

Chapter 5

Cybersecurity Risks in the Digitisation of Cultural Heritage in India: A Legal and Governance Analysis

Priyanka Das, Assistant Professor of Law, Swami Vivekananda University

Abstract

India is using digitization to both safeguard and promote the country's heritage through its cultural institutions like museums, manuscripts, archives, and other historical records. Digital forms of preservation are often considered a more secure and permanent way to preserve cultural assets, and many continue to subscribe to a larger myth associated with cybersecurity and how technology is assumed to be safe; therefore, this chapter will discuss if the current legal and governance framework created in India is sufficient to protect digitized cultural heritage from cyber-related threats. Most current literature discusses cultural heritage protection and cybersecurity governance in conjunction, but little existing analysis focuses directly on how current cybersecurity law applies to digital heritage institutions. This gap is important to note, as digital repositories become subject to various cyber threats, including data breaches, ransomware attacks, unplanned access via hacking, and weaknesses with the organizations that rely upon digital assets. This chapter uses doctrinal and analytical methods to review relevant laws related to this area of study, including but not limited to the IT Act, 2000, the Digital Personal Data Protection Bill 2023, and any other relevant heritage legislation and policy documents, along with secondary sources of information. By studying the intersection between digitization initiatives and cybersecurity regulatory initiatives, this study highlights the disparity between the intended benefits of digital preservation and the obstacles associated with cyber governance.

Keywords: *Digital Preservation, Cybersecurity Law, Cultural Heritage Protection, Data Governance, Institutional Vulnerability.*

Introduction

Cultural heritage is the artistic, scientific, or historical heritage of a culture or society. The term “cultural heritage” has various of definitions at both national and international level. However, it lacks any uniform definition. As per the UNESCO, “cultural heritage” includes “artefacts, monuments, a group of buildings and sites, museums that have a diversity of values including symbolic, historic, artistic, aesthetic, ethnological or anthropological, scientific and social significance. It includes tangible heritage, movable, immovable and underwater, intangible cultural heritage (ICH) embedded into cultural, and natural heritage artefacts, sites or monuments. The definition excludes ICH related to other cultural domains such as festivals, celebration etc. It covers industrial heritage and cave paintings.”¹¹⁰ The preservation of the immense variety of heritage has long been viewed as a priority for India, where numerous cultures have existed

¹¹⁰ UNESCO Institute for Statistics, *2009 UNESCO Framework for Cultural Statistics (FCS)* (UNESCO 2009).

throughout its history. Historically, preservation was limited to the physical preservation of monuments and artefacts via statutory methods. However, digitalisation has become an emerging model of preserving and promoting cultural heritage in recent years. There has been a greater commitment to digitalisation as a preservation method because digitisation allows cultural institutions to convert tangible materials into digital formats, which makes for greater access to cultural heritage, promotes research opportunities, and helps prevent the degradation of fragile resources.¹¹¹

In addition, the creation of digital repositories and archives allows for a greater possibility of public engagement through the access to cultural heritage, as well as allowing for new ways to document and disseminate cultural heritage. The result of this belief is that many people now trust that digital preserving solutions for the conservation of heritage will be the most reliable and secure option to meeting the difficulties of heritage conservation in the future. This trust reflects the confidence most people have in technology systems as providing a safe and long-term method for completing the process of preserving cultural, historical, or scientific heritage.

However, the assumption that digitisation automatically guarantees security overlooks the vulnerabilities associated with digital infrastructures. Cultural institutions that rely on digital platforms are exposed to cyber risks such as data breaches, ransomware attacks, unauthorised access and systemic institutional weaknesses. When heritage resources are integrated into digital environments, they become subject to the same threats that affect other information systems. Any compromise of digital heritage may have consequences that extend beyond operational disruption and may affect cultural continuity and public trust.

