NDSA LEVELS OF DIGITAL PRESERVATION: A REVIEW IN TERMS OF TRUSTWORTHINESS OF DIGITAL RECORDS

Özhan Sağlık

Bursa Uludag University /
University of British Columbia
Türkiye / Canada
ozhansaglik@uludag.edu.tr
0000-0002-1436-7431

Abstract – Records created in organizations that have archival value should be preserved for a long time, and to achieve this, digital preservation techniques are used. These techniques also contribute to the preservation of the trustworthiness of the records. In order to assess the situation of organizations in the implementation of their digital preservation activities, there is a need for an analysis tool. Many models have been prepared to meet this need. One is the Levels of Preservation (LoP) developed by the National Digital Stewardship Alliance (NDSA). The LoP provides guidance to organizations in their digital preservation activities. Therefore, it is thought that the LoP can be associated with trustworthiness which aims at long-term preservation of the records. This study examines the levels of digital preservation specified in the LoP in terms of the trustworthiness of digital records. As a result of this research, the goal is to provide the basis for a methodology for organizations wishing to assess their level of digital preservation and to align their digital preservation capabilities with trustworthiness. This study used document analysis as a qualitative research design. Both field observations and research show that organizations are not sufficiently aware of the level of digital preservation and trustworthiness. Then, the question of the study is "how the levels that are specified in the LoP can be associated with the trustworthiness". As a result of the study, it has been observed that the levels of digital preservation specified in the LoP can be used in the analysis of the trustworthiness of the records. It is expected that this study will raise awareness in the organizations to do a better job of preserving the records that have archival value.

Keywords – Digital records, digital preservation, trustworthiness

Conference Topics – Sustainability: Real and Imagined; Immersive Information

I. INTRODUCTION

Records created in the ordinary course of business functions that have archival value are preserved for the long-term. It is known that digital preservation techniques are used to successfully meet this requirement. Digital preservation is defined as the series of managed activities necessary to ensure continued access to digital materials for as long as necessary [1].

These digital preservation activities cause organizations to analyze their current situation. Therefore, organizations may need an analysis tool. If so, methods such as developing a maturity model, obtaining certification, and conducting an internal assessment can be used. These methods are also used in preservation of the trustworthiness of the records. Here, trustworthiness means possessing the characteristics that the records are supposed to have according to recordkeeping principles and law.

iPRES 2023: The 19th International Conference on Digital Preservation, Champaign-Urbana, IL, US.

https://hdl.handle.net/2142/1210899

As a matter of fact, various approaches have been developed in this regard, both in the academic research and in scientific field studies. Electronic Resource Preservation and Access Network (ERPANET) [2], Cultural, Artistic and Scientific Knowledge for Preservation, Access and Retrieval (CASPAR) [3], Preservation and Long-Term Access Through Networked Services (PLANETS) [4], Alliance Permanent Access to the Records of Science in Europe Network (APARSEN) [5], CoreTrustSeal [6], Go FAIR [7] and International Research on Permanent Authentic Records in Electronic Systems (INTERPARES) [8] can be given as an example.

In evaluating academic research, it has been found that Basma Makhlouf Shabou [9], Devan Ray Donaldson [10, 11, 12], Mpho Ngoebe and Jonathan Mukwevho [13] and Özhan Sağlık [14] have conducted studies on trustworthiness. Shabou criticized trustworthiness in Switzerland, Ngoebe and Mukwevho in South Africa, and Donaldson in the US. Sağlık, on the other hand, examined the evidential value of electronically signed records created in Turkish ministries in terms of archival trustworthiness in his doctoral thesis.

