PRZEGLĄD BIBLIOTECZNY 2025
e-ISSN 2545-2487

MACIEJ SASKOWSKI
Institute of Information Science
University of National Education Commission in Kraków
e-mail: maciej.saskowski@uken.krakow.pl
ORCID 0000-0003-1611-7062

CYBERSECURITY IN LIBRARY PRACTICE: BETWEEN DATA PROTECTION AND DIGITAL EDUCATION

Maciej Saskowski (PhD) is a lecturer at the Institute of Information Science at the University of National Education Commission in Kraków and serves as secretary of the editorial board of *AUPC Studia ad Bibliothecarum Scientiam Pertinentia*. He is the author of articles on information security and social communication in cyberspace. His research combines perspectives from bibliology, information science, and media studies, with a focus on disinformation, digital culture, and data protection in public institutions. He teaches academic courses on digital media and information systems. In addition, he works as a music journalist and choreographer, and in his free time he enjoys mountain hiking.

KEYWORDS: Cybersecurity. Digital libraries. Personal data protection. Digital education. Information ethics. Open technologies.

ABSTRACT: **Thesis/purpose** – The article addresses the issue of cybersecurity in the librarianship, focusing on the protection of personal data and user privacy. The aim of the analysis is to identify the risks associated with collecting and processing information in digital libraries and to present possible models of responsible practice. **Research methods** – A case study was used, comparing approaches from the United States (Library Freedom Project), Europe (OBA Amsterdam), and Poland (FRSI). **Conclusions** – The results indicate the need to combine technology, education, and institutional ethics. The author advocates

for the development of libraries as local digital competence centers and active participants in the debate on information rights.

INTRODUCTION

Modern libraries operate in a digital environment which – while opening new possibilities for access to knowledge and services – also carries a number of threats related to data security and user privacy. The transformation of the library from a physical space to an information-technology space necessitates a redefinition of the role of the librarian, who ceases to be merely an intermediary between the book and the reader and becomes also a custodian of data, a guardian of privacy, and a participant in the digital information battlefield.

Cybersecurity in library practice is no longer just the domain of IT specialists and system administrators. It is a real challenge for every institution that collects, processes, and provides access to data – and libraries do this every day, recording loans, browsed catalogs, personal data of readers, and increasingly their online activity. For this reason, the library can no longer be treated as a technologically neutral institution – on the contrary, it is becoming an actor immersed in a complex information environment, exposed to risks related to surveillance, data commercialization, and cyberattacks.

The aim of this article is to present the threats associated with cybersecurity in the library environment, with particular emphasis on issues of privacy and user data protection. The author points out that the protection of personal data should not be regarded solely as a formal legal obligation arising from the GDPR, but also as an ethical foundation of the mission of libraries in the information society.

The article also presents examples of specific actions taken by libraries in various parts of the world in the form of a comparative case study. Three models of privacy protection approaches are compared: the American (Library Freedom Project), the European (Openbare Bibliotheek Amsterdam), and the Polish (local educational activities under FRSI). This comparison allows for showcasing the diversity of possible strategies, from activist and technological approaches, through normative-institutional, to educational and local, and for drawing conclusions about effective and scalable practices.

The later sections of the article also discuss the most important tools for privacy protection, the role of digital education, and the potential for collaboration between libraries and independent experts and hacker communities. This analysis leads to the formulation of recommendations aimed at building libraries as safe, transparent, and responsible entities in the information age.

THE LIBRARY AS A (NON)PRIVATE SPACE

The library has always been a social space – a place for meetings, education, the exchange of ideas, and access to information. In Western culture it has been seen as a public trust institution whose operation is based on the values of openness, neutrality, and respect for user autonomy. However, with the digitization of resources and the widespread use of information and communication technologies, this classic image of the library is undergoing fundamental changes.

