

**The legal framework for fourth-generation libraries: balancing personal data protection with ensuring open access to information.**

الإطار القانوني لمكتبات الجيل الرابع: بين حماية البيانات الشخصية وضمان الوصول الحر للمعلومات

**Aicha AMAIRIA <sup>1\*</sup>**

University of Ahmaed ZABANA Relizane (Algeria), Laboratory of Social, Psychological and Anthropological Studies (LESPA)

[Aicha.amairia@univ-relizane.dz](mailto:Aicha.amairia@univ-relizane.dz)

Received: 2026-03-15 Accepted: 24-04-2026 Published: 2026-05-19

**Abstract :**

This study aims to analyse the legal framework governing the operation of fourth-generation libraries, which represent a qualitative leap in the field of libraries and information by relying on Fourth Industrial Revolution technologies such as artificial intelligence, the Internet of Things, big data and analytics. The study focuses on the core issue created by this advanced digital environment: the tension between strict adherence to personal data protection laws, such as the General Data Protection Regulation (GDPR), and the established principles of open access to information that form the philosophy of library institutions in the digital age. Employing a descriptive analytical approach, the study extrapolates relevant legal texts and analyses applied policies, utilising a case study methodology to analyse smart library models. It concludes that a significant 'privacy paradox' exists, whereby library data collection practices mirror commercial ones, raising complex ethical and legal issues. It also reveals a lack of awareness among librarians and a gap in their training to handle these challenges. The study emphasises the necessity of adopting a 'Compliance and Privacy by Design' methodology as a proactive framework to achieve the desired balance. It also presents a comprehensive vision for policies and procedures that can integrate data protection into the core services of smart libraries without undermining the principle of open access.

**Keywords:** Fourth generation libraries; personal data protection; General Data Protection Regulation (GDPR); open access to information; information ethics.

ملخص:

تهدف هذه الدراسة إلى تحليل الإطار القانوني الناظم لعمل مكتبات الجيل الرابع، التي تمثل نقلة نوعية في عالم المكتبات والمعلومات من خلال اعتمادها على تقنيات الثورة الصناعية الرابعة، مثل الذكاء الاصطناعي وإنترنت الأشياء والبيانات الضخمة وتحليلات التعلم. تركز الدراسة على الإشكالية الجوهرية التي تخلقها هذه البيئة الرقمية المتقدمة، والمتمثلة في التوتر القائم بين الالتزام بقوانين حماية البيانات الشخصية الصارمة (كاللائحة العامة لحماية البيانات GDPR) من جهة، وبين المبادئ الراسخة لـ الوصول الحر للمعلومات التي تشكل الفلسفة الأساسية للمؤسسات المكتبية في العصر الرقمي من جهة أخرى. تعتمد الدراسة المنهج التحليلي الوصفي لاستقراء النصوص القانونية ذات الصلة وتحليل السياسات المطبقة، مع الاستعانة بمنهج دراسة الحالة لتحليل نماذج من المكتبات الذكية. توصلت الدراسة إلى وجود "مفارقة خصوصية" حادة، حيث تحاكي ممارسات المكتبات في جمع البيانات الممارسات التجارية، مما يؤثر إشكاليات أخلاقية وقانونية معقدة. كما كشفت عن فجوة في وعي أمناء المكتبات وتأهيلهم للتعامل مع هذه التحديات. تخلص الدراسة إلى ضرورة تبني منهجية "الامتثال والخصوصية حسب التصميم" (Compliance and Privacy by Design) كإطار استباقي لتحقيق التوازن

\* Corresponding Author.

المنشود، مع تقديم تصور متكامل للسياسات والإجراءات الكفيلة بدمج حماية البيانات في صميم خدمات المكتبات الذكية دون المساس بمبدأ الوصول الحر.  
الكلمات المفتاحية: مكتبات الجيل الرابع؛ حماية البيانات الشخصية؛ اللائحة العامة لحماية البيانات (GDPR)؛ الوصول الحر للمعلومات؛ الأخلاقيات المعلوماتية.

