International Journal of Multidisciplinary Research Updates

Journal homepage: https://orionjournals.com/ijmru/

ISSN: 2783-0179 (Online)

(REVIEW ARTICLE)

Check for updates

Advancing ethical AI practices to solve data privacy issues in library systems

Ugochukwu Francis Ikwuanusi [1, *], Peter Adeyemo Adepoju [2] and Chinekwu Somtochukwu Odionu [1]

[1] *Texas A and M University -Commerce, Texas, USA.*
[2] *Independent Researcher, United Kingdom.*

International Journal of Multidisciplinary Research Updates, 2023, 06(01), 033-044

Publication history: Received on 08 July 2023; revised on 20 September 2023; accepted on 24 September 2023

Article DOI: https://doi.org/10.53430/ijmru.2023.6.1.0063

Abstract

As libraries increasingly integrate Artificial Intelligence (AI) to enhance operations and user experiences, data privacy has emerged as a critical concern. Libraries collect vast amounts of user data, including borrowing histories, digital interactions, and demographic information, making them susceptible to privacy risks such as unauthorized access, data breaches, and algorithmic profiling. This study investigates the role of ethical AI practices in addressing these data privacy issues, ensuring trust, transparency, and compliance with global privacy standards. Ethical AI emphasizes principles such as user consent, data ownership, and the minimization of bias, which are essential for safeguarding privacy in library systems. Privacy-preserving AI techniques, including differential privacy and federated learning, offer robust solutions by anonymizing data and enabling decentralized processing. Additionally, encryption, secure storage methods, and real-time monitoring systems enhance data security while mitigating risks of unauthorized access. This highlights the importance of explainable AI (XAI) in fostering user trust by ensuring transparency in how AI systems process and utilize data. Ethical frameworks tailored for libraries emphasize stakeholder involvement, accountability, and adherence to global privacy regulations such as the GDPR and CCPA. Case studies of libraries implementing ethical AI demonstrate the feasibility and benefits of these practices, including improved user confidence and compliance with legal standards. However, challenges such as balancing personalization with privacy, addressing resource constraints, and overcoming resistance to change are explored. Recommendations include fostering global collaborations, advancing open-source ethical AI tools, and conducting regular audits to uphold privacy standards. By advancing ethical AI practices, libraries can build secure, user-centric ecosystems that protect data privacy while leveraging AI's transformative potential. This research underscores the necessity of proactive measures to ensure libraries remain trusted guardians of information in the digital age.

Keywords: Ethical AI; Practices Data privacy issues; Library systems; Artificial Intelligence

1. Introduction

Modern library systems have undergone a profound transformation, transitioning from traditional review-based repositories to digital hubs of knowledge (Ansovini *et al*., 2022). These changes, driven by technological advancements, bring immense opportunities for efficiency and innovation but also introduce complex challenges. Among the most pressing of these challenges is the protection of data privacy in an era increasingly dominated by artificial intelligence (AI) (Bello *et al*., 2023). Libraries, as custodians of sensitive user data, must navigate the intersection of technological progress and ethical responsibilities.

Data privacy is a cornerstone of trust between libraries and their users. Modern library systems collect and manage vast amounts of personal information, ranging from borrowing histories and reading preferences to academic credentials and search behaviors (Lippincott *et al*., 2021). While this data enables libraries to deliver personalized services and improve operational efficiency, it also makes them vulnerable to data breaches and misuse. Inadequate data protection

* Corresponding author: Ugochukwu Francis Ikwuanusi

can compromise user trust, exposing individuals to risks such as identity theft and unauthorized surveillance (Ogonji *et al*., 2020). Moreover, libraries often serve as public institutions that champion intellectual freedom and privacy. The American Library Association (ALA), for instance, underscores privacy as a fundamental right necessary for free inquiry. When libraries fail to protect data privacy, they risk undermining this principle. Hence, implementing robust data governance frameworks and privacy-preserving technologies is essential to safeguard user confidentiality and uphold the ethical standards libraries are meant to embody (Mandinach and Gummer, 2021; Bello *et al*., 2023).

Artificial intelligence has revolutionized library operations, introducing tools that enhance efficiency and enrich user experiences (Panda and Chakravarty, 2022). AI-powered systems enable advanced cataloging, resource recommendations, predictive analytics, and seamless user interactions through virtual assistants. For example, machine learning algorithms can analyze borrowing patterns to predict demand for specific resources, ensuring optimal inventory management. Similarly, AI-driven chatbots can provide real-time assistance, improving accessibility for users with diverse needs (Singh, 2022). AI also plays a pivotal role in managing the ever-growing volumes of data that libraries handle. Through natural language processing (NLP), AI can automate the organization and indexing of digital collections, making vast repositories more accessible. Tools like optical character recognition (OCR) facilitate the digitization of physical texts, preserving valuable historical documents while making them searchable online (Liu, 2020). However, the adoption of AI in library systems is not without risks. These technologies often require the collection and analysis of personal data, raising significant privacy concerns. The challenge lies in balancing the benefits of AI with the imperative to protect user information, highlighting the importance of ethical AI practices.

The deployment of AI in libraries must align with ethical principles that prioritize user privacy and data security (Ryan and Stahl, 2020). Ethical AI practices involve transparency, accountability, and the minimization of data collection to what is strictly necessary. For instance, libraries should employ techniques such as anonymization and encryption to protect sensitive information. Additionally, AI systems must be designed to avoid biases that could inadvertently marginalize certain user groups. Regulations like the General Data Protection Regulation (GDPR) provide a legal framework for ensuring data privacy, but ethical considerations often go beyond compliance (Manda, 2022). Libraries must actively engage stakeholders, including users, policymakers, and technology providers, in discussions about the ethical use of AI. Implementing user-centric policies, conducting regular audits, and fostering a culture of digital literacy are crucial steps in mitigating the risks associated with AI-driven data management. Moreover, libraries should advocate for the development of AI systems that prioritize privacy by design. This involves integrating privacy safeguards into the architecture of AI tools from the outset, rather than treating them as an afterthought. By adopting such proactive measures, libraries can harness the potential of AI while respecting their users' rights and expectations.