The Indian government has enacted legislation to deal with cyber issues. The legislation currently in place includes the Information Technology Act, of 2000 and the Digital Personal Data Protection Act, of 2023. The two laws set up a general framework to regulate cybercrime, but there has been very little attention given to how they are to be applied specifically to institutions with digitized cultural heritage. Most of the available literature on the issue has treated the two areas of research i.e Cultural Heritage Protection and Cyber Security as separate and neither area has had much in the way of scholarly examination that touches on the intersection between the two.¹¹²

The purpose of this chapter is to determine if current cyber governance and the legal framework in place in India is adequate to protect digitized Cultural Heritage from the potential of being harmed by cyber related threats. In order to accomplish this, this chapter will incorporate a doctrinal and analytical methodology in order to conduct an examination of the applicable statutes, legislation governing Heritage Sites, policy documents, and applicable secondary academic sources. This chapter will examine the applied relationship between digitized Cultural Heritage, digitization initiatives and Cyber Security Regulation, and will highlight gaps between the declared intent of

¹¹¹ Press Information Bureau, 'Digitization of Cultural Heritage in India' (17 March 2025) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2111884®=3&lang=2> accessed 2 March 2026.

¹¹² DLA Piper, 'Data Protection Laws of the World: India – Data Protection in India' <https://www.dlapiperdataprotection.com/?t=law&c=IN> accessed 2 March 2026.

the policies and practices that are implemented to preserve Cultural Heritage Digitally and the challenges that exist in Nurturing Cyber Governance.

Digitisation of Cultural Heritage in India: Policy Context and Institutional Framework

India is working hard to create a digital representation of its cultural past. This is part of an initiative to create better government services and improve the uses of the internet. There has been a shift by many sources of cultural goods towards using computers to help preserve the information about their items, recording that information, and making it available to the public. The aims of these different agencies go beyond just needing to keep records, they want to provide access to their records, allow people to see them, and involve people once they have been made available.

Several successful projects have been supported by the Indian government to help digitise material.¹¹³ All major projects have aimed to create online collections of items that could be used by everyone to learn about India's history. The national cultural institutions responsible for these projects include the National Archives of India, the Indira Gandhi National Centre for the Arts and various state museums. They have developed ways to scan and catalogue items digitally, so they can be accessed through various means online. The Digital India programme also emphasises the importance of electronic government and creates better digital infrastructure, which indirectly influences the cultural sector.

There are many benefits to digitisation. Digitisation aids in preserving delicate artefacts due to the decrease in physical handling of these items. Additionally, digitisation allows researchers, academics and the general public to have access to materials, regardless of geographic distance. Another benefit is that digitisation helps with documentation, and inventory management processes and therefore improves the administration efficiencies of institutions. Digital storage also permits duplication and backup, which potentially decreases the risk of irretrievable loss from natural disasters or deterioration of the physical object.

However, the digitisation of cultural assets results in a transformation of the cultural asset itself. Once in digital format, cultural heritage items are mere data format and stored on servers, networks and cloud systems. Consequently, protecting them will consist of information security functions rather than conservation functions. The risks associated with this changeover generally receive little or no attention. Cultural heritage institutions are generally underprepared for many digital security risks due to a lack of adequate cybersecurity infrastructure, or appropriate technical skill or financial resources to adequately manage digital threats.¹¹⁴

Also, third-party services are frequently engaged to support digitisation projects such as storage of data, software management, or cloud hosting, generating multiple futures for potential failure due

¹¹³ Ministry of Culture, 'Digital Cultural Governance and Monitoring of Cultural Initiatives' (Press Information Bureau, 2 February 2026) <https://www.pib.gov.in/PressReleaseDetailm.aspx?PRID=2222115> accessed 2 March 2026.

¹¹⁴ Samar I Bakhshi, 'Digitization and Digital Preservation of Cultural Heritage in India with Special Reference to IGNCA, New Delhi' (2016) 6(2) Asian Journal of Information Science and Technology 1, 2 <https://ajist.co/index.php/ajist/article/view/134> accessed 2 March 2026.

to additional layers of vulnerability. Cultural heritage institutions may have weak contracts with third-party service providers, as well as poor security practices, and insufficient oversight leading to unauthorised access or use of digital data repositories. In some instances, cultural heritage institutions may not consider their digital collections to be valuable information assets, thereby limiting their investment in security measures.

Another important dimension concerns the value of cultural data. Digitised manuscripts, artefacts and archival records may contain sensitive historical information, indigenous knowledge systems or rare documentation. Such data may be attractive targets for cyber criminals, whether for financial gain, political motives or ideological reasons. Ransomware attacks, in particular, pose a serious threat because they can lock institutions out of their own collections unless payment is made. The loss or manipulation of cultural data may result in reputational damage and undermine public trust.

