systematic characteristics among risks, and distills the systematic characteristics of the risk categories; finally, based on the analytical results targeted risk governance strategies are proposed, offering practical guidance for the application and management of AI in smart libraries. The detailed research framework is illustrated in Figure 2.

Identifying the risks of AI applications in smart libraries

This paper adopts the content analysis method, relies on the technostress theory, and combines the sources of technostress to categorize the risks of applying AI in smart libraries into self-risks and derivative risks. Self-risks refer to the potential risks inherent in information systems and directly related to human-computer interaction when AI technology is introduced in smart libraries. Derivative risks refer to a broader, indirect set of problems caused by self-risks. Derivative risks go beyond the technology itself and directly affect users, organizations, and the societal level. Among them, self-risks and derivative risks are interdependent, and their interdependence determines the multi-level risks identification below.

Self-risks

AI malfunction: raising techno-overload. AI malfunction is a situation where the AI becomes unpredictable and uncontrollable due to algorithmic vulnerabilities, hardware and software equipment failures, external attacks, and alienation (Coombs et al., 2021). The risk of AI malfunction is mainly in the training and deployment phases of its models. First, in the AI model training phase, an attacker can attack the model through adversarial samples or data poisoning to degrade its performance (Tian et al., 2022). Second, during the AI model deployment phase, an attacker can illegally access the AI-generated content (AIGC) data or a part of its core functionality through the intelligent model, which can lead to AI malfunction or generate incorrect responses to user inputs (Krishna et al., 2019). When AI goes haywire, it may lead to erroneous decisions or behaviors in the library service system, creating challenges for staff and users to understand, correct, or adapt to the system's abnormal behavior. This confusion may increase the cognitive load on people, which leads to techno-overload. For example, when utilizing AI algorithms for book recommendations, if the AI goes out of control, it may lead to wrong book recommendations. On one hand, this wrong recommendation will make users feel disturbed and dissatisfied and on the other hand, the staff need to spend extra time and energy to explain and correct these errors. Ultimately, it leads to the occurrence of techno-overload and increases the technostress of both parties.Therefore, we believe that AI malfunction is one of the inherent risks that smart libraries need to face when applying AI.

Emotional disconnection: raising techno-invasion perception. Emotional disconnection refers to a sense of emotional isolation in interactions with humans due to the AI's lack of real emotion and emotional understanding (Dollmat and Abdullah, 2022). In short, emotional disconnection characterizes that there is an obstacle in emotional communication between humans and AI, and users cannot feel real and emotional responses from AI systems, which leads to an incomplete or lack of humanization of the interaction experience. Among them, in traditional library services, emotional activities such as staff's attitude, affinity, and tone of voice are directly related to users' experience and satisfaction. People are also more willing to accept more enthusiastic and proactive services (Nitecki, 1996). However, current AI applications for library services are usually considered to be apathetic and ineffective in giving users an emotional experience (Liu-Thompkins et al., 2022). The library itself, as a place that values social relationships and cultural exchange, inherently embody a sense of humanistic care. However, since AI lacks the ability to establish genuine emotional connections, users may experience feelings of loneliness and emotional unfulfillment during interactions with AI. This absence of emotional connection could lead to a heightened sense of techno-invasion thereby exacerbating users' technostress. Consequently, emotional disconnection represent significant self risk that smart libraries should address when integrating AI technologies.

AI misjudgement: raising techno-complexity perception. AI misjudgement refers to the fact that AI is usually trained to learn from the input data, but due to the possible uneven sampling or underrepresentation in the training set, it leads to biased and misleading perceptions of the AI about the original data and its training results (Maity, 2019). Simultaneously, biases in the training data are amplified in the AIGC, which leads to erroneous judgments (Lund and Wang, 2023). In addition to the inadequacy of the training set, AI's neural network structure lacks deeper reasoning capabilities compared to the human mind, which may also trigger AI misjudgement.When AI misjudgement occurs, the judgment process usually lacks interpretability due to the fact that the AI system deals with massive amounts of data and is based on complex

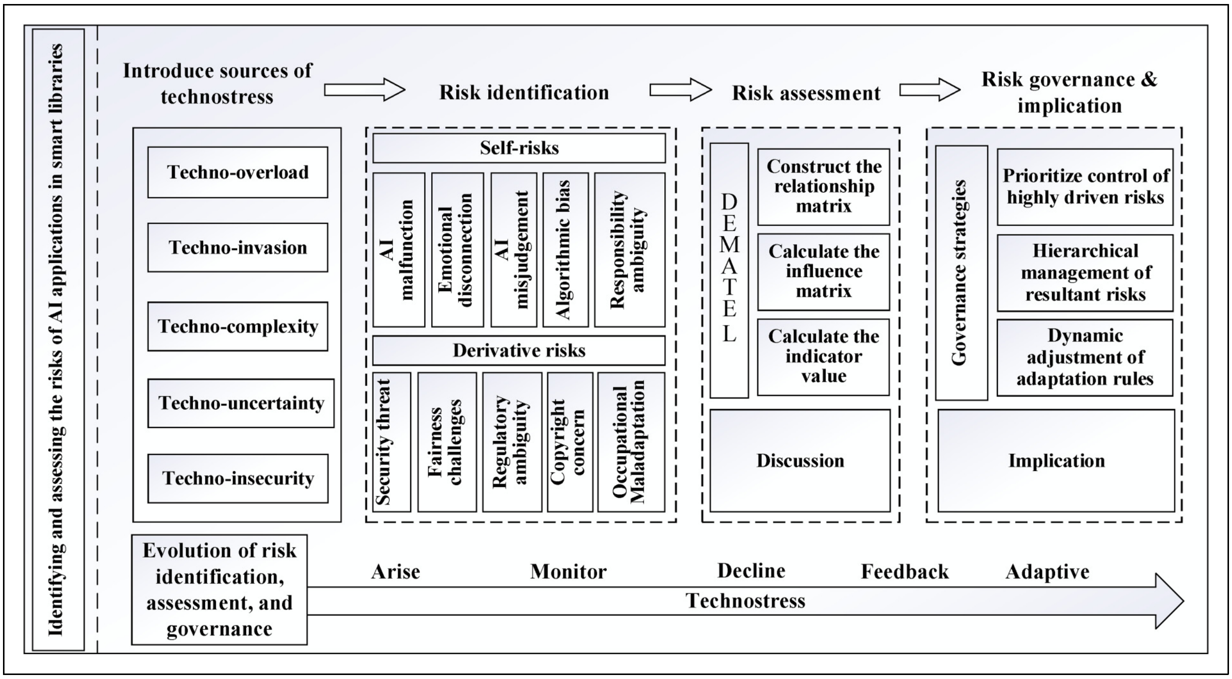

Figure 2. Research framework.
Source: Credits by authors.

deep learning algorithms (Fan et al., 2021). This ultimately makes it challenging to understand how the system reaches to a particular decision. Consequently, when librarians and users encounters AI misjudgement, identifying the root cause of the problem or suggest system improvements becomes difficult due to opaque nature of AI algorithms. This situation may trigger the perception of techno-complexity and thus increase technostress. Therefore, this paper identifies AI misjudgement as a self risk that smart libraries should address when implementing AI technologies.

Algorithmic bias: raising techno-uncertainty perception. Algorithmic bias refers to the tendency that AI may exhibit unfairness or imbalance when confronted with different groups, individuals, or features based on continuous self-learning of the training set. Although both algorithmic bias and AI misjudgement are related to the inadequacy of the training set, they have different influence (Akter et al., 2021). AI misjudgement is primarily concerned with the complexity of algorithms in the data processing and learning process, and its influence is centered on the technical level, i.e., the process by which the algorithms process the data and carry out the learning (Busuioc, 2021). Algorithmic bias focuses more on possible unfairness in the face of diverse inputs, and the influence is centered at the user level, i.e., the algorithm's determination of different groups or topics may be subject to uncertainty. Algorithmic bias is a common problem where AI may respond differently for different users. AI may show different tendencies to answer the same question in different conversations at different times or in different contexts. It is therefore difficult to guarantee that AI in a smart library can treat all users with a uniform standard at all times. However, this tendency is clearly not in line with the "digital equity" that library services are pursuing (Morales et al., 2014). In addition, unpredictability of an AI system's future biases based on its historical responses can contribute to a perception of techno-uncertainty, leading to increase the user's technostress. Therefore, this paper argues that algorithmic bias is a significant self risk that smart libraries should address when implementing AI.

Responsibility ambiguity: raising techno-insecurity perception. The design, development, and operation of AI systems usually involves the participation of multiple subjects (librarians, users, AI developers, etc.). At the same time, AI has a certain degree of autonomous decision-making ability, and its decision-making process is often not directly understandable, which will make it difficult to determine which subject is ultimately responsible for the behavior and output of the AI system (Chen et al., 2023). Therefore, smart libraries will face the problem of AIGC responsibility ambiguity when applying AI. In different stages of AI design, regulation, and operation, responsibilities usually fall on different subjects. Due to the dispersed responsibility, people may think that they do not have to be responsible for the behavior of AI, and this idea is reasonable to some extent. However, this decentralization of responsibility may reduce people's motivation to monitor and prevent AI systems. In other words, it may not incentivize people to devote more attention to improving AI security and related skills (Santoni de Sio and Mecacci, 2021). This may lead people (especially librarians) to doubt their self-social identity and their own contribution and value in smart libraries. Meanwhile, individuals may thus lose their self-identity and may develop the fear of being replaced by AI, thus triggering techno-insecurity and increasing people's technostress (Mirbabaie et al., 2022). Therefore, we consider the confusion of responsibility ambiguity to be an inherent risk that smart libraries need to face when implementing AI.