In the digital age, libraries stand at the confluence of innovation and ethical responsibility. The importance of data privacy in modern library systems cannot be overstated, as it underpins user trust and the core values of intellectual freedom (Lor *et al*., 2021). While AI offers transformative possibilities for enhancing library operations and data management, its adoption necessitates a commitment to ethical practices that address privacy concerns. By embracing a balanced approach, libraries can ensure that technological advancements serve their mission without compromising the privacy and dignity of their users.

2. Overview of Data Privacy Issues in Library Systems

The digital transformation of library systems has revolutionized the management and accessibility of information (Deja *et al*., 2021). However, it has also introduced significant data privacy challenges. Libraries now collect, store, and process extensive user data to enhance services and streamline operations, but these practices raise concerns about the protection and ethical use of such information. As libraries increasingly adopt artificial intelligence (AI) technologies, understanding the scope of data privacy issues is crucial to mitigating associated risks.

Modern library systems collect and manage various types of user data, much of which is highly sensitive and personally identifiable. This data is instrumental in improving service delivery but also makes libraries a target for potential privacy violations. Libraries record borrowing histories and usage patterns to provide personalized recommendations and track resource demand (Hou, 2022). These records reveal not only the materials a user interacts with but also their intellectual and recreational interests. Over time, such data can create a detailed profile of an individual's preferences, posing risks if accessed by unauthorized entities. Interactions with digital resources, including e-books, online databases, and multimedia content, are another source of user data. Libraries often track login times, search queries, and reading habits to enhance resource management and user experience. While these data points are valuable for analytics, they expose users to potential breaches of their privacy, particularly when interactions involve sensitive or confidential subjects. Libraries routinely collect personal information such as names, addresses, email contacts, and

demographic data during user registration (Acquisti *et al*., 2020). This information is critical for managing memberships and facilitating communication, but it also increases the risk of identity theft or misuse if not adequately protected.

The integration of AI technologies in library systems offers numerous benefits, including automation and enhanced resource recommendations. However, it also amplifies privacy risks due to the scale and sensitivity of data processed by AI systems. The centralized storage of user data, coupled with AI-driven analytics, creates a significant risk of unauthorized access (Firouzi *et al*., 2020). Cyberattacks targeting library systems can lead to data breaches that expose personal information, borrowing histories, and digital interactions. The consequences of such breaches can be severe, ranging from identity theft to reputational damage for the affected library. AI technologies rely on large datasets for training and optimization, which may inadvertently include sensitive user information. Without strict governance policies, this data could be misused by third-party vendors, exploited for commercial purposes, or shared without users' consent. Libraries face ethical dilemmas in balancing the use of AI for improved services with the obligation to safeguard user privacy. AI systems in libraries often utilize algorithms to analyze user behavior and provide personalized services. However, these algorithms can lead to profiling, where users are categorized based on their borrowing habits, demographic data, or search patterns. Such profiling may unintentionally reinforce biases or expose individuals to targeted surveillance. For instance, users researching sensitive topics could find their privacy compromised if algorithms flag or store their activities.

To tackle these data privacy issues, libraries must implement robust data protection strategies and ethical AI practices (Timan and Mann, 2021). This includes adopting encryption, anonymization, and access control measures to prevent unauthorized data access. Libraries should also establish clear policies for data collection and usage, ensuring transparency and user consent. Regular audits of AI systems are essential to identify and mitigate risks associated with algorithmic profiling and bias. Furthermore, libraries must collaborate with policymakers, technology providers, and stakeholders to develop regulations and guidelines for ethical AI usage. Educating library staff and users about privacy risks and responsible technology use is equally important in fostering a culture of data protection. The evolution of library systems into digital and AI-driven ecosystems has introduced significant data privacy challenges. By understanding the nature of user data collected and the risks associated with AI technologies, libraries can take proactive steps to protect user information and uphold ethical standards (Zhang *et al*., 2021). Addressing these privacy issues is not only a legal and ethical imperative but also vital for maintaining the trust and confidence of library users in the digital age.

2.1 Principles of Ethical AI in Libraries

The integration of artificial intelligence (AI) in library systems has transformed the way information is organized, accessed, and managed. However, this technological shift brings ethical challenges, particularly concerning data privacy, fairness, and accountability. Ethical AI principles are essential for ensuring that libraries leverage AI responsibly while safeguarding user rights and maintaining trust (Israel *et al*., 2020). Key principles include transparency, user consent, bias minimization, and alignment with global data privacy regulations.

Transparency in AI systems is fundamental to fostering trust and understanding among library users. Libraries must ensure that the operation of AI tools, including their decision-making processes, is clearly communicated to stakeholders. For example, when AI recommends resources or filters search results, users should be informed about the factors influencing these outcomes. Providing explanatory interfaces or plain-language documentation can help users understand the underlying logic and implications of AI-driven decisions. Accountability complements transparency by ensuring that libraries take responsibility for the ethical use of AI. This involves assigning clear oversight roles for monitoring AI systems, addressing errors, and responding to potential harm caused by AI outputs. Ethical AI governance frameworks should include regular audits to evaluate the system’s performance, accuracy, and compliance with established principles (Raji *et al*., 2020). Libraries must also be prepared to address grievances from users who feel adversely impacted by AI-driven processes.

User consent and data ownership are at the core of ethical AI practices. Libraries must adopt a user-centric approach, ensuring that individuals understand how their data is collected, stored, and used in AI systems. Consent mechanisms should be explicit, informed, and revocable, giving users full control over their data. For instance, libraries can implement opt-in policies for data collection and allow users to withdraw their consent at any time without repercussions. Data ownership emphasizes the right of users to access, modify, and delete their personal information. Libraries should facilitate these rights by creating transparent data management systems where users can view and manage their data. Ethical AI also requires libraries to prioritize the principle of data minimization, collecting only the information necessary for specific functions, thus reducing privacy risks (Saura *et al*., 2022).

Bias in AI systems can lead to unfair outcomes and erode the equity of library services. Since algorithms rely on datasets for training, any biases in the data are likely to propagate into the AI's decision-making processes. For example, if a library's data disproportionately represents certain demographic groups, AI recommendations or services may favor those groups while marginalizing others. To minimize bias, libraries must critically evaluate and diversify their data sources. Techniques such as balanced sampling and fairness-aware machine learning algorithms can help mitigate systemic inequities. Additionally, involving diverse stakeholders in the design and evaluation of AI systems can bring multiple perspectives to identifying and addressing bias. Regular bias audits and iterative refinement of AI models are crucial steps in creating fair and inclusive library services (Akter *et al*., 2021).