In the corpus of the International Conference on Digital Preservation (IPRES), there are many studies that assess the existing digital preservation capabilities of organizations. Although the LoP is also examined in some studies [15, 16, 17, 18], it cannot be observed that digital preservation capabilities are associated with the trustworthiness of the records. In other remarkable studies, the authors' observations at various institutions were presented [19, 20, 21, 22, 23]. However, there is a need for guidelines issued by organizations such as associations to measure the digital preservation capacity of institutions with different materials. Because these guides are designed with the needs of institutions that have many different types of materials. NDSA LoP, DigCurV Curriculum Framework and Digital Preservation Capability Maturity Model (DPCMM) and Rapid Assessment Model (DPC) developed by DPC can be given as an example [1, 24, 25, 26]. Among these studies, the LoP prepared by the NDSA stands out as a tool for organizations wishing to establish a digital preservation program.

The LoP, which can be used as a tool for organizations wishing to assess their digital preservation capacity, has five different functions and four progressive levels. These functions are storage, integrity, control, metadata, and content. The services provided by the organizations in these functions represent levels 1 through to 4 [24]. These services can be associated with trustworthiness.

In this study, the functions in the LoP are examined in terms of the trustworthiness of digital records. It is aimed to establish a methodology for organizations seeking to assess their digital preservation capability and to overlap the functions in the LoP with trustworthiness. As a result of this, it is thought that an awareness can be created in organizations to better preserve the records that have archival value. The study adopted a qualitative research design and used document analysis; the studies on this topic have been critiqued.

Both observations and studies show that organizations are not sufficiently aware of the digital preservation capabilities and trustworthiness [14, 27, 28]. In these circumstances, the question of the study is "how the levels that are specified in the LoP associated with the trustworthiness?" As a result, it is expected that an awareness will be created in organizations.

II. NDSA LEVELS OF PRESERVATION

The Levels of Digital Preservation are a tiered set of guidelines and practices for preserving the digital content. Levels can be used both education and advocacy and planning and assessment. But Levels do not reflect a holistic program that includes policies and procedures. They focus primarily on the technological aspects of a digital preservation program. There are four progressive levels in five different functional areas that can also be used to assess an organization’s digital preservation capability. Functional areas are storage, integrity, control, metadata, and content. These functions are evaluated in four progressive levels (Know, protect, monitor, and sustain) [24].

Knowing, the first level of the storage, includes criteria such as keeping content in a stable storage and having at least two copies in separate locations. An example of a level of protection criterion is keeping at least three copies, with at least one copy in a separate geographic location. Tracking the obsolescence of storage is one of the of the monitor level requirements. Performing tracked obsolescence is one of the criteria for the sustain level.

Generating integrity information and then verifying can be given as examples of the criteria questioned at the first level of integrity. One of the second-level criteria is to back up the integrity information and store the copy of it in a separate location from the content. Verifying this information at regular intervals is one of the third-level criteria. An example of a last-level criterion is to replace or repair corrupted content when necessary.

One of the exemplary criteria of the control function at the knowing level is to determine which authorization is to be exercised by whom and how. It is recommended that these authorizations be documented at the protection level. At the monitor level, the maintenance of log records can be cited as an example. Periodic review of access logs is one of the criteria at the final level.

At the first level of the metadata function, one of the first criteria is to create an inventory of the content with their current storage locations. Storing metadata is one of the criteria in the second level. At the third level, it is questioned whether a decision has been made about which metadata standards to be applied. Applying the adopted standards is one of the criteria of the last level.

The latest function is content. At the knowing level, it is sought to document the essential characteristics of file formats and content by including how and when they were identified. One of the criteria that can be given as an example at the protection level is to verify the essential characteristics of file formats and content. It is aimed to monitor the obsolescence and changes in the technology on which content is dependent at the monitor level. At the sustain level, it is asked whether activities such as migration and emulation have been performed.

The guidelines in the LoP can be considered as a milestone for digital preservation. Therefore, it is possible to examine these guidelines in the context of trustworthiness.