Derivative risks

Security threat: Exacerbating the burden of techno-overload prevention processing. Although AI has improved the efficiency of information retrieval, it has also made it easier to produce and disseminate false information, thus creating a new threat to social security. This security threat involves multiple aspects including data, cyber and public safety (Yu and Carroll, 2021). Among them, security issues are not entirely caused by AI's own algorithmic flaws; more threats may come from overuse or malicious abuse by humans. For example, fraud, defamation and data theft through AI (Floridi et al., 2018). When applying AI technology, smart libraries usually need a large amount of user data for training models, providing personalized services, etc. However, this process inevitably involves sensitive user information, which ultimately leads to the application of AI that may accelerate the creation of illegal activities.

Security threat may expose librarians and users to more security-related information processing needs, including vulnerability remediation, emergency plans, and security policies. This information overload may make it difficult for them to effectively understand and process all the information about the security aspects of AI, resulting in a feeling of techno-overload. For example, AI may make book recommendations based on users' reading history and preferences, but if the AI has security vulnerabilities, it could lead to user data leakage or recommendation of inappropriate content. This would trigger the need for librarians to handle user complaints, fix system vulnerabilities, etc. (Hussain, 2023), which would further exacerbate the perception of techno-overload by users or staff and increase technostress. Therefore, this paper argues that security threats are a smart library's need to face when applying AI derivative risks.

Fairness challenges: Exacerbating the differentiation of social identities for techno-invasion. Currently, international organizations represented by the European Commission have developed principles and guidelines on fairness aimed at developing, deploying, and governing fair and trustworthy AI systems. This initiative reflects the international community's concern about the fairness of AI. However, the specific content and operational recommendations of the fairness principles and guidelines have not yet been fully fleshed out. In this regard, many scholars have pointed out that AI systems may replicate and amplify inequalities in existing societies (Cachat-Rosset and Klarsfeld, 2023). Therefore, when applying AI in smart libraries, it is also necessary to consider such fairness challenges.Fairness challenges can be understood as the limitations of the algorithms and training sets of the AI in smart libraries in providing services, which in turn lead to the discrimination of the AI against certain users or groups, including, but not limited to, race, gender, age, etc. Users of different identities, ages, and races may be served differently by differentiated services when confronted with AI, all of which fall under the rubric of fairness challenges (Cox, 2022). Fairness challenges result in AI treating users differently, and users may feel that their personal autonomy is being violated. This is because AI without clear standards at this point may give users the impression that they are being controlled and manipulated by the AI, rather than a tool that can be used to create value for humans. This may exacerbate the perception of techno-invasion and increase people's technostress. Therefore, this paper argues that fairness challenges are a derivative risk that smart libraries need to face when applying AI.

Regulatory ambiguity: Exacerbating the degree of action rule confusion in techno-complexity. Although AI has now entered the realm of technology, finance, and other related legal regulation, many context-specific rules remain vague along with the rapid development of AI (Tobin, 2023). Regulatory ambiguity in the library context can be understood as the current inadequacy of the relevant legal framework and regulatory provisions regarding the application of AI in smart libraries (Wu and Huang, 2021). The lack of clear rules makes it impossible for people to determine which behaviors are compliant and which are not when engaging with and using AI, and how to proceed in specific situations. Without specific guidelines for action to follow, it is more difficult for people to understand the boundaries when interacting with AI. This can exacerbate the perceived complexity of the technology and increase people's technostress.Therefore, we see regulatory ambiguity as a derivative risk that smart libraries need to face when applying AI.

Copyright concern: Exacerbating techno-uncertainty blurring of property rights scenarios. The Library Copyright Alliance (LCA) of America mentions that training AI by extracting copyrighted works is usually considered fair use (Klosek, 2024). Although LCA has also identified some non-compliant scenarios, such as when the output work is essentially the same in expression as the original work, which may constitute infringement, the exact scale of the distinction has not yet been clarified. It indicates that AI in smart libraries also needs to face concern from copyright.Copyright concern can be understood as a dispute over the copyright of works that may be involved when smart libraries use AI algorithms to generate personalized book recommendations, summaries, or other content (Samberg, 2023). On one hand, AI-generated content may involve adaptation, reconstruction, or creation of the original text of a work; on the other hand, AI training and optimization require large amounts of data, and these datasets may contain copyrighted works (Yan, 2022). When staff and users in smart libraries encounters ambiguous scenarios involving potential infringement, it becomes challenging to accurately determine when infringement is involved. This ultimately exacerbates concerns about AI compliance and increases technostress. Therefore, we argue that copyright concern is a derivative risk that smart libraries should address when applying AI.

Occupational maladaptation: Exacerbating career change in techno-insecurity. AI is currently replacing more and more jobs, and the library field is no exception. While some studies have pointed out that the application of AI can help librarians to be more productive (Gul and Bano, 2019), it also requires that the individuals involved have more specialized abilities and knowledge to use AI. This change in career requirements may make librarians feel uncomfortable and regard AI as a threat (Hervieux and Wheatley, 2021). Meanwhile, this occupational maladaptation can be outlined as a problem of lower demand for library labor, reduced workloads, and even unemployment due to the increasing level of intelligence and automation in smart libraries. This phenomenon reflects a possible change in the nature of librarian's work and the skills required as a result of the application of AI in smart libraries (Tait and Pierson, 2022). If staff members' skills do not align with the new job requirements, they may feel incompetent and thus generate the fear of being replaced by technology. This concern may further exacerbate librarians' professional insecurity and increase technostress. Therefore, this paper argues that occupational maladaptation is a derivative risk that smart libraries need to consider when applying AI.

Analysis of interrelationships

The development of AI technologies such as AIGC, Natural Language Processing (NLP), audio identification, smart robots, etc., while promoting the service level and improving the service efficiency of smart libraries, also brings certain risks to smart libraries. From the perspective of technostress, the risk of AI application in smart libraries involves two types of risks: self-risks and derivative risks. Self-risks characterize the factors that exist at the level of AI technology development that cause technostress, including AI malfunction, emotional disconnection, AI misjudgement, algorithmic bias, and responsibility ambiguity.

Derivative risks characterize the factors that exist at the level of AI social applications that cause technostress, including security threat, fairness challenges, regulatory ambiguity, copyright concern, and occupational maladaptation. Both types of risks are external manifestations of technostress when AI is applied to smart libraries and can be cascaded through the sources of technostress. However these risks can exacerbate the technostress that people experience when interacting with AI in smart libraries.Challenges at the level of technology development may be further accentuated at the level of social applications, and problems at the level of social applications may feed back to the level of development. Thus self-risks and derivative risks are interconnected and transformed, and the relationships among the risk categories of AI application in smart libraries are shown in Figure 3.

Assessing the risks of AI applications in smart libraries

In the previous section, we identified the risks associated with the application of AI in libraries at the human-computer level, based on technostress. Although we matched each technostress source to a risk, this does not imply that these risks are isolated or independent. Because technostress tends to exhibit complex causal feedback, transmission and diffusion effects in systems, there is an interplay among these risks. The next step in this research is to sort out the relationships among these risks and to characterize the risk structure, and then to assess the position and influence of each risk in the risk system. This systematic analysis will enable to a comprehensive understanding of the interaction mechanism of risks from a systemic perspective, which will in turn provide a scientific basis and strategic guidance for risk governance and technology adaptation in libraries.

In this study, we chose the DEMATEL methodology due to its unique ability to assess causal relationships within complex systems. DEMATEL is well-suited for analyzing interconnected risks, as it helps identify how different risk factors influence each other, providing a clear understanding of their interdependencies. Similarly, the DEMATEL approach is suitable for assessing the multi-layered risks (technical and societal) associated with AI applications in smart libraries. In addition, DEMATEL compares favorably with Failure Mode and Effects Analysis (FMEA) and Bayesian Networks in that the FMEA approach struggles to deal with complex dependencies (Yucesan et al., 2021), such as algorithmic biases that may involve both technical issues and fairness issues. In addition, a single failure mode analysis of FMEA may not be able to fully capture these complex relationships, leading to underestimation of certain risks. Meanwhile, the existing smart library construction mode tends to be single; Bayesian Networks require a large amount of real-time data as support, which cannot be provided by the current stage of library development.

In addition, compared with risk matrices, Delphi studies, DEMATEL can enhance the precision of traditional risk assessment, and is suitable for making in-depth understanding of causal relationships among AI risk factors in smart libraries. While risk matrices, Delphi studies perform better in risk prioritization and expert consensus prediction, but not as good as DEMATEL in dealing with complex relationships and systematic analysis.Therefore, DEMATEL is beneficial to enhance the depth and systematicity of AI services for risk assessment in smart libraries. Firstly, the DEMATEL method defines the third dimension (root driving forces) of risk assessment in smart libraries through the degree of cause (R) and degree of centrality (C), forming a three-dimensional risk matrix (probability × impact × driving force) (Yang, 2021). This enhances the traditional "probability-impact" two-dimensional coordinate system for prioritizing risks (Wu and Lee, 2007). Secondly, the DEMATEL method transforms the ambiguous expert opinions from the Delphi Method into a structured causal relationship network, reducing subjective biases through iterative feedback (such as correcting "the impact of derivative risks on their own risks"). In summary, this approach provides a comprehensive and systematic understanding of the risk structure, aiding in the identification of the most critical driving factors and their ripple effects within the system. Meanwhile, DEMATEL's strength in mapping causal relationships makes it an ideal choice for this study, enabling more effective risk assessment and management strategies.