## **Introduction :**

The world of libraries and information is undergoing a radical transformation with the advent of fourth-generation libraries. These libraries are not just places to store books or provide electronic services; they have evolved into interactive smart ecosystems that use Fourth Industrial Revolution technologies to create personalised and effective experiences for users (Salubi, 2024.). Instead, they have evolved into interactive, smart ecosystems that use Fourth Industrial Revolution technologies to create personalised, effective experiences for users. These libraries use artificial intelligence to offer personalised recommendations, the Internet of Things to track materials and manage facilities, and big data and learning analytics to understand usage patterns, develop collections and evaluate performance (Misau, 2021, pp. 1-18).

This qualitative development places libraries at the centre of a delicate legal and ethical conflict, as providing these smart services fundamentally relies on collecting vast amounts of personal data about users, such as their research backgrounds, academic interests, borrowing history and patterns of library usage (Salubi, 2024.). Modern legislation affirms individuals' rights to privacy and the protection of personal data, with the General Data Protection Regulation (GDPR) in the European Union being a pioneering model that has prompted many countries to enact similar laws (Cottier, 2020, pp. 24-26.).

These regulations impose strict obligations on library institutions acting as 'data controllers' with regard to the collection, storage and processing of personal data. They emphasise the principles of informed consent, purpose specification, data minimisation and the right to be forgotten ((GDPR), 2016.). However, libraries are also committed to the principles of open access to information, and to their community mission of making knowledge available to all, regardless of financial, legal, or technological barriers. This commitment is enshrined in international charters such as Article 19 of the Universal Declaration of Human Rights (Universal Declaration of Human Rights, 1948.). This commitment stems from the democratic philosophy of libraries as institutions that promote the community's right to knowledge and support scientific and research advancement (Zahra, 2026).

This study seeks to answer the fundamental question that arises: How can current legislation and policies balance strict adherence to personal data protection laws for users of fourth-generation libraries with the core principle of ensuring open access to information, on which these institutions' missions are based? This question stems from the observation that previous studies have addressed personal data protection in the digital space in general, while other research has focused on analysing open access policies and their role in disseminating knowledge. However, a review of the available

literature reveals a clear research gap concerning the study of the intersection and tension between these two areas, specifically in the context of fourth-generation libraries.

A recent systematic review of the literature revealed that studies linking Fourth Industrial Revolution technologies in libraries and compliance with data protection legislation are limited, with most concentrating on technical aspects and failing to provide in-depth legal and ethical analysis (B. K. Avuglah, 2026). Furthermore, practical issues arising from smart services, such as personalised recommendation systems based on analysing researchers' behaviour, learning analytics applications that track student performance in university libraries and the use of facial recognition technologies for managing access, have not received adequate legal analysis in Arab or international literature (Çakmak, 2026).

This study aims to address this gap by achieving a set of interconnected goals. The most prominent of these are:

- establishing the legal and technical concept of fourth-generation libraries, and reviewing their distinctive characteristics
- analysing the main legal texts governing personal data protection, and their applicability to digital and smart library services
- examining the philosophy of open access, as one of the fundamental principles of library operation, and tracing its legal and normative development
- identifying points of tension and intersection between privacy requirements and open access demands
- assessing the adequacy of current policies and practices in smart libraries, in addressing data protection challenges
- ultimately proposing a legal vision, and practical recommendations, to achieve the desired balance between protection and openness

The significance of this study stems from several interconnected considerations. Firstly, the topic's novelty and strategic importance in light of the accelerating global trend towards adopting smart library models. Secondly, the study seeks to address a knowledge gap in both Arab and international literature, as neither has focused sufficiently on reconciling data protection and open access in the context of smart libraries. Thirdly, the study has practical significance for decision-makers and librarians, as it can inform the development of internal policies and technical procedures that protect user privacy without compromising service quality. Fourthly, there is an ethical dimension related to the responsibility of information institutions to protect the digital rights of their users at a time when data collection and analysis are becoming increasingly complex. Finally, this study aligns with the region's rapidly evolving legislative landscape on personal data protection.

## **1. The Conceptual and Legal Framework for Fourth Generation Libraries and Personal Data Protection**

Understanding the dual nature of fourth generation libraries — as knowledge institutions that rely on smart technology, while also being obligated to protect personal data — is essential for analysing the presented issue. We will first address the conceptual side of fourth-generation libraries, examining their characteristics and technologies. We will then analyse the legal framework for personal data protection that governs their operation. This will provide a comprehensive overview of the environment in which tensions between privacy and open access arise.