Global data privacy regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), provide a legal framework for ethical data handling. Libraries adopting AI systems must ensure compliance with these regulations to protect user rights and avoid legal consequences. GDPR emphasizes user consent, the right to be forgotten, and data portability, all of which align with ethical AI principles (Marelli *et al*., 2020). For example, libraries must allow users to request the deletion of their data and ensure that AI systems respect such requests. CCPA requires transparency in data collection and grants users the ability to opt out of the sale of their information, principles that libraries can adopt to enhance ethical standards. Adhering to these regulations not only protects user privacy but also reinforces institutional credibility. Libraries should develop clear privacy policies, conduct regular compliance audits, and provide training to staff on regulatory requirements and ethical AI practices. Ethical AI principles serve as a foundation for integrating artificial intelligence into library systems responsibly. Transparency and accountability ensure that AI processes are understandable and trustworthy, while user consent and data ownership empower individuals to control their information. Minimizing bias in data and algorithms promotes equity, and aligning AI practices with global privacy regulations ensures compliance and user protection. By adhering to these principles, libraries can balance innovation with ethical responsibility, maintaining their role as trusted custodians of knowledge in the digital age.

2.2 AI Solutions to Address Data Privacy Challenges

The adoption of artificial intelligence (AI) in library systems and other sectors has brought significant improvements in efficiency and user experience (Yoon *et al*., 2022). However, these advancements come with challenges in ensuring the privacy and security of user data. To address these issues, libraries and organizations can adopt AI-driven solutions that prioritize privacy-preserving techniques, secure data handling, and transparent operations.

Differential privacy is a statistical technique that adds noise to data, ensuring that individual user information cannot be inferred while maintaining the utility of the dataset. Libraries can apply differential privacy to anonymize borrowing histories, search patterns, and demographic details. For example, AI models trained on such data can generate recommendations without exposing sensitive user information. This approach safeguards privacy even when data is shared for research or collaborative purposes. Differential privacy is particularly effective in protecting against re-identification attacks, where adversaries attempt to match anonymized data with external datasets. Federated learning is a decentralized AI training approach where user data remains on local devices rather than being uploaded to a central server. The AI model is trained across multiple devices, and only the aggregated updates are shared, ensuring that raw user data never leaves its source (Nguyen *et al*., 2020). This method is ideal for libraries handling sensitive information, as it minimizes the risk of data breaches and unauthorized access. Federated learning also reduces reliance on large-scale data storage, which is often a target for cyberattacks.

Secure data storage is a cornerstone of privacy-preserving AI. Libraries can adopt advanced encryption techniques, such as end-to-end encryption, to protect user data at rest and in transit. AI systems can automate encryption processes, ensuring that sensitive information is always stored in an unreadable format unless accessed by authorized personnel with decryption keys. In addition to encryption, libraries should utilize secure cloud services and implement access control mechanisms to limit data visibility. Role-based access systems can restrict data access to authorized individuals, while AI-driven monitoring tools can identify unusual access patterns indicative of potential security breaches (Miryala and Gupta, 2022).

AI can play a pivotal role in real-time monitoring and detection of unauthorized access to sensitive data. Machine learning algorithms can analyze system logs and user behavior to identify anomalies, such as unusual login locations or excessive data requests. When suspicious activity is detected, AI systems can automatically trigger alerts, temporarily lock accounts, or even isolate affected servers to prevent data breaches. Such proactive measures are essential in library systems, where unauthorized access can expose sensitive user data. Real-time monitoring also supports incident response efforts, enabling library administrators to act swiftly in mitigating potential damage (Wolf *et al*., 2022).

Explainable AI (XAI) enhances transparency by providing users and administrators with clear insights into how AI systems make decisions. In the context of data privacy, XAI can explain how user data is processed, stored, and utilized, addressing concerns about opaque AI operations. For example, if an AI system recommends a particular book or resource, XAI tools can detail the factors influencing the recommendation, such as borrowing history or search keywords. This transparency fosters user trust by ensuring that data-driven decisions are unbiased and aligned with user expectations. Moreover, XAI allows administrators to audit AI systems, ensuring compliance with ethical and regulatory standards. AI solutions offer powerful tools for addressing data privacy challenges in modern library systems. Privacy-preserving techniques like differential privacy and federated learning minimize risks associated with data centralization and re-identification (Li *et al*., 2021). Secure data storage and encryption practices provide robust protection against breaches, while real-time monitoring ensures swift detection and response to unauthorized access. Additionally, explainable AI fosters user trust and promotes transparency in AI-driven processes. By integrating these solutions, libraries can strike a balance between leveraging AI's capabilities and safeguarding user privacy, maintaining their role as trusted custodians of knowledge in the digital era.

2.3 Ethical Frameworks for AI Deployment in Library Systems

The deployment of artificial intelligence (AI) in library systems has revolutionized the organization, retrieval, and recommendation of information. However, the ethical implications of AI in libraries such as data privacy, bias, and transparency necessitate robust ethical frameworks to ensure responsible use. A well-structured framework can guide AI implementation to align with the values of fairness, accountability, and inclusivity while maintaining user trust (Barclay *et al*., 2021). Key components of such a framework include responsible guidelines, stakeholder collaboration, open-source innovation, and regular audits.

Guidelines for responsible AI use in library systems provide a foundational structure to address ethical concerns. These guidelines should outline acceptable practices, emphasizing user privacy, transparency, and equitable access to library resources. For instance, they can define protocols for data collection, ensuring that only necessary and anonymized data is gathered. Responsible AI guidelines should also address the fairness and inclusivity of AI algorithms, ensuring that services do not inadvertently marginalize specific user groups (Schwartz *et al*., 2022). For example, AI-driven recommendation systems must avoid reinforcing biases that could lead to unequal access to resources. Clear policies on accountability, such as assigning roles for monitoring AI outputs and addressing user grievances, are essential for maintaining ethical standards.