DEMATEL method

DEMATEL is a system analysis method that utilizes graph theory and matrix tools. Through the logical relationship among the elements in the system and the direct influence matrix, the degree of influence of each element on the other elements and the degree of being influenced can be calculated. The degree of cause and the degree of centrality of each element are then calculated as the basis for constructing a model, which in turn determines the causal relationship among the elements and their position in the system (Shieh et al., 2010). The essence of DEMATEL modeling is to view the system as a directed graph with weights. There will be relationships among elements in the system that influence each

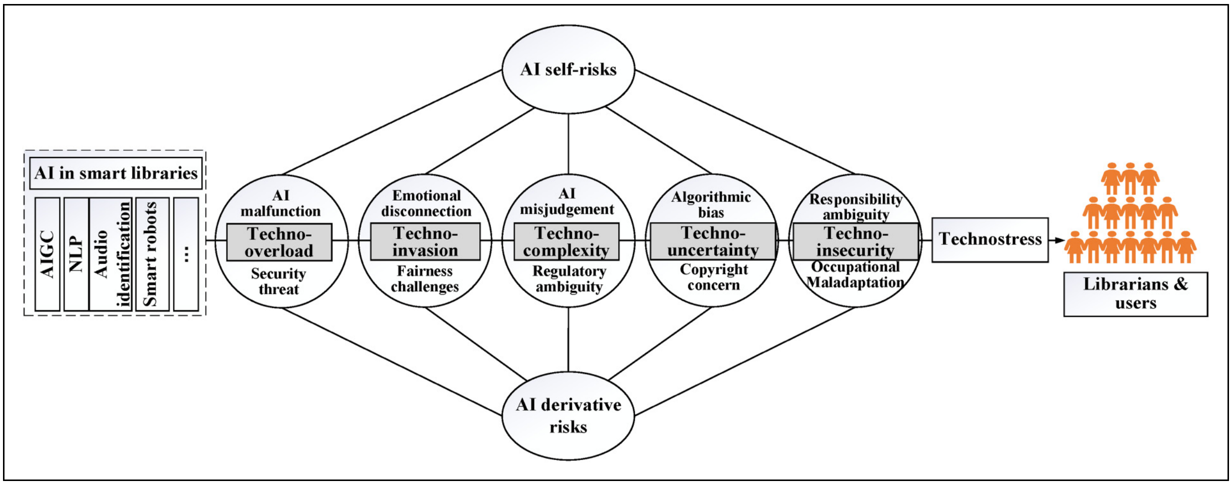

Figure 3. Risk categories relationships resulting from AI application in smart libraries.
Source: Credits by authors.

other, and also different strengths of such relationships (Tzeng et al., 2007). We regard the risk categories arising from the application of AI in smart libraries as a system (AISL system). Then the various types of risks identified in the previous section are the elements in the system, and the connection among these elements can be used as the basis for DEMATEL analysis.

Meanwhile, the results obtained from DEMATEL can clarify the positioning and role of each element in the AISL system and be mapped by the influence degree, influenced degree, centrality, and causality. Specifically, risks with high influence degree tend to be key risks that the AISL system needs to prioritize and that can have a significant influence on a number of other risks, while risks with high influenced degree risks may be the result of being driven by other risk factors, and therefore the governance strategies for these risks should focus on the factors that are the source of these risks. Risks with high centrality usually have strong systemic dependencies, and their presence may lead to a concentration of other risks; risks with high causality may be the source of a chain reaction, and these risks usually have wide-ranging external influence, and their root causes need to be identified and eliminated in a timely manner. Through the DEMATEL method, we can systematically assess the multiple risks that smart libraries may bring in the process of applying AI and formulate more precise risk prevention and governance strategies based on the interrelationships among the risks. This will provide theoretical support and practical guidance for libraries when introducing AI for human-computer interaction optimization, which will ensure that AI can be safely and effectively integrated into library services.

The survey process

The DEMATEL analysis is based on the direct influence matrix, which consists of the influence relationship between each element, where each element indicates the direct influence value of that row element on that column element. The direct influence values in this paper are obtained through an expert survey, and the panel of experts consists of a total of eight professors and associate professors from the library and information science (LIS) direction. The expert panel in this study consisted of eight professors and associate professors, selected for their expertise in areas relevant to AI and smart library systems. Their areas of expertise included artificial intelligence and machine learning (three experts), library and information science (two experts), AI ethics (two experts), and risk management and decision-making frameworks (one expert). This diverse panel provided a well-rounded perspective on the risks of AI applications in smart libraries, ensuring a comprehensive analysis from both technical and social viewpoints. The expert surveys conducted in this study revealed several key findings regarding the risks of AI applications in smart libraries. Experts identified both technical and social risks, with AI malfunction, algorithmic bias, and AI misjudgment being major technical concerns. They emphasized that AI systems must be transparent and reliable to prevent errors and ensure fairness. Social risks, including privacy concerns, the potential for AI to amplify inequalities, and the need for clear regulatory frameworks, were also highlighted. Additionally, the surveys revealed that technical and social risks are interconnected, as failures in AI can directly affect user trust and experience. These findings guided the development of a comprehensive risk assessment framework in this study.

Influence matrix modeling and calculation

During the survey, experts were asked to assess the influence relationships between different research topics based on their expertise and practical experience. They rated the strength of these relationships using a 5-level scale (from 0 to 4), where 0 indicates no influence, and 4 indicates a strong influence. Based on these ratings, we created a direct influence matrix, shown in Figure 4. The values on the diagonal of the matrix are all 0, since each risk category does not need to be compared to itself. The numbers on the axes correspond to different risks: 1 for AI malfunction, 2 for AI misjudgement, 3 for security threats, 4 for algorithmic bias, 5 for responsibility ambiguity, 6 for copyright concerns, 7 for emotional disconnection, 8 for regulatory ambiguity, 9 for fairness challenges, and 10 for copyright concerns. For example, in the matrix, the first column of the second row shows that AI misjudgement has a moderate-to-low influence on AI malfunction in the context of AI applications in smart libraries.

To continue with the analysis, the direct influence matrix was normalized, as shown in Figure 5, and used in further calculations. We then calculated the indirect effects among the risk categories by multiplying the normalized direct influence matrix with itself. Finally, we summed up all the indirect influences to create the comprehensive influence matrix, which is calculated using the formula below:

$$\mathbf{T} = \mathcal{N} + \mathcal{N}^2 + \mathcal{N}^3 + \cdots\cdots + \mathcal{N}^k = \sum_{k=1}^{\infty} \mathcal{N}^k = \mathcal{N}(\mathbf{I} - \mathcal{N})^{-1} \tag{1}$$

where $\mathbf{T}$ is the integrated influence matrix, $\mathcal{N}$ is the normalized influence matrix, and $\mathbf{I}$ is the unit matrix. The whole analysis process is completed based on Python, and the comprehensive influence matrix is obtained, as shown in Figure 6.

Based on the comprehensive influence matrix T, the influence degree, influenced degree, centrality, and causality of each risk in risk categories arising from the application of AI in smart libraries can be further calculated.

Influence factors assessment and results

Influence degree refers to the sum of the matrix values of the rows in $\mathbf{T}$, and represents the comprehensive influence value of the elements of each row on all other elements. The influence degree of element i is denoted as $Influence\ Degree_i$ and t_{ij} denotes the direct influence of element i on element j. At this

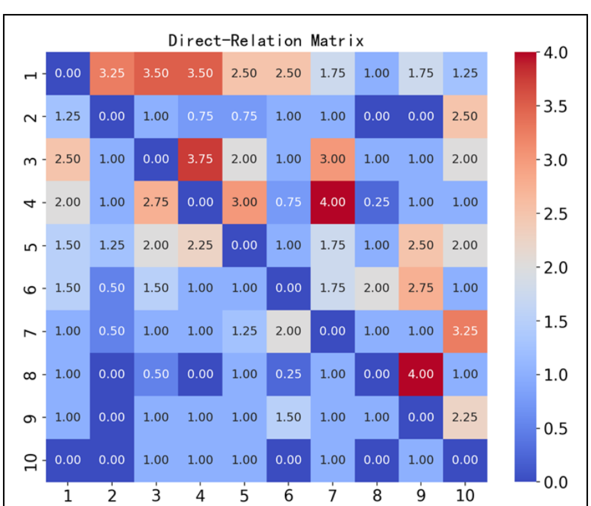

Figure 4. Direct influence matrix. Source: Credits by authors.

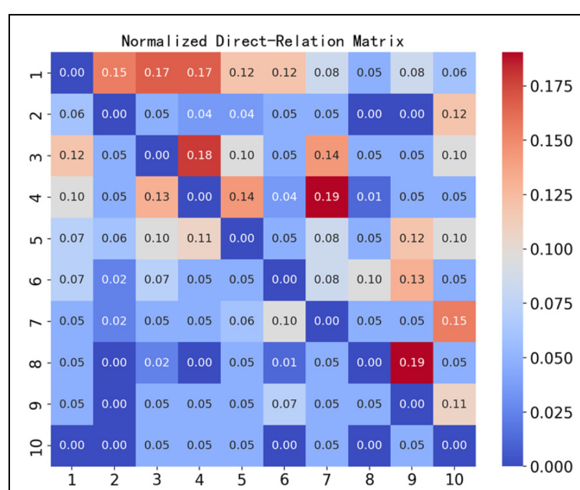

Figure 5. Normalization influence matrix. Source: Credits by authors.