The modern library is no longer just a physical building – it is also becoming a digital environment in which significant amounts of data are gathered and processed. This includes data about the collections themselves, as well as personal and behavioral information about users: login data, search histories, reading preferences, borrowed titles, frequency of use of digital resources, as well as location information. In the case of browser systems, the user's location can be estimated based on the IP address or data provided during registration (e.g., home address). In contrast, mobile applications – after the user grants the appropriate permissions – can access precise geolocation data in real time (e.g., via GPS), significantly increasing the scope of potential profiling. Although these actions most often serve to improve the quality of service, tailor the offer to local needs, or automate communication with the user, they simultaneously create an infrastructure susceptible to abuses, both external and internal.

In this context, the library ceases to be a safe enclave of anonymity: it becomes a structure in which user privacy can be restricted not only by unauthorized external access (e.g. hacking attacks) but also by internal practices of data collection and analysis. Moreover, tools such as library management systems (LMS) can further complicate this issue[1]. The use of software for tracking activity or integration with external databases may inadvertently lead to sharing information with third parties such as commercial suppliers or government institutions (American Library Association, 2021).

This raises the question: to what extent can a user of a digital library feel safe and their data be protected? Does the model of social trust, on which the role of libraries has relied for decades, stand a chance of surviving in an environment dominated by the logic of data collection, profiling, and commercialization? And can librarians, often technologically unprepared to manage the realm of cybersecurity, take on this challenge?

These questions serve as a starting point for further reflection on the risk factors associated with data processing in library institutions, as well as on the possibility of building a model of the library as an entity responsible not only for access to knowledge but also for the digital security of citizens.

[1] In the context of libraries, also known as ILS (Integrated Library System).

THREATS TO USER DATA: TECHNOLOGICAL AND INSTITUTIONAL RISKS

In library practice, the collecting and processing of user data is unavoidable. Borrows, reservations, logins to catalogs, use of digital databases, Wi-Fi hotspots, or mobile applications – all of these generate streams of information that may be of a personal nature, and are sometimes even sensitive. Although librarians are not always aware of it, libraries are increasingly participating in the digital surveillance ecosystem.

The technological dimension of these threats is twofold. On the one hand, it concerns the possibility of data interception by third parties – hackers, criminal groups, but also analytics or advertising companies. On the other hand, it relates to the infrastructural weaknesses of library systems themselves: lack of updates, use of default passwords, unencrypted connections, lack of security audits, or failure to adhere to basic principles of digital hygiene by staff and users (Wydawnictwo SBP, 2019).

However, institutional threats are no less significant in terms of how libraries handle the data they collect themselves. In some cases data is stored longer than necessary, processed without clear purpose, or shared with external entities – for example, providers of analytical tools or cataloging services. Furthermore, many library systems are integrated with commercial services (e.g., Google Books, Amazon Web Services, external search engines), which means that information about users' reading behaviors may end up outside the library (Amazon Web Services, 2019).

From the perspective of privacy protection, particularly concerning are situations where data regarding reading preferences can lead to user profiling, especially if the chosen topics concern worldviews or political, religious, or medical issues. Although GDPR classifies such data as sensitive, in practice not all LMS systems are appropriately adapted to this (European Data Protection Supervisor, 2021).

To complete the picture we must include human factors: insufficient training of employees, lack of awareness of threats, an organizational culture that downplays privacy issues, as well as a lack of information security specialists within the structures of many libraries. As a result, the library, instead of being a guardian of privacy, may unintentionally become a link in the chain of personal data breaches.

In the literature, it is emphasized that the protection of privacy should be one of the pillars of contemporary library ethics, alongside the freedom of access to information and ideological neutrality (American Library Association, 2021). Meanwhile, as studies show, many users are unaware that by using library resources their activities may be monitored and data analyzed in a manner similar to corporate practices known from digital platforms (Deloitte, n.d.).

LIBRARIES IN THE AGE OF ALGORITHMIC SURVEILLANCE

The contemporary digital infrastructure in which libraries operate increasingly relies on algorithmic logic. From book recommendations in online catalogs, through intelligent management systems for loans, to integrations with cloud and analytical tools – almost every element of the operation of a modern library is indirectly or directly shaped by algorithms. Although they are often perceived as neutral tools that support the efficiency of services, in reality they become elements of structural surveillance over information and the user.