III. TRUSTWORTHINESS OF DIGITAL RECORDS

Trustworthiness is known as the preservation of attributes such as the medium, the content, the author, and the context of the records. The law, diplomatic and history disciplines that work directly with records have also developed various approaches regarding to preserving these attributes and maintaining trustworthiness. It is noteworthy that trustworthiness is defined differently in each of these disciplines. For example, for legal trustworthiness it has checked whether a record has the characteristics specified in the legislation; it has also checked whether the authorization mechanism is applied, and whether procedures are established in the records management processes [14, 29, 30, 31]. Diplomatic trustworthiness evaluates whether the form elements describing the records' characteristics are found appropriately. The procedures are analyzed by criticizing the features such as carrier, content, form elements, actions and persons in the record, archival bond, metadata, and context. It also examines digital signatures, seals, features of hardware and the software used, logs, audit trails and database transactions [14, 29, 31]. Another approach is historical trustworthiness. Here, it is checked whether the information contained in the record, the place and the events are given correctly. In particular, the information must match the date, place, person, and period of the record [14, 29, 30].

However, the above-mentioned approaches alone may not be sufficient to analyze the trustworthiness of digital records. Because the legislation and the information technologies used as a source for the formation of the records have brought the issue to be discussed from a broader perspective. This perspective is called archival trustworthiness [14, 32, 33]. As with other notions of the trustworthiness, authenticity, accuracy, and reliability are critical [14, 32].

Authenticity, which is defined as the fact that the attributes of the record do not change during the period in which it is processed, filed, and archived after it has produced, is examined in two steps, identity and integrity. Identification refers to the qualification of the characteristic elements that distinguish them from other records and occurred according to their type. Examples of these are persons in the record, date of creation and transmission, subject, archival bond, file code, and appendix of the record. Another level of authenticity is integrity, which means that the record is undecomposed and unaltered, with all its components. It is aimed to preserve the context, form features and content of the record in integrity [14, 29, 34, 35].

In addition to authenticity, another element of trustworthiness is accuracy. An accurate record seeks to be precise, correct, consistent, and free from falsification. Reliability, which is another element of trustworthiness, is evaluated based on the completeness of the record form through the controls in the record production procedures. These controls are specified as the production and receiving of the record, its placement in its folder, and the authorization of the persons in the records. The completeness of the record form refers to the presence of all elements of the intellectual form that make the record suitable for legal consequences [14, 29, 35]. Therefore, it was thought that the functions in the LoP could be related to the trustworthiness analysis developed by Sağlık. In this analysis, the trustworthiness of records is critiqued at the layers of records, technological conditions, organization, legislation, and society [14].

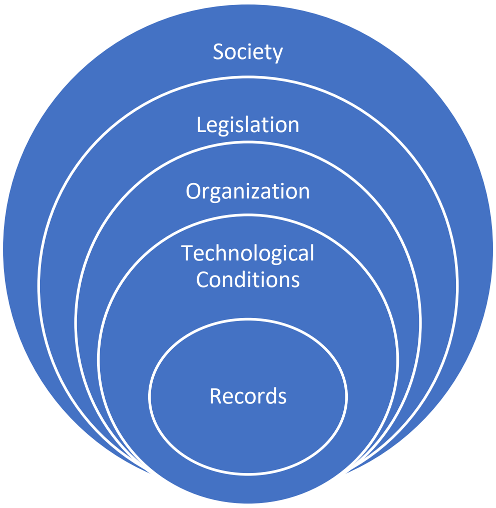

Figure 1. Layers of the Trustworthiness

The records layer evaluates the elements that make up the record such as context, archival bond, metadata and medium. Questions such as which metadata was used, whether or not a format change is required, and if the form elements were recorded are asked here. The technological conditions layer examines the application software and hardware used to produce, transfer, and store the records. Issues such as performing integrity checks, diversifying storage methods, and access privileges are analyzed. At the organization layer, policies and procedures regarding records management and archiving are evaluated. Issues such as the existence of a records management policy and the ongoing training of instructors are considered [14].

Although organizations prepare policies and procedures for records management and archiving, develop technological conditions in accordance with the needs of the service, and assign prospective metadata, they act in accordance with the relevant legislation while performing their functions. The legislation might include issues such as the retention period of the records, form elements, and technological conditions to be adopted. As such, these issues are critical elements of the legislation layer. Another aspect of this layer is evaluating the records management and archiving practices of the national archives. Therefore questions such as whether the national archives have determined the archiving rules for the records, whether migration procedures have been established, and the formats to be used have been specified [14].