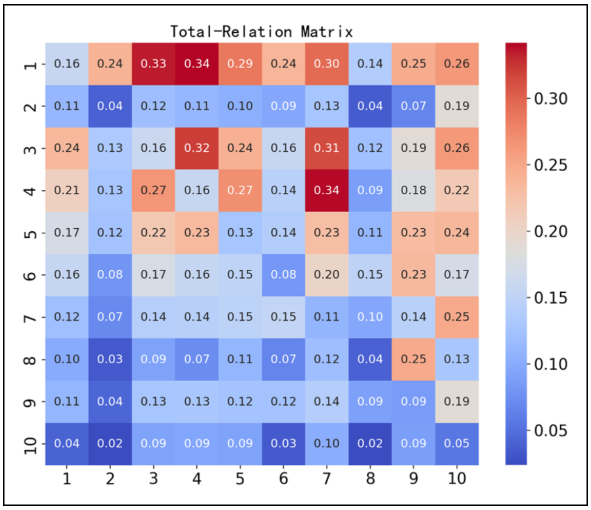

Figure 6. Comprehensive influence matrix.
Source: Credits by authors.

point:

$$Influence\ Degree_i = \sum_{j=1}^{n} t_{ij},\ (i = 1, 2, 3, \ \ldots\ldots, n) \tag{2}$$

The influenced degree refers to the sum of the matrix values of the columns in T, and represents the comprehensive influence value of all other elements to which each column element is exposed. In this paper, the influenced degree of element i is denoted as $Influenced\ Degree_i$. At this point:

$$Influenced\ Degree_i = \sum_{j=1}^{n} t_{ji},\ (i = 1, 2, 3, \ \ldots\ldots, n) \tag{3}$$

Centrality refers to the position of the element in the system and the magnitude of the role it plays and is denoted as $Centrality_i$. At this point:

$$Centrality_i = Influence\ Degree_i + Influenced\ Degree_i \tag{4}$$

Causality refers to the difference between the degree of influence and the degree of being influenced; if causality is greater than 0, it is called the cause element, and if causality is less than 0, it is called the result element. That is to say, the larger the absolute value of causality, the stronger the effect of the element as a cause or effect, which will be denoted as $Causality_i$. At this point:

$$Causality_i = Influence\ Degree_i - Influenced\ Degree_i \tag{5}$$

According to the above formula, the value of each element is obtained (Table 1), and the differences between the various risks on each indicator can be visualized through Figure 7.

In this paper, we obtain a two-dimensional scatterplot based on DEMATEL analysis (see Figure 8), which shows the location and role of each risk factor in “risk categories arising from the application of AI in smart libraries as a system” (AISL system) through the two dimensions of “centrality” and “causality”. Two dashed lines (horizontal and vertical axes) are plotted in the figure to represent the mean of centrality and causality, respectively, and are used to delineate the quadrants. The intersection of the dashed lines divides the graph into four quadrants to help identify different types of risk factors. Risks located in quadrant 1 have high centrality and positive causality, which indicates that these risks not only have a strong influence in AISL but also act as drivers of other risks in the AISL system. In Figure 8, AI malfunction and AI misjudgement are located in Quadrant I, indicating that they are key drivers in the AISL system with significant causal influence on other risks. These factors are often the “source risks” of the AISL system, and their management and control can significantly mitigate other cascading risks in the risk category. Quadrant 2 risks exhibit high centrality and negative causality, meaning that they are also of significant importance (high centrality) in the AISL system, but they are more often the result of being driven by other risks.

In Figure 8, factors such as algorithmic bias are close to the boundaries of Quadrant 2, and although they are mainly controlled factors, they also have an impact on other risks in the “risk categories arising from the application of AI in smart libraries as a system” (AISL system). These risks are often at the center and are “indirect risks” that should be managed in conjunction with the factors that drive the core to form a comprehensive risk control. Quadrant 3 factors have low centrality and negative causality and are minor risk factors in the AISL system that are not only driven by other factors (negative causality), but also have less impact on the risk category as a whole (low centrality). In Figure 8, regulatory ambiguity and occupational maladaptation are located in Quadrant 3, which suggests that these factors are relatively independent and weakly influential, and may be the result of a combination of other factors in the AISL system. For such peripheral secondary factors, there is less urgency to control their

Table 1. The value of each element.

Risk types	Influence degree	Influenced degree	Centrality	Causality
AI malfunction	2.54	1.41	3.95	1.13
AI misjudgment	2.14	1.72	3.86	0.41
Security threats	1.55	1.23	2.78	0.32
Algorithmic bias	1.99	1.76	3.75	0.24
Responsibility ambiguity	1.82	1.65	3.47	0.17
Copyright concerns	1.01	0.89	1.9	0.12
Emotional disconnection	1	0.92	1.91	0.08
Regulatory ambiguity	1.16	1.71	2.87	−0.55
Fairness challenges	1.37	1.97	3.35	−0.6
Occupational maladaptation	0.64	1.96	2.6	−1.32

Source: Credits by authors.

risk directly, but their risk level can be reduced indirectly by managing related drivers. The factors in Quadrant 4 exhibit a lower degree of centrality and positive causality, indicating that these factors have less overall influence on the AISL system, but have some driving force. Fairness challenges are located in this quadrant in Figure 8, and they are not the core risks in the system, but as secondary driven factors, they may indirectly affect the overall service level and service efficiency of the smart library by affecting some areas of the AISL system. In risk governance, they can be used as secondary control points to avoid their spreading influence.

Discussions, countermeasures and implications

Based on the results of the DEMATEL assessment, for the risk categories of applying AI in smart libraries, we can discuss the status and mechanism of the role of each risk factor in the AISL system from a systemic perspective, and explore the potential governance insights from a scholarly viewpoint.

Discussions

Relative importance of technical and social risks. Based on the DEMATEL analysis, technical risks are the highest concern. AI malfunction and AI misjudgment have the highest influence degree and centrality, making them the main drivers of risk. These technical issues can disrupt services and affect the reliability of AI in smart libraries. While social risks like responsibility ambiguity and copyright concerns are important, they are more likely to arise from technical failures. For instance, AI malfunctions or biases can lead to fairness issues or accountability concerns. Thus, addressing technical risks, especially AI malfunction and misjudgment, should be the priority, as they directly influence both the functionality of AI systems and the social risks that follow.

Core risks identification and discussion. In terms of the self-risks arising from the application of AI in smart libraries, the more centrality risks (e.g., AI malfunction, AI misjudgement, and algorithmic bias) show strong correlation and dominance in the "risk categories arising from the application of AI in smart libraries as a system" (AISL system). This suggests that these risks are critical nodes in the AISL system. High-centrality risks are both a source of influencing other risks and, simultaneously, form complex interactions with other risks. Therefore, from the perspective of systems theory, AI malfunction and AI misjudgement are not only individual risk factors, but also "risk transmitters" or "interaction centers" in the AISL system, and their changes will trigger cascading effects in the network (Lin et al., 2023), which in turn can affect the stability and security of the AISL system (Galaz et al., 2021). In addition, algorithmic bias is at the center of the AISL system in terms of centrality despite its low causality, suggesting that the risk is broadly system-dependent and that its changes may affect the performance of multiple other risks through a complex network. Notably, the embedded nature of algorithmic bias in the AISL system makes it easy to solidify in the entire AI model once it develops a bias, which in turn affects the long-term fairness and credibility of the AISL system (Ferrara, 2024).

Risk discussion based on causal chain. The causality analysis above shows that AI malfunction, AI

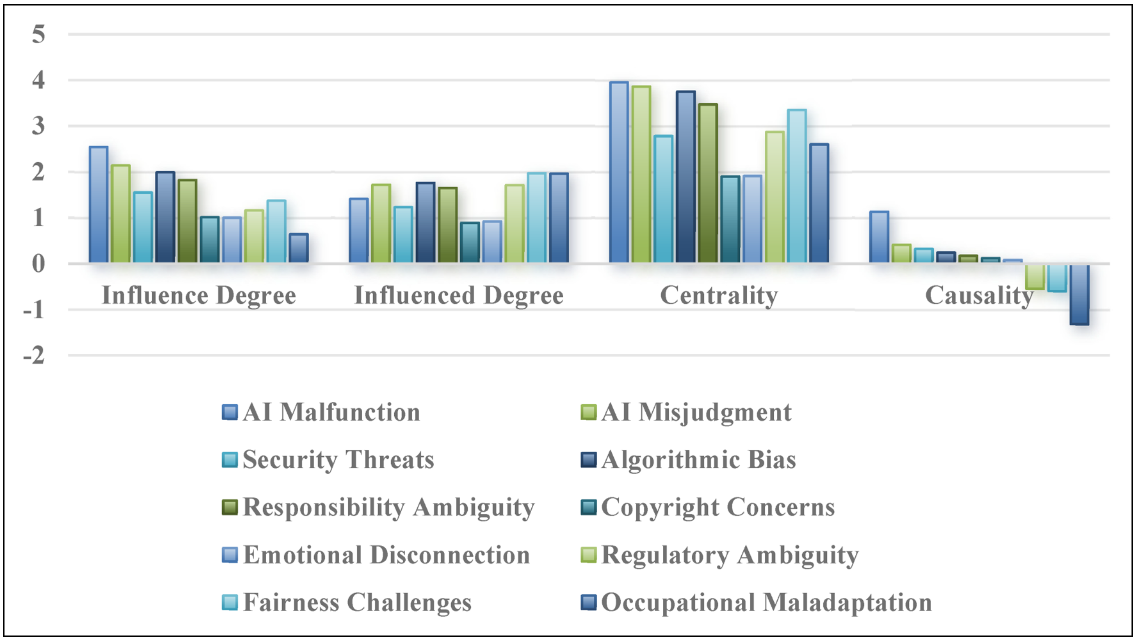

Figure 7. DEMATEL analysis indicators for each risk.
Source: Credits by authors.