### **1.1. Concept, characteristics and technologies of fourth generation libraries**

Fourth generation libraries represent a natural evolution of libraries through their previous generations, from traditional libraries (first generation), which focused on printed collections, to automated libraries (second generation), which introduced electronic cataloguing systems, to digital libraries (third generation), which provided digital content and electronic services (Misau, 2021). However, the fourth generation is considered a smart library in the broadest sense, where Fourth Industrial Revolution technologies are integrated into the core of its infrastructure, operations and services to create an interconnected environment characterised by adaptability, predictability and personalisation (E. O. Makori and C. Bitso, 2026).

Fourth generation libraries rely on several key technologies:

**Firstly, the Internet of Things (IoT)** enables library collections (books, devices and equipment), sensors and smart tags (RFID) to be connected into a single network. This allows for the real-time tracking of materials, automatic inventory management and innovative services such as self-checkout and smart notifications (A. D. Kounoudes et al., 2026). This connectivity generates vast amounts of data about material movements and user interactions, forming the basis for advanced analytics, but also raising questions about the privacy of this data.

**Secondly, artificial intelligence is used to provide personalised services**, such as recommendation systems that suggest materials based on the user's borrowing history and research interests, and chatbots that can answer user enquiries and analyse texts and abstracts (Tella, 2026). These applications rely on analysing user behaviour and preferences, necessitating careful handling of personal data.

#### **Third: Big Data and Learning Analytics**

Smart libraries generate vast amounts of data, including acquisition data, borrowing data, search data, and interaction with digital platforms and facility usage. Analysing this data provides a deeper understanding of user behaviour, enables the evaluation of library performance and facilitates evidence-based decision-making regarding the development of collections and services. In academic libraries, learning analytics relate library usage to students' academic performance (Hinchliffe, 2026).

This level of intelligence and personalisation fundamentally relies on collecting and analysing vast amounts of personal data about users, such as their research backgrounds, academic interests, borrowing history, library visit patterns and interactions with chatbots and smart systems. The greatest ethical and legal challenge lies in reconciling the requirements of these smart services with users' rights to privacy (B. K. Avuglah, 2026).

As is clear from the above, fourth-generation libraries represent a qualitative leap in the concept of library services, transitioning from a reactive role to a proactive one in predicting and meeting user needs. However, these advanced capabilities come at the cost of increased personal data collection, placing libraries under dual legal and ethical responsibilities. This reality necessitates an analysis of the legal framework governing the collection and use of this data, which will be addressed in the next section.

## **1.2. The Legal Framework for Personal Data Protection: The General Data Protection Regulation (GDPR) and Comparative Models**

Personal data protection is now a fundamental pillar of modern legislation at international and national levels. Personal data has become a high-value commodity, necessitating legislative intervention to impose strict controls on its collection, processing, storage and transfer (Levallois-Barth, 2015, pp. 137–205). The General Data Protection Regulation (GDPR) of the European Union, which came into effect in May 2018, is regarded as the gold standard in this field and has inspired legislation worldwide (Papoutsoglou, 2025. Accessed 2 March 2026).

The GDPR and many similar laws, such as the Protection of Personal Information Act (POPIA) in South Africa and the California Consumer Privacy Act (CCPA), are based on a set of fundamental principles ((GDPR), 2016.).

### **First: Lawfulness, fairness and transparency**

Data must be collected and processed lawfully and fairly, and data subjects must be clearly and understandably informed about how their data will be used. This imposes an obligation on libraries to be fully transparent with their users about their data collection practices.

**Secondly, data should be collected for specific,** explicit and legitimate purposes, and not processed in a manner that is incompatible with these purposes. This means that libraries cannot use collected user data for purposes other than those explicitly stated for service improvement.

**Third: data minimization:** The data collected must be adequate, relevant and limited to what is necessary for the purpose for which it was collected. This limits the tendency of smart systems to collect as much data as possible 'just in case'.

**Fourthly, accuracy:** reasonable steps must be taken to ensure that the personal data stored is accurate and up to date.

**Fifthly, storage limitation:** personal data should be retained in a form that permits identification of data subjects for no longer than is necessary for processing purposes.