Algorithms can not only catalog and organize information – they can also filter it, prioritize it, and in extreme cases exclude it. If a recommendation system suggests certain items while omitting others, it can influence the intellectual horizons of the user. If the system automatically hides titles deemed 'controversial,' it restricts access to content that should be available under the freedom of information. Libraries that use ready-made digital platforms rarely have full control over these processes (Noble, 2018).

In media and information literature it is pointed out that algorithms are not only tools but also "forms of power" – decision-making structures that shape access to knowledge and information (Beer, 2018). In this context, the library ceases to be solely a place for archiving and sharing – it also becomes an algorithmically mediated space where neutrality is illusory and priorities are hidden in code. This threat becomes even more apparent in situations where library systems are linked to commercial services or managed by third-party companies. Information about user behaviors can then become part of a broader analytical ecosystem used for advertising, behavioral, or political purposes (Zuboff, 2019). It is difficult to speak of full privacy protection under such conditions, even if the intentions of the library itself remain consistent with its ethos.

At the same time, it is worth noting that not all libraries are aware of how the algorithms they use function – much less what data is collected by them, how long it is stored, and to whom it is shared. There is a lack of appropriate algorithmic audits, training for staff, and documentation provided by technology vendors. Meanwhile, the responsibility for data protection – including that processed automatically – still rests on the library as the information administrator.

The phenomenon of algorithmization of library practice thus requires critical reflection. It is essential not only to ensure technical security but also to guarantee transparency in technological processes and the ability to control these processes – by both staff and users. Otherwise, libraries, willingly or unwillingly, may become part of a digital surveillance system rather than serving as a counterbalance to its abuses.

ALLIES OR ENEMIES? ON THE POTENTIAL FOR COLLABORATION BETWEEN LIBRARIES AND HACKERS

In public debate, the word "hacker" still often has negative connotations: it is associated with cybercrime, data theft, or sabotage activities. Meanwhile, in the modern world of technology, hackers are a heterogeneous group – alongside those who actually exploit their skills for illegal activities, there exists a large community of so-called ethical hackers (white hats), who test systems to detect security vulnerabilities, educate society, and support open technologies (Himanen, 2002).

It is this second group that may prove to be a valuable – albeit unconventional – partner for libraries. These institutions, due to their limited resources and lack of specialized IT support, often cannot independently monitor and secure all aspects of their digital infrastructure. Meanwhile, ethical hackers possess the knowledge, experience, and tools that can significantly enhance the level of cybersecurity in library practice.

Examples of potential collaboration are numerous: from organizing open workshops on privacy protection and data encryption, to conducting informal penetration tests (so-called pentests) at the request of libraries, to creating joint educational initiatives in the spirit of open source and hacker culture. In many countries, communities such as CryptoParty or Hackerspace operate, eager to engage in social and educational activities (Sauter, 2014).

It is also worth noting that libraries and hacker communities have surprisingly similar values: promoting access to knowledge, openness, independence of thought, protection of privacy, and counteracting information monopoly. Although they differ in language and form of operation, their goals often overlap, especially in the context of defending information freedom against commercial and state influences.

Instead of treating hackers as a potential threat, libraries can consider them as educational and technology partners. Such a partnership, although it requires courage and openness, can bring mutual benefits: for libraries, competences and support; for hackers, social trust and scope for constructive activities.

This does not, of course, imply a resignation from caution. The library, as a public trust institution, must maintain control over data security and cannot allow for unauthorized activities. However, if the approach to cybersecurity is to be not only reactive but also preventive and educational, collaboration with hackers could represent a new, creative form of achieving this mission.

PRIVACY PROTECTION TOOLS AVAILABLE FOR LIBRARIES

In the face of threats related to digital data processing, libraries are not helpless. There are many tools and technological solutions that, when properly implemented, can significantly increase the level of user privacy protection. The key challenge today is not the lack of available technologies, but rather the lack of awareness of their existence, limited technical resources, and shortages of staff and competencies for handling them.