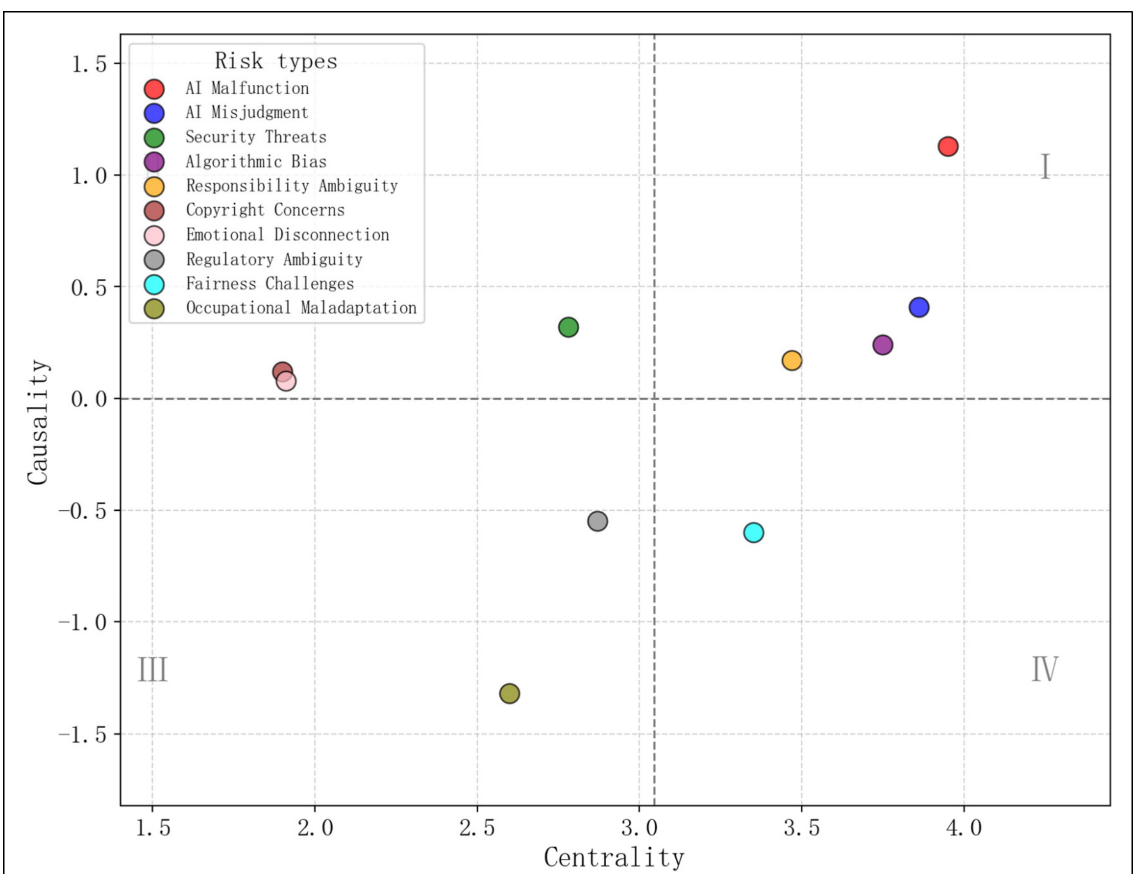

Figure 8. Two-dimensional scatterplot based on DEMATEL analysis.
Source: Credits by authors.

misjudgement, and security threats are highly driven, representing the "upstream risk" or "initial risk" that these risks play in the "risk categories arising from the application of AI in smart libraries as a system" (AISL system). Driven risks are often caused by external conditions or technical factors within the system, which have strong diffusion and permeability in the risk transmission process and can directly or indirectly trigger downstream risks. Therefore, when governing AI risks in smart libraries, the focus should be on the formation mechanisms of the driving risks, such as the algorithmic stability of the AI model, data integrity, and the security protection strategies inside and outside the system. Effective control of driving risks will be a fundamental means to suppress other derivative risks (Bhasin et al., 2021). In contrast, the derivative risks arising from the application of AI in smart libraries, such as regulatory ambiguity, fairness challenges, and occupational maladaptation, show strong consequentiality (i.e., negative causality), which indicates that these risks are more dependent in the AISL system. These risks are significantly influenced by the upstream risks, which are "reactive risks" or "dependent risks". From the perspective of causal chain, the existence of these consequential risks is due to the chain reaction of upstream risks (e.g., AI malfunction) within the AISL system in specific contexts. Therefore, optimizing driven risk management can reduce the probability of occurrence of resultant risks and effectively reduce the "passive diffusion" of downstream risks.

Multi-level risks governance discussion. Identifying the risks of AI applications in smart libraries and Assessing the risks of AI applications in smart libraries mention that the interdependence between self-risks and derivative risks in AI applications for smart library services determines that the risks are multi-level. In terms of the self-risks arising from the application of AI in smart libraries, our analysis from a system management perspective reveals that the combined effect of high centrality and high driven risks constitutes the main threat of "risk categories arising from the application of AI in smart libraries as a system" (AISL system) instability. AI malfunction, as a high-influence, high-causality, and high-centrality risk, directly affects the operational logic and technical performance of the AISL system. Its risk management strategy not only needs to improve the anti-interference and stability of the AISL system at the technical level, but also should improve the emergency response capability at the operational and decision-making levels, which reduces the chain effect of other risks triggered by the system going out of control (Baron and Pate-Cornell, 1999). In addition, the drive and centrality of AI misjudgement requires special attention. The reasons for the formation of this risk factor usually involve the representativeness of the data training set and the adaptability of the algorithms. In this context, the fault-tolerant design and real-time monitoring of the AISL system are particularly important (Goldfarb and Lindsay, 2022). In terms of academic research, increasing the diversity of the training set and adjusting the sensitivity factor of the algorithm can be an effective countermeasure against AI misjudgment to reduce the triggering effect of AI misjudgment on other risks.

Risk transmission and diffusion pathway discussion. The results of the DEMATEL assessment show that the smart library application of AI generates its self-risks such as AI malfunction and AI misjudgement, that occupy a critical position in the system, and their influence can be felt along multiple transfer and diffusion paths in the system. Combined with the study of transfer and diffusion mechanisms, the risk of AI malfunction mainly triggers other risks by directly interfering with other subsystems (e.g., data security and user experience). Algorithmic bias, although not highly causative, forms an "implicit bias pathway" through its high correlation with fairness challenges, which may gradually affect the fairness of the system and user acceptance in the long run. In addition, derivative risks arising from the application of AI in smart libraries, such as regulatory ambiguity and occupational maladaptation, as consequential risks, are mainly driven by other factors within the system, and their risk transmission and diffusion paths are more indirect. Regulatory ambiguity stems from the imperfect regulatory framework of smart libraries' inadequate regulatory framework, while occupational maladaptation arises from changes in the occupational environment brought about by a high level of dependence on AI systems (Cox and Mazumdar, 2024; Dyer et al., 1993). Therefore, the negative feedback of these outcome risks to the system should be reduced at the management level through the establishment of clear operational guidelines and a well-developed career support system.

Governance countermeasures

Prioritize control of highly driven risks. In terms of the risks arising from the application of AI in smart libraries, highly driven risks (e.g., AI malfunction and AI misjudgement) are the core "source risks" in the risk system of smart libraries, and their high influence and transmissibility make it possible to quickly trigger a systematic chain effect once they are out of control. Therefore, prioritizing the control of these risks is the key to guaranteeing the safety of intelligent libraries.

Specifically, it is recommended that smart libraries establish an all-encompassing risk control system that includes anomaly detection, real-time feedback, and iterative updating. In terms of anomaly detection, the security of equipment can be diagnosed regularly by deploying advanced monitoring technologies and setting up multiple firewalls with high security levels (Asemi et al., 2020). For example, the establishment of an abnormal behavior analysis model based on machine learning, real-time capture of the system's possible loss of control signals, and timely prevention, control, and detection. In terms of real-time feedback, the system needs to have an efficient automatic response mechanism, such as triggering the emergency abortion function or switching to manual intervention mode, which can prevent the risk from further spreading. In terms of iterative updating, the algorithm design and data training set of the AI model should be optimized regularly to reduce the possibility of loss of control triggered by data deviation or algorithmic loopholes. At the same time, contingency plans and rehearsal mechanisms for unexpected risks should be established to ensure that library staff can quickly identify problems and take effective measures to control risks within a localized scope.

Furthermore, enhancing AI computing power and model optimization will accelerate the transformation of smart libraries. AI technologies help self-service terminal devices ensure data security, thereby improving service efficiency. Meanwhile, the use of large AI technologies enable real-time processing of multimodal data, precise retrieval, personalized recommendations, and the creation of an immersive interactive space for smart libraries. By integrating AI technologies, smart libraries are propelled from digitalization to cognitive intelligence, pioneering a new paradigm driven by the dual engines of "computing power and algorithms," and establishing a self-evolving, continuously optimized service system for smart libraries.