**Sixth: Security and confidentiality:** Data must be processed in a manner that ensures appropriate security and confidentiality, including protection against unauthorised access, unlawful processing, loss or destruction.

**Seventh: Accountability:** The ‘controller’ (the institution responsible for determining how and why data is processed; in our case, the library) is responsible for complying with these principles and must be able to demonstrate this compliance.

When applying fourth-generation services, libraries have a duty to comply with these rules, which presents them with significant technical and regulatory challenges. While relying on commercial service providers (e.g. cloud-based integrated library system, analytics platform and chatbot providers) shifts some of the responsibility to these suppliers, the library remains legally accountable as the ‘controller’ for ensuring these partners (as ‘processors’) comply with the law (Zimmer, 2017, pp. 23–37.). Many library suppliers have been found to lack adequate privacy policies or clear compliance mechanisms, exposing documentary institutions to significant legal risks (Turp, 2022, pp. 145–168.).

Analysis of the legal framework reveals that personal data protection laws impose precise and complex obligations on libraries. These obligations extend beyond the establishment of general policies, necessitating the integration of data protection into the core design of services and systems. However, these obligations may conflict with another fundamental principle on which libraries are based: open access to information. The tension between these two principles will be analysed later to propose a way of reconciling them.

We conclude that fourth-generation libraries, with their smart features and personalised services, inevitably rely on collecting and processing personal data from users. This places them under an obligation to comply with stringent data protection laws. Compliance with these laws is not merely a formal procedure; it requires systems and services to be redesigned according to the principles of transparency, purpose specification, data minimisation and accountability. Nevertheless, the most important question remains: How can these obligations be reconciled with the principle of open access, which embodies the spirit of library work? This question is the focus of the following section.

## **2. The principle of open access and the challenge of reconciling it with personal data protection**

After presenting the nature of fourth-generation libraries and the legal framework for data protection that governs them, we will address the principle of open access to information. First, we will examine the legal and normative foundations of this principle. Then, we will discuss the challenge of reconciling it with privacy requirements and review

the 'privacy by design' methodology as a practical framework to achieve the desired balance.

## **2.1 The Legal and Normative Framework for Ensuring Open Access to Information**

Open access to information is one of the key principles enshrined in international and regional charters. Article 19 of the Universal Declaration of Human Rights states that 'everyone has the right to freedom of opinion and expression, which includes the right to hold opinions without interference, and to seek, receive and impart information and ideas through any media and regardless of frontiers'. Binding international covenants, such as the International Covenant on Civil and Political Rights, have also affirmed this right and extended its scope (International Covenant on Civil and Political Rights, 1966).

In an academic or scientific context, open access means making scientific and research outputs (such as peer-reviewed articles, doctoral theses and research reports) freely available online without financial, legal or technical barriers. This allows any user to read, download, copy, distribute, print, search and link to full texts (Suber, 2015). The philosophy of open access is based on several justifications:

### **Enhancing scientific progress**

Open access accelerates the pace of scientific research and avoids duplication of efforts. It enables researchers worldwide, especially in developing countries, to access the latest scientific findings (Al-Haj, 2026).

- Increasing research impact: studies indicate that articles published under open access receive a higher number of citations than subscription-based articles (Gayshun, 2015, pp. 93–95.).

- Social responsibility: research funding institutions (governments and universities) are obliged to maximise the return on investment by making research outputs available to the public that funded them (Suber, 2015).

This principle imposes a positive obligation on libraries, especially academic and university libraries, to remove all barriers preventing users from accessing information. This involves providing the necessary technical infrastructure and support and encouraging researchers to publish in open access journals and repositories. The International Federation of Library Associations (IFLA) has issued statements and guidelines emphasising the role of libraries in protecting and promoting the right to access information as a fundamental human right (J. Hansson, 2026).

Analysis of the normative framework for open access highlights that libraries are not merely repositories of information but are active institutions in promoting the right to knowledge and democracy. This role requires them to work on removing barriers and increasing openness. However, how can this approach be reconciled with the constraints

imposed by data protection laws? Answering this question necessitates shifting from viewing the two principles as opposing poles to exploring practical frameworks for reconciling them, which we will address later.