The first step is to ensure an appropriate level of encryption for communication, both internal and with users. Using secure protocols (e.g., HTTPS, TLS), employing VPNs for access to library networks, and promoting tools such as Tor or Tails among more aware users are the basics of digital hygiene. Some libraries even choose to run Tor nodes as a form of engagement in protecting privacy in the public space[2].

The second area of action is system security: regular software updates, implementing two-factor authentication for employees, strong passwords and a policy of regular changes, monitoring logs and unauthorized access. Although these are basic practices, their absence is often the cause of the most common data breaches in the public institutions sector (IBM Security, 2024).

Libraries can also use open-source software for cataloging and managing collections (e.g., Koha, Evergreen), which allows for greater control over what data is collected and how it is processed. An important criterion for choosing a library management system today should not only be its functional scope but also its compliance with privacy principles and the possibility of audit (American Library Association, n.d.).

At the operational level, it is worth considering the use of tools such as:

- Privacy Badger, uBlock Origin – for eliminating trackers in the browsers used in the library,
- CryptPad, Etherpad, Jitsi Meet – alternatives to commercial group work and communication tools,

[2] The most well-known case was the Kilton Library in New Hampshire (USA), which in 2015 launched an exit node of the Tor network in collaboration with the Library Freedom Project – an initiative promoting information freedom and digital rights in public institutions. This project sparked a wide social and media debate – both praise for its brave support of privacy and criticism due to the associations of Tor with criminal activities. Ultimately, despite a temporary suspension, the project was resumed, and the Kilton Library remains the only known library facility in the USA operating such a node. Although other libraries did not follow this path, the very idea – providing users with a space for safe and anonymous access to internet resources – remains a significant demand from communities advocating for digital human rights. Although the practical implementation of projects like Tor in libraries is currently limited, the need to provide users with a neutral, secure technological infrastructure remains relevant – especially in the context of increasing surveillance and data commercialization (Koebler, 2015).

- GNU/Linux and FOSS software – safer alternatives to commercial operating systems and applications,
- Matomo – an alternative to Google Analytics for tracking traffic on the library's website.

It is also worth applying the principle of data minimization – collecting only the information that is necessary, storing it for the shortest time possible, and clearly informing users about their rights and the scope of processing. According to the GDPR, users should not only have access to their data but also the ability to delete or correct it (Parlament Europejski i Rada UE, 2016).

The cultural aspect is also significant: technologies alone are not enough if they are not accompanied by a culture of privacy protection, supported by institutional policies and managerial decisions. Libraries that implement privacy codes, promote transparency, and educate users in this area not only create a safe environment but also an informed information community.

THREE MODELS OF PRIVACY PROTECTION IN PRACTICE: A COMPARISON OF LIBRARIES FROM THE USA, EUROPE, AND POLAND

In the context of cyber threats and challenges related to the protection of personal data, libraries around the world are taking actions aimed at increasing the level of digital security. However, these practices vary depending on the cultural, legal, and technological context. This chapter presents three distinctly different operating models – American, European, and Polish – which illustrate possible directions for the development of cybersecurity in library practice.

1. The American Model: The Library as a Privacy Activist (Library Freedom Project, USA) One of the most well-known and radical privacy projects is the Library Freedom Project (LFP), initiated in Massachusetts by activist Alison Macrina. This project combines librarianship ethics with the movement for digital freedom and user privacy. The LFP aims to train librarians, implement privacy protection tools, and create a network of libraries operating under the principle of "privacy by default"[3].

As part of the project, some libraries have deployed Tor nodes (anonymizing internet traffic), installed encrypted search engines,

[3] The principle of "privacy by default" means that the controller – both when determining the means of processing and during the processing itself – implements appropriate technical and organizational measures, such as pseudonymization, designed to effectively implement data protection principles, such as data minimization, and to incorporate the necessary safeguards into the processing to meet the requirements of the GDPR and protect the rights of data subjects (Library Freedom, n.d.).

stopped tracking loan histories, and begun organizing workshops on encrypted communication, digital identity management, and combating online surveillance. Importantly, the project is grassroots and educational in nature – its strength lies not in technical infrastructure, but in awareness and engagement. The LFP model demonstrates that libraries can be not only passive recipients of technologies but also active co-creators and commentators. The Library Freedom Project's activities clearly demonstrate that libraries can become spaces where users not only gain knowledge but also learn how to protect their digital identities, recognize privacy threats, and use tools that enable secure and independent online communication.