The final layer of trustworthiness analysis examines what elements citizens look for to trust digital records. Therefore, this stage is called the society layer. Questions such as what are the tools that build trust among citizens, how much trust is placed in records, and how can this trust be increased will be explored [14].

Considering all these trustworthiness analyses, it is thought that institutions are more effective at records, technological conditions and organization layers. Because there are activities outside of the organizations' own savings at the layer of society and legislation. For example, at the community level, the opinions of citizens are critiqued, and at the legislation level, laws, regulations and circulars issued by government are reviewed. When this is the case, both citizen opinion and legislation are not directly in the hands of the organizations themselves. Organizations are more dynamic at the records, technological conditions, and organizations level [14].

It is possible to assess functions in the LoP according to trustworthiness layers. The functions may not be related to the same layers in all levels, for example, the first level of the Metadata function may be related to records layer, but in the second level it may be associated to the technological conditions. Table 1 shows the relation of LoP and the trustworthiness layer. R shows “Records”, T demonstrates “Technological Conditions” and the O indicates “Organization” layer.

Table 1. Relations of LoP to the Trustworthiness

Functions	Level 1 (Know)	Level 2 (Protect)	Level 3 (Monitor)	Level 4 (Sustain)
Storage	T, O	O	T, O	T, O
Integrity	R, T	R, T, O	R, O	R, T
Control	O	O	T	T, O
Metadata	R, T, O	R	O, R	R
Content	R	R, T	T	T

Since these functions are shaped by the activities of the organizations, the legislation and society layers of trustworthiness could not naturally find a place at the table. At the same time, a function may be related to the three layers in which organizations are more active. However, the layer is assumed to be formed directly by the corresponding function is indicated in the table. R shows records, T demonstrates technological conditions and O indicates organization layer.

The activities in the storage function are related to both to the technological conditions and to the organization layer. It is thought that, adopting a solid storage system is related to technological conditions; and keeping copies of the content in separate locations shapes the organization layer.

The integrity function is associated with almost all the trustworthiness layers. It is thought that generating integrity information structures the record layer, virus checking and backing up integrity information forms the technological conditions layer, and documenting integrity embodies the organization layer.

Determining access privileges in the control function is associated with the organization layer. Issues related to logs and audit trails are thought to shape the technological conditions layer. The metadata function is associated with almost all trustworthiness layers. It is thought that the creation of the inventory content is related to records, the backing up metadata is connected with technological conditions, and the determination of which metadata standards to apply is relevant to the organization layer.

Finally, the content function is associated with both the records and technological conditions layers. Identifying characteristics of the record embodies the records layer, and actions related to technological aspects of the record format such as emulation and migration figures the technological conditions layer.

IV. CONCLUSION

This study was an attempt to have a relationship between the LoP and the trustworthiness of digital records. Thus, it is intended to shed light on which layers of trustworthiness can be successful if organizations implement the functions in the LoP. The goals included in the LoP have been shown to be highly correlated with trustworthiness. These goals can be used as a benchmark when analyzing the trustworthiness of records created in organizations. The things that organizations should do to achieve the relevant goal can also be considered as trustworthiness criteria.

The LoP was developed to provide organizations with a goal in related functions. No mandatory criteria have been developed to allow flexibility for organizations. However, the lack of specific criteria in the LoP is considered a deficiency in terms of trustworthiness analysis. There is a need for criteria that are routinely checked and questioned for fulfillment.

As a result of the study, it has been seen that the trustworthiness of digital records can be successfully preserved after the realization of the LoP goals. However, examples of good practice are also in demand. This can be done by creating the criteria of the targets in the LoP. These criteria can be developed in a way that is flexible and not overly prescriptive.

1. REFERENCES

[1] Digital Preservation Coalition [DPC], “DPC Rapid Assessment Model”, *DPC*. [Online]. Available: https://www.dpconline.org/digipres/dpc-ram [Accessed: Mar. 06, 2023].