## **2.2. The Area of Tension and Intersection: Towards a Privacy by Design Methodology**

The greatest challenge lies in managing the dialectical relationship between data protection and ensuring open access. While privacy laws such as the General Data Protection Regulation require the restriction of the flow of personal information and the precise definition of the purposes for collecting it, open access necessitates the unrestricted flow of knowledge and the removal of all barriers to its dissemination. This is the 'privacy paradox' in the context of libraries. How can a library provide smart, personalised services, which require intensive data collection and analysis, while maintaining the privacy of its users and complying with the law? (B. K. Avuglah, 2026).

Rather than viewing these two elements as absolute opposing poles, a 'Reconciliation Zone' can be envisaged where balance is achieved by adopting innovative methodologies and techniques. The 'Privacy by Design' methodology is the most promising framework for achieving this alignment (Cavoukian, 2009.). Developed by Ann Cavoukian in the 1990s, this methodology is based on seven core principles: being proactive rather than reactive; making privacy the default setting; embedding privacy into design; ensuring full functionality (a positive sum rather than a zero sum game); providing security throughout the lifecycle; offering visibility and transparency; and respecting user privacy (al, 2026). In the context of fourth-generation libraries, 'Privacy by Design' means integrating data protection into the architecture of systems and services from the initial design stage rather than adding it as an afterthought.

This principle can be applied in practice through several integrated mechanisms.

**1. Privacy-Enhancing Technologies (PETs):** Technologies such as the anonymisation and pseudonymisation of data used in analytics allow for the analysis of collection usage patterns, enabling the development of services that meet users' needs without infringing on their privacy. Rather than analysing the behaviour of a specific user, the behaviour of a specific age group or academic specialisation is analysed.

**2. Informed consent and transparency:** Develop clear, simplified privacy policies that explain to users exactly what data is being collected, why, how it will be used and with whom it may be shared. These policies should be presented to users in an interactive manner that allows them to make informed choices and provide easy mechanisms for exercising their rights, such as the rights of access, rectification, erasure and data portability (al N. A., , 2022).

**3. Privacy by Default:** Privacy settings in library systems should be set to the highest level by default. No additional data should be collected or shared with third

parties without the user's explicit consent. Furthermore, data collected for statistical purposes should be anonymised automatically (Project, 2026).

**4. Data Protection Impact Assessments (DPIAs):** Conduct regular and systematic assessments for new library projects and services involving the processing of personal data, particularly those using modern technologies such as artificial intelligence. These assessments should be 'living documents' that evolve with the development of the project, rather than being a one-time formal procedure ((2017), 2026).

### **Training and capacity building**

Investing in training for librarians to raise their awareness of legal and technical requirements for data protection, and enabling them to promote privacy within their institutions. Studies indicate that there is a significant knowledge gap in this area among library staff, necessitating intensive qualification programmes (Chisholm, pp. 305–327.).

**Vendor management:** Develop strict criteria for selecting vendors, including evaluating their privacy policies and security practices, and incorporating clear contractual clauses obliging them to comply with data protection laws and define their responsibilities (A. N. Hess, 2026).

A review of the privacy by design methodology reveals that reconciling data protection with open access is possible, but requires institutional willpower and proactive planning. Integrating privacy into service design from the outset, utilising privacy-enhancing technologies and adopting transparency with users are all mechanisms that enable libraries to provide smart services without compromising user rights. This approach transforms "compliance" from a burden into an opportunity to build trust.

The principle of open access is thus a fundamental pillar of the library's mission, but not an absolute one, as it must be balanced with other rights, such as the right to privacy. The privacy by design methodology offers a practical framework that enables libraries to strike this balance without compromising either aspect. Therefore, the future of smart libraries depends not only on their ability to adopt the latest technologies, but also on their ability to build systems that respect privacy and enhance trust. This will form the basis of our recommendations at the conclusion of the study.

### **3. Conclusion:**

In conclusion, it is evident that fourth-generation libraries represent an advanced model for serving the knowledge community. However, this development presents complex legal and ethical challenges. Rather than being an inevitable conflict where one must choose one over the other, the relationship between personal data protection and ensuring open access is a dialectical one that can be managed and engineered through smart policies, flexible legislation and conscious professional practices.