Therefore, in the LFP model, the library becomes a participant in the debate on digital rights – not as an observer, but as an engaged social actor who takes responsibility for shaping citizens' digital competencies. Collaboration with ethical hackers and technology activists becomes not only a means to improve the security of IT infrastructure but also a manifestation of librarian values such as accessibility, freedom of information, independence, and equality. LFP demonstrates that it is possible to run a library that, instead of adapting to corporate solutions and closed systems, prioritizes open source software, source code transparency, encryption, and local autonomy. Workshops organized as part of the project, dedicated to topics such as Tor, PGP, Signal, and metadata encryption, represent a practical form of resistance to dominant models of surveillance and commercial data analysis. In this approach, the library becomes an ally of civil society, not just a neutral point of access to information.

This model inspires thinking about the library as a digital literacy laboratory – a place that not only provides access to technologies but also equips users with the tools to understand, modify, and use them consciously. In an era of growing digital capitalism, where data is becoming currency, a library operating according to the principles of digital literacy can serve as a counterweight to the mechanisms of knowledge commercialization and information surveillance.

2. The European Model: GDPR Compliance and Institutional Transparency (Openbare Bibliotheek Amsterdam, Netherlands).

Another approach to protecting user privacy and data is the European model, which, unlike the activist and decentralized approach of the Library Freedom Project, relies on a strong legal and institutional framework. This model is based on full compliance with the General Data Protection Regulation (GDPR), which applies in all European Union member states and defines standards for personal data processing, process transparency, and the rights of data subjects (Openbare Bibliotheek Amsterdam, 2025).

The Openbare Bibliotheek Amsterdam (OBA), the largest public library in the Netherlands, is a model example for implementing this approach. The library has developed a detailed, publicly available privacy policy that governs every step of data collection, from collection, through storage and processing, to the ability to delete data at the user's request. OBA has also implemented a range of technical and procedural tools: pseudonymization of loan data, automatic deletion of catalog search history, and the option to manage consent in a simple, intuitive way – all within the user account.

Communication is a key element of this strategy. Users don't have to guess what data is being collected – the library actively informs them about the processing purposes, retention period, legal basis, and their rights. This model assumes that transparency builds trust, but also meets the requirements of the GDPR, which emphasizes privacy by design and privacy by default. OBA has also invested in staff training to ensure that only authorized and properly trained employees have access to sensitive data. The library management system is designed with data minimization in mind: by default, it collects no more information than is necessary to provide the service. This approach helps reduce the risk of data breaches while strengthening the institutional sense of responsibility for data protection.

Unlike the American model, which embraces grassroots initiatives and often operates in opposition to state or corporate institutions, the European model is highly institutionalized and compliant with regulations. It operates based on legal standards, audit procedures, and accountability mechanisms that are part of a broader administrative culture. Its goal is not only to protect data but also to build public trust through standardization and a systematic approach to privacy.

Thus, the OBA model demonstrates that libraries can effectively protect user data without necessarily utilizing the most advanced technologies, but rather through consistent, lawful action, institutional accountability, and transparency.

3. The Polish Model: Digital Education as a Protection Tool (FRSI, Local Programs).

The Polish model is distinguished by an approach that—given limited technological resources and a lack of uniform institutional procedures—focuses primarily on digital education and improving users' information literacy. At the heart of this model are local libraries, operating as open knowledge centers, supporting the community not only in accessing books and the internet, but also in understanding digital threats, protecting privacy, and safely using new technologies (Fundacja Rozwoju Społeczeństwa Informacyjnego, 2018).