Hierarchical management of resultant risks. In terms of derivative risks arising from the application of AI in smart libraries, resultant risks (e.g., regulatory ambiguity, fairness challenges, and occupational maladaptation) are characterized by high dependency and indirectness, and they are mainly influenced by upstream driving risks. Therefore, the governance of this type of risk should adopt a layered management strategy, starting with optimizing upstream risks in order to reduce their reactive manifestations while formulating targeted mitigation measures for the characteristics of resultant risks.

In layered management, it is first necessary to clarify the conduction path between upstream-driven risks and downstream resultant risks. For example, by strengthening the transparency construction of the AI system, the operational confusion caused by regulatory ambiguity is reduced; by optimizing the algorithm design and data processing process, the incidence of fairness challenges is reduced; and through the vocational skills enhancement training, the staff's adaptability to technological changes is strengthened. In addition, it is also necessary to formulate refined management strategies for the specific manifestations of resultant risks. For example, to address fairness challenges, a more inclusive and transparent algorithm review mechanism can be constructed to ensure the fairness and consistency of services; to address occupational maladaptation, occupational psychology support and staff retraining programs can be strengthened. Among them, the vocational retraining program includes one or even more aspects of competence, such as readers' diversified demand collection, generative AI equipment operation and maintenance, big data management and analysis, knowledge product development and service, scientific research support, etc., so as to enhance the vocational skills of the library staff and to help the staff integrate into the intelligent service pattern of the smart library more quickly (Ke et al., 2024; Wu and Liu, 2022).

Meanwhile, in hierarchical management, libraries should set up risk management departments. The personnel of the risk management department are responsible for supervising the process of AI design, manufacturing, application, updating, and upgrading (Harisanty et al., 2023), which improves the efficiency of the risk prevention and control governance of the smart library through the exchange of information between the departments. and avoids the deterioration and spread of risks (Yoon et al., 2022). First, the personnel of relevant departments need to regularly conduct data security risk assessments and hidden danger investigations to determine the priority of security protection and protective measures. Second, strengthen technical security protection measures, including but not limited to data encryption, access control, network security, and system security. Third, establish a data security monitoring and daily inspection mechanism to grasp the system security status in real time. Fourth, improve the emergency response plan, including data leakage, rapid response to security incidents, and handling and recovery of detailed steps to establish a security training and education system to improve the security awareness of all employees and the ability to deal with security incidents. Fifth, as a public data hub, libraries need to establish a governance framework encompassing security protection, privacy computing, and copyright verification. By implementing data tiered authorization and algorithm auditing mechanisms, they can provide trustworthy services, prevent algorithmic biases, and ensure service fairness. Sixth, integrating data ethics and AI safety into reader education programs, and enhancing public algorithmic literacy through immersive human-computer interaction training, will foster a new reading community equipped with digital rights awareness and critical thinking towards technology.

Through the layered risk management model of "upstream regulation and downstream elimination", smart libraries are able to more efficiently deal with the interaction of multi-level issues in the complex risk system, thus improving the overall risk management effect.

Dynamic adjustment of adaptation rules. In terms of derivative risks arising from the application of AI in smart libraries, the emergence of risks such as regulatory ambiguity and occupational maladaptation is usually closely related to the rapid iteration of AI technology and changes in application scenarios. Effective governance of such risks requires smart libraries to maintain dynamic adjustments in rule-making and adaptive measures to adapt to changes in technological development and user needs.

In terms of rule adjustments, smart libraries need to establish a regular review and update mechanism to dynamically assess existing rules and management norms for technology applications. For example, for sensitive areas such as copyright issues and data privacy protection, the relevant system should be revised in a timely manner according to the latest regulatory requirements to ensure the legitimacy and compliance of technology applications. In terms of adaptive measures, systematic occupational support programs need to be provided for library staff in response to changes in occupational requirements brought about by AI technology, including skills enhancement training, career development guidance, and mental health protection. This not only reduces the risk of occupational maladaptation but also enhances the staff's sense of participation and belonging in the intelligent environment.

In addition, in order to enhance the humanization of smart libraries in the application of AI technology, two-way communication with users and staff should be emphasized, feedback should be widely collected, and rules and service strategies should be adjusted according to actual needs. For example, user experience surveys can help identify the risks perceived by users in AI services so as to improve the technical design; staff suggestions can provide a practical basis for the optimization of operational specifications. What's more, Smart libraries service platforms can optimize collection management through comprehensive AI upgrades, enabling cross-media digital displays. For instance, a unified model can integrate searches across text, images, and audio, enhancing the accuracy of retrieval and recommendations; automatically generate textual, pictorial, and video content to create interactive virtual exhibitions and intelligent cultural innovation platforms, enriching audience experiences; and utilize multimodal models to improve the efficiency of digital resource management, thereby boosting the competitiveness and appeal of smart libraries. Through this human-centered, dynamic adjustment of rules, smart libraries are able to find a balance between technology and management and reduce risks caused by vague rules or operational doubts.

Implications

Theoretical implications. At the theoretical level, we first introduced the technostress theory into the research field of AI risk in smart libraries, identifying and analyzing its sources of risk from five dimensions: techno-overload, techno-invasion, techno-complexity, techno-insecurity, techno-uncertainty, and techno-insecurity. AI risks can be summarized from both technical and social dimensions. AI risks characterizing the technical dimension include AI malfunction, emotional disconnection, AI misjudgement, algorithmic bias, and responsibility ambiguity; AI derivative risks characterizing the social dimension include security threat, fairness challenges, copyright concern, regulatory ambiguity, and occupational maladaptation. Secondly, we apply the DEMATEL method to quantify the causal relationships among risks, assess the degree of linkage and relevant influencing factors among risks at both the technological and societal levels, and emphasize the critical status of high-driven risks, such as AI malfunction, AI misjudgement, etc. Lastly, the core-risk identification, causal-chain-based risk, multilevel risk governance, and other related risk characteristics are discussed, and the governance strategies of prioritizing the control of high risks, hierarchically managing resultant risks, and dynamically adjusting the adaptive rule level are proposed. In summary, this paper provides a theoretical basis for the governance of AI technology in smart libraries.

Practical implications. At the practical level, we analyze the risks of applying AI in smart libraries from a technostress perspective, identify their risk causes, and assess their risk categories. According to the risk categories, we propose hierarchical and multilevel risk governance countermeasures, including prioritizing the control of high-driven risks, hierarchical management of resultant risks, and dynamic adjustment of adaptive rules. This paper aims to provide practical guidance for the application and management of AI in smart libraries. Meanwhile, this study not only offers valuable references for smart library development but also expands the conceptual framework of AI technology risk governance to other domains, such as art galleries, archives, museums, and similar public cultural institutions.

Conclusion and future work

This study adopts the content analysis method and systematically explores the sources of risks and their causal mechanisms in the application of AI in smart libraries based on the technostress theory; the interrelationships and transmission and diffusion paths among the risks are revealed through the DEMATEL method, and in-depth discussions are conducted. The main contents of the research in this paper are reflected in the following aspects: first, it is the first time to introduce the technostress theory into the research field of AI risks in smart libraries, and identify and analyze the sources of risks; second, it applies DEMATEL method to quantify the causality between risks and assess the risks, emphasizing the high-drivenness risks, such as AI malfunction and AI misjudgement, etc.; third, multi-level governance strategies based on risk characteristics are proposed, which provide theoretical support and practical guidance for technology application and risk management in smart libraries.

Prospectively, the development of smart libraries needs to deepen the research and practice from several aspects. First, at the policy and technology level, we should improve the standards and regulations for the application of AI technology in smart libraries and enhance the transparency and interpretability of the model, which will provide a more solid foundation for the development of smart libraries. Second, the risks brought by AI technology have dynamic evolution characteristics, so we need to build a dynamic adaptive risk governance system to achieve accurate early warning and control through time series analysis and real-time monitoring. Once again, AI risk governance for smart libraries should advocate a multi-party collaboration model, encouraging in-depth cooperation among libraries, users, technology developers, and policymakers to jointly promote the development of technology and management optimization.

Meanwhile, we should base our decision on the possible risks of data intelligence-enabled library smart services and explore the risk governance system from the aspects of rule-based governance, procedural governance, and technical governance to promote the sustainable development of data intelligence-enabled library smart services. Finally, the application of AI technology in smart libraries may exacerbate ethical and fairness challenges, and in the future we should strengthen the research on algorithmic transparency and ethical norms to ensure the fairness and inclusiveness of technology application. In summary, the future of smart libraries lies in the deep integration of technology and the humanities. Through further theoretical exploration and practical application, smart libraries are expected to become a model of technological innovation in the public cultural service system, to meet the diversified needs of society in a safe, inclusive, and efficient way, and to realize the coordination and unification of technology-driven and humanistic services.

Although this study provides comprehensive risk governance strategies, further research is essential to explore how risk manifest in different socio-cultural contexts and levels of technological development. Therefore, we will reveal the specific performance and governance effects of AI risks in smart libraries in different environments through cross-cultural comparative studies, so as to propose more precise and detailed solutions. Furthermore, the functions and boundaries of AI technology-enabled smart libraries are constantly expanding, and we in the deep information ecosystem should constantly explore how to use AI technology to improve the level of personalized services for users and the sustainable development of smart libraries.

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported by the National Social Science Fund of China (No. 24CTQ051).

ORCID iDs

Xu Wang https://orcid.org/0000-0002-8789-7951
Fang Xie https://orcid.org/0009-0001-9695-1024
Guanghui Cheng https://orcid.org/0000-0003-4950-3816
Kiran Shehzadi https://orcid.org/0009-0005-8020-5800

Supplemental material

Supplemental material for this article is available online.