Policies governing digitalisation tend to put emphasis on growth/as well as access, with little thought given to Security arrangements. Most of the time, Innovation, and access are seen as high priority in relation to Technology, however, Security is viewed as secondary. Thus, there seems to be an implied belief that Digital Technologies, by virtue of being more advanced than other technologies, automatically provide Security. With the increased dependence on Digital Technology Infrastructures, one of the most important questions regarding Digital Heritage management will be whether or not the current legal and regulatory framework in India is sufficient for the Cybersecurity risks cultural institutions experience. In order to have an answer to this question, the appropriate statutes dealing with Cybercrime and Data Privacy should be reviewed and their relevance to the Heritage sector evaluated. This will be done in the following chapter.¹¹⁵

Cybersecurity Law in India and Its Applicability to Digital Heritage Institutions

Cybersecurity in India is primarily governed by legal regulation through the Information Technology Act of 2000, which was originally intended to enable e-commerce through the use of electronic signatures and provide a legal framework for e-businesses.¹¹⁶ As it has evolved into a comprehensive piece of legislation, it now regulates various types of cyber-related misconduct, including cyber terrorism, as well as providing a legal framework for electronic records and electronic documents. The IT Act was amended to include provisions for data protection, victimisation and intermediary liability in 2008.

The IT Act includes several provisions that apply to digital cultural heritage institutions, including Section 43 that is unauthorised access to computer systems, theft of data and damage to computer systems and Section 66 that states about acts against computer systems that are done dishonestly or fraudulently. Both of these provisions would apply if a person accessed a digital archive or museum database without authorisation or altered, copied or deleted information from a digital

¹¹⁵ National Archives of India, 'Information Technology' <https://nationalarchives.nic.in/Information-Technology> accessed 2 March 2026.

¹¹⁶ 'Understanding the Information Technology Act, 2000 in E-commerce' (Lloyd Law College, 24 June 2025) <https://www.lloydlawcollege.edu.in/blog/it-act-2000-e-commerce-legal-framework.html> accessed 2 March 2026.

collection of cultural heritage. Additionally, Section 66F or cyber terrorism could become applicable if an attack on a cultural heritage repository creates a threat to national security or public order.

The objective of protecting sensitive personal information and requiring reasonable security practices with respect to sensitive personal data are among the several areas in which these two statutes overlap. While earlier regulations around Section 43A of the Act provided a basis for understanding how to meet the standards of data protection, the Digital Personal Data Protection Act of 2023 has now significantly enhanced this regulation by establishing a clear, structured system of providing adequate safeguards for processing personal data, including specifying the responsibilities and rights of individual data fiduciaries and data principals, respectively.

Although many cultural heritage organizations do not routinely have access or use large volumes of personal data, some archives or historical records may still contain information that is identifiable to persons, groups or communities who are the subjects of that collection.¹¹⁷ This will therefore create a legal obligation to comply with all applicable provisions of the Act as it specifically relates to data processing activities and records. Rather, the primary and only purpose of most cultural heritage organizations that hold archival materials is to preserve and disseminate historical records, not to collect and store data for commercial purposes. Thus, it is highly debatable whether the cybersecurity requirements established pursuant to the Digital Personal Data Protection Act, 2023 satisfy the cybersecurity needs of cultural heritage organizations.¹¹⁸

The corporate and regulatory statutory provisions in India are only one of many systems for governing digital Heritage organizations and their controls. The National Computer Emergency Response Team functions under the authority of the Information Technology Act, which includes guidelines for reporting and responding to incidents related to cyber security. Many of the organizations outlined above operate digital systems and may be subject to reporting obligations established in the guidelines from N-CERT; however, the current level of awareness and compliance in this sector is unclear. The significant limitation within this existing framework is its general applicability. The Information Technology Act and Digital Personal Data Protection Act were designed and implemented across all sectors of the economy. Neither specifically identifies Digitized Cultural Heritage organizations as critical information infrastructure nor does either provide cultural repository organizations with sector-specific guidelines for implementing standards that enable the preservation of these types of collections.