An example of this approach is the work of the Information Society Development Foundation, which, in collaboration with libraries, has been implementing numerous educational initiatives for years, such as the "Click. Check. Understand" campaign, which provides support to librarians in organizing workshops on topics such as personal data protection, password management, recognizing fake content, and using online services in an informed and safe manner.

Unlike the Dutch or American models, Polish libraries rarely have advanced IT infrastructure, and user privacy protection is not yet widely integrated into their internal policies. However, their strength lies in their proximity to local communities and the high availability of educational services, including for the digitally excluded such as seniors, residents of small towns, and young people lacking media literacy.

In many cases, librarians become users' first guides to the world of safe online presence. Libraries organize meetings, lectures, courses, and individual consultations, and also provide access to educational materials created by NGO partners[4] and formal education.

This model is based on the premise that awareness is the best form of protection. In a situation where advanced technical tools or institutional privacy protection procedures are lacking, the digital competencies of users and librarians become the first line of defense against information abuse and cyberthreats.

While the Polish model is still in its developmental stages and faces financial and organizational barriers, its potential lies in its flexibility, adaptability, and strong social roots. As public policies and digital library strategies develop, it can serve as a foundation for a more integrated approach to cybersecurity in the cultural and educational sectors.

Table 1. A Comparison of Three Models of Privacy Protection in Libraries

Model	Main Features	Strength	Constraints
American (LFP)	activism, open source, cooperation with hackers	innovation, independence	lack of systemic support
European (OBA)	legality, institutionalization	transparency, stability	limited flexibility
Polish (FRSI)	educational activities, local community	availability, coverage	lack of infrastructure, internal policies

Source: prepared by the author

[4] NGO (non-governmental organization) – the third sector (also spelled "III Sektor" or "3 Sektor") is the term used to refer to all non-governmental organizations. This term, transferred from the English language (third sector), refers to the concept of dividing the socio-economic activity of modern democratic states into three sectors.

All three models demonstrate that privacy protection in libraries can take various forms, from technical, through legal and institutional, to educational. However, the best results are achieved by combining these approaches: a library that combines technological awareness with a legal framework and active user education has the greatest chance of becoming a space of true information security.

DIGITAL EDUCATION AND INFORMATION LITERACY AS A FORM OF CYBERSECURITY

While technology plays a key role in ensuring data security, educational initiatives are equally crucial, both among library staff and users. Modern cyberthreats often stem not from advanced attacks but from human unawareness: clicking on a fake link, using a weak password, or sharing too much information online. In this context, digital education is becoming one of the most important and affordable tools for protecting privacy and personal data.

Libraries, as institutions of public trust and places of informal education, are particularly well-suited to serve as local digital literacy centers. They can conduct workshops on safe internet use, online identity management, recognizing phishing, and using encryption tools. Even simple actions such as learning how to use password managers, educating people about privacy settings on social media, or promoting secure browsers can significantly increase the level of information awareness in the local community.

Initiatives supporting libraries in implementing such initiatives are emerging in many countries. One example is the American Library Freedom Project, which connects libraries with privacy experts, offering training, technical consultations, and educational resources on topics such as Tor, PGP, and privacy policies. In Poland similar functions can be performed by library programs supported by the Information Society Development Foundation or initiatives of non-governmental organizations operating at the intersection of education and technology.

At the same time, the need to improve the competencies of library staff should not be overlooked. Librarians should be prepared to recognize threats, apply data minimization principles, respond to privacy incidents, and provide basic information to users about digital security. In practice, however, the topic of cybersecurity still rarely appears in library science curricula, which raises the need for systemic support and professional development in this area.

In the age of ubiquitous digitalization, education is becoming a form of cybersecurity that is just as important as firewalls, protocols, and certificates. A library that invests in developing information literacy skills not only better protects its users' data but also strengthens their position as citizens in a digital society. Ultimately, it is knowledge, awareness, and the ability to critically use technological tools that provide the most effective protection against manipulation, data leaks, and digital exclusion.

SUMMARY

Cybersecurity in libraries is no longer optional or a technological add-on – it is becoming one of the fundamental pillars of their responsible functioning in the information society. With the increasing digitization of services, libraries are increasingly collecting, processing, and sharing data, which – if not properly protected – can become a source of serious violations of privacy and public trust.