References

Adetayo AJ (2023) Artificial intelligence chatbots in academic libraries: The rise of ChatGPT. *Library Hi Tech News* 40(3): 18–21.

Ahmad UNU and Amin SM (2012) The dimensions of technostress among academic librarians. *Procedia-Social and Behavioral Sciences* 65: 266–271.

Aittola M, Ryhänen T and Ojala T (2003) Smartlibrary–location-aware mobile library service. In: Human-Computer Interaction with Mobile Devices and Services: 5th International Symposium, Mobile HCI 2003, Udine, Italy, September 2003. Proceedings 5. Berlin Heidelberg: Springer, pp.411–416.

Akter S, McCarthy G, Sajib S, et al. (2021) Algorithmic bias in data-driven innovation in the age of AI. *International Journal of Information Management* 60: 102387.

Arnetz BB and Wiholm C (1997) Technological stress: Psychophysiological symptoms in modern offices. *Journal of Psychosomatic Research* 43(1): 35–42.

Asemi A, Ko A and Nowkarizi M (2020) Intelligent libraries: A review on expert systems, artificial intelligence, and robot. *Library Hi Tech* 39(2): 412–434.

Asim M, Arif M, Rafiq M, et al. (2023) Investigating applications of artificial intelligence in university libraries of Pakistan: An empirical study. *The Journal of Academic Librarianship* 49(6): 102803.

Aslam S, Jabeen M and Jabeen M (2025) Fostering innovation in smart library services: An in-depth exploration of empowered capabilities and dynamic strategies among university librarians in Pakistan. *Information Development*. https://doi.org/10.1177/02666669241305379

Ayyagari R, Grover V and Purvis R (2011) Technostress: Technological antecedents and implications. *MIS Quarterly* 35(4): 831–858.

Baron MM and Pate-Cornell EB (1999) Designing risk-management strategies for critical engineering systems. *IEEE Transactions on Engineering Management* 46(1): 87–100.

Barsha S and Munshi SA (2023) Implementing artificial intelligence in library services: A review of current prospects and challenges of developing countries. *Library Hi Tech News* 41(1): 7–10.

Bhasin S, Garg S and Regazzoni F (2021) Special section on attacking and protecting artificial intelligence. *CAAI Transactions on Intelligence Technology* 6(1): 1–2.

Bi S, Wang C, Zhang J, et al. (2022) A survey on artificial intelligence aided internet-of-things technologies in emerging smart libraries. *Sensors* 22(8): 2991.

Bichteler J (1987) Technostress in libraries: Causes, effects and solutions. *The Electronic Library* 5(5): 282–287.

Borgohain DJ, Bhardwaj RK and Verma MK (2024) Mapping the literature on the application of artificial intelligence in libraries (AAIL): A scientometric analysis. *Library Hi Tech* 42(1): 149–179.

Bradley F (2022) Representation of libraries in artificial intelligence regulations and implications for ethics and practice. *Journal of the Australian Library and Information Association* 71(3): 189–200.

Brod C (1984) *Technostress: The Human Cost of the Computer Revolution*. Reading, USA: Addison-Wesley Publishing Company.

Brown R, Duck J and Jimmieson N (2014) E-mail in the workplace: The role of stress appraisals and normative response pressure in the relationship between e-mail stressors and employee strain. *International Journal of Stress Management* 21(4): 325.

Busuioc M (2021) Accountable artificial intelligence: Holding algorithms to account. *Public Administration Review* 81(5): 825–836.

Cachat-Rosset G and Klarsfeld A (2023) Diversity, equity, and inclusion in artificial intelligence: An evaluation of guidelines. *Applied Artificial Intelligence* 37(1): 2176618.

Califf CB, Sarker S and Sarker S (2020) The bright and dark sides of technostress: A mixed-methods study involving healthcare IT. *MIS Quarterly* 44(2): 809–856.

Cao G, Liang M and Li X (2018) How to make the library smart? The conceptualization of the smart library. *The Electronic Library* 36(5): 811–825.

Chen C, Wu Z, Lai Y, et al. (2023) Challenges and Remedies to Privacy and Security in AIGC: Exploring the Potential of Privacy Computing, Blockchain, and Beyond. https://doi.org/10.48550/arXiv.2306.00419

Chesterman S (2020) Artificial intelligence and the limits of legal personality. *International & Comparative Law Quarterly* 69(4): 819–844.

Cheung HC, Lo YYM, Chiu DK, et al. (2023) Development of smart academic library services with Internet of Things technology: a qualitative study in Hong Kong. *Library Hi Tech*. https://doi.org/10.1108/LHT-06-2023-0219.

Coombs C, Stacey P, Kawalek P, et al. (2021) What is it about humanity that we can't give away to intelligent machines? A European perspective. *International Journal of Information Management* 58: 102311.

Cox AM (2021) Exploring the impact of artificial intelligence and robots on higher education through literature-based design fictions. *International Journal of Educational Technology in Higher Education* 18(1): 3.

Cox AM (2022) The ethics of AI for information professionals: Eight scenarios. *Journal of the Australian Library and Information Association* 71(3): 201–214.

Cox AM (2023) How artificial intelligence might change academic library work: Applying the competencies literature and the theory of the professions. *Journal of the Association for Information Science and Technology* 74(3): 367–380.

Cox AM (2024) Artificial intelligence and the academic library. *The Journal of Academic Librarianship* 50(6): 102965.

Cox AM and Mazumdar S (2024) Defining artificial intelligence for librarians. *Journal of Librarianship and Information Science* 56(2): 330–340.

Dezuanni M, Osman K, Burton AL, et al. (2024) *IFLA Trend Report 2024: Facing the Future of Information with Confidence*. Brisbane: Digital Media Research Centre.

Dollmat KS and Abdullah NA (2022) Machine learning in emotional intelligence studies: A survey. *Behaviour & Information Technology* 41(7): 1485–1502.

Dube TV, Rammutloa MW and Matatiele R (2024) Skills and competencies of academic librarians to use information technology tools in the digital era: A systematic literature review. *Information Development*. https://doi.org/10.1177/02666669241302054

Dyer H, Fossey D and McKee K (1993) The impact of automated library systems on job design and staffing structures. *Program* 27(1): 1–16.

Ekstrand M and Strandberg L (2023) Technological trends in Swedish medical libraries. *Health Information & Libraries Journal* 40(3): 326–331.

Fan FL, Xiong J, Li M, et al. (2021) On interpretability of artificial neural networks: A survey. *IEEE Transactions on Radiation and Plasma Medical Sciences* 5(6): 741–760.

Ferrara E (2024) The butterfly effect in artificial intelligence systems: Implications for AI bias and fairness. *Machine Learning with Applications* 15: 100525.

Floridi L, Cowls J, Beltrametti M, et al. (2018) AI4People—An Ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines* 28(4): 689–707.

Galaz V, Centeno MA, Callahan PW, et al. (2021) Artificial intelligence, systemic risks, and sustainability. *Technology in Society* 67: 101741.

Giorgi G, Ariza-Montes A, Mucci N, et al. (2022) The dark side and the light side of technology-related stress and stress related to workplace innovations: From artificial intelligence to business transformations. *International Journal of Environmental Research and Public Health* 19(3): 1248.

Goldfarb A and Lindsay JR (2022) Prediction and judgment: Why artificial intelligence increases the importance of humans in war. *International Security* 46(3): 7–50.

Gul S and Bano S (2019) Smart libraries: An emerging and innovative technological habitat of 21st century. *The Electronic Library* 37(5): 764–783.

Hamad F, Al-Fadel M and Fakhouri H (2023) The provision of smart service at academic libraries and associated challenges. *Journal of Librarianship and Information Science* 55(4): 960–971.

Harisanty D, Anna NEV, Putri TE, et al. (2023) Is adopting artificial intelligence in libraries urgency or a buzzword? A systematic literature review. *Journal of Information Science*. https://doi.org/10.1177/01655515221141034

Hervieux S and Wheatley A (2021) Perceptions of artificial intelligence: A survey of academic librarians in Canada and the United States. *The Journal of Academic Librarianship* 47(1): 102270.

Howard HA, Habashi MH and Reed JB (2020) The gender wage gap in research libraries. *College & Research Libraries* 81(4): 662.

Huang Y, Cox AM and Cox J (2023) Artificial intelligence in academic library strategy in the United Kingdom and the mainland of China. *The Journal of Academic Librarianship* 49(6): 102772.

Hussain A (2023) Use of artificial intelligence in the library services: Prospects and challenges. *Library Hi Tech News* 40(2): 15–17.

Hussain A and Ahmad P (2021) Adoption of smart technologies in university libraries of Pakistan: A qualitative review. *Library Philosophy and Practice* 2021(1): 1–10.

Jena RK (2015) Technostress in ICT enabled collaborative learning environment: An empirical study among Indian academician. *Computers in Human Behavior* 51: 1116–1123.

Ke P, Wang J and Liu QW (2024) The key path of smart library construction in the perspective of generative AI. *Journal of Modern Information* 44(01): 4–10.

Klosek K (2024) Training Generative AI Models on Copyrighted Works Is Fair Use. Available at: https://www.arl.org/blog/training-generative-ai-models-on-copyrighted-works-is-fair-use/

Krishna K, Tomar GS, Parikh AP, et al. (2019) Thieves on Sesame Street! Model Extraction of BERT-based APIs. https://doi.org/10.48550/arXiv.1910.12366

Krishnan S (2017) Personality and espoused cultural differences in technostress creators. *Computers in Human Behavior* 66: 154–167.

Kwon D (2024) Publishers are selling papers to train AIs—and making millions of dollars. *Nature* 636(8043): 529–530.