The development and implementation of AI in library systems must involve diverse stakeholders, including librarians, users, and policymakers. Librarians, as custodians of information, provide valuable insights into operational requirements and user needs. Their expertise ensures that AI tools align with the mission of libraries to provide equitable access to information (Nitecki and Alter, 2021). Users, as the primary beneficiaries, should have a voice in decision-making processes, particularly regarding how their data is collected and used. Surveys, focus groups, and advisory committees can facilitate meaningful user engagement. Involving policymakers ensures that AI systems comply with legal and ethical standards, such as data protection regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Stakeholder involvement not only fosters trust but also creates a sense of collective ownership over AI systems, promoting transparency and accountability in their deployment.

Open-source, community-driven AI tools play a vital role in democratizing AI technology in library systems. These tools enable libraries to adapt and customize AI solutions according to their unique needs while ensuring transparency (Bello *et al*., 2023). Unlike proprietary software, open-source tools allow stakeholders to review and modify the underlying code, reducing the risk of hidden biases or unethical practices. Community-driven development also promotes collaboration between libraries, academic institutions, and technology developers, fostering innovation and knowledge sharing. By pooling resources and expertise, libraries can create AI tools that reflect shared ethical values and address common challenges. For example, open-source tools for cataloging, resource recommendation, or data privacy management can be tailored to the needs of different library systems while adhering to ethical principles.

Ethical frameworks for AI in libraries must include mechanisms for regular audits to evaluate compliance with established standards (Shneiderman, 2020). These audits should assess various aspects of AI deployment, such as data handling practices, algorithmic fairness, and system transparency. By identifying potential issues early, audits help prevent harm and maintain user trust. Audits should be conducted by independent experts to ensure impartiality. They can include technical evaluations of AI models to detect biases, as well as reviews of data privacy policies to ensure adherence to regulations. Periodic user feedback and surveys can complement technical audits, providing insights into how AI tools impact library users and whether they align with ethical objectives. Libraries can further enhance audit processes by publishing audit results and creating action plans to address identified issues. Such transparency

reinforces accountability and demonstrates a commitment to ethical AI use. Ethical frameworks are indispensable for guiding the deployment of AI in library systems. By establishing guidelines for responsible AI use, involving diverse stakeholders in decision-making, and developing open-source tools, libraries can ensure that AI aligns with their mission of equitable and inclusive access to information (McLarney *et al*., 2021). Regular audits provide a mechanism for ongoing oversight, enabling libraries to address challenges proactively and maintain compliance with ethical standards. Through these measures, libraries can leverage AI's potential while safeguarding the trust and rights of their users.

2.4 Case Studies and Practical Implementations

The integration of ethical AI practices in library systems has become a critical focus as libraries strive to balance technological advancements with user privacy and trust. Examining case studies and collaborative efforts reveals how libraries worldwide are adopting ethical AI, the lessons learned from these implementations, and the broader impact on data privacy. These examples provide practical insights into effective strategies and challenges in aligning AI technologies with ethical principles.

The National Library of Sweden has implemented AI for analyzing large volumes of historical texts, enabling improved digitization and resource accessibility. Ethical considerations are embedded into the project by employing differential privacy techniques to anonymize user interactions and prevent re-identification of individuals who access sensitive or rare documents (Hanisch *et al*., 2021). This approach demonstrates how ethical AI practices can coexist with ambitious technological goals. The NYPL leverages AI to enhance user experiences through personalized book recommendations. To address privacy concerns, the library uses federated learning to train recommendation algorithms on decentralized data. User data remains local to the device, significantly reducing privacy risks. This practical application highlights how privacy-preserving AI methods can be integrated into routine library functions. Several libraries across the European Union have adopted AI systems aligned with GDPR guidelines. These systems ensure data transparency and user consent, emphasizing accountability in how user data is collected and used. For instance, libraries notify users about data collection practices and offer options to opt out of AI-driven services, setting an example for user-centric AI deployments.

Case studies emphasize the significance of transparency in building user trust. Libraries that openly communicate their use of AI, the purpose behind it, and the safeguards in place have reported higher user acceptance. Clear data policies, combined with explainable AI (XAI) tools, help demystify AI processes for users and stakeholders (Langer *et al*., 2021). Libraries implementing ethical AI practices have encountered challenges such as algorithmic bias and data security vulnerabilities. The adoption of regular audits and independent assessments has proven effective in identifying and mitigating these risks. For example, in the NYPL case, iterative testing and updates to AI models helped eliminate biases in book recommendations. Collaborative efforts between libraries, policymakers, and technology developers have significantly advanced ethical AI implementations. Partnerships foster resource sharing and ensure adherence to global data privacy standards, minimizing implementation errors and costs.

The International Federation of Library Associations and Institutions (IFLA) has spearheaded initiatives to develop ethical AI guidelines tailored for library systems. By fostering dialogue among global stakeholders, IFLA's framework addresses core concerns such as data ownership, algorithmic fairness, and inclusivity. Libraries worldwide have adopted these guidelines to align their AI systems with ethical best practices (Murphy *et al*., 2021). This collaborative initiative focuses on creating open-source AI tools designed specifically for library needs. Supported by universities and library consortia, the project promotes transparency and community-driven development. Its tools are not only customizable but also compliant with regulations like GDPR and CCPA, ensuring widespread applicability. Several libraries have partnered with AI Ethics Labs to standardize practices in AI deployment. These collaborations involve joint research, training sessions for library staff, and development of ethical auditing tools. For instance, such partnerships have led to the creation of fairness metrics for assessing bias in AI-driven cataloging systems.

Case studies and collaborative initiatives provide valuable insights into the practical implementation of ethical AI in library systems. Examples from Sweden, New York, and the European Union showcase diverse approaches to embedding ethical considerations into AI processes. These implementations highlight lessons such as the need for transparency, proactive risk management, and the benefits of collaboration. By learning from these examples and engaging in standardization efforts through organizations like IFLA and OpenAI for Libraries, libraries can effectively integrate AI while upholding the highest ethical standards. The collective commitment to ethical AI ensures that libraries continue to serve as trusted custodians of knowledge in the digital age.