The findings of this study suggest that unconsidered adoption of fourth-generation technologies in libraries without accompanying legal and ethical frameworks

can lead to a “privacy paradox” that sharply undermines user trust in these institutions and exposes them to significant legal risks (Noh, 2014, pp. 53–78.). The principles of ‘compliance and privacy by design’ provide a robust framework for achieving the desired balance by integrating data protection into the core design of services and systems, adopting transparency as an institutional value and empowering users to control their data.

The ultimate goal is to create a smart library environment that respects individual privacy as a fundamental right, while also allowing knowledge to flow freely for the benefit of all. This reaffirms the timeless mission of libraries as beacons of enlightenment, democracy and knowledge.

#### **4. Recommendations:**

- Updating laws and regulations related to libraries: Legislators in Arab countries should reassess and amend library laws to include clear provisions governing activities related to artificial intelligence and big data analysis. These provisions should be compatible with new personal data protection legislation and take into account the cultural and social privacy considerations of each country.

- Issuing unified national standards relating to the security and protection of personal data, and mandating the application of privacy-by-design principles in smart library systems.

- Adopting transparent and comprehensive privacy policies: Library administrations should establish clear, easy-to-understand privacy policies that are compatible with technological advancements. These policies should specify how personal data is collected, the legal basis for each processing operation, the purposes for which data is collected and retained, the security measures in place, and the rights of users and how these can be exercised. The policies should be accessible and written in a language that everyone can understand, and they should be subject to regular review.

- Implementing Data Protection Impact Assessments (DPIAs): The implementation of data protection impact assessments is an indispensable step before launching any new service that uses fourth-generation technologies or involves substantial processing of personal data. Regular reviews of these assessments are required.

- Developing technical infrastructure: Invest in technological systems that support the implementation of privacy principles from the outset. Examples include information management systems that allow for anonymisation and secure encryption, secure access mechanisms, and data storage solutions that comply with national data sovereignty requirements.

- Awareness and continuous training: Design and implement mandatory periodic training programmes for librarians and all staff to raise awareness of data protection requirements and educate them about the latest information security and user privacy

practices. Additionally, efforts should be made to educate users about their digital rights within the smart library framework.

- Encourage interdisciplinary research by supporting the implementation of studies and research that connect law, information technology and library sciences. These studies should aim to explore the practical aspects of privacy challenges in smart libraries.

- Conduct comparative studies of the experiences of libraries in developed countries to learn about their data protection practices.

### 5. Bibliographie

- (2017), E. D. (2026, February 25). 'Guidelines on Data Protection Impact Assessments (DPIA)'. Accessed. Retrieved from <https://ec.europa.eu/newsroom/article29/items/611236>.
- (GDPR), G. D. (2016.). *European Union, Articles 5, 6, 17*.
- A. D. Kounoudes et al., '... (2026, February 20). *A mapping of IoT user-centric, privacy-preserving approaches to the GDPR*. Retrieved from Internet of Things, Vol. 11, 2020. : <https://www.sciencedirect.com/science/article/abs/pii/S2542660520300196>
- A. N. Hess, R. (2026, March 17). *LaPorte-Fiori and K. Engwall (2015). 'Preserving patron privacy in the 21<sup>st</sup> century academic library'*. Retrieved from The Journal of Academic Librarianship, Vol. 41, No. 1.: <https://www.semanticscholar.org/paper/Pre>
- al, N. A. (, 2022). *'Developers Say the Darndest Things: Privacy compliance processes followed by developers of child-directed apps'*. Proceedings of the Privacy Enhancing Technologies.
- al, P. S. (2026, February 25). *'A taxonomy for mining and classifying privacy requirements in issue reports*. Retrieved from vol. 162, Information and Software Technology: <https://www.sciencedirect.com/science/article/abs/pii/S09>
- Al-Haj, G. S. (2026, January). *'Open Access and Digital Repositories', Faculty of Media and Information Management, Lebanese University*. Retrieved from <https://fr.slideshare.net/slideshow/pdf-b500/267357313>.
- B. K. Avuglah, C. M.-A.-D. (2026). *"Privacy issues in libraries with online services: Attitudes and concerns of academic librarians and university students in Ghana,"*. vol. 81, no. 6, College & Research Libraries. 2020. Accessed January 7.
- Çakmak, Ş. E. (2026). *"Personal data perceptions and privacy in Turkish academic libraries: An evaluation for administrations,"*. vol. 6, no. 6, The Journal of Academic Librarianship. 2020. Accessed February 9.
- Cavoukian, A. (2009.). *'Privacy by Design: The 7 Foundational Principles'*. Canada,: Information and Privacy Commissioner of Ontario.
- Chisholm, S. H.-C. (n.d.). *'Privacy literacy instruction practices in academic libraries: Past, present, and possibilities'*. Vol. 46, No. 4, IFLA Journal, 2020.
- Cottier, G. G. (2020). *"2020 ends a decade of 62 new data privacy laws," \*Privacy Laws & Business International Report\*, University of New South Wales, Sydney.*
- E. O. Makori and C. Bitso. (2026). *"Information profession in digital transformation and development: Future directions," in B. J. Hollard (ed.), \*Handbook of research on knowledge and organization systems in library and information science IGI Global, New York., 2021, p. 24. Accessed February 9.*
- Gayshun, I. V. (2015). *'IFLA statement on privacy in the library environment'*. Russian Journal of Library Science, no. 5.