This absence ultimately creates a situation where Digitized Cultural Heritage organizations must interpret the broad statutory provisions and statutory obligations on their own, without having access to meaningful assistance from the statutes. Moreover, cybersecurity governance requires more than just adherence to legal obligations. These organizations typically operate with limited

¹¹⁷ T.K. Gireesh Kumar, 'Digital meets culture: towards a national portal for aggregating Indian cultural heritage' (2026)

Journal of Cultural Heritage Management and Sustainable Development 1, 5 <https://doi.org/10.1108/JCHMSD-022024-0031> accessed 2 March 2026.

¹¹⁸ DLA Piper (n 4).

technical capacity and financial means; therefore, even when statutory obligations exist, it may not be possible for them to properly implement those obligations. The difference between the formal protections provided by law and the institutional capacity to adhere to the law demonstrates a structural flaw within the existing systems.¹¹⁹

In summary, an analysis of the extent to which heritage specific laws and policies complement or contradict the wider cyber security framework must occur following this assessment. This will require that the intersection of cyber regulation with heritage protection laws in India.

Heritage Protection Laws and the Regulatory Disconnect in the Digital Context

Historically, the legal protection of India's cultural heritage has been aimed at preserving tangible monuments, sites and artefacts. The main legislation regarding the protection of ancient monuments is the Ancient Monuments and Archaeological Sites and Remains Act 1958. This Act primarily regulates and preserves monuments classified as being of 'national importance'. Another piece of legislation regarding antiquities is the Antiquities and Art Treasures Act 1972, which governs the export and trade in antiquities and art objects, amongst other things. Both pieces of legislation emphasise physical protection and regulatory oversight in the safeguarding of material heritage.

These pieces of legislation, while still important for protecting material heritage, are applicable only to the material heritage that existed before the rise of the internet and online technology. None of these statutes take into account the effects of digitisation and do not seek to provide for protection against hacking, data manipulation or the digital destruction of records. Once material culture has been converted to a digital format, it is no longer clearly covered by traditional heritage statutes.

The regulatory gap becomes apparent when we consider the holdings of archival and manuscript collections. Archival institutions, such as the National Archives, and public libraries operate from administrative structures and frameworks of rules, but these rules are usually more about custodial or facility responsibility than about securing the information that resides there.¹²⁰ Although many policy efforts have encouraged these institutions to digitize their manuscript and archival collections, there are currently few cybersecurity standards specifically tailored to their digital holdings.

This disconnection points to a larger systemic problem within the administrative framework for managing digital heritage. Heritage law and cybersecurity law exist in parallel with respect to the protection of cultural property versus addressing digital systems. Digital heritage occupies a hybrid reality that spans both areas of law. Digital heritage is, by nature, both a cultural good and,

¹¹⁹ Ministry of Electronics and Information Technology, 'Digital India Programme' <https://www.digitalindia.gov.in/> accessed 2 March 2026.

¹²⁰ National Archives of India (n 7).

therefore, a data resource. The lack of explicit legal recognition of digital heritage creates an incomplete and fragmented protection of this unique type of property.

In addition to ownership and authenticity, there are many other issues related to cultural materials in a digital environment including their copying, altering and redistributing. Questions about intellectual property rights and the moral rights of the original creator of the work are common; as are ethical questions about the integrity of digital reproductions. Although copyright law provides some protection from infringement, copyright law does not provide protections related to the broader security risks associated with unauthorised access or systemic cyberattacks on repositories.

In India, since cultural institutions are not generally classified as critical information infrastructure under the Indian cybersecurity policy, therefore cultural materials do not get the level of protection provided by the sector focus for critical infrastructure sectors such as finance, energy and telecommunications. Because damage to these critical infrastructure sectors has more immediate economic and security implications, the greater priority is to ensuring that they are able to operate without interruption or threat. Cultural heritage continues to be a significant part of a country's identity and helps to establish historical continuity, but they are often not perceived as being strategic targets for cyber-attacks. The perception of risk in this area may contribute to insufficient investment in cyber resilience for the cultural sector.