2.5 Challenges and Limitations

The deployment of artificial intelligence (AI) in library systems presents numerous opportunities to enhance user experience, streamline operations, and increase access to resources. However, integrating AI in a way that is ethical, transparent, and respects user privacy introduces a set of complex challenges (Bello *et al*., 2022). These challenges span issues of balancing privacy with personalization, addressing resource constraints, and overcoming resistance to change among stakeholders. Understanding and addressing these challenges are critical for ensuring the responsible and effective use of AI in library systems.

One of the fundamental challenges in implementing AI in library systems is finding a balance between maintaining user privacy and offering personalized services. AI-driven tools, such as recommendation systems, often rely on user data such as borrowing history, search queries, and engagement patterns to deliver tailored experiences. However, the collection and analysis of such data can raise concerns about privacy and data security. Users are increasingly aware of the risks associated with data collection, including the potential for misuse and breaches. Library systems must navigate the tension between offering personalized services and ensuring that personal information is adequately protected (Bello *et al*., 2023). Implementing privacy-preserving AI techniques, such as differential privacy, federated learning, and data anonymization, can help mitigate some of these risks. However, the challenge lies in striking the right balance between providing personalized experiences while not infringing on users' privacy rights. Moreover, adhering to global data privacy regulations, such as the General Data Protection Regulation (GDPR) in Europe, adds another layer of complexity, as libraries must ensure compliance without compromising the effectiveness of their AI tools.

Implementing AI safeguards, such as ethical auditing, secure data storage, and real-time monitoring, requires significant resources in terms of time, personnel, and technology (Paul and Joshua, 2020). Many libraries, particularly those in smaller or underfunded institutions, face resource constraints that hinder their ability to fully implement these safeguards (Agupugo and Tochukwu, 2021). The costs associated with developing and maintaining AI systems that adhere to privacy and ethical standards can be prohibitive, especially for libraries operating with limited budgets. Smaller libraries may not have the infrastructure or technical expertise to deploy privacy-preserving AI tools, conduct regular audits, or establish secure data storage practices. Additionally, the integration of AI requires ongoing maintenance, training, and updates to ensure that systems remain aligned with ethical standards and privacy regulations. This resource gap is particularly concerning as AI adoption continues to grow in libraries, potentially creating disparities between well-funded and under-resourced institutions in terms of AI capabilities and ethical compliance. Addressing these constraints requires collaborative initiatives, such as shared resources or partnerships with technology providers, that allow libraries to pool resources and expertise. Open-source AI tools and community-driven projects also present opportunities for libraries to implement AI systems that align with ethical standards without incurring significant costs (Ikwuanusi, 2023).

The integration of AI in library systems often encounters resistance from various stakeholders, including librarians, users, and administrators. Librarians, while enthusiastic about the potential benefits of AI, may be hesitant to adopt new technologies due to concerns about job displacement, technical difficulties, or disruption to established workflows (Chi *et al*., 2020). Some may feel that AI systems, particularly those that involve automation or algorithmic decision-making, threaten the traditional human-centered approach to library services. Users may also exhibit reluctance to embrace AI-driven services, especially if they are not adequately informed about how their data will be used or if they perceive AI systems as invasive (Pizzi *et al*., 2020; Yun *et al*., 2020). Concerns about data privacy, algorithmic bias, and the transparency of AI processes can fuel skepticism about the use of AI in libraries. Overcoming this resistance requires transparent communication, robust training programs, and the active involvement of stakeholders in decision-making processes (Neely *et al*., 2021). Providing clear explanations about the benefits of AI and how ethical practices are embedded in the system can help alleviate concerns. Additionally, fostering a culture of collaboration, where stakeholders are engaged in the design and implementation of AI tools, can facilitate buy-in and reduce resistance. Libraries should also emphasize that AI is a tool to enhance, rather than replace, human expertise, ensuring that the technology supports rather than undermines the core mission of the library. While the integration of AI in library systems offers significant advantages, it is not without its challenges. Balancing user privacy with data-driven personalization, addressing resource constraints, and mitigating resistance to change are critical obstacles that need to be addressed for the successful implementation of AI (Rao and Sahani, 2022; Aouedi *et al*., 2022). By adopting privacy-preserving techniques, collaborating across institutions to share resources, and fostering transparency and stakeholder engagement, libraries can overcome these challenges and ensure that AI enhances, rather than compromises, the ethical standards of library services. Effective management of these issues will allow libraries to harness the full potential of AI while safeguarding user privacy and maintaining trust (Jimmy, 2021).

2.6 Future Directions and Opportunities

As libraries continue to adopt artificial intelligence (AI) to improve their services, the future holds significant potential for innovations that enhance privacy protection, promote ethical standards, and focus on user-centric solutions (Yigitcanlar *et al*., 2020; Cirqueira *et al*., 2020). These advancements promise to not only safeguard sensitive user data but also contribute to a more transparent, equitable, and secure environment in library systems worldwide. The future directions and opportunities for AI in libraries can be viewed through the lenses of AI innovations for privacy, global collaborations for standardizing ethical AI practices, and the expanding field of research in user-centric privacy solutions.

One of the most pressing challenges in the integration of AI in library systems is ensuring that privacy is maintained while providing personalized and efficient services (Deebak *et al*., 2022). As AI technologies evolve, so too must the methods for protecting user data. Future innovations in AI are likely to focus on privacy-preserving techniques that allow libraries to collect and analyze user data without compromising privacy (Majeed *et al*., 2022). One promising area is differential privacy, which ensures that the output of data analysis cannot be traced back to individual users. Researchers are continually improving differential privacy methods, making them more scalable and efficient. Libraries could adopt these advances to protect user anonymity while still benefiting from AI-driven insights. Another area of development is federated learning, which enables AI systems to learn from data without centralizing it. Instead of collecting all user data in one place, federated learning allows libraries to process data locally on user devices or within decentralized servers. This reduces the risk of data breaches and enhances user privacy by keeping personal data within the user's control. Moreover, the use of secure multi-party computation (SMPC) holds promise for AI applications in libraries (Chris *et al*., 2021). SMPC allows multiple parties to jointly compute data without sharing their private inputs, which could be useful for libraries working with other institutions while keeping user data protected.