[2] Electronic Resource Preservation and Access Network [ERPANET], “ERPA studies ”, *ERPANET*. [Online]. Available: https://www.erpanet.org/studies/index.php [Accessed: Mar. 06, 2023].

[3] Cultural, Artistic and Scientific Knowledge for Preservation, Access and Retrieval [CASPAR], “CASPAR website”, *CASPAR*. [Online]. Available: http://casparpreserves.digitalpreserve.info [Accessed: Mar. 06, 2023].

[4] Preservation and Long-Term Access Through Networked Services [PLANETS], “Publications”, *PLANETS*. [Online]. Available: https://planets-project.eu/publications [Accessed: Mar. 06, 2023].

[5] Alliance Permanent Access to the Records of Science in Europe Network [APARSEN], APARSEN deliverables", *APARSEN*. [Online]. Available: http://www.alliancepermanentaccess.org/index.php/about-aparsen/aparsen-deliverables [Accessed: Mar. 06, 2023].

[6] CoreTrustSeal, "Data repositories requirements", *CoreTrustSeal*. [Online]. Available: https://www.coretrustseal.org/why-certification/requirements [Accessed: Mar. 06, 2023].

[7] Go FAIR, "FAIR principles", *GO FAIR*, [Online]. Available: https://www.go-fair.org/fair-principles [Accessed: Mar. 06, 2023].

[8] International Research on Permanent Authentic Records in Electronic Systems [INTERPARES], "INTERPARES Project", *INTERPARES*. [Online]. Available: http://www.interpares.org [Accessed: Mar. 06, 2023].

[9] B. M. Shabou, "Digital diplomatics and measurement of electronic public data qualities what lessons should be learned?", *Records Management Journal*, vol. 25, no. 1, pp. 56-77, Mar. 2015, doi: 10.1108/RMJ-01-2015-0006.

[10] R. D. Donaldson, "Development of a scale for measuring perceptions of trustworthiness for digitized archival documents", Ph.D. dissertation, University of Michigan, Michigan, United States, 2015. [Online]. Available: https://deepblue.lib.umich.edu/handle/2027.42/111489.

[11] R. D. Donaldson, "The digitized archival document trustworthiness scale", *International Journal of Digital Curation*, vol. 11, no. 1, pp. 252-270, Nov. 2016, doi: 10.2218/ijdc.v11i1.387.

[12] R. D. Donaldson, "Trust in archives–trust in digital archival content framework", *Archivaria*, no. 88, pp. 50-83, Nov. 2019. [Online]. Available: https://archivaria.ca/index.php/archivaria/article/view/13697.

[13] M. Ngoepe and J. Mukwevho, "Ensuring authenticity and reliability of digital records to support the audit process", INTERPARES, Jul 9, 2018. Accessed: Mar 6, 2023. [Online]. Available: http://interparestrust.org/assets/public/dissemination/AF06-FinalReport.pdf

[14] Ö. Sağlık, "Elektronik belge yönetimi uygulamalarındaki koşullar ışığında e-imzalı belgelerin delil değerinin arşivsel güvenilirlik açısından Incelenmesi", Ph.D. dissertation, Istanbul University, Istanbul, Türkiye, 2021. [Online]. Available: https://www.proquest.com/pqdtglobal/docview/2754923369.

[15] M. Schultz et al., "Building institutional capacity in digital preservation", in *Proc. 10th IPRES 2013*, J. Borbinha, M. Nelson, S. Knight, Eds. Sep. 2013, pp. 322-325.

[16] B. J. Daigle et al., "Level up on preservation: Updating and mapping the next generation of the Levels of Preservation", in *Proc. 16th IPRES 2019*, M. Ras, B. Sierman, A. Puggioni, Eds. Sep. 2019, pp. 512-513.

[17] M. Haunton, "Incorporating digital preservation and access maturity models into wider assessment programmes: Archive service accreditation and the levels of digital preservation and born-digital access", in *Proc. 18th IPRES 2022*, Sep. 2022, pp. 441-442.