This regulatory disconnect operates on several levels: the statutory level, the institutional coordination level, and the level of government priorities. While within the area of heritage legislation there is not a requirement to conduct a digital risk assessment, there is also not any way for the cyber-security legislation to provide any protective measures for the heritage sector. Consequently, a regulatory framework that is designed to deal with cyber threats in general but fails to take into account or provide for the cultural significance of the information being protected.

Cybersecurity Risks and Governance Challenges in Digital Heritage

Acting as a bridge between digital and physical collections, cultural heritage institutions are digitising their manuscripts, artefacts, and archival records so that they are stored as digital assets in networked systems.¹²¹ Even though improving access to collections and preserving collections through digitisation are invaluable benefits, digitisation puts cultural institutions at a higher risk of cybersecurity. A major cybersecurity concern facing cultural institutions is unauthorised access to a database that could allow a hacker to copy or change the digitised collection. This could put the authenticity and the integrity of the digitised collection at risk. Unlike physical damage, digital evidence of manipulation might not be readily apparent.

This creates long-term risks associated with the distortion of the historical record. Apart from the risk of unauthorised access, ransomware attacks present another serious concern.¹²² If an attacker

¹²¹ T.K. Gireesh Kumar, 'Digital meets culture: towards a national portal for aggregating Indian cultural heritage' (2026) *Journal of Cultural Heritage Management and Sustainable Development* 1, 3.

¹²² CERT-In, 'Notes on Ransomware Prevention and Response' (2023) <https://www.cert-in.org.in> accessed 2 March 2026.

can encrypt digital repositories, institutions may have no way of recovering access to the digitised collections. If an institution does not have secure backups in place, this circumstance may result in the permanent loss of the digitised collection and could also result in reputational damage to the institution. Data that is inappropriately accessed can also create potential liability exposure for institutions if the archives contain personal or sensitive information.

Lastly, cultural institutions often operate with limited financial and technological resources. Portfolio risk may limit the priority given to cybersecurity at many museums and archives. Cultural institutions are often reliant on third party service providers for solutions related to cloud storage and database management, creating further complications when it comes to establishing responsibility and liability in the event of a breach.

Conclusion and Recommendations

The digitisation of India's cultural heritage is vital in preserving it, making it more accessible and allowing distribution of knowledge democratically. Digital methods also expand the audiences that can engage with historical materials and limit the physical deterioration of fragile items.¹²³ However, moving from traditional methods of preserving items to digital preservation involves a set of new vulnerabilities, which cannot be solved simply by advancing technology. As demonstrated through the analysis provided in this chapter, India has some comprehensive cybersecurity legislation; for example, the information technology Act 2000 and the Digital Personal Data Protection Act 2023 provide some protections for all sectors of industry.

However, neither the IT Act nor the Digital Personal Data Protection Act were written with the unique needs of institutions with digitally preserved cultural heritage in mind. In contrast, laws to support the preservation of cultural heritage institutions primarily address the physical preservation of cultural artifacts and do not adequately address the risks associated with the digital preservation of these items. This gap in laws exposes cultural repositories to the potential threat of losing access to cultural heritage through cyber-related incidents.⁹⁹

Several approaches can be explored to close this divide. Firstly, guidelines providing policy direction for the digital heritage sector should be created, incorporating cybersecurity standards within strategies for cultural preservation. Secondly, heritage institutions must follow a set of minimum-security standards, including routine evaluations of risk, secure backup systems for data, and clear channels to report incidents related to cybersecurity. Thirdly, building capacity will provide staff within heritage institutions with a stronger technical knowledge of cyber-related hazards, as well as raise their level of awareness in relation to these risks.

Finally, it is essential that there is improved coordination between cultural bodies and cybersecurity agencies to clarify regulations and enhance institutional preparedness. Digitisation alone cannot be relied upon as the sole solution to the challenges of preservation; it needs to be backed by sufficient systems of governance that acknowledge digital heritage as an asset that is both cultural

¹²³ Sudipta Shee, 'Digital preservation of cultural heritage in India: A digital age' (2025) 7(1) International Journal of Humanities and Education Research 260. ⁹⁹ DLA Piper (n 4).

and informational; protecting it calls for more than regulatory compliance institutions must demonstrate their ongoing commitment and co-ordinate their efforts through policies that all government entities support.