As AI becomes more pervasive in libraries and other sectors, the need for global collaborations to establish standardized ethical guidelines becomes more pressing (Uzwyshyn *et al*., 2022). While many countries have implemented their own data protection laws, such as the European Union's General Data Protection Regulation (GDPR) or California's California Consumer Privacy Act (CCPA), these regulations vary widely. This presents challenges for libraries operating in multiple regions or sharing data across borders. Promoting global collaborations among libraries, technology developers, and policymakers will be critical in ensuring that AI systems meet ethical standards regardless of geographic location. Organizations like the International Federation of Library Associations and Institutions (IFLA) and other professional bodies have already begun to address this need by drafting ethical guidelines for AI implementation in libraries. However, further international cooperation is required to create universally accepted standards for data privacy, algorithmic fairness, and transparency. Global collaborations can also drive research into AI models that are robust, explainable, and less prone to biases. Developing such AI systems will require expertise and input from diverse stakeholders worldwide, as well as a shared commitment to ethical AI development.

As AI continues to shape library services, one of the key areas for future research is the development of user-centric privacy solutions that prioritize the needs and concerns of library users. Much of the current AI research focuses on building algorithms that optimize performance and efficiency. However, the evolving landscape of privacy and data protection calls for research that places the user at the center of the AI design process. Future research can explore new models for informed consent in AI systems. Users must have clear and accessible ways to understand what data is being collected, how it is being used, and what rights they have regarding their data (Andrus *et al*., 2021). Research could focus on developing tools for transparent consent management, allowing users to easily control their data preferences, modify consent in real time, and even withdraw consent without facing barriers. Another promising research area is the development of adaptive privacy settings based on user preferences and contexts. By leveraging AI's capability to understand patterns in user behavior, libraries could create dynamic privacy settings that automatically adjust to provide optimal levels of privacy protection while maintaining personalized experiences. Furthermore, research can explore how to make AI systems more explainable to users. AI-driven decisions, such as book recommendations or search results, should be transparent and easily understood by library users. Tools that provide users with explanations of how AI systems made specific recommendations or decisions could enhance trust and encourage more responsible AI usage. The future of AI in libraries is full of exciting opportunities, particularly in terms of enhancing privacy protection, promoting global ethical collaborations, and prioritizing user-centric solutions (Zidaru *et al*., 2021; Verma *et al*., 2022). Innovations like differential privacy, federated learning, and secure multi-party computation offer promising pathways for safeguarding user data. Global collaborations will help standardize ethical AI practices across borders, ensuring libraries worldwide maintain user trust and privacy. Finally, research into user-centric privacy solutions holds the potential to create AI systems that not only respect but also empower users, fostering an environment of transparency and security. As these developments unfold, libraries can continue to leverage AI in a way

that aligns with ethical principles and fosters a safe, personalized experience for all users (Auld *et al*., 2022; Pelletier *et al*., 2022).

3. Conclusion

In conclusion, ethical AI plays a crucial role in addressing data privacy issues within library systems, where the use of AI technologies must be carefully balanced with user privacy and security. The growing reliance on AI in libraries for personalized services, resource management, and data analysis highlights the need for ethical frameworks that prioritize privacy, transparency, and accountability. By implementing privacy-preserving techniques such as differential privacy and federated learning, libraries can enhance their AI systems without compromising the trust of their users.

It is essential for library systems to proactively adopt ethical AI practices, ensuring that their deployment of AI technologies aligns with privacy regulations and ethical standards. This involves incorporating guidelines that emphasize transparency, data ownership, and user consent, as well as minimizing biases in AI algorithms. Stakeholders, including librarians, users, and policymakers, must collaborate to establish clear, consistent ethical frameworks to guide AI adoption across libraries globally. This proactive approach will help mitigate privacy risks, ensure compliance with evolving regulations, and protect user rights.

Looking ahead, the vision for a secure, user-centric, and transparent library ecosystem powered by ethical AI practices is achievable. By fostering a culture of ethical AI deployment, libraries can provide more personalized, efficient, and inclusive services while safeguarding user privacy. This future will be built upon strong collaborations, innovative privacy-preserving technologies, and a shared commitment to ethical standards. Ultimately, ethical AI in libraries can create an environment where users feel confident in the security and privacy of their data while enjoying the benefits of enhanced, AI-driven library services.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Acquisti, A., Brandimarte, L. and Loewenstein, G., 2020. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, *30*(4), pp.736-758.

[2] Agupugo, C.P. and Tochukwu, M.F.C., 2021. A model to assess the economic viability of renewable energy microgrids: A case study of Imufu Nigeria.

[3] Akter, S., McCarthy, G., Sajib, S., Michael, K., Dwivedi, Y.K., D'Ambra, J. and Shen, K.N., 2021. Algorithmic bias in data-driven innovation in the age of AI. *International Journal of Information Management*, *60*, p.102387.

[4] Andrus, M., Spitzer, E., Brown, J. and Xiang, A., 2021, March. What we can't measure, we can't understand: Challenges to demographic data procurement in the pursuit of fairness. In *Proceedings of the 2021 ACM conference on fairness, accountability, and transparency* (pp. 249-260).

[5] Ansovini, D., Babcock, K., Franco, T., Jung, J.A., Suurtamm, K. and Wong, A., 2022. Knowledge Lost, Knowledge Gained: The Implications of Migrating to Online Archival Descriptive Systems. *KULA*, *6*(3), pp.1-19.

[6] Aouedi, O., Sacco, A., Piamrat, K. and Marchetto, G., 2022. Handling privacy-sensitive medical data with federated learning: challenges and future directions. *IEEE journal of biomedical and health informatics*, *27*(2), pp.790-803.

[7] Auld, G., Casovan, A., Clarke, A. and Faveri, B., 2022. Governing AI through ethical standards: Learning from the experiences of other private governance initiatives. *Journal of European Public Policy*, *29*(11), pp.1822-1844.

[8] Barclay, I., Taylor, H., Preece, A., Taylor, I., Verma, D. and de Mel, G., 2021. A framework for fostering transparency in shared artificial intelligence models by increasing visibility of contributions. *Concurrency and Computation: Practice and Experience*, *33*(19), p.e6129.