- Hinchliffe, K. M. (2026, 25 February). *Ethical issues and learning analytics: Are academic library practitioners prepared?*, Vol. 49, No. 1, *The Journal of Academic Librarianship*, 2023. Retrieved from <https://www.sciencedirect.com/sc>
- International Covenant on Civil and Political Rights, U. N. (1966). Article 19 .
- J. Hansson. (2026, February 15). *Professional value and ethical self-regulation in the development of modern librarianship: The Documentality of Library Ethics*. Retrieved from Vol. 73, No. 6, *Journal of Documentation*, 2017, pp. 1261–1280. : <https://www.emerald.com/jd/article-abstract/73/6/1261/203528/Professional-value-and-ethical-self-regulation-in?redirectedFrom=fulltext>
- Levallois-Barth, M. L. ( 2015). *Privacy management and protection of personal data*, in *Digital Identity Management*.
- Misau, A. A. (2021). *"Application of artificial intelligence in academic libraries in Nigeria," \*Library Philosophy and Practice\**.
- Noh, D. S. (2014). *'A study of public library patrons' understanding of library records and data privacy*. vol. 4, no. 1, *International Journal of Knowledge Content Development & Technology*, .
- Papoutsoglou, G. M. (2025. Accessed 2 March 2026). *Evolution of repositories and privacy laws: Commit activities in the GDPR and CCPA era*. Retrieved from Vol. 230, *Journal of Systems and Software*: <https://doi.org/10.48550/Arxiv.250>
- Project, D. P. (2026, January 30 ). *'Compliance by design of data/ AI operations and pipelines'*. Retrieved from KU Leuven Research, 2025–2027: <https://ceur-ws.org/Vol-3996/paper-6.pdf>
- Salubi, Y. O. (2024.). *"Privacy Paradox in Industry 4.0: A review of library information services and data protection," vol. 26, no. 1, \*South African Journal of Information Management\**.
- Suber, P. (2015). *A Brief Introduction*, translated by Mohammed Al-Husseini. Riyadh: King Fahd National Library.
- Tella, A. O. (2026, Vol. 40, No. 7, pp. 7–11 25 February). *'Libraries and librarians' roles in ensuring cyberethical behaviour'*. Retrieved from Library Hi Tech News: <https://www.emerald.com/lhtn/article/40/7/7/264624/Libraries->
- Turp, D. M. (2022). *'Are library vendors doing enough to protect users? A content analysis of major ILS privacy policies'*. *Library Trends*, Vol. 70, No. 2.
- Universal Declaration of Human Rights, . (1948.). *United Nations, Article 19*.
- Zahra, H. ( 2026). *"The role of digital repositories in supporting scientific research at Algerian universities: A study of the preferences of professors in the Computer Engineering Department at the University of Annaba towards publishing in digital reposito*. *Cybrarians Journal*. December 2021, p. 13. Accessed January 2.
- Zimmer, K. C. (2017). *'Privacy policies and practices with cloud-based services in public libraries: An exploratory case of Bibliocommons*. *Journal of Intellectual Freedom & Privacy*, Vol. 2, No. 1.