[18] S. McMeekin, A. Currie, "Ain't no mountain high enough: Developing a new competency framework for digital preservation", in *Proc. 18th IPRES 2022*, Sep. 2022, pp. 99-107.

[19] M. Humbert, S. Roussel, E. Vasseur, "Building the future of digital preservation in French archival services: Processes, functions and staffing for an effective digital preservation", in *Proc. 16th IPRES 2019*, M. Ras, B. Sierman, A. Puggioni, Eds. Sep. 2019, pp. 46-52.

[20] P. Lucker et al., "Preservation watch at the National Archives of The Netherlands", in *Proc. 15th IPRES 2018*, Sep. 2018.

[21] J. van der Nat, M. Ras, "A Dutch approach in constructing a network of nationwide facilities for digital preservation together", in *Proc. 14th IPRES 2017*, Sep. 2017, pp. 99-107.

[22] F. Berghaus et al., "CERN services for long term data preservation", in *Proc. 13th IPRES 2016*, Oct. 2016, pp. 168-176.

[23] M. Pennock, P. Wheatley, P. May, "Sustainability assessments at the British Library: Formats, frameworks, & findings", in *Proc. 11th IPRES 2014*, S. Coates et al., Eds. Oct. 2014, pp. 141-148.

[24] NDSA. "Levels of Digital Preservation", *NDSA*. [Online]. Available: https://osf.io/QGZ98 [Accessed: Mar. 07, 2023].

[25] DigCurV. "DigCurV Curriculum Framework", *DigCurV*. [Online]. Available: https://digcurv.gla.ac.uk [Accessed: Mar. 07, 2023].

[26] DPCMM. "Digital preservation capability maturity model", *DPCMM*. [Online]. Available: https://www.securelyrooted.com/dpcmm [Accessed: Mar. 07, 2023].

[27] Ö. Külcü, "INTERPARES 3 kurumsal bilgi sistemleri içerisinde belge yönetimi: Türkiye'deki kamu üniversitelerinde gerçekleştirilen uygulamalara yönelik bir durum analizi", The Scientific and Technological Research Council of Türkiye, 2014.

[28] Ö. Sağlık, "Sayısal Koruma Koalisyonu Hızlı Değerlendirme Modeli: Elektronik belgelerin güvenilirliği açısından bir inceleme", *Bilgi Yönetimi*, vol. 5, no. 2, pp. 211-223, Dec. 2022, doi: 10.33721/by.1199232.

[29] Ö. Sağlık, "Arşivlenen elektronik belgelerin güvenilirliğini tehdit eden riskler: Teknolojik koşullar açısından bir inceleme. *Bilgi ve Belge Araştırmaları Dergisi*, no. 16, pp. 29-47.

[30] N. Çiçek, *Modern belgelerin diplomatiği*. Istanbul, Türkiye: Derlem Yayınları, 2009.

[31] H. MacNeil, *Trusting records: Legal, historical and diplomatic perspectives*. Springer, 2000.

[32] L. Duranti and R. Preston, Eds. *INTERPARES 2: Experiential, Interactive and Dynamic Records*. 2008. [Online]. Available: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf. Accessed: Mar 7, 2023.

[33] J. Bushey, "The archival trustworthiness of digital photographs in social media platforms", Ph.D. dissertation, University of British Columbia, Vancouver, Canada, 2016. [Online]. Available: http://hdl.handle.net/2429/57606.

[34] C. Rogers, "Virtual authenticity: Authenticity of digital records from theory to practice". Ph.D. dissertation, University of British Columbia, Vancouver, Canada, 2015. [Online]. Available: http://hdl.handle.net/2429/52722.

[35] N. Çiçek, Ö. Sağlık. "Blokzincir teknolojisinin elektronik belgelerin güvenilirliğinin korunmasında başarıya katkısı, in *Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ*, B. Yalçınkaya et al., Ed., Ankara: Ankara Üniversitesi, 2019, pp. 141-170.