The analysis conducted in this article shows that threats to user data are not only technological but also institutional, organizational, and cultural. Lack of privacy policies, shortages of skills, dependence on commercial technology providers, and lack of awareness of algorithmic surveillance – all of this means that libraries may unwittingly participate in processes that limit users' freedom and information security.

In this context, adopting a holistic approach to cybersecurity seems crucial, encompassing not only technology but people, procedures, organizational culture, and relationships with the environment. Based on this several practical recommendations for library institutions can be formulated:

1. Strengthening staff competencies. Libraries should invest in training in information security, risk management, incident response, and data ethics. These topics should also be included in librarian education programs.

2. Transparency and Privacy Policies. Every library should have a clear privacy policy that is accessible, understandable, and enforceable. Users must know what data is being collected, for what purpose, who has access to it, and how long it is retained.

3. Collaboration with Independent Experts. Institutions should consider collaborating with ethical hackers, digital activists, or non-governmental organizations working to protect privacy. Such partnerships can be a source of knowledge, technical support, and innovative solutions.

4. Using the right tools. Libraries should choose information management systems based on the "privacy by design" principle, use open source tools, encrypt communications, and limit reliance on commercial platforms.

5. User education. Libraries should serve as local digital education centers, offering training and support in privacy, safe internet use, and digital identity management.

Ultimately, cybersecurity isn't just a technical task—it's a matter of trust, responsibility, and ethical commitment to the community. Libraries, as public and educational institutions, have a special role to play in shaping citizens' digital literacy. To continue fulfilling this role, they must become aware and resilient entities themselves, including in the digital dimension.

BIBLIOGRAPHY

Amazon Web Services (2019, october). *Zgodność usług AWS w odniesieniu do postanowień GDPR (RODO).* https://d1.awsstatic.com/whitepapers/compliance/PL_Whitepapers/pl_pl__GDPR_Compliance_on_AWS.pdf.

American Library Association (n.d.). *Library Privacy Guidelines*. https://www.ala.org/advocacy/privacy/guidelines.

American Library Association (2021, october). *Privacy: An Interpretation of the Library Bill of Rights*. https://www.ala.org/advocacy/privacy.

Beer, D. (2018). *The Data Gaze: Capitalism, Power and Perception*. London: SAGE Publications.

Deloitte (n.d.). *Era danych w sieci*. https://www2.deloitte.com/pl/pl/pages/risk/articles/era-danych-w-sieci.html.

European Data Protection Supervisor (2021). *Guidelines on Data Protection in Libraries and Archives*. Brussels.

Fundacja Rozwoju Społeczeństwa Informacyjnego (2018, 12 december). *Kliknij. Sprawdź. Zrozum. Jak świadomie korzystać z informacji*. https://frsi.org.pl/kliknij-sprawdz-zrozum-jak-swiadomie-korzystac-z-informacji/.

Himanen, P. (2002). *The Hacker Ethic and the Spirit of the Information Age*. New York: Random House.

IBM Security (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/reports/data-breach.

Koebler, J. (2015, 30 june). *Public Libraries Will Operate Tor Exit Nodes to Make the Service More Secure*. https://www.vice.com/en/article/public-libraries-will-operate-tor-exit-nodes-to-make-the-service-more-secure.

Library Freedom (n.d.). *We are Library Freedom Project*. https://libraryfreedom.org/.

Openbare Bibliotheek Amsterdam (2025, 19 june). *Privacy beleid*. https://www.oba.nl/privacy.html.

Parlament Europejski i Rada UE (2016, 27 april). *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=-CELEX:32016R0679.

Sauter, M. (2014). *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury.

Wydawnictwo SBP (2019). *Poradnik RODO dla bibliotek*. Warszawa. https://wydawnictwo.sbp.pl/pdf/Poradnik_RODO.pdf.

Zuboff, Sh. (2019). *The Age of Surveillance Capitalism*. New York: PublicAffairs.