[9] Bello, O.A., Folorunso, A., Ejiofor, O.E., Budale, F.Z., Adebayo, K. and Babatunde, O.A., 2023. Machine Learning Approaches for Enhancing Fraud Prevention in Financial Transactions. *International Journal of Management Technology*, *10*(1), pp.85-108.

[10] Bello, O.A., Folorunso, A., Ogundipe, A., Kazeem, O., Budale, A., Zainab, F. and Ejiofor, O.E., 2022. Enhancing Cyber Financial Fraud Detection Using Deep Learning Techniques: A Study on Neural Networks and Anomaly Detection. *International Journal of Network and Communication Research*, *7*(1), pp.90-113.

[11] Bello, O.A., Folorunso, A., Onwuchekwa, J. and Ejiofor, O.E., 2023. A Comprehensive Framework for Strengthening USA Financial Cybersecurity: Integrating Machine Learning and AI in Fraud Detection Systems. *European Journal of Computer Science and Information Technology*, *11*(6), pp.62-83.

[12] Bello, O.A., Folorunso, A., Onwuchekwa, J., Ejiofor, O.E., Budale, F.Z. and Egwuonwu, M.N., 2023. Analysing the Impact of Advanced Analytics on Fraud Detection: A Machine Learning Perspective. *European Journal of Computer Science and Information Technology*, *11*(6), pp.103-126.

[13] Bello, O.A., Ogundipe, A., Mohammed, D., Adebola, F. and Alonge, O.A., 2023. AI-Driven Approaches for Real-Time Fraud Detection in US Financial Transactions: Challenges and Opportunities. *European Journal of Computer Science and Information Technology*, *11*(6), pp.84-102.

[14] Chi, O.H., Denton, G. and Gursoy, D., 2020. Artificially intelligent device use in service delivery: A systematic review, synthesis, and research agenda. *Journal of Hospitality Marketing & Management*, *29*(7), pp.757-786.

[15] Chris, E., John, M. and Mercy, G., 2021. Secure Multi-Party Computation (SMPC).

[16] Cirqueira, D., Nedbal, D., Helfert, M. and Bezbradica, M., 2020, August. Scenario-based requirements elicitation for user-centric explainable AI: A case in fraud detection. In *International cross-domain conference for machine learning and knowledge extraction* (pp. 321-341). Cham: Springer International Publishing.

[17] Deebak, B.D., Memon, F.H., Dev, K., Khowaja, S.A. and Qureshi, N.M.F., 2022. AI-enabled privacy-preservation phrase with multi-keyword ranked searching for sustainable edge-cloud networks in the era of industrial IoT. *Ad Hoc Networks*, *125*, p.102740.

[18] Deja, M., Rak, D. and Bell, B., 2021. Digital transformation readiness: perspectives on academia and library outcomes in information literacy. *The Journal of Academic Librarianship*, *47*(5), p.102403.

[19] Firouzi, F., Farahani, B., Barzegari, M. and Daneshmand, M., 2020. AI-driven data monetization: The other face of data in IoT-based smart and connected health. *IEEE Internet of Things Journal*, *9*(8), pp.5581-5599.

[20] Hanisch, S., Arias-Cabarcos, P., Parra-Arnau, J. and Strufe, T., 2021. Privacy-protecting techniques for behavioral data: A survey. *arXiv preprint arXiv:2109.04120*.

[21] Hou, D., 2022. [Retracted] Personalized Book Recommendation Algorithm for University Library Based on Deep Learning Models. *Journal of Sensors*, *2022*(1), p.3087623.

[22] Ikwuanusi, U.F., 2023. Real time classification of facial expressions for effective and intelligent video communication. Master's thesis, Texas A&M University-Commerce

[23] Israel, M.J., Graves, M. and Amer, A., 2020, December. On Trusting a Cyber Librarian: How Rethinking Underlying Data Storage Infrastructure Can Mitigate Risksof Automation. In *International Conference on Intelligent Technologies for Interactive Entertainment* (pp. 25-42). Cham: Springer International Publishing.

[24] Jimmy, F., 2021. Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, pp.564-574.

[25] Langer, M., Oster, D., Speith, T., Hermanns, H., Kästner, L., Schmidt, E., Sesing, A. and Baum, K., 2021. What do we want from Explainable Artificial Intelligence (XAI)?–A stakeholder perspective on XAI and a conceptual model guiding interdisciplinary XAI research. *Artificial Intelligence*, *296*, p.103473.

[26] Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., Liu, X. and He, B., 2021. A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*, *35*(4), pp.3347-3366.

[27] Lippincott, S., Kennedy, M.L., Lynch, C., Calvert, S. and Cozzo, J., 2021. Mapping the current landscape of research library engagement with emerging technologies in research and learning.

[28] Liu, Z., 2020. Optical character recognition and the smart ancient script database. *Journal of Chinese Writing Systems*, *4*(4), pp.255-269.

[29] Lor, P., Wiles, B. and Britz, J., 2021. Re-thinking information ethics: truth, conspiracy theories, and librarians in the COVID-19 era. *Libri*, *71*(1), pp.1-14.

[30] Majeed, A., Khan, S. and Hwang, S.O., 2022. A comprehensive analysis of privacy-preserving solutions developed for online social networks. *Electronics*, *11*(13), p.1931.

[31] Manda, J.K., 2022. Data Privacy and GDPR Compliance in Telecom: Ensuring Compliance with Data Privacy Regulations like GDPR in Telecom Data Handling and Customer Information Management. *MZ Computing Journal*, *3*(1).

[32] Mandinach, E.B. and Gummer, E.S. eds., 2021. *The ethical use of data in education: Promoting responsible policies and practices*. Teachers College Press.

[33] Marelli, L., Lievevrouw, E. and Van Hoyweghen, I., 2020. Fit for purpose? The GDPR and the governance of European digital health. *Policy studies*, *41*(5), pp.447-467.

[34] McLarney, E., Gawdiak, Y., Oza, N., Mattmann, C., Garcia, M., Maskey, M., Tashakkor, S., Meza, D., Sprague, J., Hestnes, P. and Wolfe, P., 2021. NASA framework for the ethical use of artificial intelligence (AI).