La Torre G, Esposito A, Sciarra I, et al. (2019) Definition, symptoms and risk of techno-stress: A systematic review. *International Archives of Occupational and Environmental Health* 92: 13–35.

Lee GW, Shao B and Vinze A (2018) The role of ICT as a double-edged sword in fostering societal transformations. *Journal of the Association for Information Systems* 19(3): 1.

Lenharo M (2024) ChatGPT turns two: How the AI chatbot has changed scientists' lives. *Nature* 636(8042): 281–282.

Lin Y, Ruan M, Cai K, et al. (2023) Identifying and managing risks of AI-driven operations: A case study of automatic speech recognition for improving air traffic safety. *Chinese Journal of Aeronautics* 36(4): 366–386.

Lindén M, Salo I and Jansson A (2018) Organizational stressors and burnout in public librarians. *Journal of Librarianship and Information Science* 50(2): 199–204.

Liu-Thompkins Y, Okazaki S and Li H (2022) Artificial empathy in marketing interactions: Bridging the human-AI gap in affective and social customer experience. *Journal of the Academy of Marketing Science* 50(6): 1198–1218.

Lund BD and Wang T (2023) Chatting about ChatGPT: How may AI and GPT impact academia and libraries? *Library Hi Tech News* 40(3): 26–29.

Maity S (2019) Identifying opportunities for artificial intelligence in the evolution of training and development practices. *Journal of Management Development* 38(8): 651–663.

Mirbabaie M, Brünker F, Möllmann Frick NRJ, et al. (2022) The rise of artificial intelligence – understanding the AI identity threat at the workplace. *Electronic Markets* 32(1): 73–99.

Morales M, Knowles EC and Bourg C (2014) Diversity, social justice, and the future of libraries. *portal: Libraries and the Academy* 14(3): 439–451.

Nguyen A, Ngo HN, Hong Y, et al. (2023) Ethical principles for artificial intelligence in education. *Education and Information Technologies* 28(4): 4221–4241.

Nitecki DA (1996) Changing the concept and measure of service quality in academic libraries. *The Journal of Academic Librarianship* 22(3): 181–190.

Panda S and Kaur N (2023) Exploring the viability of ChatGPT as an alternative to traditional chatbot systems in library and information centers. *Library Hi Tech News* 40(3): 22–25.

Riedl R (2012) On the biology of technostress: Literature review and research agenda. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 44(1): 18–55.

R-Moreno MD, Castaño B, Barrero DF, et al. (2014) Efficient services management in libraries using AI and wireless techniques. *Expert Systems with Applications* 41(17): 7904–7913.

Roshanaei M (2024) Towards best practices for mitigating artificial intelligence implicit bias in shaping diversity, inclusion and equity in higher education. *Education and Information Technologies* 29(14): 18959–18984.

Salanova M, Llorens S and Ventura M (2014) Technostress: The dark side of technologies. In: Korunka C and Hoonakker P (eds) *The Impact of ICT on Quality of Working Life*. Dordrecht: Springer Netherlands, pp.87–103.

Samberg R (2023) UC Berkeley Library to Copyright Office: Protect fair uses in AI training for research and education. Available at: https://update.lib.berkeley.edu/2023/10/24/uc-berkeley-library-to-copyright-office-protect-fair-uses-in-ai-training-for-research-and-education/

Sami LK and Pangannaiah NB (2006) "Technostress" A literature survey on the effect of information technology on library users. *Library Review* 55(7): 429–439.

Santoni de Sio F and Mecacci G (2021) Four responsibility gaps with artificial intelligence: Why they matter and how to address them. *Philosophy & Technology* 34(4): 1057–1084.

Sasidharan S (2022) Technostress in the workplace: A social network perspective. *Information Technology & People* 35(4): 1219–1238.

Self RJ and Aquilina C (2013) Technostress in the 21st century; does it still exist and how does it affect knowledge management and other information systems initiatives. In: 7th International Conference on Knowledge Management in Organizations: Service and Cloud Computing, pp.117–127. Berlin Heidelberg: Springer.

Shen Y (2019) Create synergies and inspire collaborations around the development of intelligent infrastructure for human-centered communities. *Journal of the Association for Information Science and Technology* 70(6): 596–606.

Shieh JI, Wu HH and Huang KK (2010) A DEMATEL method in identifying key success factors of hospital service quality. *Knowledge-Based Systems* 23(3): 277–282.

Tait E and Pierson CM (2022) Artificial intelligence and robots in libraries: Opportunities in LIS curriculum for preparing the librarians of tomorrow. *Journal of the Australian Library and Information Association* 71(3): 256–274.

Tarafdar M, Pullins EB and Ragu-Nathan TS (2015) Technostress: Negative effect on performance and possible mitigations. *Information Systems Journal* 25(2): 103–132.

Tarafdar M, Tu Q, Ragu-Nathan BS, et al. (2007) The impact of technostress on role stress and productivity. *Journal of Management Information Systems* 24(1): 301–328.

Tarafdar M, Tu Q and Ragu-Nathan TS (2010) Impact of technostress on end-user satisfaction and performance. *Journal of Management Information Systems* 27(3): 303–334.

Teddy-Ang S and Toh A (2020) AI Singapore: Empowering a smart nation. *Communications of the ACM* 63(4): 60–63.

Tian Z, Cui L, Liang J, et al. (2022) A comprehensive survey on poisoning attacks and countermeasures in machine learning. *ACM Computing Surveys* 55(8): 1–35.

Tiwari V (2021) Countering effects of technostress on productivity: Moderating role of proactive personality. *Benchmarking: An International Journal* 28(2): 636–651.

Tobin J (2023) Artificial intelligence: Development, risks and regulation. Available at: https://lordslibrary.parliament.uk/artificial-intelligence-development-risks-and-regulation/

Tzeng GH, Chiang CH and Li CW (2007) Evaluating intertwined effects in e-learning programs: A novel hybrid MCDM model based on factor analysis and DEMATEL. *Expert Systems with Applications* 32(4): 1028–1044.

Upadhyaya P and Vrinda A (2021) Impact of technostress on academic productivity of university students. *Education and Information Technologies* 26: 1647–1664.

Van Eck NJ and Waltman L (2017) Citation-based clustering of publications using CitNetExplorer and VOSviewer. *Scientometrics* 111: 1053–1070.

Wang MH (2020) The development dilemma and countermeasure of intelligent library. *Journal of Academic Library and Information Science* 38(2): 35–39.

Weil MM and Rosen LD (1997) *Technostress: Coping with Technology@ Work@ Home@ Play*, Vol. 13. New York: J. Wiley, p.240.

Wheatley A and Hervieux S (2024) Comparing generative artificial intelligence tools to voice assistants using reference interactions. *The Journal of Academic Librarianship* 50(5): 102942.

Wu D and Liu J (2022) Analysis and competency framework construction. *Journal of Library Science in China* 48(6): 43–56.

Wu D, Hu XK and Yang XM (2024) Research on smart feature recognition of information services in smart libraries in China. *Library Development* 326(2): 9–20.

Wu D and Liu J (2022) Algorithmic Literacy in the Era of Artificial Intelligence: Connotation.

Wu G and Huang X (2021) Study on the design of fair use rules for text and data mining in the age of artificial intelligence. *Library and Information Service* 65(22): 3–13.

Wu WW and Lee YT (2007) Developing global managers' competencies using the fuzzy DEMATEL method. *Expert Systems with Applications* 32(2): 499–507.

Xu F (2024) Application scenarios and legal issues of generative artificial intelligence in smart libraries. *Information and Documentation Services* 45(2): 24–29.

Yamson G (2023) Immediacy as a better service: Analysis of limitations of the use of ChatGPT in library services. *Information Development*. Advance online publication. https://doi.org/10.1177/02666669231206762

Yan YC (2022) Research on the infringement risk and countermeasures in the text data mining of smart libraries in China. *Journal of the National Library of China* 31(1): 106–113.

Yang JW (2021) Research on key influencing factors of ethical risks in intelligent governance: Based on DEMATEL method. *Science and Society* 11(4): 80–97.

Yoon J, Andrews JE and Ward HL (2022) Perceptions on adopting artificial intelligence and related technologies in libraries: Public and academic librarians in North America. *Library Hi Tech* 40(6): 1893–1915.

Yu S and Carroll F (2021) Implications of AI in national security: Understanding the security issues and ethical challenges. In: Montasari R and Jahankhani H (eds) *Artificial Intelligence in Cyber Security: Impact and Implications: Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges*. Switzerland: Springer International Publishing, pp.157–175. https://doi.org/10.1007/978-3-030-88040-8_6

Yucesan M, Gul M and Celik E (2021) A holistic FMEA approach by fuzzy-based Bayesian network and best–worst method. *Complex & Intelligent Systems* 7: 1547–1564.

About the authors

Xu Wang received his PhD in information science from School of Information Management of Wuhan University in 2020. He was a postdoctoral researcher at the Institute of Scientific and Technical Information of China. He is now working at the School of Economics and Management of Yanshan University. His research interests include library service, informetrics and science evaluation, information resource management. He has published more than 80 academic papers and 3 academic books.

Fang Xie is currently studying at Yanshan University and is pursuing the master's degree. He enjoys researching informetrics and information resource management.

Guanghui Cheng is currently studying at Southeast University and is pursuing the doctorate's degree. He enjoys researching user behavior and data governance.

Kiran Shehzadi is currently studying at Yanshan University and is pursuing the master's degree. She enjoys researching user intelligent service and data governance.