[35] Miryala, N.K. and Gupta, D., 2022. Data security challenges and industry trends. *IJARCCE International Journal of Advanced Research in Computer and Communication Engineering*, *11*(11), pp.300-309.

[36] Murphy, K., Di Ruggiero, E., Upshur, R., Willison, D.J., Malhotra, N., Cai, J.C., Malhotra, N., Lui, V. and Gibson, J., 2021. Artificial intelligence for good health: a scoping review of the ethics literature. *BMC medical ethics*, *22*, pp.1-17.

[37] Neely, C.L., Bourne, M., Chesterman, S., Vågen, T.G., Lekaram, V., Winowiecki, L.A. and Prabhu, R., 2021. Inclusive, cross-sectoral and evidence-based decision-making for resilience planning and decision-making in a devolved context. *The European Journal of Development Research*, *33*(4), pp.1115-1140.

[38] Nguyen, D.C., Cheng, P., Ding, M., Lopez-Perez, D., Pathirana, P.N., Li, J., Seneviratne, A., Li, Y. and Poor, H.V., 2020. Wireless AI: Enabling an AI-governed data life cycle. *arXiv preprint arXiv:2003.00866*, (00866).

[39] Nitecki, D.A. and Alter, A., 2021. Leading FAIR Adoption Across the Institution: A Collaboration Between an Academic Library and a Technology Provider. *Data Science Journal*, *20*, pp.6-6.

[40] Ogonji, M.M., Okeyo, G. and Wafula, J.M., 2020. A survey on privacy and security of Internet of Things. *Computer Science Review*, *38*, p.100312.

[41] Panda, S. and Chakravarty, R., 2022. Adapting intelligent information services in libraries: A case of smart AI chatbots. *Library Hi Tech News*, *39*(1), pp.12-15.

[42] Paul, D. and Joshua, C., 2020. Securing Data Warehouses with Cloud-Based AI: A Comprehensive Framework. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(1), pp.86-102.

[43] Pelletier, K., Mccormack, M., Reeves, J., Robert, J., Arbino, N., Dickson-Deane, C., Guevara, C., Koster, L., Sanchez-Mendiola, M., Bessette, L.S. and Stine, J., 2022. *2022 educause horizon report teaching and learning edition* (pp. 1-58). EDUC22.

[44] Pizzi, M., Romanoff, M. and Engelhardt, T., 2020. AI for humanitarian action: Human rights and ethics. *International Review of the Red Cross*, *102*(913), pp.145-180.

[45] Raji, I.D., Smart, A., White, R.N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D. and Barnes, P., 2020, January. Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 conference on fairness, accountability, and transparency* (pp. 33-44).

[46] Rao, A. and Sahani, S.K., 2022. Adoption and Diffusion of Big Data Innovations: A Cross-Industry Analysis of Enabling Factors. *International Journal of Social Analytics*, *7*(12), pp.26-38.

[47] Ryan, M. and Stahl, B.C., 2020. Artificial intelligence ethics guidelines for developers and users: clarifying their content and normative implications. *Journal of Information, Communication and Ethics in Society*, *19*(1), pp.61-86.

[48] Saura, J.R., Ribeiro-Soriano, D. and Palacios-Marqués, D., 2022. Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*, *39*(4), p.101679.

[49] Schwartz, R., Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A. and Hall, P., 2022. *Towards a standard for identifying and managing bias in artificial intelligence* (Vol. 3, p. 00). US Department of Commerce, National Institute of Standards and Technology.

[50] Shneiderman, B., 2020. Bridging the gap between ethics and practice: guidelines for reliable, safe, and trustworthy human-centered AI systems. *ACM Transactions on Interactive Intelligent Systems (TiiS)*, *10*(4), pp.1-31.

[51] Singh, P., 2022. AI-Powered IVR and Chat: A New Era in Telecom Troubleshooting. *African Journal of Artificial Intelligence and Sustainable Development*, *2*(2), pp.143-185.

[52] Timan, T. and Mann, Z., 2021. Data protection in the era of artificial intelligence: trends, existing solutions and recommendations for privacy-preserving technologies. In *The elements of big data value: Foundations of the research and innovation ecosystem* (pp. 153-175). Cham: Springer International Publishing.

[53] Uzwyshyn, R., Balnaves, E., Boffy, F.X., Chakarova, J., Kleinveldt, L., Sánchez Nogales, E., Pastrana García, A., Cerdán Medina, J.C., Lorca González, M., Malliari, A. and Nitsos, I., 2022. Trends and Issues in Library Technology, June 2022.

[54] Verma, A., Bhattacharya, P., Madhani, N., Trivedi, C., Bhushan, B., Tanwar, S., Sharma, G., Bokoro, P.N. and Sharma, R., 2022. Blockchain for industry 5.0: Vision, opportunities, key enablers, and future directions. *Ieee Access*, *10*, pp.69160-69199.

[55] Wolf, K., Dawson, R.J., Mills, J.P., Blythe, P. and Morley, J., 2022. Towards a digital twin for supporting multi-agency incident management in a smart city. *Scientific reports*, *12*(1), p.16221.

[56] Yigitcanlar, T., Desouza, K.C., Butler, L. and Roozkhosh, F., 2020. Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature. *Energies*, *13*(6), p.1473.

[57] Yoon, J., Andrews, J.E. and Ward, H.L., 2022. Perceptions on adopting artificial intelligence and related technologies in libraries: public and academic librarians in North America. *Library Hi Tech*, *40*(6), pp.1893-1915.

[58] Yun, J.T., Segijn, C.M., Pearson, S., Malthouse, E.C., Konstan, J.A. and Shankar, V., 2020. Challenges and future directions of computational advertising measurement systems. *Journal of advertising*, *49*(4), pp.446-458.

[59] Zhang, Y., Wu, M., Tian, G.Y., Zhang, G. and Lu, J., 2021. Ethics and privacy of artificial intelligence: Understandings from bibliometrics. *Knowledge-Based Systems*, *222*, p.106994.

[60] Zidaru, T., Morrow, E.M. and Stockley, R., 2021. Ensuring patient and public involvement in the transition to AI-assisted mental health care: A systematic scoping review and agenda for design justice. *Health Expectations*, *24*(4), pp.1072-1124